Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2772

(04/2016)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

Réseaux de prochaine génération – Sécurité

Mécanismes applicables aux éléments de réseau avec prise en charge de l'inspection approfondie des paquets

Recommandation UIT-T Y.2772

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999
INTERNET DES OBJETS ET VILLES ET COMMUNAUTÉS INTELLIGENTES	
Considérations générales	Y.4000–Y.4049
Termes et définitions	Y.4050–Y.4099
Exigences et cas d'utilisation	Y.4100–Y.4249
Infrastructure, connectivité et réseaux	Y.4250–Y.4399
Cadres, architectures et protocoles	Y.4400–Y.4549
Services, applications, calcul et traitement des données	Y.4550–Y.4699
Gestion, commande et qualité de fonctionnement	Y.4700–Y.4799
Identification et sécurité	Y.4800–Y.4899
Evaluation et analyse	Y.4900-Y.4999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.2772

Mécanismes applicables aux éléments de réseau avec prise en charge de l'inspection approfondie des paquets

Résumé

La Recommandation UIT-T Y.2772 décrit les mécanismes applicables aux éléments de réseau prenant en charge l'inspection approfondie des paquets (DPI), notamment les aspects liés aux procédures et aux méthodes d'inspection approfondie des paquets (DPI) relatives aux réseaux en mode paquet. Cette Recommandation vise à permettre de mieux comprendre les méthodes liées à l'inspection DPI, les aspects interface, protocole et procédure de cette inspection, ainsi que les aspects processus des produits liés à l'inspection DPI.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.2772	2016-04-29	13	11.1002/1000/12709

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2772

Mécanismes applicables aux éléments de réseau avec prise en charge de l'inspection approfondie des paquets

1 Domaine d'application

La présente Recommandation décrit les mécanismes de mise en oeuvre applicables à l'inspection approfondie des paquets (DPI) dans les réseaux en mode paquet. Elle a essentiellement pour but de décrire les modèles d'application, les protocoles associés, les interfaces, les procédures relatives aux méthodes et les processus liés à l'inspection DPI pouvant être utilisés pour identifier les flux d'information entre les fonctions DPI et les autres fonctions du réseau.

Le domaine d'application de la présente Recommandation est le suivant:

– Définition du mécanisme d'inspection DPI.

– Aperçu des mécanismes d'inspection DPI à l'appui de l'identification des applications.

– Procédures et flux d'information sous l'angle opérationnel.

– Procédures et flux d'information sous l'angle de la gestion, par exemple la gestion des politiques d'inspection DPI.

– Autres procédures et flux d'information pour les interfaces possibles de l'entité fonctionnelle (FE) DPI.

Les éléments suivants n'entrent pas dans le cadre de la présente Recommandation:

– Aspects opérationnels et relatifs à la gestion qui ne concernent pas expressément les entités DPI.

– fonctions de gestion relatives aux éléments de réseau communs, telles qu'elles ont déjà été précisées dans les Recommandations UIT-T des séries M et X.

Les responsables de la mise en oeuvre et les utilisateurs de la présente Recommandation doivent se conformer à l'ensemble des lois, règlements et politiques applicables aux niveaux national et régional. Le mécanisme décrit dans la présente Recommandation pourra ne pas s'appliquer aux correspondances internationales afin d'en assurer le secret et de respecter les dispositions juridiques nationales en matière de souveraineté pour ce qui est des fournisseurs de télécommunication, ainsi que les dispositions de la Constitution et de la Convention de l'UIT.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Y.2111] Recommandation UIT-T Y.2111 (2011), *Fonctions de commande de ressource et d'admission dans les réseaux de prochaine génération*.

[UIT-T Y.2704] Recommandation UIT-T Y.2704 (2010), *Mécanismes et procédures de sécurité applicables aux réseaux de prochaine génération*.

[UIT-T Y.2770] Recommandation UIT-T Y.2770 (2012), *Spécifications relatives au contrôle approfondi des paquets dans les réseaux de prochaine génération*.

[UIT-T Y.2771] Recommandation UIT-T Y.2771 (2014), *Cadre pour l'inspection approfondie des paquets (DPI).*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 inspection approfondie des paquets (DPI, *deep packet inspection*) [UIT-T Y.2770]: analyse, conformément au modèle OSI-BRM [b-ITU-T X.200] à architecture de protocoles en couches:

– des propriétés des données utiles et/ou des paquets (voir la liste des propriétés possibles au paragraphe 3.2.11/[UIT-T Y.2770]) plus approfondies que les informations d'en-tête des couches de protocole 2, 3 ou 4 (L2/L3/L4); et

– d'autres propriétés des paquets,

afin d'identifier l'application sans ambiguïté.

NOTE – Les informations obtenues par la fonction DPI, de même que certaines informations supplémentaires comme des informations sur le flux, sont généralement employées par les fonctions suivantes telles que la communication de données et l'exécution d'actions sur le paquet.

3.1.2 analyseur DPI [UIT-T Y.2771]: entité suivante présente sur le trajet de traitement DPI (à l'intérieur d'une fonction d'application de politique DPI) qui assure essentiellement des fonctions de comparaison entre les en-têtes et les données utiles de paquets particuliers des flux de paquets présélectionnés. L'analyseur DPI vise avant tout à évaluer les *conditions* de politique DPI sur les paquets entrants *présélectionnés*.

NOTE – L'analyseur DPI peut être situé après un scanner DPI (voir le paragraphe 3.2.5 de la Recommandation [UIT-T Y.2771]). Sa fonctionnalité peut être celle d'un analyseur avec système de détection des intrusions (IDS).

3.1.3 moteur DPI [UIT-T Y.2770]: sous-composante et partie centrale de l'entité fonctionnelle DPI qui exécute toutes les fonctions de traitement sur le trajet des paquets (par exemple la fonction d'identification des paquets et d'autres fonctions de traitement des paquets de la Figure 6-1 de la Recommandation [UIT-T Y.2770]).

3.1.4 noeud DPI [UIT-T Y.2771]: élément de réseau ou dispositif qui intègre les fonctions relatives à l'inspection DPI. Il s'agit donc d'un terme générique employé pour désigner la réalisation d'une entité physique DPI.

NOTE – Sur le plan fonctionnel, la fonction de noeud DPI (DPI-NF) comporte la fonction d'application de politique DPI (DPI-PEF) et la fonction de décision de politique locale (L-PDF) (facultative); la fonction DPI-NF est donc équivalente sur le plan fonctionnel à l'entité fonctionnelle DPI.

3.1.5 action de politique DPI (action en abrégé) [UIT-T Y.2771]: définition de ce qu'il faut faire pour appliquer une règle de politique, lorsque les conditions de la règle sont respectées. Les actions de politique peuvent se traduire par l'exécution d'une ou de plusieurs opérations pour modifier et/ou configurer le trafic de réseau et les ressources de réseau, voir également la référence [b-IETF RFC 3198].

3.1.6 condition de politique DPI (également appelée signature DPI) [UIT-T Y.2770]: représentation de l'état et/ou des conditions préalables nécessaires qui identifient une application et définissent si des actions d'une règle de politique doivent être exécutées. L'ensemble des conditions

de politique DPI associées à une règle de politique indique si la règle de politique est applicable (voir aussi la référence [b-IETF RFC 3198]).

Une condition de politique DPI doit contenir des conditions au niveau de l'application et peut contenir d'autres options telles que les conditions concernant l'état et/ou les conditions au niveau du flux:

1) Condition concernant l'état (facultatif):
   a) conditions concernant le niveau de service dans le réseau (par exemple l'encombrement rencontré sur les trajets des paquets); ou
   b) l'état de l'élément de réseau (par exemple la condition locale de surcharge de l'entité DPI-FE).
2) Descripteur de flux ou conditions au niveau du flux (facultatif):
   a) contenu des paquets (champs d'en-tête);
   b) caractéristiques d'un paquet (par exemple le nombre d'étiquettes MPLS);
   c) traitement des paquets (par exemple l'interface de sortie de l'entité DPI-FE).
3) Descripteur d'application ou conditions au niveau de l'application:
   a) contenu des paquets (champs d'en-tête de l'application et données utiles de l'application).

NOTE – La condition se rapporte à la "condition simple" dans les descriptions formelles des conditions au niveau du flux et des conditions au niveau de l'application.

3.1.7 scanner DPI (ou "fonction de balayage DPI") [UIT-T Y.2771]: première entité sur le trajet de traitement DPI (à l'intérieur d'une fonction d'application de politique DPI), qui fournit une présélection (pour l'analyseur DPI, voir le paragraphe 3.2.8 de la Recommandation [UIT-T Y.2771]) en vérifiant *toutes* les *conditions* de politique DPI sur *tous* les paquets entrants.

3.2 Termes définis dans la présente Recommandation

Néant.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

BRAS serveur d'accès distant à large bande (*broadband remote access server*)

CLI interface à ligne de commande (*command line interface*)

CMIP protocole commun d'information de gestion (*common management information protocol*)

DPI inspection approfondie des paquets (*deep packet inspection*)

DPI-PDFE entité fonctionnelle de décision de politique DPI (*DPI policy decision functional entity*)

DPI-PIB base d'informations de politique DPI (*DPI policy information base*)

EMS système de gestion d'éléments (*element management system*)

GUI interface utilisateur graphique (*graphical user interface*)

IP protocole Internet (*Internet protocol*)

IPFIX exportation d'informations de flux IP (*IP flow information export*)

LAN réseau local (*local area network*)

L-PDF fonction PDF locale (*local PDF*)

NMS système de gestion de réseau (*network management system*)

OAM gestion, exploitation et maintenance (*operation, administration and maintenance*)

PDF fonction de décision de politique (*policy decision function*)

PIB base d'informations de politique (*policy* information base)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SR routeur de service (*service router*)

TCAM mémoire ternaire adressable par le contenu (*ternary content addressable memory*)

CP protocole de commande de transmission (*transmission control protocol*)

UDP protocole de datagramme utilisateur (*user datagram protocol*)

VLAN réseau local virtuel (*virtual local area network*)

5 Conventions

Néant.

6 Définition du mécanisme DPI

Dans la présente Recommandation, on considère que le terme "mécanisme" englobe les moyens, les méthodes, les processus et les procédures à mettre en oeuvre pour réaliser une fonction ou répondre à des besoins. Compte tenu de ces considérations, un mécanisme DPI peut être décrit de la manière suivante:

– Processus concret pouvant être utilisé pour mettre en oeuvre les fonctions et fonctionnalités définies dans la Recommandation [UIT-T Y.2771] ainsi que les besoins définis dans la Recommandation [UIT-T Y.2770].

– Procédures détaillées pouvant être adoptée pour mettre en oeuvre les fonctions et fonctionnalités définies dans la Recommandation [UIT-T Y.2771] ainsi que les besoins définis dans la Recommandation [UIT-T Y.2770].

– Méthodes appropriées pouvant être utilisées pour mettre en oeuvre les fonctions et fonctionnalités définies dans la Recommandation [UIT-T Y.2771] ainsi que les besoins définis dans la Recommandation [UIT-T Y.2770].

– Outils ou moyens spécialisés pouvant être utilisés pour mettre en oeuvre les fonctions et fonctionnalités définies dans la Recommandation [UIT-T Y.2771] ainsi que les besoins définis dans la Recommandation [UIT-T Y.2770].

7 Aperçu des mécanismes DPI à l'appui de l'identification de l'application

7.1 Aspects généraux des mécanismes DPI

Les mécanismes DPI comprennent deux aspects principaux:

– mécanismes DPI relatifs au noeud DPI;

– mécanismes DPI correspondant au réseau prenant en charge les fonctions DPI.

Avant de préciser ces deux aspects, il est nécessaire de mettre en place la structure de base du noeud DPI et le réseau type prenant en charge les fonctions DPI.

7.2 Structure de base d'un noeud DPI

La structure de base d'un noeud DPI a été décrite sur la Figure 6-1 de la Recommandation [UIT-T Y.2770] et sur la Figure 7-2 de la Recommandation [UIT-T Y.2771]; la mise en oeuvre d'un noeud DPI peut reposer sur la structure.

7.3 Réseau type prenant en charge les fonctions DPI

Un réseau type déployé avec des noeuds DPI est décrit sur la Figure 7-1, sur laquelle, de haut en bas, les cinq couches logiques sont les suivantes: nuage, couche centrale, couche agrégée, couche d'accès et couche terminal. Il convient de souligner qu'il existe un lien logique entre chaque noeud DPI et le système de gestion d'éléments (EMS) ou le système de gestion de réseau (NMS), encore que toutes les couches logiques ne soient pas illustrées sur la Figure 7-1. Tous les noeuds DPI peuvent coopérer avec les entités du réseau (routeur, commutateur et serveur d'accès distant à large bande (BRAS), etc.) et les noeuds DPI indiqués sur la Figure 7-1 sont indépendants des entités de réseau ci-dessus.

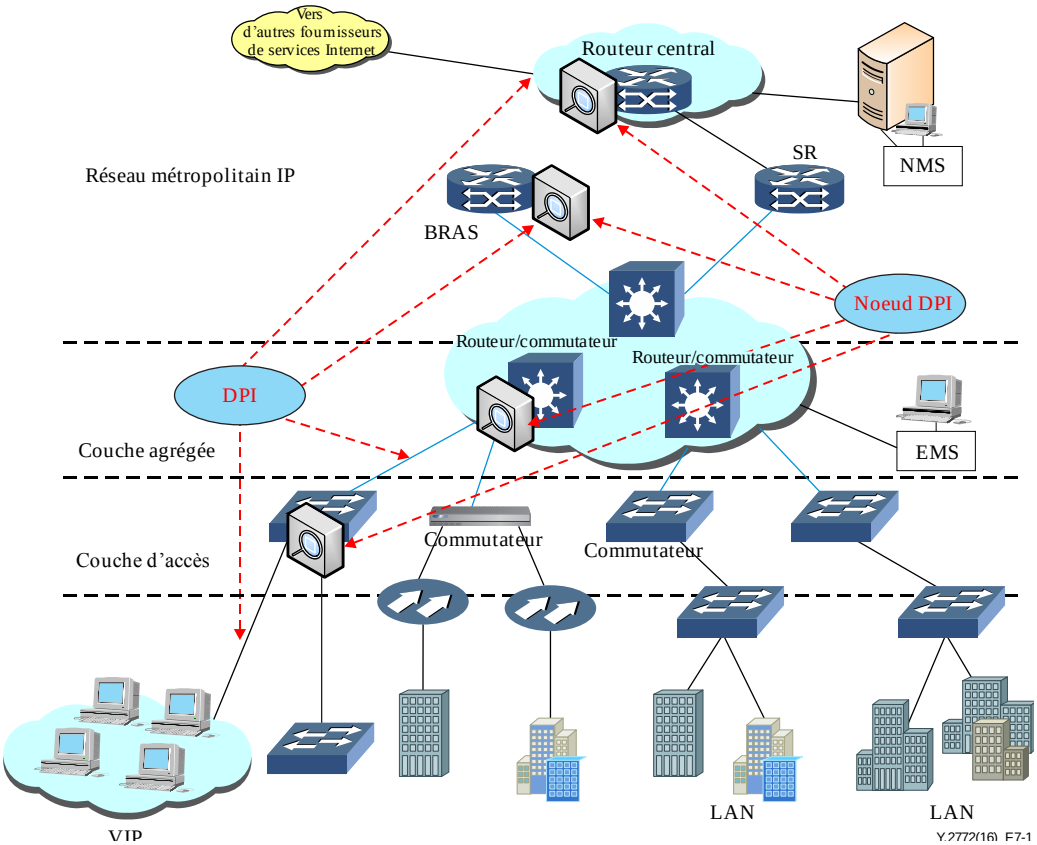

Figure 7-1 – Exemple de topologie de réseau déployée avec des noeuds DPI

Pour obtenir de plus amples renseignements, voir l'exemple de réseau prenant en charge l'inspection DPI décrit sur la Figure 6-3 de la référence [b-ITU-T Y-Sup.25].

7.4 Mécanisme DPI relatif au noeud DPI

Le mécanisme DPI du noeud DPI comprend essentiellement les trois aspects suivants:

1) Méthode de représentation des informations

Dans le cas d'un élément de réseau prenant en charge des fonctions DPI, plusieurs types d'informations et de données doivent être représentés dans l'élément, par exemple, les règles DPI. La méthode de représentation des informations est très importante pour l'élément de réseau, étant donné que différentes méthodes de représentation permettent des gains différents en termes d'efficacité de traitement.

2) Méthodes et procédures de traitement

Les méthodes et procédures de traitement comprennent des méthodes intéressantes pour la mise en oeuvre des fonctions relatives à l'inspection DPI ainsi que les procédures qu'un élément de réseau exécute pour prendre en charge ces fonctions DPI.

3) Interface et protocole approprié

L'interface et le protocole approprié permettent la mise en oeuvre des interfaces qui sont définies dans la Recommandation [UIT-T Y.2770] (par exemple e1, e2) et le protocole approprié qui est utilisé pour l'échange d'informations entre les types d'interfaces ci-dessus.

7.5 Mécanisme d'un réseau déployé avec des noeuds DPI

Les mécanismes correspondant aux réseaux prenant en charge des fonctions DPI comprennent essentiellement les aspects suivants:

– aspects liés à l'exploitation;

– aspects liés à la gestion.

8 Méthodes de représentation de l'inspection DPI – Règle de politique de la base d'informations de politique DPI (DPI-PIB)

8.1 Vue d'ensemble

La condition applicable à la règle de politique DPI de la base d'informations de politique DPI (DPI-PIB) constitue l'une des parties principales d'un noeud DPI et presque toutes les actions du noeud DPI sont fondées sur les conditions de la règle de politique DPI. En conséquence, il est très important que la condition applicable à la règle de politique DPI soit représentée efficacement et soit facile à traiter. Trois méthodes de représentation de la condition applicable à la règle de politique DPI sont décrites: méthode de représentation des données et du gabarit, méthode de représentation d'expression régulière et méthode de représentation hybride.

8.2 Méthode de représentation des données et du gabarit pour les conditions applicables à la règle de politique DPI

La méthode de représentation de l'adresse IP et du gabarit est généralement utilisée dans la pile de protocoles TCP/IP et les dispositifs de réseau connexes; la méthode de représentation des données et du gabarit est analogue à la méthode de représentation de l'adresse IP et du gabarit. Selon la méthode de représentation des données et du gabarit, une chaîne d'octets (données) est utilisée pour représenter le mot étiqueté qui identifie un certain flux de données, et une série de bits (gabarit) correspondant à la chaîne d'octets est utilisée pour décider s'il convient de vérifier ou non un certain bit de la chaîne d'octets. En général, si un bit a la valeur "1", le bit correspondant de la chaîne d'octets n'est pas vérifié. Inversement, si un bit a la valeur "0", le bit correspondant de la chaîne d'octets doit être vérifié.

En ce qui concerne la base DPI-PIB, il convient d'utiliser la méthode de représentation des données et du gabarit, qui présente les avantages suivants:

− Cette méthode est simple et facile à comprendre.

− Elle est très efficace, étant donné qu'un seul élément peut être partagé par un grand nombre de flux de données.

− Elle est bien adaptée aux dispositifs couramment utilisés, tels que les dispositifs à mémoire ternaire adressable par le contenu (TCAM).

Les deux exemples ci-dessous illustrent la méthode de représentation des données et du gabarit:

1) Adaptation des flux de données dont l'accès de source TCP est compris entre 0x2100 et 0x21ff

Dans la base DPI-PIB, seul un élément est nécessaire pour répondre aux besoins:

Elément 1: données: 0x2100, gabarit: 0x00ff

2) Adaptation des flux de données dont le réseau local virtuel (VLAN) se trouve dans l'ensemble 16-63

Dans la base DPI-PIB, deux éléments sont nécessaires pour répondre aux besoins:

Elément 1: données: 0x0010, gabarit: 0x000f

Elément 2: données: 0x0020, gabarit: 0x001f

8.3 Méthode de représentation d'expression régulière pour les conditions applicables à la règle de politique DPI

La méthode de représentation des données et du gabarit convient pour représenter un mot étiqueté avec une position fixe et une valeur déterminée. En général, les en-têtes de protocole de la couche 2 à la couche 4 (L2-L4) sont très bien adaptés à ce type de demande.

Toutefois, les mots étiquetés des applications de couche supérieure sont généralement mal connus et faciles à modifier. Dans ces conditions, l'utilisation de la méthode de représentation des données et du gabarit est difficile à appliquer. Dans ces applications, la méthode de représentation d'expression régulière convient mieux pour ces types de mots étiquetés.

Une expression régulière [b-ITU-T X.680] est une méthode de description connue en informatique; la présentation et l'analyse détaillées des expressions régulières sortent du cadre de la présente Recommandation.

Les deux exemples ci-dessous illustrent la méthode de représentation d'expression régulière:

1) Adaptation du flux de données qui comprend le mot "Bittorrent" ou "Bitcomment"

Dans la base DPI-PIB, un seul élément est nécessaire pour répondre aux besoins:

Elément 1: "/Bit(torrent|comment)/".

2) Adaptation du flux de données qui comprend le mot "Worm", où le mot suivant n'est pas "v1" ou "v2"

Dans la base DPI-PIB, un seul élément est nécessaire pour répondre aux besoins:

Elément 1: "Worm(?<!v1|v2)".

8.4 Méthode de représentation hybride pour les conditions applicables à la règle de politique DPI

Les fonctions DPI peuvent prendre effet sur la couche 2-couche 7. Lorsqu'on examine la couche 2-couche 4, l'utilisation de la méthode de représentation des données et du gabarit s'avère être un choix judicieux pour construire la base DPI-PIB. Par ailleurs, lorsqu'on envisage d'utiliser des mots étiquetés dans la couche 7, le choix de la méthode de représentation d'expression régulière convient mieux pour construire la base DPI-PIB.

En conséquence, il est utile d'associer les deux méthodes de représentation décrites ci-dessus pour un grand nombre d'environnements d'applications; selon cette méthode, appelée méthode de représentation hybride, certains mots étiquetés sont représentés par l'intermédiaire de la méthode de représentation des données et du gabarit, tandis que les autres mots étiquetés sont représentés sur la base de la méthode de représentation d'expression régulière

La méthode de représentation hybride est illustrée dans les exemples suivants:

1) Adaptation du flux de données qui comprend le mot "Bittorrent" ou "Bitcomment" et où le réseau VLAN du flux de données se trouve dans l'ensemble 8-15

Dans la base DPI-PIB, un seul élément est nécessaire pour répondre aux besoins:

Elément 1: première moitié: données: 0x0008, gabarit: 0x0007

deuxième moitié: "/Bit(torrent|comment)/"

Ces deux moitiés peuvent être stockées dans une mémoire différente, mais elles sont connectées logiquement entre elles.

9 Flux d'information, procédures de traitement et méthodes pour une entité DPI

9.1 Vue d'ensemble

Une entité DPI comprend un grand nombre de fonctions nécessaires et la mise en oeuvre de ces fonctions repose sur de nombreux aspects, à savoir:

- mise en oeuvre de certaines interfaces nécessaires (voir le paragraphe 9.2);
- mise au point du flux d'information entre les composantes fonctionnelles (voir le paragraphe 9.3);
- procédures de traitement des principales composantes fonctionnelles (voir le paragraphe 9.4);
- méthodes à appliquer pour renforcer la fiabilité (voir le paragraphe 9.5);
- méthodes à appliquer pour assurer l'échange d'informations et la synchronisation des données avec efficacité (voir le paragraphe 9.6);
- autres méthodes utiles pour la mise en oeuvre de l'entité DPI.

9.2 Mise en oeuvre de l'interface

9.2.1 Vue d'ensemble de l'interface

Plusieurs interfaces sont définies et illustrées dans la Recommandation [UIT-T Y.2770], notamment les interfaces externes e1 et e2 et les interfaces internes i1, i2 et i3. Parmi ces interfaces, les interfaces externes e1 et e2 sont illustrées sur la Figure 8-1 de la Recommandation [UIT-T Y.2770] et les interfaces internes i1, i2 et i3 sont indiquées sur la Figure 8-2 de la Recommandation [UIT-T Y.2770]. Théoriquement, toutes ces interfaces devraient être mises en oeuvre à l'intérieur d'un noeud DPI.

Cependant, d'autres interfaces devraient également être mises en oeuvre en fonction des besoins des applications. Ainsi, dans le contexte de l'inspection DPI bidirectionnelle, l'interface externe spéciale e3 (voir la Figure 11-4) sera peut-être nécessaire à l'intérieur d'un noeud DPI.

9.2.2 Interfaces internes

Les interfaces internes (voir la Figure 8-2 de la Recommandation [UIT-T Y.2770]) servent à échanger des informations entre des composantes fonctionnelles internes à l'intérieur d'un noeud DPI. Il y a trois interfaces internes: i1, i2 et i3. Les mises en oeuvre de ces interfaces internes sont présentées dans les paragraphes qui suivent.

9.2.2.1 Interface i1

L'interface interne i1 est une interface entre la fonction d'identification de paquets et d'autres fonctions de traitement de paquets dans une entité DPI-FE. En général, l'interface i1i est une interface physique réalisée sous forme matérielle en vue de garantir la qualité du traitement d'un noeud DPI. L'Interface i1 peut être mise en oeuvre au moyen de diverses méthodes, notamment la mémoire partagée, les accès de communication parallèle internes et les accès de communication série internes, etc.

9.2.2.2 Interface i2

L'interface interne i2 est une interface entre la fonction d'identification de paquets et la fonction de gestion locale dans une entité DPI-FE. L'interface i2 est une interface physique réalisée sous forme logicielle et il existe plusieurs méthodes permettant de la concevoir.

Si la fonction d'identification de paquets et la fonction de gestion locale sont exécutées, contrôlées ou gérées par une unité CPU identique, alors l'interface i1 peut être mise en oeuvre à l'aide de diverses

méthodes, telles qu'un groupe de fonctions d'interfaces de programmation d'applications (API), la mémoire partagée et la communication entre processus.

Si la fonction d'identification de paquets et la fonction de gestion locale sont exécutées, contrôlées ou gérées par des unités CPU différentes, alors l'interface i1 peut être mise en oeuvre au moyen de méthodes de communication de données. Ainsi, les deux composantes fonctionnelles ci-dessus peuvent échanger des informations par l'intermédiaire des protocoles TCP ou UDP.

9.2.2.3 Interface i3

L'interface interne i3 est une interface entre la bibliothèque de signatures DPI et la fonction de gestion locale dans une entité DPI-FE. L'interface i3 est une interface logique réalisée sous forme logicielle. En général, la bibliothèque de signatures DPI et la fonction de gestion locale sont conçues de façon à pouvoir être contrôlées par une unité CPU identique, tandis que l'interface i3 peut être mise en oeuvre par un groupe de fonctions API.

9.2.3 Interface externe

Les interfaces externes (voir la Figure 8-1 de la Recommandation [UIT-T Y.2770]) sont utilisées pour échanger des informations entre un noeud DPI et d'autres entités fonctionnelles, telles que le système NMS. Il existe également trois interfaces externes: e1, e2 et e3. Les interfaces externes e1 et e2 sont illustrées sur la Figure 8-1 de la Recommandation UIT-T Y.2770], tandis que l'interface externe e3 est illustrée sur la Figure 11-4 de la présente Recommandation. La mise en oeuvre de ces interfaces externes est présentée aux paragraphes 9.2.3.1 à 9.2.3.3.

9.2.3.1 Interface e1

L'interface externe e1 est une interface entre une entité fonctionnelle de décision de politique DPI (DPI-PDFE) et une entité fonctionnelle DPI (DPI-FE). La Recommandation [UIT-T Y.2770] fournit une solution permettant de mettre en oeuvre l'interface: l'interface e1 peut être à titre facultatif un point de référence de l'interface Rw, tel qu'il est défini dans la Recommandation [UIT-T Y.2111]. Bien que le point de référence Rw constitue une solution possible, il n'est ni univoque, ni obligatoire.

Quelle que soit la solution adoptée pour concevoir l'interface e1, il convient de s'assurer que les données transportées par le biais de l'interface puissent être comprises à la fois par l'entité DPI-PDFE et par l'entité DPI-FE, si les entités DPI-PDFE et DPI-FE ne sont pas conçues par le même fournisseur.

9.2.3.2 Interface e2

L'interface externe e2 est une interface entre une entité DPI-FE et une entité de réseau distant autre que l'entité DPI-PDFE (par exemple un système NMS). La Recommandation [UIT-T Y.2770] fournit également une solution permettant de mettre en oeuvre l'interface: il est recommandé d'utiliser l'interface e2 pour utiliser les protocoles d'exportation d'informations de flux IP (IPFIX, voir la référence [b-IETF RFC 5101]). Bien que les protocoles d'exportation IPFIX puissent être utilisés par l'interface e2, les informations échangées entre une entité DPI-FE et des entités de réseau distant autres que l'entité fonctionnelle de décision de politique DPI (DPI-PDFE) sont également possibles avec d'autres solutions.

Quel que soit le type de solution adopté pour concevoir l'interface e2, il convient de s'assurer que les informations transmises par le biais de l'interface puissent être comprises à la fois par l'entité de réseau distant et l'entité DPI-FE, que l'entité de réseau distant et l'entité DPI-FE appartiennent ou non au même fournisseur.

9.2.3.3 Interface e3

L'interface externe e3 est une interface entre deux entités indépendantes DPI-FE lorsqu'il est nécessaire de satisfaire à des prescriptions d'application DPI bidirectionnelle. Les spécifications détaillées de cette interface font l'objet du paragraphe 11.

9.3 Flux d'information

9.3.1 Flux d'information orienté vers le moteur DPI

La Figure 9-1 décrit le flux d'information provenant du moteur DPI. L'échange de données entre le moteur DPI et la fonction de décision de politique locale (L-PDF) s'effectue à l'intérieur de l'entité DPI, tandis que l'échange de données entre la fonction L-PDF et l'entité PD-FE s'effectue en dehors de l'entité DPI.

L'échange de données relatif à l'inspection DPI devrait être très fiable. Par ailleurs, la communication de données à l'intérieur d'une entité DPI est plus fiable que la communication de données entre deux entités indépendantes. En conséquence, il vaut mieux utiliser des approches fondées sur la connexion pour l'échange de données entre deux entités indépendantes, de façon à garantir la fiabilité de cet échange. De plus, l'échange de données à l'intérieur d'une entité DPI peut s'effectuer en mode sans connexion, afin de limiter les ressources du système et d'améliorer l'efficacité de l'échange de données.

Ainsi, sur la Figure 9-1, il est recommandé de concevoir l'échange de données entre le moteur DPI et la fonction L-PDF en mode sans connexion, étant donné que le moteur DPI et la fonction L-PDF se trouvent dans une entité DPI unique. Cependant, il est recommandé de concevoir l'échange de données entre la fonction L-PDF et la fonction PD-EF en mode connexion, étant donné que l'entité PD-FE ne se trouve pas dans une entité DPI unique.

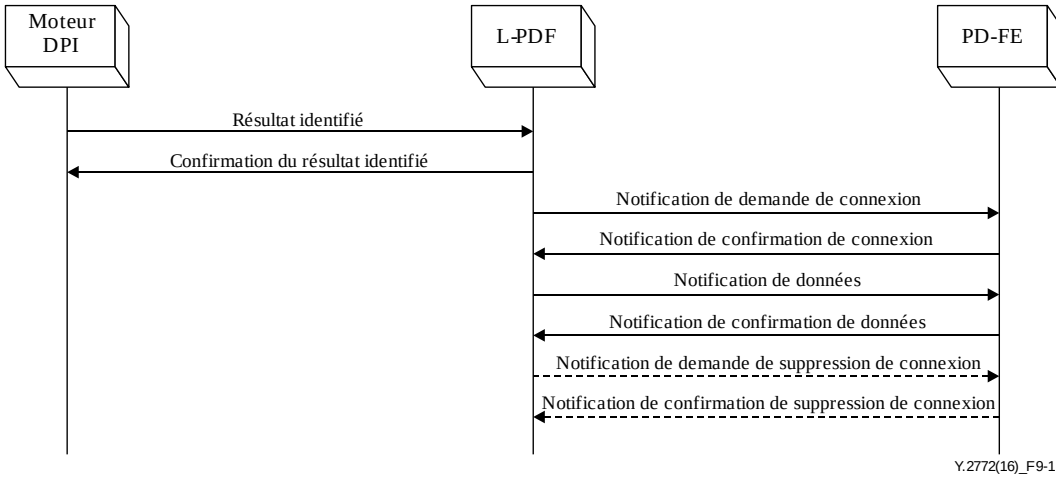

Figure 9-1 – Flux d'information orienté vers le moteur DPI

Sur la Figure 9-1, la primitive "Résultat identifié" est utilisée pour transporter les données générées par un moteur DPI et la primitive "Confirmation de résultat identifié" est utilisée pour informer le moteur DPI que les données ci-dessus ont été reçues. Le couple de primitives "Notification de demande de connexion" et "Notification de confirmation de connexion" est utilisé pour établir une connexion, tandis que le couple de primitives "Notification de données" et "Notification de confirmation de données" est utilisé pour transporter les données notifiées. Une fois terminé l'échange de toutes les données notifiées, le couple de primitives "Notification de demande de suppression de connexion" et "Notification de confirmation de suppression de connexion" est utilisé à titre facultatif pour supprimer la connexion (représenté par la ligne en pointillés sur la Figure 9-1).

9.3.2 Flux d'information orienté vers la base DPI-PIB

La Figure 9-2 décrit le flux d'information reposant sur la base DPI-PIB. L'échange de données entre la base DPI-PIB et la fonction L-PDF s'effectue à l'intérieur de l'entité DPI, tandis que l'échange de données entre la fonction L-PDF et l'entité PD-FE s'effectue en dehors de l'entité DPI.

Sur la Figure 9-2, il est recommandé de concevoir l'échange de données entre la base DPI-PIB et la fonction L-PDF en mode sans connexion et il est recommandé de concevoir l'échange de données entre la fonction L-PDF et la fonction PD-EF en mode connexion.

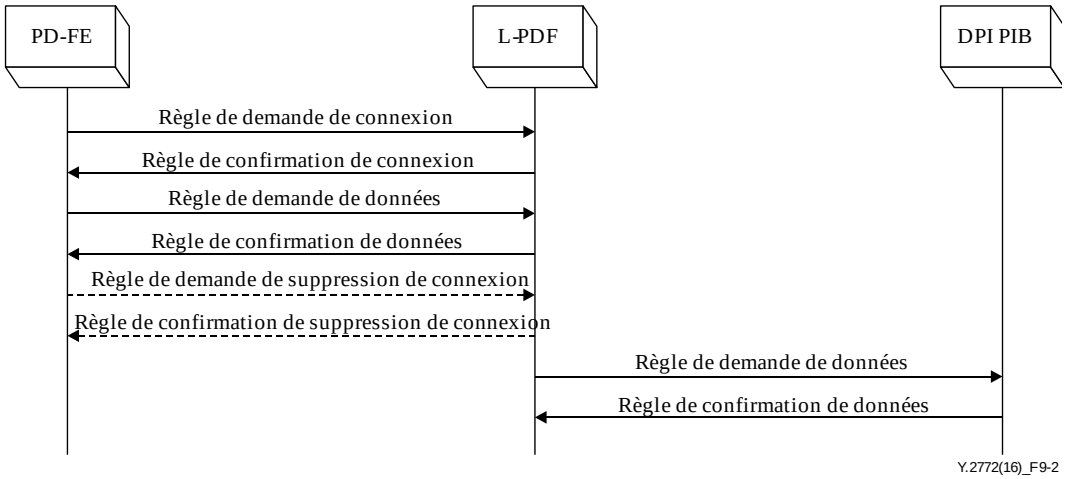

Figure 9-2 – Flux d'information orienté vers la base DPI-PIB

Sur la Figure 9-2, le couple de primitives "Règle de demande de connexion" et "Règle de confirmation de connexion" est utilisé pour établir une connexion, et un autre couple de primitives "Règle de demande de données" et "Règle de confirmation de données" est utilisé pour transporter les données concernant les règles. Une fois terminé l'échange de toutes les données concernant les règles, le couple de primitives "Règle de demande de suppression de connexion" et "Règle de confirmation de suppression de connexion" est utilisé à titre facultatif pour supprimer la connexion (représenté par la ligne en pointillés sur la Figure 9-2).

9.3.3 Flux d'information orienté vers la fonction DPI L-PDF

La Figure 9-3 décrit le flux d'information orienté vers la fonction DPI L-PDF. L'échange de données entre la fonction L-PDF et l'entité PD-FE et l'échange de données entre la fonction L-PDF et l'entité de gestion s'effectuent en dehors de l'entité DPI.

Sur la Figure 9-3, parmi les trois composantes fonctionnelles comprenant l'entité PD-FE, la fonction L-PDF et l'entité de gestion, deux composantes n'appartiennent pas à une entité unique. En conséquence, il est recommandé de concevoir l'échange de données mutuel en mode connexion.

Sur la Figure 9-3, quatre couples de primitives (à savoir "Règle de demande de connexion" et "Règle de confirmation de connexion", "Règle de demande de connexion de synchronisation" et "Règle de confirmation de connexion de synchronisation", "Notification de demande de connexion" et "Notification de confirmation de connexion", et "Configuration de demande de connexion" et "Configuration de confirmation de connexion") sont utilisés pour établir une connexion correspondante. Parallèlement, quatre autres couples de primitives (à savoir: "Notification de demande de données" et "Règle de confirmation de données", "Règle de demande de données" et "Règle de confirmation de données", "Notification de demande de données" et "Notification de confirmation de données", "Configuration de demande de données" et "Configuration de confirmation de données") sont utilisés pour transporter les données correspondantes. En outre, pour chaque type de connexion, une fois achevé l'échange de toutes les données correspondantes, le couple de primitives "… Demande de suppression de connexion" et "… Confirmation de la suppression de la connexion" est utilisé à titre facultatif pour supprimer la connexion. Ces derniers couples de primitives ne sont pas décrits sur la Figure. 9-3 pour éviter toute complication et toute confusion sur la figure, mais présentent des fonctions analogues au couple de primitives "Règle de demande de suppression de connexion " et "Règle de confirmation de suppression de connexion".

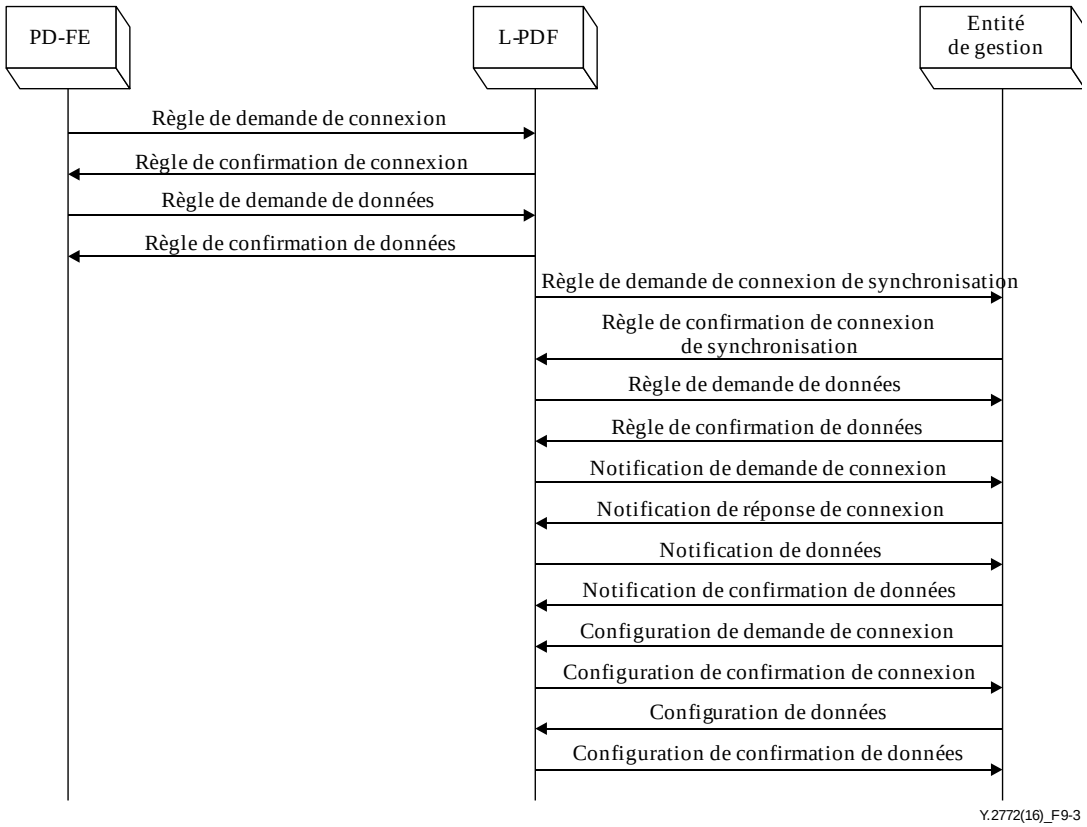

Figure 9-3 – Flux d'information orienté vers la fonction L-PDF

9.4 Procédure applicable au processus

9.4.1 Procédure applicable au processus du moteur DPI

Lorsqu'un paquet entre dans le moteur DPI, celui-ci explore et identifie les paquets en fonction de la règle de politique définie dans la base DPI-PIB. L'analyseur du moteur DPI analyse alors le paquet identifié et enregistre le résultat analysé. Par la suite, l'action de politique sera exécutée en fonction du résultat identifié.

Si le paquet n'est pas identifié, l'action "non identifié" sera exécutée. Si le paquet est identifié, le moteur DPI exécutera l'action correspondante en fonction de la règle de politique définie dans la base DPI-PIB.

Dans l'intervalle, le moteur DPI enregistre le résultat identifié de chaque paquet et place en mémoire cache plusieurs résultats similaires Il transmet périodiquement les résultats à l'entité de gestion La période de notification est propre à la réalisation et n'entre pas dans le cadre de la présente Recommandation.

9.4.2 Procédure applicable au processus de la base DPI-PIB

La base DPI-PIB contient un ensemble d'une ou de plusieurs entrées concernant les règles de politique DPI. La base DPI-PIB reçoit les données concernant les règles de la fonction L-PDF après réception par la fonction L-PDF des données concernant les règles provenant de l'entité PD-FE.

9.4.3 Procédure applicable au processus de la fonction L-PDF

La fonction L-PDF met à jour les entrées concernant les règles pour la base DPI-PIB lorsqu'elle reçoit des données concernant les règles en provenance de la ou des fonctions distantes de décision en matière de politique (PDF(s)). La fonction L-PDF envoie le résultat identifié aux fonctions PDF(s) distantes lorsqu'elle reçoit le résultat identifié provenant du moteur DPI. La fonction L-PDF peut aussi être chargée de la résolution des éventuels problèmes d'interaction entre les règles de l'ensemble des règles de politique DPI.

9.5 Méthode de protection

La Recommandation [UIT-T Y.2771] a défini le groupe de redondance "1+N" pour la réalisation de la tolérance aux dérangements. Il existe deux modèles de protection différents: le modèle "1+1" (N=1) et le modèle "1+N" (N>1). Le modèle "1+1" est utilisé pour une composante active et une composante de secours, tandis que le modèle "1+N" (N>1) est utilisé pour une composante active et N composantes de secours.

9.5.1 Modèle "1+1"

Le modèle "1+1" est également appelé modèle actif/de secours et représente en quelque sorte un modèle de reprise sur défaillance, selon lequel, en cas de défaillance, une composante de secours à l'état "repos" prend le relais de la composante défaillante. Avec ce modèle, la composante de secours utilise un mécanisme de pulsations pour détecter la défaillance de la composante active. Le niveau de disponibilité élevée dépend de la stratégie de reproduction pour l'état de la composante. Dans le cas d'un modèle actif/de secours, il est recommandé d'utiliser la solution de secours immédiat. Une solution de secours immédiat fournit une redondance matérielle ainsi qu'une redondance logicielle. Toutefois, l'état de la composante active est reproduit sur la composante de secours en cas de modification, c'est-à-dire que l'état de la composante de secours est toujours actualisé. En cas de défaillance de la composante active, la composante de secours remplace la composante défaillante et continue de fonctionner sur la base de l'état actuel.

L'état de la composante est copié au moyen de la reproduction active. On utilise un protocole d'engagement pour annoncer les changements d'état à la composante de secours avant que ceux-ci ne soient exécutés au niveau de la composante active. Une fois exécutée, la composante de secours reçoit un second message pour l'engagement du changement d'état. Les changements d'état non engagés sont exécutés par la composante de secours en cas de reprise sur défaillance. Le protocole d'engagement est propre à la réalisation particulière et n'entre pas dans le cadre de la présente Recommandation.

Le modèle actif/de secours immédiat assure une disponibilité permanente sans interruption de service.

9.5.2 Modèle "1+N" (N>1)

Le modèle "1+N" (N>1) est fondé sur plusieurs composantes redondantes, et deux composantes DPI ou plus ((en d'autres termes, un groupe de redondance "1+N" DPI dans lequel les composantes DPI sont les composantes fonctionnelles) sont prévues à l'intérieur d'un noeud DPI, une composante DPI étant la composante active tandis que les autres composantes DPI sont les composantes de secours.

Les procédures applicables au processus de ce mode sont analogues au modèle "1+1". Les composantes de secours utilisent des messages de pulsations pour détecter la défaillance d'une composante active. Lorsque la composante active connaît une défaillance, l'une des composantes de secours prend le relais de la composante défaillante.

9.6 Méthode de synchronisation des données

La synchronisation des données doit être prise en considération en cas de basculement de la protection. Il est recommandé que les composantes fonctionnelles actives et les composantes fonctionnelles de secours conservent des informations totalement identiques (base PIB par exemple) par le biais d'une méthode de synchronisation des données.

9.6.1 Synchronisation des données en mode "1+1"

En cas de défaillance de la composante active (y compris le noeud DPI, le moteur DPI et l'entité DPI-FE), la composante de secours prend en charge le travail de la composante active. La composante de secours doit envoyer la "Règle de demande de synchronisation" à l'entité de gestion. L'entité de gestion enverra les données concernant la règle à la composante de secours.

9.6.2 Synchronisation des données au niveau des composantes en mode "1+N" (N>1)

La synchronisation des données au niveau des composantes en mode "1+N" est analogue au mode "1+1". En cas de défaillance de la composante active (y compris le noeud DPI, le moteur DPI et l'entité DPI-FE), la composante de secours prend en charge le travail de la composante active. La composante de secours doit envoyer la "Règle de demande de synchronisation" à l'entité de gestion. L'entité de gestion enverra les données concernant la règle à la composante de secours.

9.6.3 Synchronisation des données au niveau du noeud en mode "1+N" (N>1)

Le mode"1+N" (N>1) au niveau du noeud est réalisé au moyen du mode de groupe. En mode de groupe, si le noeud maître connaît une défaillance, le noeud de secours prend en charge le travail du noeud maître. Le noeud de secours synchronisera les données concernant règle provenant de l'entité de gestion.

En cas de défaillance du noeud asservi, le trafic acheminé vers le noeud défaillant sera redistribué vers les autres noeuds asservis par des routeurs en amont en fonction de l'algorithme de répartition de charge. Ces noeuds asservis seront activés de manière à synchroniser les nouvelles règles provenant de l'entité de gestion.

10 Spécification du mécanisme opérationnel

10.1 Vue d'ensemble

Le présent paragraphe décrit les aspects opérationnels des technologies d'inspection DPI, et notamment les aspects suivants:

- objectifs des technologies d'inspection DPI adoptées;
- aspect qualité du déploiement du système d'inspection DPI;
- analyse des réseaux actuels sans inspection DPI;
- déploiement d'entités physiques DPI et mise en place des réseaux correspondants;
- gestion, exploitation et maintenance des réseaux DPI correspondants;
- modification et amélioration des réseaux actuels sur la base de la surveillance de la qualité de fonctionnement des réseaux actuels.

Le processus général de construction et d'exploitation d'un réseau doté de noeuds DPI est décrit sur la Figure 10-1. Les fonctions des six étapes décrites sur cette figure sont présentées aux paragraphes 10.3 à 10.8.

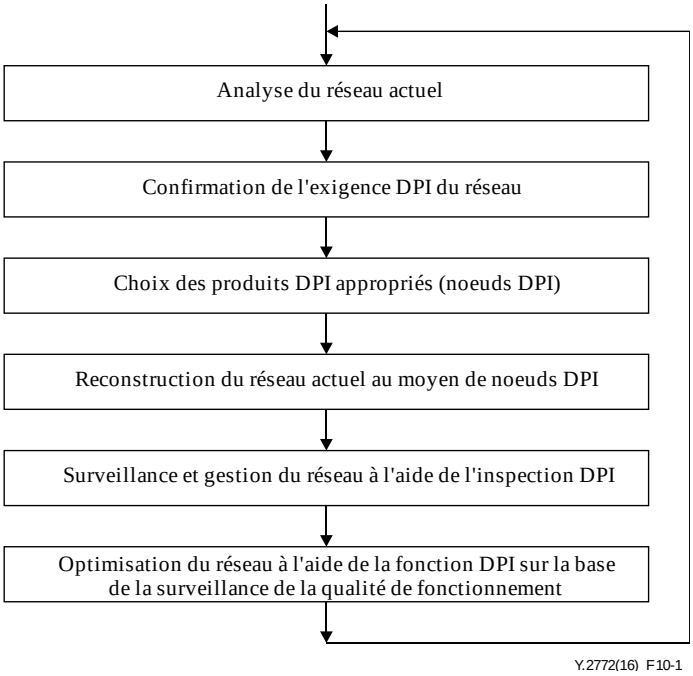

Figure 10-1 – Illustration du processus de construction et d'exploitation d'un réseau avec des noeuds DPI

10.2 Objectifs du mécanisme d'exploitation

10.2.1 Objectif général

Les objectifs généraux de l'utilisation de technologies DPI sont au nombre de trois:

1) surveiller l'état du réseau actuel;
2) donner des instructions aux opérateurs pour la reconstruction et l'optimisation du réseau;
3) améliorer la qualité de fonctionnement du réseau.

10.2.2 Objectifs particuliers

Les objectifs particuliers du mécanisme d'exploitation sont les suivants:

- déployer des noeuds DPI sans influer sur le service en ligne actuel;
- surveiller tous les types de trafic du réseau actif;
- identifier le trafic non valide défini dans les règles de politique;
- analyser l'état du réseau sur la base de la surveillance détaillée de la qualité de fonctionnement du réseau;
- réattribuer les ressources du réseau sur la base de l'analyse de l'état du réseau;
- reconstruire et améliorer le réseau sur la base de l'état du réseau;
- améliorer le niveau de satisfaction des utilisateurs du réseau.

10.3 Aspect qualité de fonctionnement ou déploiement de noeuds DPI

En principe, le déploiement de noeuds DPI ne devrait pas interrompre les services et les applications du réseau actuels. Toutefois, dans la pratique, l'installation d'un noeud DPI dans le réseau peut avoir un certain nombre de conséquences négatives sur les services et applications du réseau. Après l'installation, les effets négatifs résultant du déploiement de noeuds DPI devraient satisfaire certaines exigences particulières.

10.3.1 Spécification du déploiement de noeuds DPI hors du trajet

Lorsqu'un noeud DPI hors du trajet est inséré dans un réseau, la durée d'interruption des services et applications du réseau actuel devrait être inférieure à 50 ms. Théoriquement, le déploiement de noeuds DPI hors du trajet peut être effectué sans interruption des services et applications.

10.3.2 Spécification du déploiement de noeuds DPI sur le trajet

Lorsqu'un noeud DPI sur le trajet est inséré dans un réseau, la durée d'interruption des services et applications du réseau actuel devrait être inférieure à 50 ms. Le recours à des méthodes ou à des instruments auxiliaires permet d'atteindre l'objectif d'une durée d'interruption inférieure à 50 ms Par exemple, on utilisera tout d'abord une liaison redondante avant le déploiement d'un noeud DPI sur le trajet, puis on supprimera la liaison redondante lorsque le noeud DPI sur le trajet pourra fonctionner normalement.

10.4 Analyse des réseaux actuels

Avant de déployer un noeud DPI, il faut obtenir un certain nombre de renseignements sur le réseau actuel, par exemple la largeur de bande maximale de tous les segments du réseau, le trafic moyen actif des segments du réseau, la répartition du trafic sur les segments du réseau en fonction de la date et de l'heure, le degré d'influence lors du déploiement d'un noeud DPI. En général, ces renseignements pourront être obtenus par le système NMS du réseau actuel.

L'analyse de ces renseignements permet d'obtenir le schéma de conception de la construction d'un réseau doté de fonctions DPI.

10.5 Confirmation de l'exigence DPI du réseau

Etablir et confirmer l'exigence du noeud DPI sur la base de l'analyse ci-dessus du réseau actuel.

10.6 Choix des entités ou des systèmes DPI appropriés

Les entités DPI utilisées pour construire le réseau avec des fonctions DPI devraient satisfaire aux prescriptions décrites au paragraphe 10.4.

10.7 Reconstruction du réseau actuel au moyen de l'inspection DPI

Le déploiement de dispositifs DPI ne devrait pas limiter la qualité de fonctionnement du réseau actuel, et ne devrait pas en particulier influer sur le service en ligne Les entités physiques DPI hors du trajet peuvent être mises en place plus facilement que les entités physiques DPI sur le trajet, mais il se peut qu'un fonctionnement incorrect influence le service. En conséquence, il convient de choisir l'heure et l'emplacement appropriés de façon à limiter au maximum les effets décrits ci-dessus et le choix de l'heure et de l'emplacement devrait dépendre du trafic en ligne sur le réseau.

Il convient de souligner qu'un noeud DPI devrait prendre en charge une fonction de contournement interne lorsqu'il est déployé dans le réseau et qu'il fonctionne en tant que noeud DPI sur le trajet. La Figure 10-2 décrit la fonction de contournement interne et la ligne en pointillés représente le contournement. Lorsque les flux de paquets sont acheminés sur le contournement, cela revient à dire que le noeud DPI ne se trouve pas dans le réseau. En d'autres termes, pour les flux de paquets, il semble que le dispositif de réseau précédant le noeud DPI se connecte avec le dispositif de réseau suivant directement le noeud DPI.

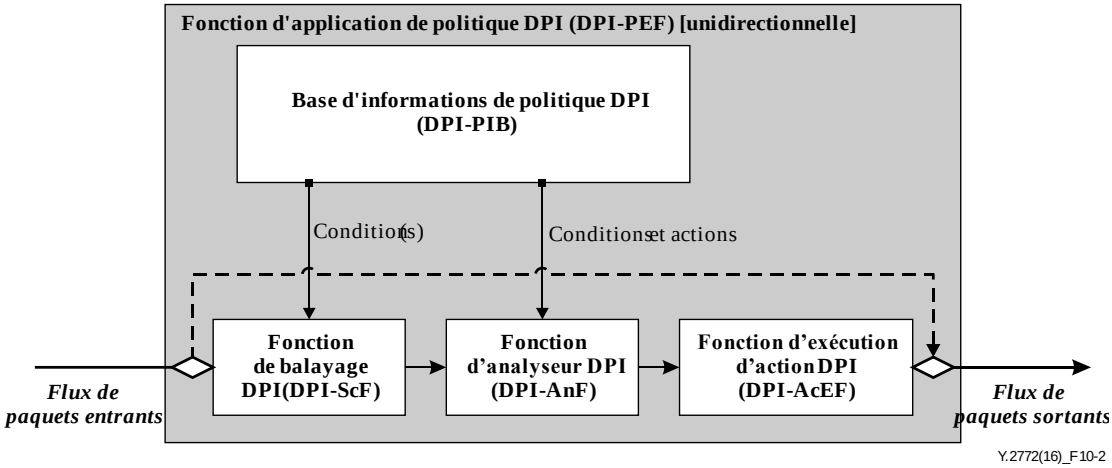

Figure 10-2 – Fonction de contournement interne d'un noeud DPI

10.8 Surveillance et gestion du réseau à l'aide de l'inspection DPI

En général, les réseaux intégrant des fonctions DPI sont plus complexes que les réseaux dépourvus de ces fonctions. En conséquence, un réseau DPI devrait toujours utiliser la gestion, l'exploitation et la maintenance (OAM). Autrement dit, les noeuds DPI et leur base PIB devraient être tenus à jour et gérés.

10.9 Reconstruction du réseau doté de l'inspection DPI sur la base de la surveillance de la qualité de fonctionnement

En général, la construction d'un réseau intégrant des fonctions DPI est un processus adaptatif. La structure du réseau devrait être adaptée progressivement sur la base de l'évolution de l'état de la qualité de fonctionnement du réseau. La surveillance de l'état du réseau dépend d'analyses appropriées des données et des statistiques.

11 Spécification du mécanisme de gestion

11.1 Aperçu de la gestion d'un réseau DPI

Comme tout élément type de réseau, un noeud DPI devrait prendre en charge des fonctions de gestion de la configuration, des dérangements, de la qualité de fonctionnement et de la sécurité. Ces fonctions de gestion ont été définies dans d'autres Recommandations et n'entrent pas dans le cadre de la présente Recommandation. Toutefois, il convient de prendre en considération les facteurs particuliers ci-après pour la gestion des réseaux DPI.

Dans les environnements d'applications DPI bidirectionnelles, les fonctions DPI bidirectionnelles peuvent être réalisées soient par un seul noeud DPI (mode à noeud unique, voir la Figure 11-1), soit par une paire de noeuds DPI (mode double noeud, voir la Figure 11-2). Dans bien des cas, le mode double noeud est plus avantageux que le mode à noeud unique. Ainsi, lorsqu'un type particulier de trafic doit être bloqué, l'utilisation du mode double noeud permet de bloquer plus rapidement ce type particulier de trafic.

Etant donné qu'il se peut que les deux noeuds DPI associés soient déployées de manière physiquement indépendante et que la gestion de ces noeuds DPI doive être unifiée, la gestion sera plus complexe, dans la mesure où dans ces conditions, la gestion du réseau devra être effectuée au niveau du sous-réseau et non pas au niveau des noeuds.

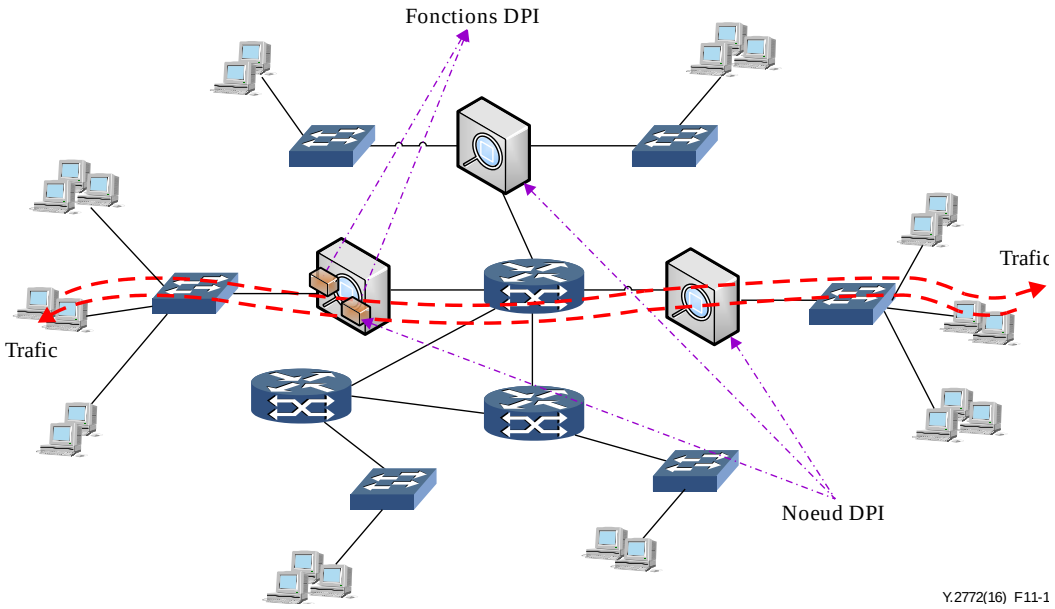

Figure 11-1 – Fonctions DPI bidirectionnelles mises en oeuvre par un noeud DPI unique (mode à noeud unique)

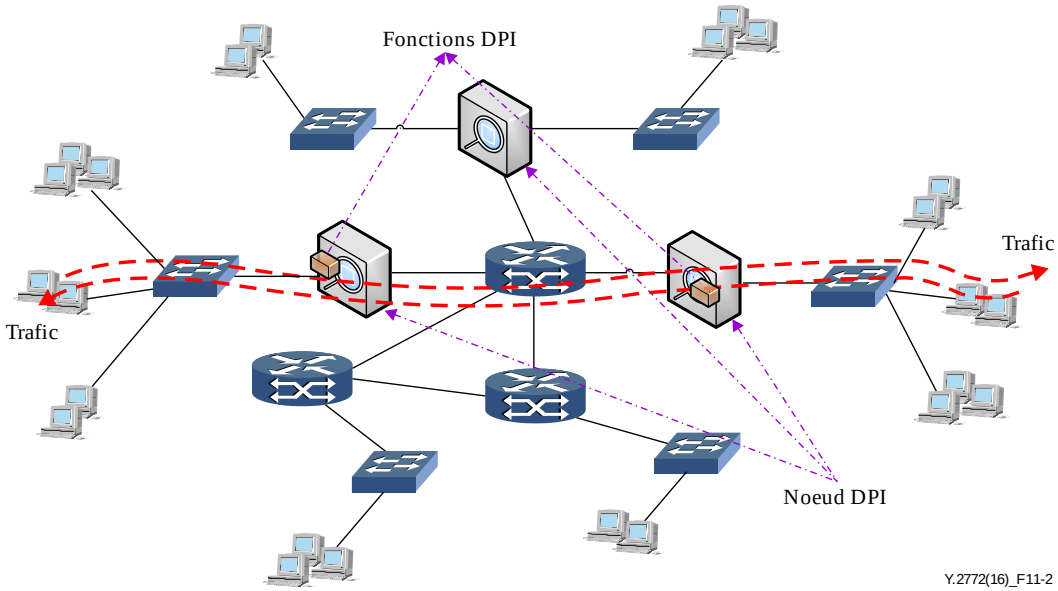

Figure 11-2 – Fonctions DPI bidirectionnelles mises en oeuvre par une paire de noeuds DPI (mode double noeud)

11.2 Interface de gestion

11.2.1 Interface de gestion DPI unidirectionnelle

La gestion générale de l'inspection DPI unidirectionnelle peut être effectuée comme indiqué sur la Figure 11-3, où la connexion entre un noeud DPI et le système de gestion du réseau (NMS) n'est pas une connexion physiquement directe, mais plutôt une connexion logique assurée par l'intermédiaire d'un sous-réseau. Cette liaison entre un noeud DPI et un système NMS est représentée par une ligne en pointillés sur la figure. Logiquement, l'interface de gestion entre le noeud DPI et le système NMS peut être décrite de la façon suivante.

Interface à ligne de commande (CLI): le système NMS gère et contrôle le noeud DPI par l'intermédiaire d'un port série et l'action de gestion prend effet grâce à une série de commandes à ligne unique. Le système NMS ne peut gérer qu'un seul noeud DPI en ligne à la fois.

Interface d'utilisateur graphique (GUI): le système NMS gère et contrôle le noeud DPI par l'intermédiaire d'un port Ethernet ou de l'autre type de port physique et l'action de gestion prend effet par le biais de l'échange d'un groupe de paquets de protocole entre le noeud DPI et le système NMS. Le système NMS peut gérer un ou plusieurs noeuds DPI en ligne en même temps.

Interface Telnet: le système NMS gère et contrôle le noeud DPI par l'intermédiaire d'un port Ethernet ou de l'autre type de port physique et l'action de gestion prend effet grâce à une série de commandes à ligne unique. Le système NMS ne peut gérer qu'un seul noeud DPI en ligne à la fois.

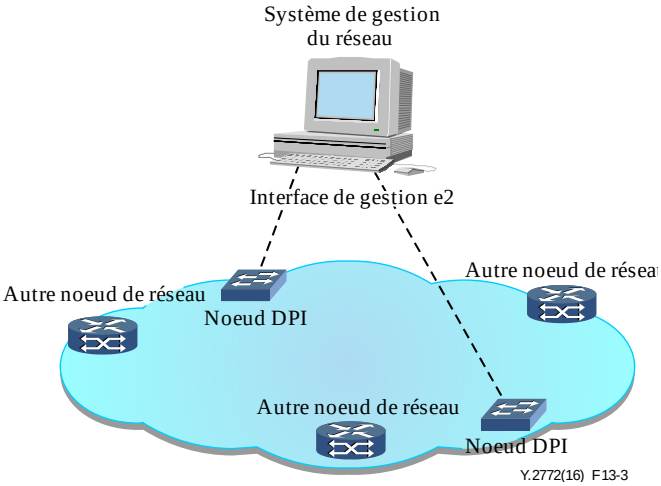

Figure 11-3 – Gestion du réseau avec inspection DPI unidirectionnelle

11.2.2 Interface de gestion DPI bidirectionnelle

La gestion de l'inspection DPI unidirectionnelle peut être effectuée comme indiqué sur la Figure 11-4. Comparé à la gestion DPI unidirectionnelle, la gestion DPI bidirectionnelle (voir les Figures 11-1 et 11-2 ci-dessus) peut-être plus complexe, étant donné que deux ou plusieurs noeuds DPI sont interdépendants. En conséquence, certaines connexions entre deux noeuds DPI devraient manifestement être mises en place. Ces connexions ne sont pas nécessairement des connexions physiquement directes, mais peuvent être des connexions assurées par l'intermédiaire d'un sous réseau ou d'un système NMS. Ces liaisons sont représentées par les lignes en pointillés sur la Figure 11-4. En plus de l'interface de gestion DPI unidirectionnelle, il convient d'utiliser l'interface de gestion suivante lors de la gestion DPI bidirectionnelle:

Interface e3 (voir la Figure 11-2): interface entre deux noeuds DPI correspondants qui est utilisée pour garantir l'unité de l'information des deux noeuds DPI et pour maintenir la connexion logique entre deux noeuds DPI correspondants.

Dans les scénarios d'applications DPI bidirectionnelles, il est plus efficace et économique de réaliser les fonctions DPI bidirectionnelles sur la base de la coopération entre une paire de noeuds DPI avec un noeud DPI responsable de la fonction DPI dans une direction, l'autre noeud DPI étant responsable de la fonction DPI dans la direction opposée. En conséquence, il devrait exister une corrélation entre les bases PIB dans les deux noeuds DPI; les modifications de la base PIB dans un noeud DPI devraient entraîner une modification associée de la base PIB dans un autre noeud DPI.

Par exemple, si des fonctions DPI bidirectionnelles sur le trafic entre les dispositifs de réseau A et B doivent être mises en oeuvre, la règle de contrôle des politiques par rapport à un flux de A vers B devrait être mise en place dans un noeud DPI, tandis que la règle de contrôle des politiques par rapport à un flux de données de B vers A devrait être configurée dans un autre noeud DPI. Il convient de noter que le système de gestion du réseau doit uniquement informer les noeuds DPI qu'ils doivent réaliser la fonction DPI bidirectionnelle sur le trafic entre A et B. La configuration de la base PIB dans les deux noeuds DPI devrait être effectuée automatiquement par les noeuds DPI, de sorte que l'échange d'informations entre les noeuds DPI est nécessaire et est effectuée par l'intermédiaire de l'interface e3.

En outre, afin d'échanger des informations entre les noeuds DPI, il convient d'utiliser un protocole pour rendre les noeuds DPI connectifs et les paquets de données de protocole sont également communiqués via l'interface e3.

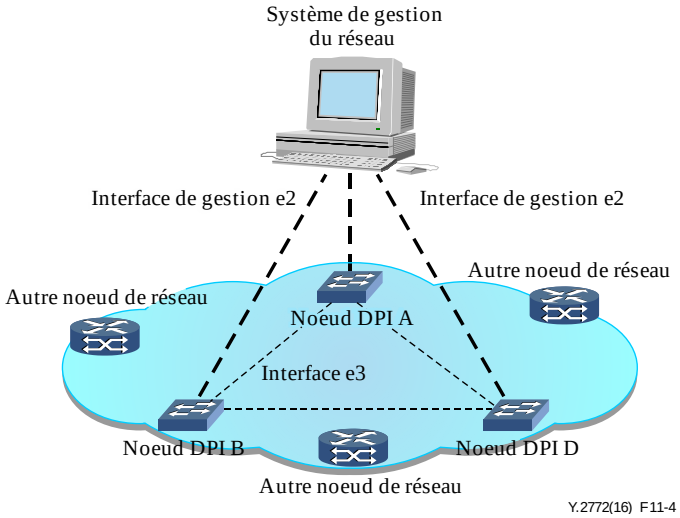

Figure 11-4 – Gestion du réseau avec inspection DPI bidirectionnelle

11.3 Protocole et fonctions de gestion

Le protocole de gestion entre le système MMS et le noeud DPI ou le sous-réseau DPI peut être un protocole de gestion de réseau simple (SNMP), un protocole d'information de gestion commun (CMIP) ou tout autre protocole de gestion.

Les fonctions de gestion comprennent la gestion traditionnelle de configuration, des alarmes et de la qualité de fonctionnement. En outre, la fonction de tenue à jour de la base PIB du sous-réseau DPI bidirectionnel devrait être adoptée dans le système NMS.

12 Considérations relatives à la sécurité

Les aspects liés à la réglementation, à la confidentialité et à la sécurité des applications DPI n'entrent pas dans le cadre de la présente Recommandation. Les fournisseurs, les opérateurs et les prestataires de services doivent tenir compte de la réglementation et des politiques nationales lorsqu'ils appliquent la présente Recommandation.

Conformément à la Recommandation [UIT-Y.2770], l'entité DPI-FE et les informations concernant les opérations DPI devraient être protégées contre les menaces. Les mécanismes indiqués dans la Recommandation [UIT-T Y.2704] répondent aux exigences de sécurité énoncées dans la Recommandation [UIT-T Y.2770].

Bibliographie

[b-ITU-T X.200] Recommandation UIT-T X.200 (07/1994), *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: modèle de référence de base*.

[b-ITU-T X.680] Recommandation UIT-T X.680 (08/2015), *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): spécification de la notation de base*.

[b-ITU-T Y-Sup.25] Recommandations de la série UIT-T Y.2770 – Supplément 25 (2015), *Supplément sur les cas d'utilisation et les scénarios d'application de l'inspection DPI*.

[b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.

[b-IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération, Internet des objets et villes intelligentes**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2016