Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

DIRECTIVE

RESEAU IP EES

Édition 2017 V1.20
ASTRA 13040

Impressum

Auteur(s) / groupe de travail

Jean-Paul Schnetz	(OFROU, N-ST, présidence)
Markus Glanzmann	(OFROU, N-ST)
Urs Luther	(OFROU, N-ST)
Eugen Fuchs	(OFROU, N-ST)
Martin Wyss	(OFROU, I-B, GT EES)
Bendicht Hirschi	(OFROU, I-FU, GT EES)
Jörg Dreier	(OFROU, N-VMZ)
Markus Eisenlohr	(OFROU, I-FU, GT EES)
Markus Riederer	(OFROU, N-VIM)
Robert Hämmerli	(OFROU, I-F4)
Andreas Wüst	(UT VII)
Grégory Champion	(UT IX)
Ivo Achermann	(UT X)
Manfred Lussmann	(UT XI)
Brundo Widrig	(UT XI)
Yvan Wyser	(OFROU, N-VMZ)
Daniel Gähwiler	(CSI Consulting AG, élaboration)
Patrick Gerber	(CSI Consulting AG, élaboration)

Traduction (version originale en allemand)
Services linguistiques OFROU (traduction française)

Éditeur
Office fédéral des routes (OFROU)
Division Réseaux routiers (N)
Standards et sécurité de l’infrastructure (SSI)
3003 Berne

Diffusion
Le présent document peut être téléchargé gratuitement sur le site www.astra.admin.ch.

Avant-propos

Les équipements d'exploitation et de sécurité (EES) sont essentiels à la sécurité dans les tunnels et sur les sections à ciel ouvert du réseau des routes nationales suisses.

Pour pouvoir utiliser et exploiter efficacement les installations concernées, il est nécessaire de disposer d'une infrastructure de communication homogène, performante et hautement disponible.

La présente directive décrit une infrastructure de communication pour les EES uniforme et continue à l'échelle suisse.

L'infrastructure mentionnée constitue une base solide et homogène, qui permet à l'OFROU non seulement de développer les EES, mais aussi de réaliser de nouvelles solutions en matière de gestion du trafic ou de mise en réseau des véhicules avec l'infrastructure.

Office fédéral des routes

Jürg Röthlisberger
Directeur

Table des matières

1 Introduction

1.1 But du document

La présente directive vise à standardiser la création de l'infrastructure de communication pour les EES des routes nationales et à la fonder sur des bases modernes, orientées vers l'avenir.

Elle décrit l'architecture réseau visée pour la dorsale (« *backbone* ») et les infrastructures de communication locales dans les unités territoriales (UT), y compris les interfaces avec les centres de calcul EES (EES RZ), la VMZ-CH, d'autres UT, les réseaux des cantons et de la Confédération, les réseaux de partenaires (par ex. Swisscom), et d'autres réseaux étrangers comme Internet.

Le document présente aussi les exigences posées aux appareils et aux services à utiliser dans le réseau IP EES.

Il prévoit par ailleurs la standardisation de l'adressage IP, l'utilisation de systèmes d'assistance pour la gestion des adresses IP, la configuration de services DNS et DHCP, le contrôle de l'accès au réseau et les exigences en matière de gestion du réseau pour la création et l'exploitation du réseau IP EES.

Le dernier chapitre est consacré aux dispositions et aux exigences opérationnelles.

1.2 Champ d'application

La présente directive s'applique en principe à tous les réseaux de communication pour EES.

Elle est valable en particulier dans les cas suivants :

- remplacement ou renouvellement de l'ensemble du réseau de communication pour EES d'une UT arrivé en fin de vie ;
- renouvellement partiel (ou migration sur IPv6, remplacement du système de gestion de réseau [NMS]) de l'ensemble du réseau de communication pour EES d'une UT ;
- développement ou renouvellement d'une partie du réseau de communication pour EES d'une UT (par ex. pour une section), si un investissement préalable paraît judicieux et raisonnable du point de vue économique.

1.3 Destinataires

La présente directive s'adresse aux :

- spécialistes de l'OFROU ;
- spécialistes des UT ;
- bureaux d'ingénieurs et entreprises qui effectuent, à la demande de l'OFROU, des tâches sur les infrastructures de communication pour EES.

1.4 Entrée en vigueur et modifications

La présente directive entre en vigueur le 07.12.2017. La « Liste des modifications » se trouve à la page 41.

2 Architecture de référence

2.1 Définitions

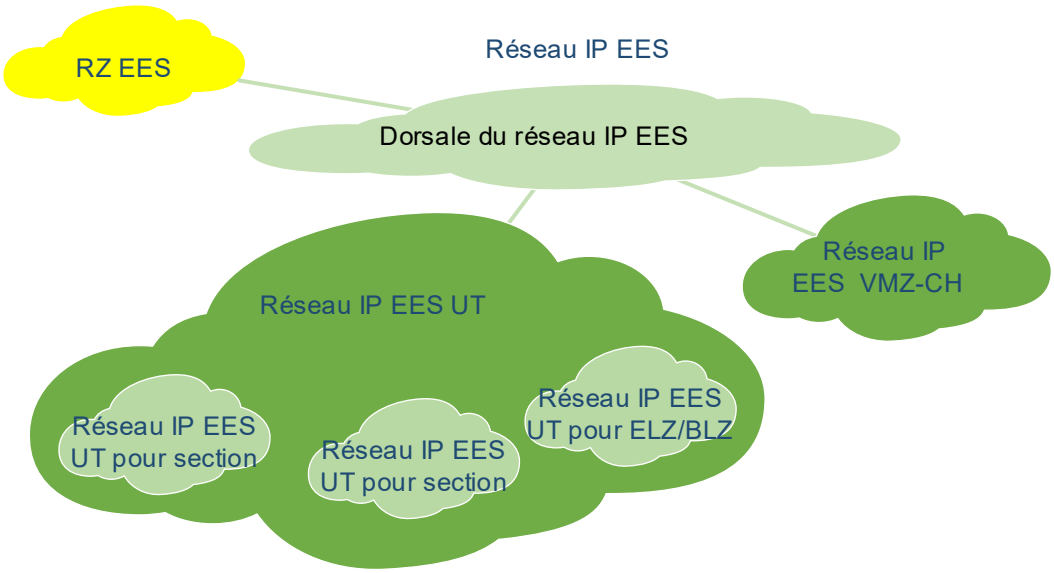

Fig. 2.1 terminologie du réseau IP EES

L'infrastructure de communication pour les EES d'une unité territoriale est appelée « réseau IP EES UT ».

Le terme « réseau IP EES UT section » désigne un réseau IP local d'une UT qui dessert une section EES (en tunnel ou à ciel ouvert). Tout réseau de ce type fait partie intégrante d'un réseau IP EES UT.

L'appellation « réseau IP EES UT pour centrale ELZ/BLZ » est employée pour désigner un réseau IP local d'une UT assurant la liaison avec un site central, comme une centrale de gestion de l'exploitation. Tout réseau de ce type fait partie intégrante d'un réseau IP EES UT.

Le réseau de communication pour EES de la centrale suisse de gestion du trafic, appelé « réseau IP EES VMZ-CH », est traité de la même manière que le réseau IP EES UT.

La « dorsale du réseau IP EES » est l'infrastructure de communication qui relie les réseaux IP EES UT et VMZ-CH (y c. niveau de gestion) aux centres de calcul EES ou qui relie lesdits réseaux entre eux (y c. niveau de gestion).

On appelle « réseau IP EES » l'ensemble formé par les réseaux IP EES UT, le réseau IP EES VMZ-CH et la dorsale du réseau IP EES.

Le réseau local des centres de calcul EES (EES RZ LAN) n'appartient pas au réseau IP EES.

2.2 Délimitation

Le réseau IP EES est conçu comme un réseau de communication SCADA[1] et utilise la dorsale du réseau IP EES. Cette dernière complète l'offre actuelle de l'administration fédérale en matière de communication (« réseau AF ») au moyen d'une solution globale SCADA adéquate ; elle est totalement séparée du réseau existant de l'administration fédérale, même si elle assure parfois la connexion avec les mêmes sites de l'OFROU.

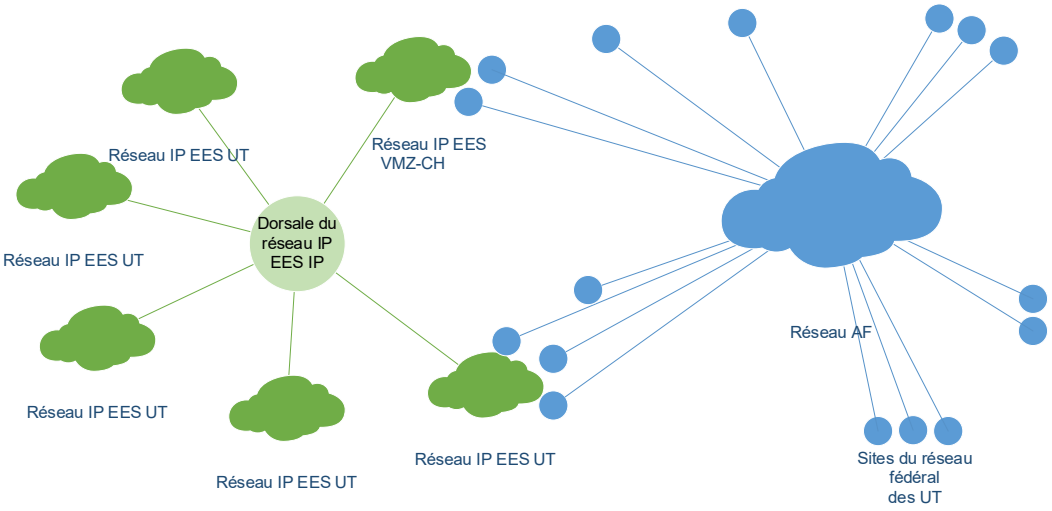

Fig. 2.2 Séparation stricte du réseau IP EES et du réseau AF

Le présent document traite exclusivement de la solution globale que constitue le réseau IP EES.

2.3 Délimitation par rapport à la fibre optique (FO)

La présente directive ne décrit pas l'organisation du réseau de FO de l'OFROU, mais elle se fonde, pour la configuration de l'architecture réseau, sur les hypothèses ci-après à ce sujet :

- il y a suffisamment de câbles à FO ou de fibres pouvant être utilisés par le réseau IP EES le long des routes nationales ;
- de même, il y a suffisamment de câbles à FO libres entre les routes nationales et les sites de l'OFROU nécessaires (par ex. centres d'entretien, centrales de gestion) ;
- l'infrastructure des câbles à FO de l'OFROU satisfait certaines exigences qualitatives minimales, par ex. s'agissant du matériel et de la construction, de sorte qu'aucune limitation ne doit être imposée à l'architecture réseau du réseau IP EES.

La fiche technique 23 001-11720 comporte de plus amples informations sur les installations à câbles à FO de l'OFROU.

[1] Les systèmes SCADA (« *Supervisory Control and Data Acquisition* »), ICS ou DCS (« *Industrial* » ou « *Distributed Control Systems* ») sont des systèmes informatiques interconnectés (systèmes de gestion) affectés à la surveillance, au pilotage et à l'optimisation d'installations industrielles.

2.4 Principes et vue d'ensemble

L'architecture réseau du réseau IP EES doit être définie de manière à garantir une disponibilité élevée et une protection fiable (sécurité ou « *security* »). Par conséquent, les règles de base ci-après s'appliquent à l'architecture :

- de conception redondante au niveau des outils et des liaisons FO, l'architecture ne présente aucun point unique de défaillance (« single point of failure ») :
  - une défaillance unique (par ex. défaillance d'un appareil réseau ou coupure de FO) dans un réseau IP EES UTsection ne doit pas paralyser l'ensemble de ce réseau ;
  - une défaillance unique dans un réseau IP EES UT ne doit pas paralyser l'ensemble du réseau IP EES ;
  - une défaillance unique entraîne tout au plus une perte de redondance ;
  - les applications ou outils raccordés de façon redondante dans le niveau d'accès peuvent toujours être rejoints malgré la perte d'un seul composant du réseau.
- une double défaillance peut entraîner une interruption du service ;
- le réseau lui-même doit déjà présenter un niveau de sécurité élevé de par sa structure.

Le réseau de communication IP EES recouvre l'ensemble de la Suisse et dessert l'ensemble des sites d'infrastructure, des centrales de gestion et des centres de calcul de l'OFROU. Il est structuré comme suit :

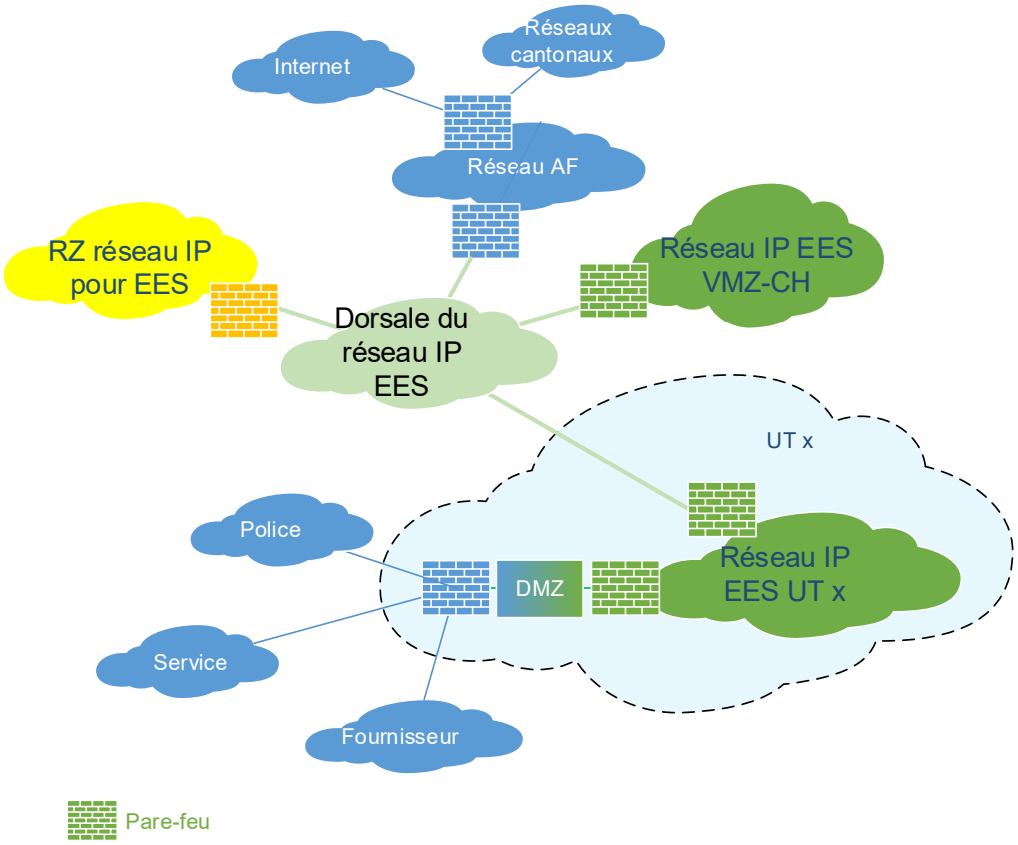

Fig. 2.3 Structure du réseau IP EES

Les réseaux IP EES UT sont des réseaux autonomes qui desservent exclusivement les sections EES des routes nationales situés sur le territoire relevant de la compétence de l'UT correspondante.

Chaque UT comporte plusieurs sections EES. Sur chacun de ceux-ci, ce sont les réseaux IP EES UT section qui assurent la communication avec les appareils compatibles IP ; ces réseaux fonctionnent de manière largement autonome.

Les réseaux IP EES UT section sont reliés entre eux par les anneaux de raccordement de l'UT en question et constituent ainsi son réseau IP EES (IP EES UT).

La dorsale du réseau IP EES assure la liaison entre les différents réseaux IP EES UT, de même que la communication entre ceux-ci et la VMZ-CH ainsi que les centres de calcul EES.

Pour permettre aux UT de garantir une exploitation sûre des installations, chaque réseau IP EES UT est séparé de la dorsale du réseau IP EES par un pare-feu.

Toutes les autres connexions entre les réseaux IP EES UT et des partenaires existants (police, fournisseurs, prestataires de services) doivent de préférence être assurées via la zone démilitarisée (DMZ) des centres de calcul EES ou via un pare-feu/une zone de transit dans les UT (DMZ UT).

La dorsale du réseau IP EES permet d'accéder aux ressources réseau de la Confédération et de les utiliser. Elle doit elle aussi être séparée des autres réseaux fédéraux par des pare-feu/zones de transit.

À l'intérieur des centres de calcul EES, il faut également séparer les zones réseau pour les applications métier EES (RZ réseau IP pour EES) des autres zones du RZ au moyen de pare-feu/zones de transit.

2.5 Raccordement en anneau du réseau IP EES UT

Le réseau IP EES UT se compose d'un ou plusieurs anneau(x) de raccordement et des réseaux IP EES UT section correspondants (ou « niveaux d'accès » au réseau), auxquels sont raccordés les appareils compatibles IP de la section EES.

Les anneaux de raccordement forment le niveau de base (« *core layer* ») du réseau IP EES UT, tandis que les réseaux IP EES UT section en forment le niveau d'accès (« *access layer* »). On a renoncé à un niveau supplémentaire de distribution.

Anneaux de raccordement et niveaux d'accès sont formés de composants actifs distincts : alors que les composants actifs d'un niveau d'accès n'appartiennent qu'à une seule section EES, ceux des anneaux de raccordement en desservent plusieurs.

Pour garantir la géo-redondance, chaque niveau accès est raccordé à l'anneau en deux emplacements différents de celui-ci, qui ne doivent se trouver ni au début ni à la fin d'un même niveau d'accès.

Les différents niveaux d'accès n'ont pas de composants actifs communs. Toutefois, un niveau d'accès peut employer les câbles à FO libres d'un autre niveau d'accès pour rejoindre un autre emplacement de l'anneau de raccordement.

Toute liaison au-delà d'une section EES est assurée exclusivement via les anneaux de raccordement et les routeurs correspondants. Chaque routeur est relié au moins à deux autres routeurs par des chemins de FO disjoints. Les FO doivent dans tous les cas être disposées de manière redondante et rester aussi éloignées que possible lors de leur entrée et distribution dans les bâtiments.

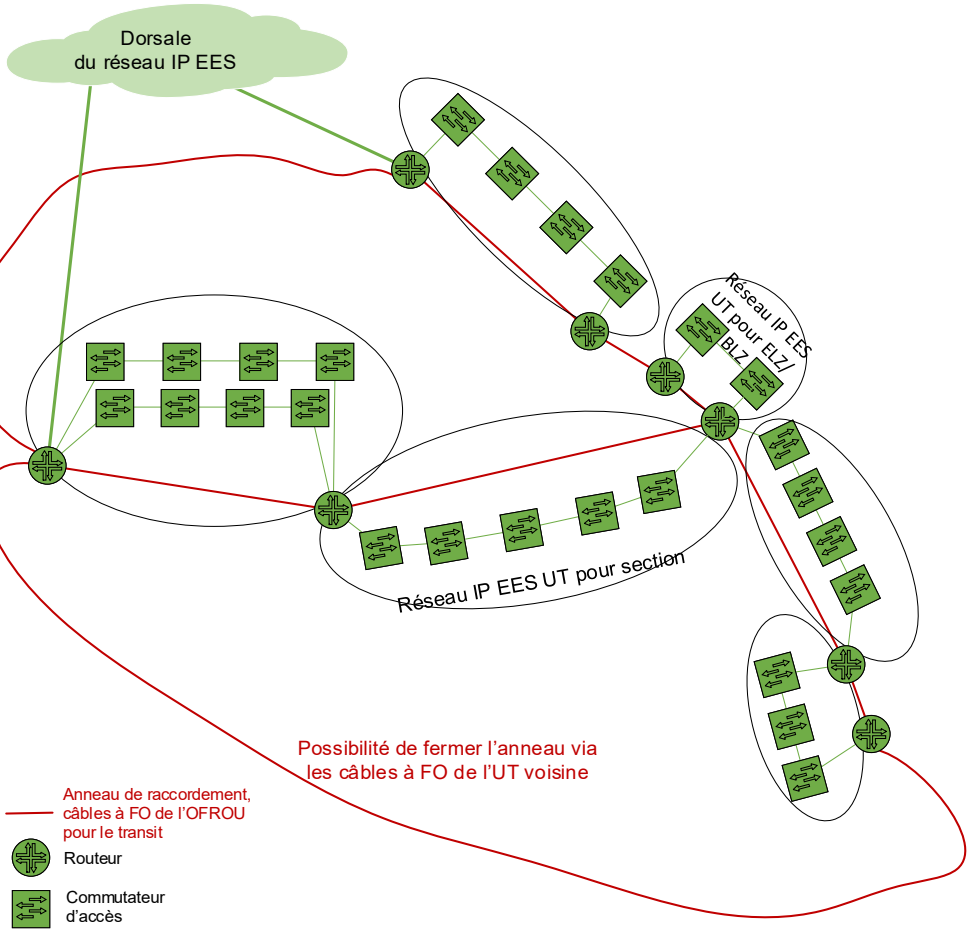

Fig. 2.4 Architecture des anneaux de raccordement du réseau IP EES UT et des niveaux d'accès correspondants (réseaux IP EES UT section)

Pour former les anneaux de raccordement, on utilise les câbles à FO de l'équipement de terrain (voir fiche technique 23 001-11720). On part du principe qu'il y a suffisamment de fibres disponibles et qu'il n'est pas nécessaire de prévoir une utilisation multiple des fibres (infrastructure WDM)[2]. Pour fermer les anneaux à leurs frontières, les UT se fournissent mutuellement des câbles à FO (composants purement passifs ; il n'y a aucun trafic de contrôle entre les équipements de réseau des différentes UT).

Les composants actifs en un emplacement de l'anneau ne doivent être redondants (deux routeurs distincts) que si les niveaux d'accès ne peuvent pas, moyennant des efforts raisonnables, être raccordés à l'anneau en deux emplacements séparés. On préfère généralement rejoindre l'anneau en un deuxième emplacement, même par une longue liaison de FO, et disposer d'emplacements sans composants actifs doubles.

Deux des emplacements de l'anneau de raccordement sont raccordés à la dorsale du réseau IP EES via un routeur (on parle donc de « *dual homing* » des UT).

[2] L'infrastructure WDM ne doit être utilisée qu'en cas de nécessité, lorsqu'il n'y a plus de fibres disponibles. L'utilisation de systèmes WDM augmente la complexité technique et opérationnelle.

2.6 Accès au sein du réseau IP local EES UT section

Les réseaux IP EES UT section constituent, au sein d'un réseau IP EES UT, les niveaux d'accès aux sections en tunnel et à ciel ouvert. Ils assurent la connexion avec l'ensemble des systèmes EES (commandes d'installation, détecteurs, acteurs, etc.). A long terme le niveau d'accès dans son intégralité se réalisera uniformément avec la technologie IP en incluant le niveau du terrain. La Fig. 2.5 montre l'architecture de toutes les possibilités de communication lors des phases intermédiaires de migration.

Un réseau IP EES UT sectionest conçu comme une cascade de commutateurs d'accès traditionnels (« *daisy chain* », connexion en cascade), dont les deux extrémités sont raccordées à l'anneau au moyen de deux routeurs différents. Au besoin, plusieurs de ces cascades peuvent être établies sur une même section EES. Les lignes en antenne ne sont en principe pas admises et doivent être évitées.

Le montage en cascade des commutateurs d'accès est effectué via les câbles à FO au niveau des objets et du terrain.

Les commutateurs permettent la connexion avec les composants suivants :

- serveurs de gestion de section (AR) / gestion régionale du trafic (rVL) ;
- commandes d'installation (AS);
- commandes locales (LS), lorsque la communication interne EES doit être utilisée ;
- acteurs/détecteurs si nécessaire (par ex. caméra ou autres composants TIC).

Les liaisons avec les composants mentionnés sont assurées via des câbles à FO ou des câbles de cuivre. De nombreux acteurs et détecteurs modernes sont alimentés en électricité par des commutateurs PoE (« *Power over Ethernet* »). Cet élément doit être pris en considération de façon adéquate pour la commutation : il ne faut pas recourir à des commutateurs PoE séparés, mais pouvoir équiper les commutateurs d'accès standard des modules PoE nécessaires.

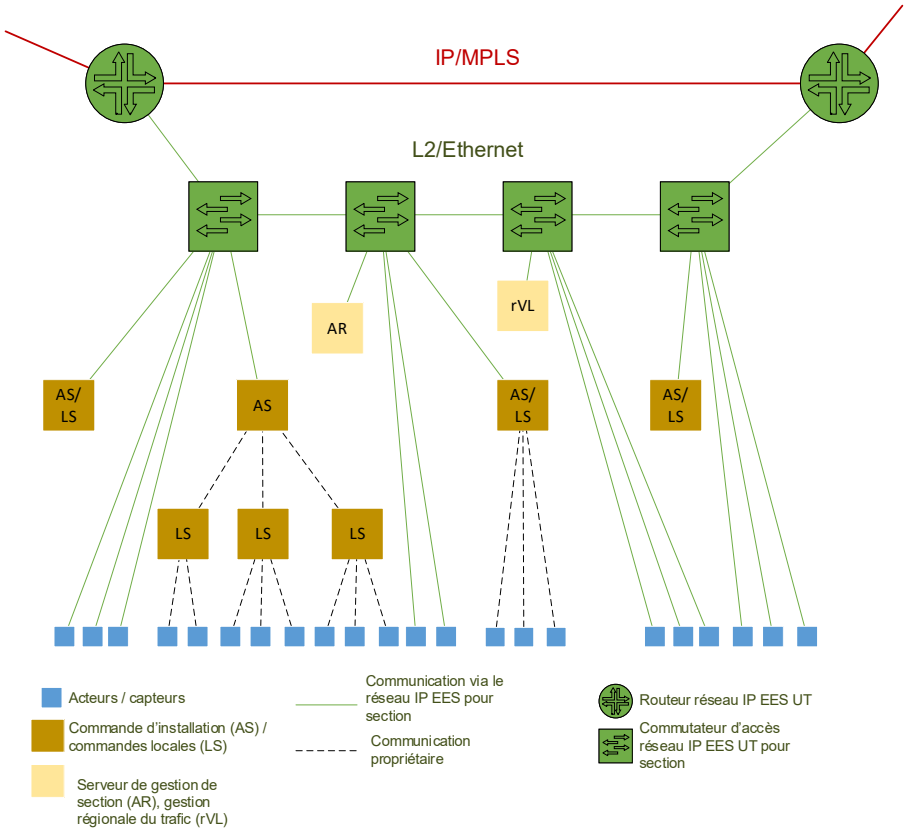

Fig. 2.5 Architecture du réseau IP EES UT section

Les cascades des réseaux IP EES UT section sont conçues conformément aux règles suivantes :

- aux extrémités, elles se terminent par des routeurs distincts ;
- elles comportent au maximum sept commutateurs qui se succèdent, pour deux raisons :
  - pour les applications critiques, la latence ne doit pas dépasser une certaine valeur maximale ;
  - une panne, par ex. suite à des changements de la configuration ou dans la cascade, peut ainsi être mieux limitée à de courts segments.
- les terminaux sont toujours reliés aux commutateurs des cascades, jamais directement aux routeurs ;
- en règle générale, plusieurs cascades sont créées pour une même section EES ;
- des commutateurs supplémentaires à des sous-niveaux ou d'autres réseaux secondaires ne sont pas admis.

Les exemples ci-après visent à illustrer les règles ci-dessus :

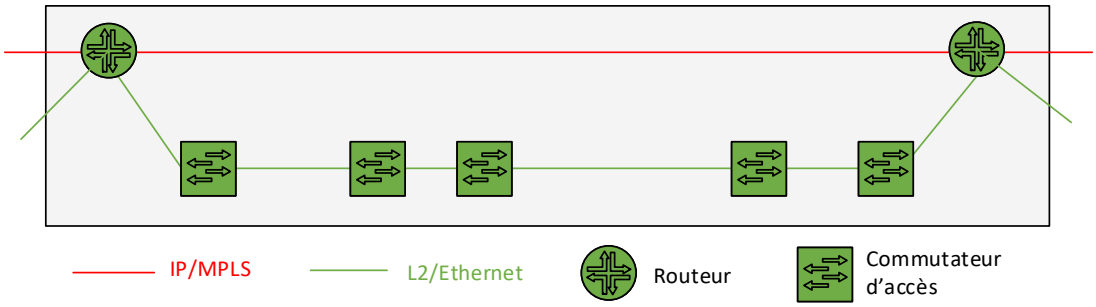

Fig. 2.6 Section à ciel ouvert – une cascade pour les deux sens de circulation

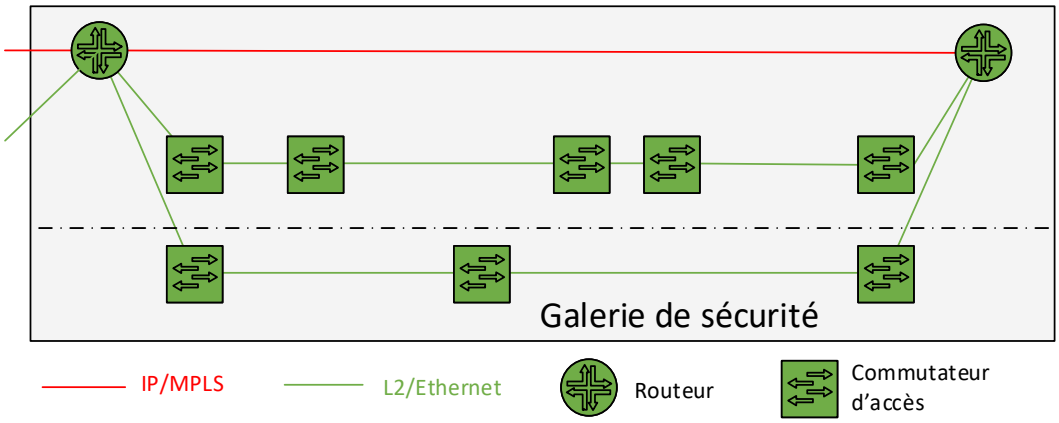

Fig. 2.7 Tunnel – une cascade par tube ou galerie de sécurité

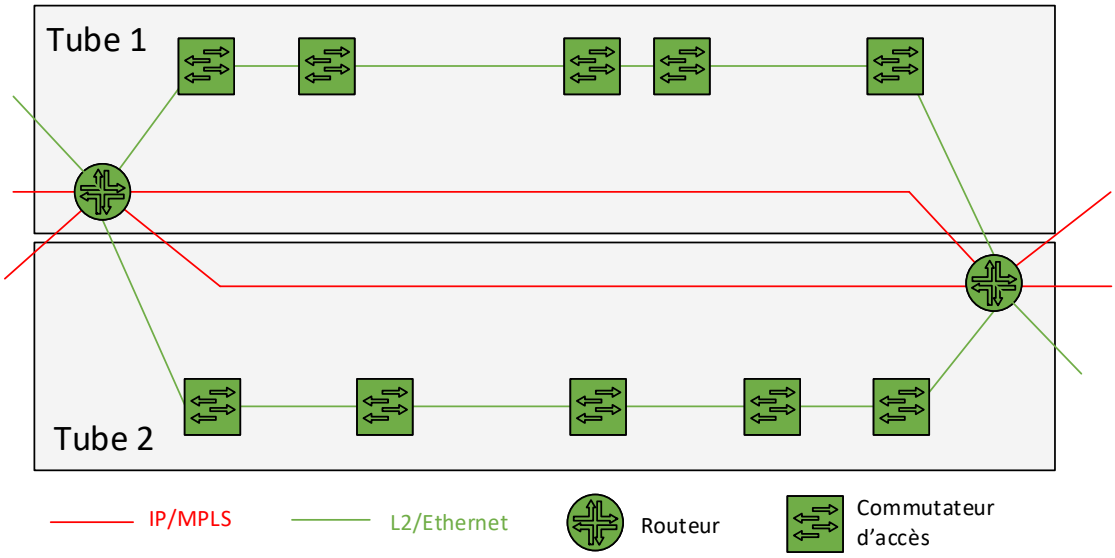

Fig. 2.8 Tunnel à 2 tubes – une cascade par tube

Plusieurs cascades sont nécessaires pour assurer la connexion à des sections comportant de nombreux commutateurs. Puisqu'on admet qu'il y a suffisamment de fibres disponibles dans un faisceau de FO (câble), plusieurs ordonnancements des commutateurs sur diverses cascades sont envisageables.

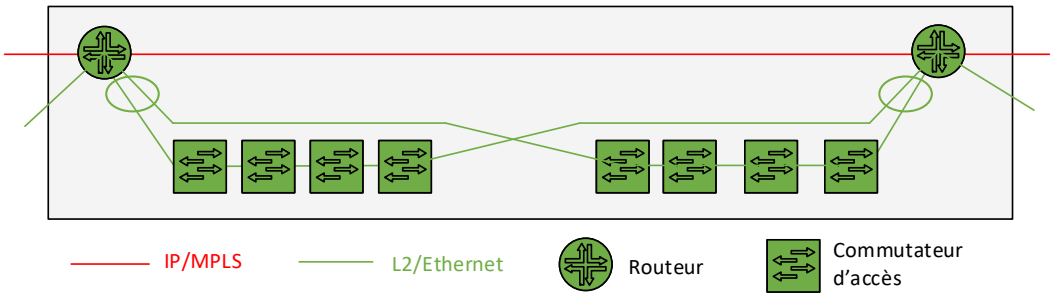

Fig. 2.9 Répartition séquentielle sur plusieurs cascades, fibres dans le même câble à FO

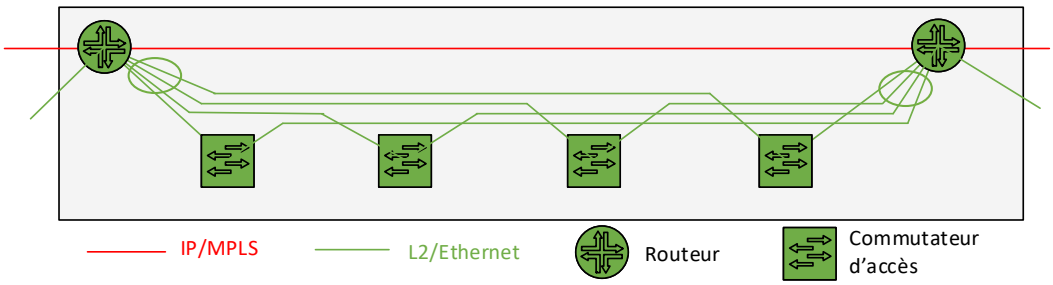

Fig. 2.10 Commutateurs raccordés en étoile, fibres dans le même câble à FO – à la place d'un commutateur, il est possible d'employer jusqu'à sept commutateurs

Les configurations ci-dessus permettent par exemple de séparer des sections en quatre cascades avec 28 commutateurs disposés de façon séquentielle et reliés par quatre fibres différentes via le même faisceau de fibres.

2.7 Accès au sein du réseau IP local EES UT pour centrale ELZ/BLZ

Les réseaux IP EES UT pour centrale ELZ/BLZ constituent, au sein d'un réseau IP EES UT, les niveaux d'accès à des sites centraux tels que les centres d'entretien et les centrales de gestion. Ils assurent la connexion avec l'ensemble des systèmes EES de ceux-ci (ordinateurs de gestion, systèmes de gestion supérieurs, places de travail des opérateurs, etc.).

Un réseau IP EES UT pour centrale ELZ/BLZ est conçu comme une cascade de commutateurs LAN traditionnels, ayant deux routeurs différents à ses extrémités pour la fermeture de l'anneau. Au besoin, plusieurs de ces cascades peuvent être établies dans un même réseau IP EES UT pour centrale ELZ/BLZ.

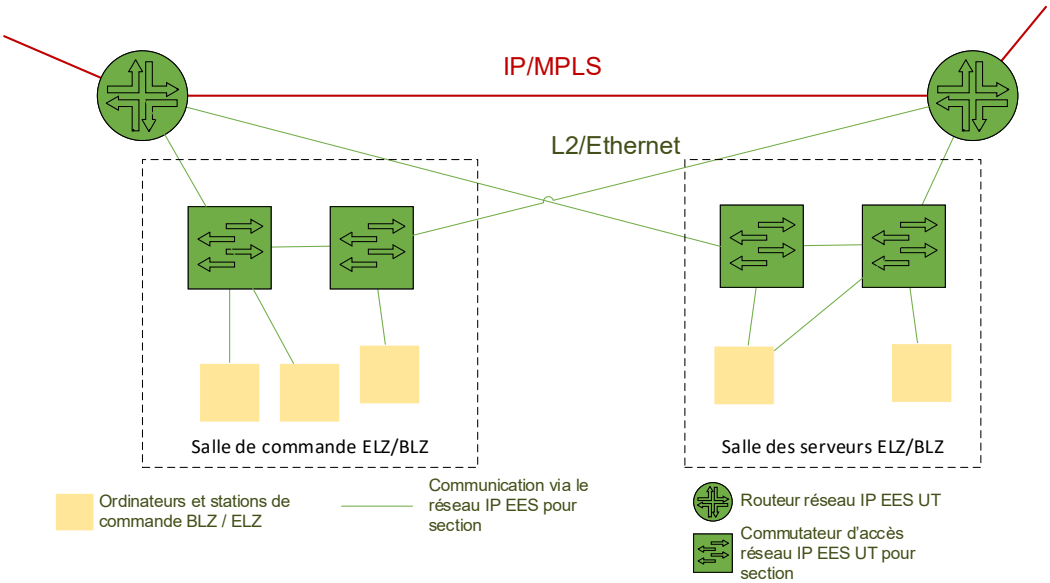

Fig. 2.11 Exemple d'architecture d'un réseau IP EES UT pour centrale ELZ/BLZ

Les commutateurs permettent d'assurer la connexion avec les composants suivants :

- systèmes de gestion supérieurs / ordinateurs de gestion ;
- serveurs nécessaires pour les EES dans les UT ;
- postes de travail / de commande.

Les cascades des réseaux IP EES UT pour centrale ELZ/BLZ sont conçues selon les mêmes règles que celles des réseaux IP EES UT section. Si certains composants doivent être connectés de manière redondante, il faut utiliser deux commutateurs différents à cette fin.

2.8 Utilisation des réseaux IP EES par des tiers

La connexion d'appareils de tiers au réseau IP EES UT est admise si des services L1 ou L2 transparents sont utilisés. Un concept SIPD doit toutefois obligatoirement être élaboré.

Sont des « services transparents » les liaisons point-à-point statiques, qui n'échangent aucune donnée de contrôle avec le réseau IP EES UT, mais utilisent seulement ce dernier comme « câble virtuel » pour le transport de données. Des câbles à FO ou des services Ethernet du réseau IP EES UT peuvent être employés à cette fin.

Exemples d'utilisation :

- radio (DAB) : antennes émettrices dans les tunnels ;
- Car2x.

2.9 Réseau local sans fil (WLAN)

Du point de vue de l'architecture réseau, rien ne s'oppose à une autorisation et à une utilisation du WLAN dans le domaine des EES.

3 Composants du réseau IP EES

3.1 Généralités

L'ensemble des composants du réseau IP EES (par ex. routeurs, commutateurs, serveurs, transformateurs de tension, disjoncteurs, ventilateurs) doivent satisfaire aux conditions ambiantes du lieu de montage et du transport sans présenter un taux de défaillance plus élevé. Ce sont essentiellement la température, l'humidité, les vibrations et la qualité de l'alimentation qui doivent être déterminées.

Afin de permettre l'utilisation d'une offre de produits aussi large que possible, les normes Telcordia GR-63-CORE et GR-1089-CORE doivent être observées pour tous les équipements conformément au niveau NEBS 1 (la conformité au niveau 3 est recommandée).

Pour ce qui est des équipements de sites exposés (c'est-à-dire en dehors des bâtiments), on exigera, selon les situations, les classes de protection 1 à 4 conformément à la norme Telcordia GR-3108.

Les équipements doivent par ailleurs être conformes aux exigences légales locales, notamment aux dispositions fédérales fixées en matière d'informatique verte (« *Green IT* ») et qui prescrivent la réduction de la consommation énergétique. Cet élément devra être pris en considération dans le cadre des différentes acquisitions.

3.2 Technologie

La technologie IP/MPLS est employée dans les routeurs des anneaux de raccordement. Les éléments de réseau actifs de ces dernières (routeurs principaux) sont des routeurs MPLS qui transfèrent des données à 10Gbit/s au minimum. On vise un débit de 100Gbit/s à l'avenir.

La technologie MPLS ne s'étend pas au niveau d'accès : dans les réseaux IP EES UT section et IP EES UT pour centrale ELZ/BLZ, on utilise Ethernet et des extensions pour la segmentation virtuelle (VLAN) et pour garantir la qualité et la capacité de transfert (qualité de service [QoS] et « *policing* »).

La commutation doit être assurée par une gestion active, c'est-à-dire que les commutateurs doivent pouvoir être gérés et configurés à distance via le NMS. Les simples commutateurs de niveau 2 sans gestion ou les commutateurs statiques ne sont pas admis.

Dans le niveau d'accès, les commutateurs 10Gbit/s sont disposés en cascade. En cas de besoin, plusieurs interfaces sont associées pour augmenter la bande passante (agrégation de liens Ethernet). On ne prévoit pas d'atteindre 100Gbit/s dans le niveau d'accès.

3.3 Redondance interne des composants de réseau

Le terme « redondance interne » sert à désigner la redondance de l'alimentation électrique, des cartes de contrôleurs et des cartes d'interface/de réseau. Il s'agit d'une protection contre la défaillance d'un seul module de l'appareil réseau ou d'un brin de l'alimentation.

On cherche à garantir la simplicité des appareils et on observe les règles ci-après s'agissant des routeurs et des commutateurs :

- une redondance interne des composants actifs (par ex. deux cartes de contrôleurs ou deux interfaces réseau) ou la présence de deux appareils distincts ne sont pas requises ;

- une redondance de l'alimentation électrique (deux brins) est recherchée, mais elle n'est obligatoire qu'aux endroits où les systèmes EES raccordés présentent eux-mêmes une alimentation électrique redondante.

3.4 Interfaces réseau (« Network-to-Network Interfaces » ou NNI)

3.4.1 Interface réseau de la dorsale

L'interface qui assure la liaison avec les autres UT, les centres de calcul (RZ) et la VMZ présente un niveau de fonctionnalité volontairement faible. Elle est néanmoins conçue pour une bande passante élevée, de manière à pouvoir faire face telle quelle aux développements futurs attendus.

L'interface réseau de la dorsale est définie en détail par le prestataire de services de la Confédération. Ses principales caractéristiques connues sont les suivantes :

- elle est basée physiquement sur Ethernet. On utilise de préférence une seule interface 100Gbit/s, mais plusieurs interfaces groupées 10Gbit/s sont aussi possibles ;
- elle supporte la répartition logique (par le VLAN selon les standards 802.1Q et QinQ issus de la norme IEEE802.1ad) ;
- elle prend en charge le Ethernet-CFM (« Connectivity Fault Management » selon la norme IEEE802.1ag) pour permettre une surveillance directe de la connectivité par les UT ;
- elle dispose de la synchronisation par Ethernet et de ses fonctions (« Precision Time Protocol » au sens de la norme IEEE 1588) pour l'obtention des informations d'horloge et de fréquence cohérentes ;
- aucun cryptage n'est exigé.

Du point de vue du réseau IP EES UT, l'interface réseau apparaît comme une interface externe, c'est-à-dire que ni les protocoles MPLS spécifiques ni les protocoles de routage généraux ne sont activés pour l'échange interne de données de la topologie réseau. Afin d'optimiser les processus de travail, une configuration de routage purement statique est toutefois abandonnée. À l'interface réseau, le protocole BGP permet d'ajuster la topologie entre les UT, les centres de calcul (RZ) et la VMZ.

3.4.2 Interface réseau des routeurs

L'interface réseau des routeurs assure la communication entre les routeurs MPLS d'une UT, lesquels relient les sections entre elles et offrent la connectivité WLAN dans l'UT.

L'interface réseau des routeurs est spécifiée comme suit :

- elle est basée physiquement sur Ethernet. Une seule interface 10Gbit/s est utilisée et doit (si possible) permettre une transmission via les câbles à FO de l'UT sans renforcement ni régénération des signaux. Il faut utiliser des composants standard pour les lasers, étant entendu que les élargissements de distance habituels dans l'industrie (par ex. 10GBASE-ZR pour des distances supérieures à 80 km) par rapport au standard officiel 10GBASE-ER (40 km) de l'IEEE sont explicitement autorisés ;
- elle dispose de la synchronisation par Ethernet et de ses fonctions (« Precision Time Protocol » au sens de la norme IEEE 1588) pour l'échange d'informations d'horloge et de fréquence cohérentes ;
- aucun cryptage n'est exigé ;
- l'interface supporte la répartition logique de l'interface MPLS ;
- à l'interface réseau, les protocoles pour la topologie MPLS (par ex. protocoles IS-IS, LDP et RSVP) ainsi que ceux pour la topologie IP (surtout iBGP) sont activés. Si les protocoles à utiliser ne sont pas imposés, ils doivent soutenir efficacement l'ensemble des services réseaux.

3.4.3 Interface réseau de l'accès

L'interface réseau de l'accès définit l'interaction entre le niveau des routeurs MPLS et le niveau d'accès, lequel est réalisé comme une structure de niveau 2 sans MPLS.

Elle est spécifiée comme suit :

- elle est basée physiquement sur Ethernet. Une seule interface 10Gbit/s ou 1Gbit/s est utilisée et permet une transmission via les câbles à FO de l'UT sans renforcement ni régénération des signaux. Des composants standard doivent être utilisés pour les lasers ;
- aucun cryptage n'est exigé ;
- l'interface supporte la répartition logique (par le VLAN selon les standards 802.1Q et QinQ issus de la norme IEEE802.1ad) ;
- pour le trafic des utilisateurs, elle est une interface de niveau 2 avec une commutation redondante résultant de la double connexion à deux routeurs MPLS. Le standard SPB (« Shortest Path Bridging », issu de la norme IEEE 802.1aq) est utilisé pour la commutation3 ;
- des réseaux logiques (VLAN) sont définis sur l'interface pour les tâches de gestion et de contrôle.

Le routeur MPLS est chargé de la représentation (« *mapping* ») des structures de réseau logiques MPLS sur les structures de réseau logiques VLAN. Dernier dispositif de routage, il assure la transmission de tous les réseaux IP à l'interface réseau de l'accès aux commutateurs d'accès de niveau 2. Pour assurer la redondance, les routeurs MPLS sont configurés selon le protocole VRRP aux deux extrémités du niveau d'accès, de sorte que les terminaux raccordés et les commutateurs d'accès de niveau 2 n'ont pas besoin de prendre en charge des protocoles spéciaux.

3.5 Interface utilisateur (« User-Network Interface » ou UNI)

Le réseau IP EES UT ne prend en charge que des services basés sur Ethernet. Il n'offre pas de services patrimoniaux (*« legacy services* », par ex. lignes louées E1 ou RS-232). Il n'offre pas non plus de services réseaux pour toutes les UT, mais la possibilité de mettre en place plusieurs routeurs virtuels à l'interface réseau de la dorsale permet des structures VPN nationales.

Les services réseaux ci-après sont disponibles au sein des UT.

Services Ethernet (« services L2 ») :

- connexion point à point entre deux ports (« Virtual Leased Lines », VLL) ;
- commutateur de niveau 2 réparti ; communication entre de nombreux ports et un point central, mais sans communication directe entre eux (« Ethernet Virtual Private Tree » ou « E-Tree ») ;
- commutateur de niveau 2 réparti ; communication entre de nombreux ports sans restriction (« Ethernet Virtual Private LAN » ou « E-LAN »).

[3] Le protocole « *Spanning Tree* » (*STP* selon les normes IEEE 802.1D, 802.1w ou 802.1s) est admis seulement pour la connexion de niveaux d'accès patrimoniaux pour lesquels une migration est impossible et dont les commutateurs de niveau 2 ne peuvent être remplacés.

Services IPv6 (« services L3 en IPv6 ») :

- connectivité multipoint à point « Hub and Spoke » (entre de nombreux points distants et un point central) ;
- connectivité multipoint à multipoint « Any to any » (routeurs virtuels répartis géographiquement).

Services IPv4 (« services L3 en IPv4 ») :

- connectivité multipoint à point « Hub and Spoke » (entre de nombreux points distants et un point central) ;
- connectivité multipoint à multipoint « Any to any » (routeurs virtuels répartis géographiquement).

Services IP en double pile (« services L3 en IPv6 et IPv4 ») :

- connectivité multipoint à point « Hub and Spoke » (entre de nombreux points distants et un point central) ;
- connectivité multipoint à multipoint « any to any » (routeurs virtuels répartis géographiquement).

L'interface est toujours une interface Ethernet, permettant une connexion par câble de cuivre ou par FO monomode (vitesses allant jusqu'à 10Gbit/s). Comme interface de service, il est possible d'utiliser aussi bien l'ensemble de l'interface physique qu'une interface VLAN logique sur celle-ci (selon le standard IEEE 802.IQ) :

- 1000Base-T;
- 1000Base-LX (avec FO monomode,) ;
- 100Base-FX (uniquement pour les systèmes existants).

Les éventuelles interfaces 10 GE sont réalisées de préférence au moyen de modules 10GBASE-LR.

Pour tous les services IP, le multicast peut être activé en plus de l'unicast. Pour les services Ethernet, le multicast et le broadcast sont en principe activés.

3.6 Qualité de service (QoS)/largeurs de bande selon l'accord sur les niveaux de service (SLA)

En principe, tous les services disposent de la largeur de bande garantie dans le SLA[4] (« *committed information rate* »). Si cette valeur n'est pas dépassée, la latence et sa variance (« jitter ») sont minimes (latence inférieure à 10 ms, variance inférieure à 2 ms). Le taux de perte de paquet est inférieur à 10^{-6}.

Pour les services dont le trafic varie fortement et pour lesquels la latence et les éventuelles pertes de paquets sont moins critiques, une largeur de bande supplémentaire (« *peak information rate* ») peut être prévue dans le SLA. Le réseau IP EES UT essaie de garantir ce niveau plus élevé pour la transmission ou l'enregistrement temporaire des données.

Les valeurs exactes pour chaque UT sont spécifiées dans le SLA, car les latences en particulier dépendent de la répartition géographique du réseau IP EES UT.

[4] SLA = Service Level Agreement ou accord sur les niveaux de service. On admet que les exigences posées au réseau sont spécifiées pour chaque service requis.

3.7 Consolidation

La consolidation des composants du réseau est en principe conforme aux prescriptions de la directive ASTRA 13030 « Sécurité informatique des systèmes de commande et de gestion des équipements d'exploitation et de sécurité »[2] (en allemand uniquement).

3.8 Synchronisation d'horloge et de fréquence

Tous les appareils réseau actifs du réseau IP EES utilisent les protocoles PTP et SyncE (G.8261/2/4 et IEEE 1588) pour la diffusion d'informations d'horloge et de fréquence précises. Aux interfaces utilisateur, les systèmes connectés peuvent obtenir ces informations grâce aux protocoles PTP/NTP et SyncE. Les appareils réseau actifs se synchronisent via les interfaces réseaux. La dorsale doit à cette fin pouvoir exécuter SyncE de manière transparente (c'est-à-dire asynchrone), comme les réseaux WDM (G.709 OTN/OTH), ou être synchrone avec la référence de l'OFROU.

Les centres de calcul EES ou les hubs EES fournissent une source d'horloge et de fréquence de la plus haute qualité (horloge atomique au césium ou équivalente). Pour des raisons liées à la sécurité de fonctionnement (blocages intentionnels), les informations d'horloge et de fréquence du réseau IP EES doivent être préférées aux références GPS. De plus, il faut vérifier les sources d'horloge du réseau (« *authentication and authorization of masters* »*)*. Pour l'obtention directe des informations d'horloge, les sorties de référence usuelles telles que BITS (« *Building Integrated Timing Supply* ») et IRIG (« *Inter-Range Instrumentation Group time code* ») devraient par ailleurs être disponibles selon les besoins des UT pour le remplacement de solutions isolées et de références d'horloge GPS.

Les UT ont aussi la possibilité d'exploiter et d'utiliser localement leur propre source de fréquence. Une synchronisation des sources de fréquence de l'ensemble des UT et des centres de calcul EES ne s'impose pas. Par contre, l'horloge de toutes les UT doit être synchronisée à l'échelon national au moyen du protocole PTP.

Tandis que seuls PTP et des appareils réseau synchrones sont utilisés dans le réseau IP EES, le protocole NTP est disponible en plus de PTP pour la connexion des dispositifs périphériques. Ainsi, les deux routeurs de la section fonctionnent toujours comme serveurs d'horloge NTP. Pour des raisons de coûts, le niveau d'accès peut aussi être réalisé avec des commutateurs qui n'exécutent pas les protocoles PTP et SyncE. Si aucune précaution particulière n'est nécessaire pour l'utilisation de NTP, celle de PTP (ou d'informations de fréquence) par les dispositifs périphériques raccordés exige une configuration du profil PTP selon la recommandation ITU-T G.8265.1.

Les dispositifs périphériques doivent obligatoirement vérifier l'identité du serveur d'horloge (« *authentication and authorization of masters* »*).*

En raison de la problématique de la seconde intercalaire, il faut travailler à l'interne non pas avec le temps universel coordonné (« *Universal Time Coordinated* », UTC), mais avec le temps atomique international (TAI) dans tous les éléments du réseau.

4 Dorsale du réseau IP EES

Le présent chapitre sera complété lorsque la solution définitive pour la dorsale aura été trouvée.

5 Adressage IP

5.1 Principes

Tous les appareils fixes qui sont connectés au réseau IP EES sont pourvus d'adresses fixes. Le protocole IP est utilisé dans sa version 6 (IPv6) pour l'ensemble du réseau IP EES. L'utilisation d'IPv6 pour l'adressage des éléments du réseau et pour la création des sous-réseaux IP/MPLS est obligatoire. Le réseau IP EES lui-même doit être à double pile IPv4/IPv6.

Il est requis d'utiliser IPv6 pour la communication aux niveaux de la gestion, de la région (BLZ/ELZ/UeLS) et de la section (AR/rVL/AS).

Comme les appareils plus anciens sur le terrain (LS/acteurs/capteurs) ne prennent pas en charge IPv6, l'utilisation du protocole IPv4 est exceptionnellement permise pour la communication entre lesdits appareils. Étant donné que l'adressage IPv4 est déjà en place dans les sous-systèmes locaux, seul le concept d'adressage pour IPv6 sera traité dans le présent chapitre ; il est valable pour l'ensemble des appareils du réseau IP EES.

5.2 Concept d'adressage IPv6

Le présent document ne fournit pas d'explications sur le format d'adresse IPv6, mais celles-ci figurent dans la norme RFC 4291.

Les principes ci-après s'appliquent à la structure de l'adresse IPv6 :

- on part du principe que l'OFROU ne gère qu'un seul domaine (bsa-ch.ch) et que la plage d'adresse assignée par la Confédération peut être entièrement utilisée pour ce domaine ;
- la plage d'adresse IPv6 mise à la disposition de l'OFROU par la Confédération (UPIC) est la suivante :

  2a07:2900:8000::/40

- seules des adresses globalement routables sont utilisées (pas d'adresses locales uniques [ULA]) pour qu'une traduction d'adresses de réseau (« Network Address Translation » [NAT]) ne soit pas nécessaire ;
- la structure de l'adresse se base sur la structure de réseau logique et sur le zonage. Il se peut que la structure géographique soit reflétée par hasard, mais ce n'est pas l'objectif ;
- la structure logique est optimisée selon les flux de données, pour que les chemins de données soient aussi courts que possible et que les données ne passent si possible que par le routeur le plus proche.

5.3 Adresses IPv6 parties réseau et hôte

Les 128 bits d'une adresse IPv6 sont répartis dans une partie réseau (les premiers 64 bits) et une partie hôte (les 64 bits restants) et sont définis pour le réseau IP EES comme suit:

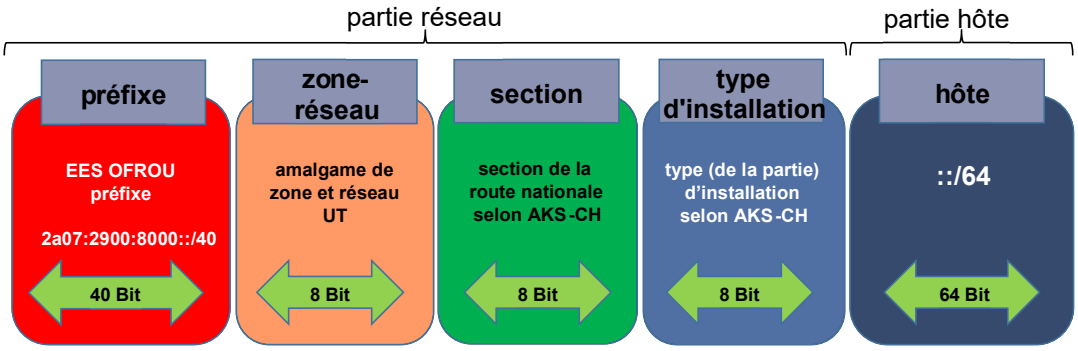

Fig. 5.1 Structure de l'adresse IPv6

La partie réseau de l'adresse IPv6 se dérive des éléments suivants :

Elément	Demi-octet	Remarques
préfixe	1 – 10	préfixe statique accordé par la Confédération
zone-réseau	11, 12	combinaison des zones prescrites par la sécurité informatique et des sous-réseaux (des UT, du RZ et de la VMZ-CH)
section	13, 14	section EES le long des routes nationales (à ciel ouvert, tunnel)
type d'installation	15, 16	types d'installation ou de partie d'installation de l'AKS-CH (énergie, éclairage, ventilation, signalisation etc.)
hôte	17-32	64 bit d'identificateur d'interface ou d'hôte

La partie hôte à son tour se construit à partir des éléments suivants :

Elément	Demi-octet	Remarques
nom de l'installation	17, 18	listes des installations (les sections tunnel, les lieux-dits) selon l'« AKS-CH » [1]. Les listes sont établies lors des révisions de la directive.
agrégat	19, 20	selon la directive 13013 [1]
numéro	21, 22	le numéro de l'agrégat (max. 255)
réserve	23, 31	9 demi-octets (36 Bit) de réserve
instance	32	instanciation ou numérotage élargi (max. 16, 0-F)

Exemple: Dans le réseau IP ESS la distribution basse tension dans le tunnel de Seelisberg reçoit l'adresse IPv6 suivante :

2a07:2900:8011:2213:8::

Les détails sont spécifiés dans la documentation OFROU 83040 Adressage IP [3].

6 DNS, DHCP et gestion des adresses IP

6.1 Gestion des adresses IP

Les règles ci-après s'appliquent à la gestion des adresses IPv4/v6 :

- la gestion des adresses IPv4 et IPv6 doit se faire via un outil IPAM/DDI ;
- le système DNS doit être utilisé pour l'attribution de noms d'hôte aux adresses. Chaque hôte doit être clairement identifiable par son nom DNS ;
- les noms d'hôte doivent en principe toujours permettre l'accès aux appareils. Cette règle vaut en particulier pour l'accès de terminaux d'utilisateurs finaux à des appareils. Exceptionnellement, l'accès peut se faire directement par les adresses IP ;
- étant donné qu'en général les noms d'hôte sont repris dans la configuration liée à l'établissement d'une connexion, il faut assurer leur transcription en une adresse. Cette opération se réalise par l'intermédiaire du serveur DNS ou du fichier hôte sur le terminal ;
- si la résolution se fait par l'intermédiaire du serveur DNS, l'accessibilité de ce dernier doit être constamment garantie ;
- dans le cas d'une résolution par l'intermédiaire du fichier hôte, il faut garantir que celui-ci corresponde toujours aux contenus du serveur DNS, qui est déterminant pour l'attribution de noms d'hôtes aux adresses.

6.2 Architecture IPAM/DDI

Les services DNS, les services DHCP et la gestion des adresses IP sont étroitement liés. Pour que la gestion des services nécessaires puisse être réalisée de manière efficace et aussi correcte que possible, il faut utiliser un outil intégré DNS, DHCP et IMAP (outil IPAM/DDI).

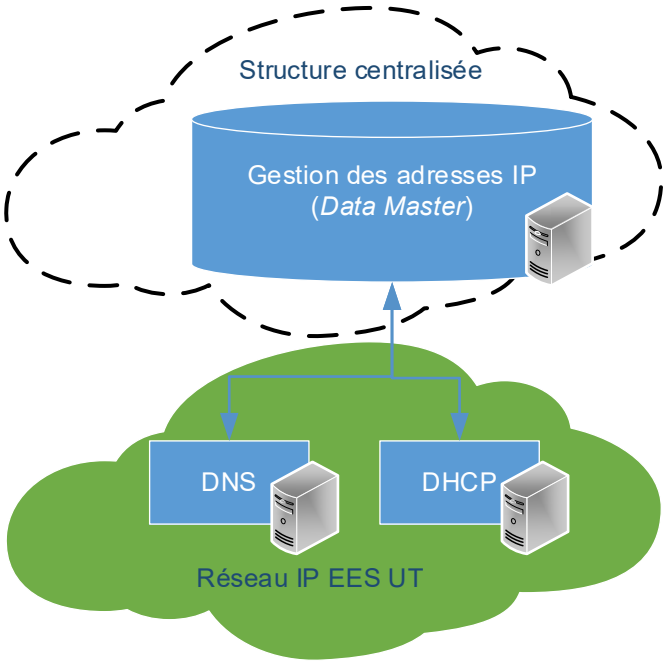

Fig. 6.1 Architecture IPAM/DDI

L'outil IPAM/DDI (« *Data Master* ») pour la gestion des adresses IP est conçu de manière centralisée. Les services DNS et DHCP sont configurés par l'intermédiaire de l'outil

IPAM/DDI. Les serveurs DNS et DHCP sont conçus de manière redondante dans les UT et réutilisés pour autant que l'infrastructure disponible puisse être administrée par l'outil IPAM.

6.3 Exigences envers l'outil IPAM/DDI

Les exigences ci-après sont posées à l'outil IPAM/DDI :

- **Gestion automatisée des adresses IP**
  Il doit être possible de scanner automatiquement les adresses IP et d'établir ainsi un inventaire actuel des adresses IP utilisées et libres. À cette fin, la gestion des adresses IPv4, IPv6 et des blocs d'adresse doit être possible sur le même réseau.
- **Gestion intégrée des serveurs DHCP et DNS**
  Les réservations DHCP et les entrées DNS doivent pouvoir être gérées par l'intermédiaire d'une console centralisée. La gestion individuelle des données se fait localement sur les différents serveurs DHCP et DNS.
- **Reconnaissance des conflits IP**
  L'outil IPAM/DDI doit signaler les conflits IP, les sous-réseaux/domaines épuisés ou des entrées DNS divergentes et générer les alarmes ou les rapports correspondants.
- **Délégation de la gestion**
  Il doit être possible de déléguer la gestion de certaines plages d'adresse IP et de tâches à différents rôles. Les UT doivent pouvoir gérer leurs plages d'adresse et assurer l'administration des serveurs DNS et DHCP de manière autonome.

6.4 Mise en place et exploitation de l'outil IPAM/DDI

La documentation ASTRA 83041 [4] régit la mise en place et l'exploitation de l'outil IPAM/DDI.

7 Sécurité (« *security* ») et zones de réseau

Les exigences de la directive ASTRA 13030 « Sécurité informatique des systèmes de commande et de gestion des équipements d'exploitation et de sécurité » [2] doivent être satisfaites. Cette directive met notamment en œuvre les prescriptions de sécurité des réseaux dans l'administration fédérale (19.12.2013).

La communication au sein du réseau IP EES est possible sans limites sur tout le territoire suisse. À cette fin, un service de réseau correspondant est mis en place dans l'UT et peut être atteint par routeur depuis les autres UT, les RZ ainsi que la VMZ.

Pour des raisons de sécurité, tous les réseaux partiels logiques ne sont pas implémentés de cette manière. De nombreux réseaux partiels sont utilisés exclusivement par les UT et ne sont pas accessibles de l'extérieur. Cette isolation se fait pendant le routage à l'interface réseau de la dorsale, par l'intermédiaire du routeur MPLS. Les mécanismes d'IPv6 doivent être utilisés de manière ciblée pour la segmentation des réseaux.

La documentation ASTRA 83042 [5] règle la mise en place et l'exploitation des zones de sécurité, et décrit les mesures techniques et opérationnelles.

8 Contrôle de l’accès au réseau (« *Network Access Control* », NAC)

8.1 Principe

Le raccordement d’appareils à un système NAC doit être surveillé et commandé ; le réseau local EES RZ fait exception (voir le chapitre 2.1).

L’objectif visé est de détecter et de signaler les changements dans les accès au réseau (« *Service Access Points* », SAP) au moyen du système NAC. Ce dernier doit donc être en mesure d’identifier l’ensemble des appareils connectés.

La nécessité de recourir à un système NAC ainsi que les exigences y afférentes sont définies dans la directive ASTRA 13030 [2]

8.2 Mise en place et exploitation de l’outil NAC

La documentation ASTRA 83043 [6] régit la mise en place et l’exploitation de l’outil NAC.

9 Système de gestion de réseau (« *Network Management System* », NMS)

Un système de gestion de réseau (NMS) doit être utilisé pour gérer un réseau IP EES UT et en surveiller l'exploitation.

Les tâches du NMS sont résumées par le sigle FCAPS[5] :

F : *Fault Management* (gestion des erreurs) ;
C : *Configuration Management* (gestion de la configuration) ;
A : *Accounting Management* (gestion de l'administration) ;
P : *Performance Management* (gestion des performances) ;
S : *Security Management* (gestion de la sécurité).

9.1 Gestion des erreurs

La gestion des erreurs est la partie la plus importante de la gestion de réseau, avec la gestion de la configuration. Les erreurs doivent être reconnues à temps pour ainsi augmenter la disponibilité du réseau.

Exigences spécifiques posées à la gestion des erreurs :

- surveillance de bout en bout de tous les services de réseau au sein du réseau IP EES UT ;
- monitoring de tous les composants du réseau et des médias (liaisons FO) au sein du réseau IP EES UT ;
- visualisation en temps réel du réseau (logiquement et physiquement) ;
- possibilité d'attribuer aux services de réseau les alarmes de composants physiques ou logiques ;
- Les alarmes doivent être mises en corrélation et les alarmes subséquentes doivent pouvoir être masquées par une analyse performante (analyse « Root-Cause »), laquelle doit être réalisable sans interruptions sur l'ensemble du réseau ;
- mise en évidence des rapports entre les erreurs, possibilité de naviguer rapidement entre l'alarme et la cause ainsi qu'entre les éléments affectés et les services ;
- possibilité de classifier et filtrer les alarmes ;
- possibilité de disposer de plusieurs fenêtres d'alarme actives en même temps ;
- possibilité de naviguer directement des fenêtres d'alarme jusqu'aux objets physiques déclencheurs/concernés (appareil/port) et aux objets logiques (services) ;
- archivage des erreurs durant 12 mois et possibilité de visualiser celles-ci durant ce laps de temps dans l'interface utilisateur graphique (GUI ; consignation des erreurs).

9.2 Gestion de l'administration

Comme les réseaux IP UT ne font pas l'objet d'un décompte, le terme « administration » est utilisé en lieu et place de « comptabilité » (« *accounting* »). L'administration comprend la gestion des utilisateurs, des mots de passe et des autorisations d'accès.

Exigences posées à la gestion de l'administration :

[5] Selon la norme ISO/IEC 7498-4 « Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base -- Partie 4 : Cadre général de gestion »

- gestion des droits d'utilisateurs (accès, limites et priorités) pour les composants de réseau comme les routeurs ou les commutateurs ;
- prise en charge des modèles de rôles avec leurs droits d'accès respectifs ;
- possibilité de définir des droits d'accès aussi bien au niveau fonctionnel que pour certains éléments de réseau (les utilisateurs ne devraient par ex. pouvoir voir que leurs propres éléments) ;
- documentation.

9.3 Gestion de la configuration

La gestion de la configuration comprend toutes les fonctions liées à la configuration du réseau et de ses composants.

Exigences spécifiques posées à la gestion de la configuration :

- configuration des éléments matériels comme les interfaces du réseau ou les ports. La configuration d'un élément du réseau via l'interface de ligne de commande (CLI) de celui-ci n'est autorisée qu'à titre exceptionnel ;
- les configurations des nouveaux services du réseau doivent pouvoir se faire au moyen d'opérations graphiques simples de bout en bout. Des modèles prédéfinis et adaptables doivent être disponibles à cette fin (choisir le service ou les modèles, choisir les points terminaux, vérifier et procéder au provisionnement automatique du chemin primaire et aussi secondaire) ;
- il faut aussi qu'en cas de remplacement de composants du réseau, des fonctions de copie soient disponibles pour reprendre la configuration existante et procéder à une adaptation rapidement ;
- simulation et vérification de configurations, indication de l'utilisation des largeurs de bande sur chaque chemin et lien physique ;
- « Traffic Shaping » (analyse du réseau, optimisation du réseau) ;
- tous les appareils du réseau doivent pouvoir être inventoriés :
    - routeurs, commutateurs ;
    - câbles, connexions au réseau ;
    - passerelles (« gateways »).
- la gestion des versions des configurations et des logiciels se fait pour chaque appareil.

9.4 Gestion de la performance

La gestion de la performance consiste à traiter des résultats de mesure quantitatifs afin de fournir des informations qualitatives.

Les exigences spécifiques posées à la gestion de la performance sont les suivantes :

- les largeurs de bande (conservées sur les chemins redondants et effectivement utilisées) doivent pouvoir être représentées ;
- la perte de paquets, la latence ainsi que sa variance, etc. doivent pouvoir être surveillés ;
- les changements de ces données doivent pouvoir être présentés sur n'importe quelle fenêtre temporelle ;
- en cas de dépassements des valeurs limites, les alarmes doivent pouvoir être exécutées ;
- les statistiques doivent être disponibles sous forme de graphique et de tableau ;
- les rapports doivent pouvoir être exportés sur MS-Office (CSV, XLSX, DOCX).

9.5 Gestion de la sécurité

La gestion de la sécurité consiste à contrôler et protéger l'autorisation d'accès aux données du réseau.

Les exigences spécifiques posées à la gestion de la sécurité sont les suivantes :

- tant les utilisateurs que les systèmes externes doivent s'identifier pour l'ensemble des activités ;
- la capacité d'audit doit être garantie dans tout le système. Des événements comme les interventions physiques sur le matériel ainsi que les accès via la CLI ou le terminal local en particulier doivent pouvoir être visibles dans les logs.

10 Exploitation

10.1 Niveaux de service (« Standard Service Levels »)

Les exigences posées à l'exploitation du réseau IP EES et à son système de support opérationnel sont définies par les niveaux de service standardisés.

10.1.1 Heures de service

Les **heures de service** sont les heures qui ont été définies pour la prestation de services. Le service fourni au point d'accès au service (« *Service Access Point* », SAP) est surveillé de manière proactive ou réactive.

Le **temps de maintenance** (fenêtre de maintenance) est une période définie dans le cadre des paramètres de niveau de service, durant laquelle des travaux de maintenance pour un service donné sont effectués et où la fourniture de service n'est donc pas prévue.

Valeur de mesure	Valeur	Méthode de mesure / remarques
Service 7x24	7x24h (365 jours)	• Lundi – dimanche 00 h 00 – 24 h 00, y compris jours fériés nationaux. • Aucune interruption planifiée, à savoir aucune fenêtre de maintenance périodique avec interruption de service, mais des maintenances prévues et annoncées. • Les maintenances et les changements impliquant une interruption de service se font seulement après entente. • Les travaux impliquant une interruption de service sont autorisés dans le cadre d'une procédure spéciale qui inclut les utilisateurs (min. 15 jours ouvrables à l'avance).

Tableau 10.2 Heures de service standard

Les heures de service pour l'ensemble des installations et des services des EES sont toujours 7x24h. Aucune heure de service alternative ne sera définie.

10.1.2 Heures d'assistance

Les **heures d'assistance** sont la période (périodes dans la journée, jours de la semaine et jours fériés nationaux) durant laquelle l'assistance pour le service offert au SAP est garantie. Durant les heures d'assistance, un ticket d'incident est ouvert dans l'espace du temps de réaction prévu dans le contrat pour lancer sans délai la procédure de rétablissement du service.

L'attribut **temps de réaction** est défini comme la période entre l'annonce de dysfonctionnement du service (par le client ou le système de surveillance) et la première information au client et l'ouverture d'un ticket d'incident dans le système.

Valeur de mesure	Valeur	Méthode de mesure / remarques
Heures d'assistance 7x24	7x24h (365 jours)	• Lundi – dimanche 00 h 00 – 24 h 00, y compris les jours fériés nationaux. • Temps de réaction du *Service Desk* ou du service de piquet en cas d'avis de dysfonctionnement : max. 15 minutes.

Tableau 10.3 Heures d'assistance standard

Les heures d'assistance pour l'ensemble des installations et des services des EES sont toujours 7x24h. Aucune heure d'assistance alternative ne sera définie.

10.1.3 Disponibilité

La **disponibilité** est une caractéristique du niveau de service d'un service ou d'un élément de service, qui décrit de quelle manière la fonctionnalité exigée et convenue doit être assurée à un moment donné ou sur une période définie.

Dans ce contexte, **l'indisponibilité (« *downtime* »)** est la somme de toutes les interruptions de service en heures et en minutes dans l'espace de la période de mesure définie, durant lesquelles un service n'est pas disponible au SAP correspondant dans les heures d'assistance convenues et, partant, où la fonctionnalité minimale n'est pas assurée.

Le niveau de service du paramètre de la disponibilité peut être choisi selon différents niveaux de qualité.

Valeur de mesure	Valeur	Méthode de mesure / remarques
***Downtime* 1h**	<= 1h par an	• Ne peut être atteint que par des connexions redondantes. • Mesuré par an et raccordement redondant (SAP redondants). • La perte de redondance, à savoir la perte d'une connexion, doit être corrigée dans l'espace de 24h. • Sont admises au max. 2 défaillances par an.
***Downtime* 8h**	<= 8h par trimestre	• Mesuré par trimestre et raccordement (SAP) • Sont admises au max. 2 défaillances par trimestre.
Downtime Best Effort	Pas de prescription	• L'objectif est de corriger une défaillance dans les 24h.

Tableau 10.4 Aperçu de la disponibilité

10.1.4 Autonomie de courant

L'**autonomie de courant** indique le temps durant lequel un système doit encore fonctionner avec sa propre alimentation électrique de secours en cas de coupure de courant du réseau public.

L'autonomie de courant sur le réseau IP EES doit permettre d'atteindre durant encore un certain temps les appareils et systèmes connectés au réseau IP EES en cas de pénurie d'électricité ou de coupure de courant. Pour certaines installations, il est fort probable qu'une autonomie de courant plus élevée soit nécessaire.

Valeur de mesure	Valeur	Méthode de mesure / remarques
Autonomie de courant 1h	> 1h	• Mesurée par événement.
Autonomie de courant *Best Effort*	Pas de prescription	• n.a.

Tableau 10.5 Aperçu de l'autonomie de courant

10.2 Attribution des niveaux de service du réseau IP EES

Le tableau ci-après montre l'attribution de chaque niveau de service aux différents éléments du réseau IP EES.

	Autonomie de courant 1h	Autonomie de courant *Best Effort*	Heures de service 7x24 (365 jours)	Heures d'assistance 7x24 (365 jours)	*Downtime* 1h (par an)	*Downtime* 8h (par trimestre)	*Downtime Best Effort*
Raccordement de la dorsale de l'UT / VMZ-CH / RZ EES (raccordement redondant, sur deux routeurs)	X	--	X	X	X	--	--
Raccordement de la connexion en cascade du réseau IP EES UT section/ELZ/BLZ (raccordement redondant, sur deux routeurs)	X	--	X	X	X	--	--
Access Switch	X	(X)	X	X	--	X	(X)
NTP	X	--	X	X	X	--	--
DMZ GE / VMZ-CH	X	--	X	X	--	X	--
NMS GE / VMZ-CH	X	--	X	X	--	X	--
Outil IPAM/DDI	X	--	X	X	--	X	--
DHCP / DNS	X	--	X	X	--	X	--
Outil NAC	X	--	X	X	--	X	--

X = Standard (X) = peut être utilisé dans des cas justifiés

Tableau 10.6 Attribution des niveaux de service pour le réseau IP EES

10.3 Exploitation centralisée et décentralisée

Les éléments du réseau IP EES sont exploités de différentes manières.

- L'exploitation des éléments ci-après reste sous la responsabilité des UT et elle est gérée par celles-ci :
    - réseau IP EES UT ;
    - NMS ;
    - serveur DNS (configuré par l'outil IPAM/DDI) ;
    - serveur DHCP (configuré par l'outil IPAM/DDI) ;
    - DMZ/pare-feu/RAS ;
    - outil NAC.

  L'infrastructure nécessaire est disponible pour chaque UT ; une organisation d'exploitation ad hoc existe également pour chaque UT.

- Les éléments ci-après sont gérés de manière centralisée :
    - outil IPAM/DDI ;
    - outil E2E-Service Monitoring ;
    - synchronisation d'horloge et de fréquence (référence pour l'heure et l'horloge de l'OFROU).

  L'infrastructure nécessaire est mise en place de manière centralisée, mais utilisée de manière décentralisée. L'organisation d'exploitation ne sera donc pas multipliée/recréée dans chaque région.

Les documentations ASTRA correspondantes doivent être consultées pour la mise en œuvre concrète.

11 Gestion du réseau IP EES

La gestion du réseau IP EES se fait de manière centralisée par le gestionnaire du cycle de vie stratégique (« *Lifecycle Manager* », LCM). Ce dernier assume les tâches suivantes :

- définir et assumer la responsabilité de l'ensemble de l'architecture du réseau IP EES, y compris les systèmes d'assistance nécessaires, et l'adapter continuellement aux besoins ;
- entretenir un contact étroit avec les partenaires internes ou externes et avec les organisations, et clarifier leurs besoins et leurs exigences en ce qui concerne les services de communication EES ;
- prendre en considération les exigences posées au réseau IP EES et définir les directives pour disposer d'une infrastructure de communication homogène, performante et hautement disponible ;
- définir le degré de standardisation du réseau, les systèmes d'assistance nécessaires et les services en étroite collaboration avec les personnes chargées de l'exploitation dans les filiales/UT et de l'exploitation des systèmes d'assistance centraux ;
- définir ce qui doit être produit à l'interne et ce qui doit être obtenu comme prestation externe (commande de service), en tenant compte des directives de l'OFROU et de la Confédération ; définir les directives correspondantes en matière d'acquisition ;
- soutenir les filiales et coordonner toutes les activités qui concernent la planification de la migration et la mise en œuvre des directives.

Glossaire

Terme	Définition
AKS-CH	Structure et désignation des équipements d'exploitation et de sécurité
AR	Serveur de gestion section (abréviation de l'allemand « *Abschnittsrechner* »)
Architecture système	Modélisation d'un système décrivant les relations et les propriétés des différents éléments de celui-ci ainsi que leurs fonctions
AS	Commande d'installation (abréviation de l'allemand « *Anlagesteuerung* »)
BGP (iBGP/eBGP)	Un protocole IP de routage à multiple fonctions qui permet la distribution de complexes informations sur la topologie. On distingue entre iBGP et eBGP pour un usage à l'intérieur du réseau ou à l'extérieur vers des tiers. De l'anglais : Border Gateway Protocol
BLZ	Centrale de commande d'exploitation
Commutateur	Appareil qui relie plusieurs ordinateurs ou segments réseau au sein d'un réseau local
Concept SIPD	Le concept de sûreté de l'information et de protection des données est la base de la définition des mesures de sûreté de l'information et de protection des données. Il indique quels sont les risques résiduels liés à l'exploitation du système informatique et à l'organisation. Il décrit le concept d'urgence.
DAB	Radiodiffusion numérique (de l'anglais « *Digital Audio Broadcoasting* »)
DDI	DNS, DHCP et gestion des adresses IP
DHCP	Protocole de communication dans la technique informatique, permettant à un serveur d'attribuer une configuration réseau à des clients et défini dans la norme RFC 2131 et s'est vu attribuer les ports UDP 67 et 68 par l'IANA (« *Internet Assigned Numbers Authority* ») (de l'anglais « *Dynamic Host Configuration Protocol* »).
DMZ	Zone de sécurité située en amont qui permet l'accès de l'extérieur dans des conditions moins rigoureuses que les zones intérieures situées en aval avec des exigences de protection plus élevées (zone démilitarisée).
DNS	Le « système de noms de domaine » (de l'anglais « *Domain Name System* ») est l'un des services les plus importants pour de nombreux réseaux IP. Sa tâche principale est de répondre à des requêtes de résolution de noms. Il fonctionne comme un service de renseignement téléphonique.
Domaine	Le domaine sert à organiser ou à regrouper des éléments. Ses utilisations à l'OFROU sont les suivantes : - espace de noms : espace dans lequel les identités sont univoques, c'est-à-dire que chaque ressource possède sa propre identité ; - domaine de fonctions : regroupement de différentes fonctions ; - domaine métier : regroupement de différents services métier ; - domaine de processus : regroupement de différents processus.
EES	Équipements d'exploitation et de sécurité
ELZ	Centrale d'engagement (de la Police).
GUI	Interface utilisateur graphique (de l'anglais « *Graphical User Interface* »
IP	Protocole Internet
IPAM	Gestion des adresses IP (de l'anglais « *IP Address Management* »)
LDP	Un protocole pour gérer et distribuer sur l'ensemble d'un réseau MPLS les chemins logiques (en anglais : label switched paths). De l'anglais Label Distribution Protocol.
LS	Commande locale (abréviation de l'allemand « *Lokalsteuerung* »)
Monitoring	Surveillance et visualisation des fonctions techniques des installations et des systèmes de commande
MPLS	La « commutation multiprotocole par étiquette » (de l'anglais « *Network Access Control* ») permet une transmission de paquets de données orientée sur les connexions au sein d'un réseau sans connexion, le long d'un chemin préétabli (« étiqueté ») (de l'anglais « *Multiprotocol Label Switching* »).
NAC	Contrôle de l'accès au réseau

Terme	Définition
Niveau de gestion	Niveau de commande du système de gestion
NMS	Système de gestion de réseau (de l'anglais « *Network Management System* »)
NNI	Interface réseau (de l'anglais « *Network-Network Interface* »)
Pare-feu	Système de sécurité qui protège un réseau informatique ou un ordinateur unique des accès non autorisés
QoS	La « qualité de service » (de l'anglais « *Quality of Service* ») décrit la qualité d'un service de communication du point de vue de l'utilisateur, à savoir à quel point la qualité du service correspond aux exigences de ce dernier.
Routeur, routeur réseau	Appareil réseau pouvant diriger des paquets réseau entre plusieurs réseaux d'ordinateurs
RSVP	Plus précisément RSVP-TE (en anglais : Resource Reservation Protocol - Traffic Engineering) sert à l'établissement des chemins (en anglais : path) pour la technologie MPLS qui est à la base du Réseau IP EES.
rVL	Gestion régionale du trafic (abréviation de « *regionale Verkehrslenkung* »)
RZ	Centre de calcul
SAP	Dans le réseau IP EES, les « points d'accès au service » (de l'anglais « *Service Access Point* ») sont en général des ports physiques d'un commutateur ou d'un routeur.
Service	Terme générique qui s'applique tant aux services métier qu'aux services de base. Les services implémentent les logiques d'accès et de traitement, mais ne disposent pas d'une interface utilisateur.
SLA	Accord sur les niveaux de service (de l'anglais « *Service Level Agreement* »)
Système de gestion	Sert aux opérateurs pour la surveillance et la commande des installations.
Système SCADA	Système informatique interconnecté (système de gestion) affecté à la surveillance, à la commande et à l'optimisation d'installations industrielles (de l'anglais « *Supervisory Control and Data Acquisition* »)
Section EES	Section de route nationale géré par un serveur de gestion de section
UeLS	Système de gestion supérieur (abréviation de l'allemand « *übergeordnetes Leitsystem* »)
ULA	Adresse locale unique (de l'anglais « *Unique Local Address* »)
UPIC	Unité de pilotage informatique de la Confédération
UT	Unité territoriale
VM-CH	Gestion du trafic en Suisse (abréviation de l'allemand « *Verkehrsmanagement Schweiz* »)
VMZ-CH	Centrale suisse de gestion du trafic (abréviation de l'allemand « *Verkehrsmanagementzentrale Schweiz* »)
WDM	Utilisation multiple (multiplex) d'une FO par plusieurs longueur d'ondes optiques (engl. Wavelength Division Multiplex)

Bibliographie

Directives et documentations de l'OFROU

[1]	Office fédéral des routes OFROU, « **Structure et désignation des équipements d'exploitation et de sécurité (AKS-CH) »,** *Directive ASTRA 13013,* www.astra.admin.ch
[2]	Office fédéral des routes OFROU, « **Sécurité informatique des systèmes de commande et de gestion des équipements d'exploitation et de sécurité »**, *Directive ASTRA 13030,* www.astra.admin.ch
[3]	Office fédéral des routes OFROU, « **IP-Adressierung für BSA »**, *Documentation 83040*
[4]	Office fédéral des routes OFROU, « **Aufbau und den Betrieb des IPAM/DDI-Tools für BSA** », *Documentation 83041*
[5]	Office fédéral des routes OFROU, « **Aufbau und den Betrieb der Security Zonen für BSA** », *Documentation 83042*
[6]	Office fédéral des routes OFROU, « **Aufbau und den Betrieb des NAC-Tools für BSA** », *Documentation 83043*

Liste des modifications

Édition	Version	Date	Modifications
2017	1.20	15.04.2019	Modifications formelles : le mot « tronçon » a été remplacé par « section » dans la version française.
2017	1.10	15.12.2018	Précisions dans les chapitres 1.2 champ d'application, 2.5 raccordement, 2.6 accès pour la section, 5.2 et 5.3 adressage IP et compléments dans le glossaire. Publication de la version française.
2017	1.00	07.12.2017	Entrée en vigueur de l'édition 2017.