√ Certifié conforme à l'original

BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 15 du 19 avril 2018

PARTIE PERMANENTE
Administration Centrale

Texte 1

DIRECTIVE N° 36/DEF/DGSIC

relative au marquage des flux IP pour la qualité de service sur les réseaux IP au sein du ministère de la défense.

Du *3 juillet 2015*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 36/DEF/DGSIC relative au marquage des flux IP pour la qualité de service sur les réseaux IP au sein du ministère de la défense.

Du 3 juillet 2015

NOR D E F E 1 5 5 2 6 4 8 X

Pièce(s) Jointe(s) :

Deux annexes.

Classement dans l'édition méthodique : BOEM 160.5.2.5.7

Référence de publication : BOC n° 15 du 19 avril 2018, texte 1.

---

1. PRÉSENSATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Objet du document.**

Cette directive définit les règles applicables pour la différenciation des flux IP au sein du ministère de la Défense, plus communément appelée marquage des flux IP pour la qualité de service (QoS) des flux réseaux IP. Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

1.2. **Niveaux de préconisation.**

Les règles présentées dans ce document ont différents niveaux de préconisation et sont conformes au [RGI] et à la [*RFC* 2119] :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Gestion du document.**

Ce document est maintenu et mis à jour par le sous-comité architecture et services du comité directeur des intranets. Les modifications sont soumises pour approbation au directeur général des systèmes d'information et de communication.

Ce document est disponible sur le [Site Synoptic] entretenu par la DGSIC.

1.4. **Modalités d'application.**

La présente directive s'applique à l'ensemble des intranets utilisés par le ministère de la Défense. Elle concerne les aspects techniques et organisationnels relatifs aux équipements matériels de réseaux, périphériques et ordinateurs, aux logiciels, aux éléments de sécurité, et aux applications.

Ces règles définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure concernant les réseaux IP du ministère de la défense.

Les armées, directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics.

1.5. **Gestion des dérogations pour les projets.**

Les éventuelles dérogations sont présentées et justifiées par un expert de haut niveau ou un directeur de projet au sous-comité architecture et services (SC2) qui statue sur la demande.

La commission ministérielle technique des systèmes d'information et de communication (CMTSIC) peut également être saisie en dernier ressort. Ces dérogations font l'objet d'une approbation par le directeur général des systèmes d'information et de communication. Elles concernent :

- les circonstances et justifications du non respect d'une règle recommandée ;

- les circonstances et justifications du non respect d'une règle déconseillée ;

- les justifications des exceptions à toute règle absolue (obligatoire ou interdit). Dans ce dernier cas, une instruction préalable des services de la DGSIC est nécessaire.

2. CADRE DOCUMENTAIRE.

2.1. **Documents abrogés.**

(QOS) Directive CTSIC portant sur la répartition des flux IP pour une offre de services différenciés, n° 149028 SPOTI/ST/DTR, version 2.2 (13 Décembre 2004) (1) repris en intégralité dans le guide interne DGA S-CAT n° 16003, 1ère édition (19 Décembre 2006). Toute référence à (QOS) dans la suite de cette directive renvoie indifféremment aux deux documents.

La présente directive est une évolution de la directive CTSIC de 2004 [(QOS)] qu'elle annule et remplace ; elle détaille en annexe II. cette évolution et effectue des recommandations pour rejoindre le nouveau cadre.

2.2. **Documents applicables.**

(ARCHI) Directive n° 20/DEF/DGSIC du 24 aout 2011 portant sur l'architecture des réseaux Internet Protocol.

2.3. **Normes et standards applicables.**

[RGI] Référentiel général d'interopérabilité, version 1.0, publié au Journal officiel [12 Juin 2009].

[RFC 2119] *Key words for use in RFCs to Indicate Requirement Levels*, S. Bradner [Mars 1997].

[RFC 2474] *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, K. Nichols, S. Blake, F. Baker, D. Black [Décembre 1998].

[RFC 2597] *Assured Forwarding PHB Group*, J. Heinanen, F. Baker, W. Weiss, J. Wroclawski [Juin 1999].

[RFC 3246] *An Expedited Forwarding PHB (Per-Hop Behavior),* B. Davie, A. Charny, J. Bennet, K. Benson, J. Le Boudec, W. Courtney, S. Davari, V. Firoiu, D. Stiliadis [Mars 2002].

[RFC 4594] *Configuration Guidelines for DiffServ Service Classes*, F. Baker, J. Barbiarz, K. Chan [Août 2006].

2.4. **Autres documents et sites de références.**

[Site Synoptic] Site intranet des systèmes d'information et de communication du ministère de la défense (http://synoptic.intradef.gouv.fr/).

[ARR20] Compte-rendu de la 20e réunion de l'autorité de régulation pour l'emploi des réseaux IP de la Défense, N° D-13-007736/DEF/EMA/CPI/PSIOC/NP du 25 Juin 2013 (1).

3. DOMAINE COUVERT ET EMPLOI.

3.1. **Services attendus.**

3.1.1. ***Contexte.***

Le protocole IP est devenu le protocole universel pour acheminer tout type de données (texte, image, voix) dans le domaine civil comme dans le monde de Défense. Contrairement aux protocoles fonctionnant en mode connecté (X.25, RNIS, ATM, Frame Relay), tous les paquets sont routés indépendamment et peuvent prendre des chemins différents pour arriver à destination. De plus, tous les paquets IP, quelles que soient leur origine, les données transportées ou leur taille, partagent le même support physique.

Initialement le protocole IP n'a pas été conçu pour prendre en compte la qualité de service. Le seul modèle proposé à l'origine est le modèle best effort. Dans ce modèle, tous les paquets sont traités de la même manière et la saturation des files d'attente des routeurs (congestion) entraîne un rejet des paquets arrivants. Ces paquets perdus peuvent être récupérés par les mécanismes de retransmission présents au niveau du protocole de transport TCP. D'autres mécanismes TCP permettent d'assurer un contrôle de flux pour prévenir ces phénomènes de congestion. Dans le cas d'un protocole de transport non fiable comme UDP, soit les données sont perdues, soit la retransmission est prise en compte au niveau applicatif.

Un tel modèle n'est pas compatible avec toutes les applications. Des flux temps réel peuvent accepter un peu de perte mais ne supportent pas la variation de délai (gigue) introduite par les files d'attente. D'autres applicatifs nécessitent de faire parvenir l'information sans perte avec un délai garanti. La différenciation des services, en regroupant les flux aux caractéristiques techniques proches dans une même classe de trafic, permet d'assurer un traitement adapté aux besoins hétérogènes des flux applicatifs.

Une forme de différenciation de services avait été définie, dès le début, dans IPv4 avec le champ ToS mais cette différenciation sur le champ ToS n'a jamais été suffisamment standardisée pour être déployée à grande échelle. L'IETF a défini une autre architecture de différenciation de services appelée DiffServ.

Le modèle DiffServ utilise une différenciation par classes de service basée sur le champ DSCP de l'en-tête IP. C'est ce modèle qui sert de base à la mise en place d'une répartition des flux IP dans les réseaux de la Défense.

Même si le marquage est de type DiffServ, il ne préjuge pas de l'utilisation dans le réseau de mécanismes que l'opérateur jugera nécessaire de mettre en œuvre : DiffServ, réservation de ressources, MPLS, etc.

3.1.2. ***Objectifs.***

Cette directive traite de la différenciation des flux IP au sein du ministère de la Défense. Les flux IP, qu'ils soient issus d'applicatifs ou générés par le réseau (plans de contrôle et de gestion), sont regroupés, suivant leurs caractéristiques techniques et opérationnelles, en classes de trafic. Chaque classe de trafic est identifiée par une valeur d'un champ de l'en-tête IP, positionné au plus proche de la source et transporté de bout en bout. Ce champ est ensuite exploité par les équipements réseau pour déterminer le traitement approprié à la nature des flux (services différenciés).

La standardisation des valeurs de ce champ est destinée à améliorer l'interopérabilité des systèmes en évitant d'avoir recours à des stratégies de marquages hétérogènes.

Depuis 2004, les principaux réseaux ont progressivement mis en œuvre en leur sein un traitement différencié des flux IP sur la base de la directive CTSIC de décembre 2004 ([QOS]). Pour permettre d'obtenir une qualité de service de bout en bout et optimiser l'exploitation d'une bande passante toujours plus contrainte, les futures versions des systèmes d'information doivent également intégrer ce mécanisme et marquer les paquets IP.

3.1.3. ***Périmètre et limites.***

La qualité de service permet d'offrir aux applications un traitement approprié à la nature technique et opérationnelle des flux qu'elles génèrent.

Pour mettre en place un service de QoS, plusieurs fonctions sont nécessaires :

- une répartition des flux en classes de trafic ;

- des contrats de service (SLA) passés entre opérateurs et entre opérateurs et clients ;

- des mécanismes réseau utilisés pour traiter les flux en fonction de leur appartenance à une classe de trafic ;

- des mécanismes permettant de contrôler la conformité des flux aux contrats de service.

La qualité de service dans les réseaux de la Défense ne sera pleinement opérationnelle que lorsque l'ensemble de ces fonctions sera en place.

Cette directive fixe une répartition des flux en classes de trafic et recommande des mécanismes à mettre en œuvre dans le réseau pour implémenter la qualité de service.

Cette directive affecte à chaque classe de trafic une ou plusieurs valeurs du champ DSCP. Le vocabulaire utilisé est celui défini dans le modèle *DiffServ*. Les valeurs spécifiées sont conformes aux classes définies dans *DiffServ*.

3.2. **Principes et définitions.**

3.2.1. ***Classes de trafic.***

Les différents flux IP transitant sur les réseaux de la Défense (qu'ils soient applicatifs ou générés par le réseau) peuvent être caractérisés en fonction :

- de leur tolérance aux pertes, au délai et à la gigue ;

- de leur caractère élastique ou inélastique ;

- de la taille des paquets émis ;

- du rythme d'émission (débit fixe ou variable, en rafale) ;

- de leur capacité d'adaptation éventuelle aux conditions de trafic.

Ainsi des regroupements de flux peuvent être effectués au sein de « classes de trafic » sur la base de caractéristiques similaires. Le tableau suivant illustre ces regroupements. Il est inspiré de [RFC 4594].

CLASSE DE TRAFIC.	CARACTERISTIQUES PRINCIPALES.	TOLERANCE.		
		AUX PERTES.	AUX DELAIS.	A LA GIGUE.
Services Réseau.	a) Paquets IP de taille variable b) Flux inélastique c) Surtout des messages courts d) Émission pouvant être en rafale	Faible	Faible	Oui
Signalisation.	a) Paquets de taille variable b) Émission en rafale et à courte durée de vie	Faible	Faible	Oui
Voix.	a) Petits paquets de taille fixe b) Débit relativement constant c) Flux inélastique d) Débit faible	Très faible	Très faible	Très faible
Vidéo interactive.	a) Paquets de taille variable b) Intervalle de temps constant entre les émissions c) Adaptation automatique du débit d) Réaction automatique aux pertes de paquets	Faible à moyenne	Très faible	Faible
Données temps contraint.	a) Protocole de transport temps-réel (RTP/UDP) b) Débit variable c) Flux inélastique	Faible	Très faible	Faible
Diffusion Vidéo bufferisée.	a) Paquets IP de taille variable b) Débit variable c) Flux élastique	Faible à moyenne	Moyenne	Oui
Diffusion Vidéo *Live.*	a) Débit variable ou constant b) Flux inélastique c) Absence d'émission en rafale des paquets	Très faible	Moyenne	Faible
Semi-interactif.	a) Débit variable b) Émission en rafale et à courte durée de vie de paquets c) Flux élastique	Faible	Faible à moyenne	Oui
Gestion.	a) Paquets IP de taille variable b) Flux élastique et inélastique	Faible	Moyenne	Oui
Transferts volumineux.	a) Débit variable b) Émission en rafale et à longue durée de vie de paquets c) Flux élastique	Faible	Moyenne à forte	Oui
Standard.		Indifférente	Indifférente	Indifférente

Cette classification ou coloration va permettre d'appliquer un traitement adapté à chaque type de flux en cas de congestion du réseau.

Le marquage de la classe de trafic utilise les 3 bits de poids fort du champ DSCP (la longueur totale du champ est de 6 bits), les bits suivants permettant de différencier les niveaux de priorité opérationnelle des flux. La valeur xxx000 est un cas particulier permettant de définir huit classes de trafic supplémentaires : CS0 (Best Effort) à CS7.

3.2.2. ***Caractérisation liée à la priorité opérationnelle des flux.***

Les classes de trafic telles que définies précédemment n'ont pas vocation à définir entre elles de priorité opérationnelle au niveau réseau : les contrats de service (SLA) et mécanismes réseau permettent par ailleurs d'assurer à chacune des classes de trafic une bande passante et des performances négociées.

Au sein d'une même classe de trafic, le niveau de priorité opérationnelle réseau peut permettre en cas de congestion d'éliminer les paquets des flux de plus basse priorité ; les flux de plus haute priorité opérationnelle réseau bénéficient alors d'une disponibilité plus importante. Le niveau de priorité opérationnelle réseau est porté par le champ DSCP, tout comme l'appartenance à une classe de trafic. Le marquage DSCP des paquets IP d'un flux correspondant à un couple « classe de trafic » / « priorité opérationnelle » est précisé dans le chapitre suivant.

L'affectation d'un niveau de priorité opérationnelle réseau à un flux est indépendante du choix de la classe de trafic (dans la limite où cette classe de trafic permet de différencier des priorités opérationnelles).

Les niveaux de priorité opérationnelle définis sont P1 (priorité haute), P2 (priorité moyenne) et P3 (priorité basse). Deux autres niveaux (P1+, P3+) sont également mentionnés dans ce document mais réservés à une utilisation future.

3.2.3. ***Classe de service.***

C'est une vision opérateur de la QoS. Un opérateur peut en effet décider de grouper des classes de trafic dans une même classe de service.

La notion de classe de service est propre à un réseau et définit les traitements appliqués à un ensemble de classes de trafic regroupées au sein de cette classe de service. Le nombre de classes de services défini pour un réseau dépend des caractéristiques de ce réseau et notamment des contraintes de débits.

4. LES RÈGLES.

4.1. **Règles techniques.**

4.1.1. ***Marquage des flux.***

Le champ DSCP présent dans l'en-tête des paquets IP permet de spécifier l'appartenance d'un flux à une classe de trafic. Le niveau de qualité du service qui sera offert à ce flux est fonction de cette valeur.

RT 01. Il est obligatoire que le champ DSCP soit exploité à tous les niveaux :

- systèmes applicatifs (client, serveurs, proxies, etc.) ;

- équipements réseaux (routeurs, sondes d'optimisation, etc.) ;

- équipements de sécurité (chiffreurs, firewalls, etc.) ;

car il représente l'unique moyen de véhiculer de bout en bout l'information sur le niveau de qualité de service requis.

Précision. Cela concerne les flux issus d'applicatifs (flux utilisateurs) ou générés dans le réseau par les différents systèmes (flux de contrôle et de gestion).

RT 02. Il est déconseillé d'implémenter de manière statique la liste des valeurs du champ DSCP dans chacun de ces systèmes.

Précision. Une configuration statique ne permettrait pas de s'adapter à d'éventuels changements (évolution de la politique de marquage, adaptation de la priorité opérationnelle sur décision de commandement etc.).

RT 03. Il est obligatoire que les flux utilisés dans les réseaux de la Défense soient marqués en fonction de leur classe de trafic d'appartenance et leur priorité opérationnelle selon les valeurs définies dans le tableau suivant.

Précision. En cas de non-respect de ce marquage, la qualité de service perçue par les utilisateurs risquerait d'être fortement dégradée.

CLASSE DE TRAFIC.	EXEMPLES DE FLUX.	NOM ET DSCP GÉNÉRIQUE.	PRIORITÉ OPÉRATIONNELLE DU FLUX (P1=Haute, P2=Moyenne, P3=Basse).	MARQUAGE DSCP FLUX.	VALEUR DSCP FLUX (BINAIRE).	VALEUR DSCP FLUX (DÉCIMAL).
	Réservé	CS7 (1)	sans objet	CS7	111000	56
Services Réseau.	Protocoles de routage (OSPF, BGP, etc) Signalisation réseau (RSVP-TE, IKE…) Alarmes (SNMP, …) Messages d'erreur ICMP	CS6	sans objet	CS6	110000	48
Voix.	VoIP (et signalisation associée)	EFx (2) (101xxx)	P1+ P1 P2 P3+ P3	EF1+* EF1* EF2* EF3+* EF	101001 101010 101100 101101 101110	41 42 44 45 46
Signalisation.	Signalisation : SIP, H.323, MEGACO, etc	CS5 (2)	sans objet	CS5	101000	40
Vidéo interactive.	Visioconférence (et signalisation associée)	AF4x (2) (100xxx)	P1+ P1 P2 P3+ P3	AF41+* AF41 AF42 AF43+* AF43	100001 100010 100100 100101 100110	33 34 36 37 38
Données temps contraint.	Liaisons de données tactiques, commande de drônes, …	CS4	sans objet	CS4	100000	32
Diffusion Vidéo (Live ou Bufferisée) (3).	Streaming audio ou vidéo Diffusion TV Évènement audio ou vidéo live Vidéosurveillance Vidéo drônes	AF3x (011xxx)	P1+ P1 P2 P3+ P3	AF31+* AF31 AF32 AF33+* AF33	011001 011010 011100 011101 011110	25 26 28 29 30
	Réservé	CS3	sans objet	CS3	011000	24
Semi-interactif.	Navigation, Transactionnel, Clientserveur Messages courts (SIP, IM…) Chat, présence Services	AF2x (010xxx)	P1+ P1 P2 P3+ P3	AF21+* AF21 AF22 AF23+* AF23	010001 010010 010100 010101 010110	17 18 20 21 22

	communs (DNS (4) , NTP, DHCP,...)					
Gestion.	Flux de gestion (sauf alarmes) : SNMP, Syslog, COPS, etc Administration à distance (SSH, RDP, VNC…) AAA (Radius, …) Interrogation annuaires (LDAP,…) Ping (5) pour gestion réseau	CS2	sans objet	CS2	010000	16
Transfert volumineux.	Transfert fichiers, Messagerie, réplications (annuaires, DNS, antivirus…)	AF1x (001xxx)	P1+ P1 P2 P3+ P3	AF11+* AF11 AF12 AF13+* AF13	001001 001010 001100 001101 001110	9 10 12 13 14
	Réservé	CS1	sans objet	CS1	001000	8
Standard (*Best Effort*).	Autres flux	BE	sans objet	BE	000000	0

* Nouvelle dénomination introduite par cette version de la directive Les valeurs DSCP grisées sont réservées pour une utilisation future.

5 niveaux de priorité opérationnelle sont désormais proposés pour chacune des classes AFx/EFx. Par souci de cohérence avec le marquage et la dénomination de la précédente directive [QOS] les valeurs initiales (P1, P2, P3) gardent leur signification. Les nouveaux niveaux sont appelés P1+ et P3+.

Un nouveau marquage est proposé pour la classe de trafic Voix disposant désormais de 2 valeurs utilisables de champ DSCP EF1/EF. Il permettra d'offrir un routage différent, fonction de la priorité opérationnelle des flux, dans le cas de réseaux utilisant la valeur du champ DSCP pour l'aiguillage des paquets. Les traitements effectués dans le réseau (mécanismes de file d'attente,…) seront identiques.

(1) L'utilisation de la classe de trafic CS7 n'est pas préconisée. Cependant elle pourrait être utilisée pour le marquage de certains flux critiques non diffusés à l'extérieur du réseau. Dans le cas de fluxayant été marqués en CS7 conformément à la directive de 2004 ([QOS]) et devant transiter sur différents réseaux, l'opérateur en charge de transmettre les paquets au réseau de transit suivant devra remarquer ces paquets en CS6.

(2) Il est recommandé de marquer la signalisation VoIP/visioconférence de la même manière que les flux data associés (EFx ou AF4x) afin de s'assurer que l'ensemble de ces flux suivra le même chemin dans le réseau. Une attention particulière devra toutefois être portée sur le dimensionnement réseau lors de l'utilisation de ces marquages. En effet, des mécanismes spécifiques liés aux contraintes temps réel de ces flux sont généralement mis en oeuvre dans les réseaux. Par exemple pour un opérateur civil, un dimensionnement précis en nombre de canaux à réserver peut être exigé, ayant un impact direct sur la facturation ; tout trafic excédant ce débit contractualisé sera éliminé.

(3) Les classes de trafic « Diffusion Vidéo Bufferisée » et « Diffusion Vidéo Live », bien qu'ayant des caractéristiques différentes, ont été regroupées en une même classe « Diffusion Vidéo » afin de ne pas multiplier le nombre de classes de trafic et de rester cohérent avec le filtrage des champs DSCP par les chiffreurs gouvernementaux actuels. Il n'est pas exclu d'activer, dans une future version de la directive, la classe CS3 pour traiter de la vidéo live. Cette modification sera liée aux besoins exprimés dans l'avenir sur ce type de flux.

(4) Le service DNS est utilisé dans l'accès et le fonctionnement des applications mais également au sein du réseau lui-même. Une forte disponibilité du service est donc nécessaire, il convient de lui attribuer la valeur de marquage AF22.

(5) Il s'agit des *ping* utilisés par les administrateurs réseau pour tester l'activité des équipements. Les *ping* envoyés par les utilisateurs pour tester un applicatif doivent utiliser le même marquage que l'applicatif lui-même ou par défaut le marquage BE.

Les messages RSVP de réservation de ressource utilisent les mêmes classes de trafic que le flux de données qui utilisera la réservation de ressource.

RT 04. Il est recommandéque chaque réseau de transit élémentaire transmette, au réseau de transit voisin, les paquets avec un marquage du champ DSCP non modifié par rapport à sa valeur d'entrée ([ARCHI]).

Précision. Le niveau de priorité opérationnelle doit être conservé en cas de regroupement de classes de trafic en classes de service dans les réseaux de transit Un re-marquage du champ DSCP aurait pour conséquence de modifier la priorité opérationnelle des flux. L'opérateur d'un réseau de transit peut être amené à traiter les paquets IP suivant un marquage du champ DSCP qui lui est propre. Cette opération est envisageable mais ne dispense pas l'opérateur de délivrer les paquets avec le marquage initial.

RT 05. Il est interditd'utiliser les marquages CS6 et CS7 pour des flux utilisateurs ([ARCHI]).

Précision. Des flux utilisateurs CS6 ou CS7 pourraient venir perturber les flux réseau utilisant ces mêmes marquages et ainsi altérer le fonctionnement global du réseau. Dans le cas de flux utilisant déjà ces marquages, conformément à la directive de 2004 ([QOS]), et transitant jusqu'au poste client (DNS, NTP…) il faudra prévoir de les re-marquer conformément à cette nouvelle directive au sein d'un équipement réseau au plus proche de la source.

4.1.2. ***Prise en compte du marquage.***

4.1.2.1. Services applicatifs.

L'application doit indiquer à la couche réseau comment celle-ci doit marquer les paquets IP. L'application sait quels types de flux elle génère, par contre il lui est plus difficile de déterminer de manière automatique la priorité de ces flux.

Plusieurs possibilités s'offrent lors des spécifications et dépassent actuellement le cadre de cette directive :

- fixer le niveau maximum de priorité en fonction de l'identité ou de la fonction de l'utilisateur et laisser une certaine marge de manœuvre à l'utilisateur pour choisir parmi les priorités qui lui sont proposées ;

- imposer le niveau de priorité en fonction de l'utilisateur et de l'applicatif utilisé ou de tout autre information significative (ex : adresse web du serveur distant).

RT 06. Les services applicatifs sont responsables du marquage (champ DSCP) des flux qu'ils génèrent. Il est recommandé qu'ils fournissent aux couches réseaux un champ DSCP complètement renseigné, à savoir la classe de trafic relative au flux considéré mais aussi la priorité opérationnelle de celui-ci.

Précision : les services applicatifs comprennent les applications elles-mêmes mais également les relais applicatifs (i.e. relais de messagerie) et les proxies (i.e. HTTP, SSL). Une application peut générer des flux de nature et de priorité opérationnelle différentes.

RT 07. Il est recommandé que le marquage fourni par les applications soit le même dans les deux sens de transmission.

4.1.2.2. Services de sécurité.

Chiffrement IP.

Les nouvelles architectures réseau IP de la Défense sont basées sur des cœurs de réseau dans lesquels tous les flux utilisateurs sont protégés en confidentialité par des chiffreurs IPsec, qu'ils soient gouvernementaux ou civils [ARCHI].

RT 08. Il est RECOMMANDÉ, pour un équipement de chiffrement IP, de copier à l'identique le champ DSCP issu de l'en-tête initial dans l'en-tête du tunnel IPsec.

Précision. Si pour des raisons de sécurité, le champ DSCP est repositionné à une valeur fixe ou déterminée par un tableau de correspondance, le niveau de service attendu par les utilisateurs pourrait ne pas être rendu.

RT 09. Si l'équipement de chiffrement IP implémente des mécanismes de compteur anti-rejeu par valeur de marquage, il est OBLIGATOIRE d'activer ces mécanismes.

Précision. Ces mécanismes de compteur anti-rejeu par valeur de marquage permettent d'éviter que des paquets retardés en file d'attente soient détruits par le chiffreur destination.

Fonctions de filtrage.

Un certain nombre de dispositifs (*firewall*, chiffreur IP, etc.) peuvent mettre en place des règles de filtrage sur les valeurs du champ DSCP. Ce filtrage doit prendre en compte l'ensemble des valeurs définies dans cette directive. Il doit également pouvoir évoluer en fonction de l'évolution de la directive (cf RT 02).

RT 10. Il est recommandé que les équipements de sécurité (*firewalls*, chiffreurs, etc.) qui filtrent les flux sur la valeur du champ DSCP utilisent une liste configurable pour tenir compte de l'évolution du marquage.

4.1.2.3. Services réseaux.

Dans la mesure où le flux n'a pas été marqué par l'application, il est indispensable que les équipements réseau les plus proches de la source (routeurs, boîtiers QoS spécifiques, etc.) prennent en charge cette fonction.

Ces équipements devront être en mesure :

- de classer les flux en fonction de leurs adresses source et destination, des ports source et destination, du type de protocole et d'associer à chaque classe de trafic son code DSCP.

- de retrouver dans la charge utile des paquets IP les informations qui leur permettraient de déterminer la priorité du flux et donc d'affiner le marquage.

Des règles sont donc à définir pour déterminer quelles sont les informations disponibles dans la charge utile des paquets qui sont susceptibles de jouer sur la priorité des flux. Ces règles sont à définir pour chaque applicatif.

RT 11. Dans le cas où l'application n'est pas en mesure d'effectuer correctement le marquage des flux, il est recommandé qu'il soit effectué par un autre équipement (commutateur, routeur, boîtier spécialisé, etc.) placé en coupure sur le réseau, avant chiffrement par un équipement de chiffrement IP.

Précision. Les flux non marqués ou marqués de manière non conforme à la présente directive (i.e dont la valeur du champ DSCP n'est pas prévue dans le tableau point 4.1.1) seront, par défaut, traités comme des flux standard (*Best effort*).

RT 12. Il est obligatoire que la version du protocole IP (IPv4 ou IPv6) utilisé n'ait pas d'influence sur le marquage du champ DSCP ainsi que sur le traitement des paquets par le réseau.

Précision. Le champ DSCP est un champ commun aux en-têtes IPv4 et IPv6.

RT 13. Il est obligatoire dans le cas de transit par des réseaux maitrisés de la Défense que les équipements IP, chargés d'encapsuler des flux IP dans d'autres flux IP, recopient à l'identique le champ DSCP du paquet encapsulé dans l'en-tête du tunnel.

Précision. Cette recopie du champ DSCP permet au nouveau paquet constitué de bénéficier du même niveau de qualité de service que le paquet d'origine.

4.2. **Règles organisationnelle.**

4.2.1. ***Priorité opérationnelle.***

Les niveaux de priorité opérationnelle (P1+, P1, P2, P3+, P3) étant communs à l'ensemble des flux IP du ministère de la Défense, des règles d'emploi (hors cadre de cette directive) doivent être mises en œuvre afin d'assurer que l'affectation d'un niveau de priorité à un flux corresponde à son besoin opérationnel.

RO 01. Pour les flux de type AF dont la priorité opérationnelle ne peut être finement gérée, il est recommandé d'affecter, par défaut, le niveau de priorité opérationnelle P3.

RO 02. Afin de s'assurer que l'affectation d'un niveau de priorité à un flux soit en adéquation à son besoin opérationnel, il est recommandé de faire valider l'usage d'un niveau supérieur à P3 par une entité de régulation.

Précision. L'autorité de régulation pour l'emploi des réseaux IP de la Défense (ARR) a acté à sa charge l'attribution des priorités opérationnelles aux différents flux de chaque système [ARR20].

4.2.2. ***Relations avec fournissuers de services.***

RO 03. Si des prestations de QoS différenciés sont attendues du fournisseur de services, il est obligatoire que le SLA soit négocié en tenant compte des classes de trafic.

RO 04. Dans le contrat de service négocié avec le fournisseur (SLA), il est recommandé de demander explicitement de ne pas re-marquer les flux, c'est-à-dire que les paquets restitués devront être identiques aux paquets injectés (i.e. sans altération du champ DSCP).

Précision. Lors de l'utilisation, en transit, d'un fournisseur de services IP extérieur à la Défense, le marquage doit être effectué par les réseaux de la Défense. Les flux seront donc injectés avec le marquage spécifique Défense. Le fournisseur de service devra prendre en compte le marquage Défense et la nature des flux correspondants. A ce marquage, il devra faire correspondre ses propres classes de services en utilisant les mécanismes réseau à sa disposition : translation des champs DSCP en entrée et en sortie (bijection entre codes DSCP client et fournisseur), encapsulation IP supplémentaire avec marquage DSCP spécifique, utilisation de classes d'équivalence MPLS, etc.

RO 05. Si le fournisseur de service n'est pas en mesure de restituer le paquet sans altération du champ DSCP, il est obligatoire que le ministère de la défense mette en place des mécanismes en amont et en aval de son réseau de transit pour garantir la cohérence et la continuité du marquage.

Pour le ministre de la défense et par délégation :

L'ingénieur général de l'armement hors classe,
directeur général des systèmes d'information et de communication,

Marc LECLERE.

---

(1) n.i. BO.

ANNEXE I.

GLOSSAIRE.

TERMES.	DÉFINITION - COMMENTAIRE.
AF *Assured Forwarding.*	Cf. PHB
BE *Best Effort.*	Cf.PHB
Champ DS *Champ DiffServ.*	Champ présent dans les en-têtes IPv4 et IPv6 défini dans [RFC 2474]. En IPv6, le champ DS redéfinit le champ *Traffic Class*. En IPV4, le champ DS redéfinit le champ ToS. Le champ DS est lui-même divisé en 2 parties : - les 6 premiers bits constituent le champ DSCP ; - les 2 derniers bits sont utilisés pour de la notification de congestion. Ils ne sont pas couverts par ce présent document.
Classes de trafic.	Regroupement de flux ayant des caractéristiques techniques ou opérationnelles semblables
Classes de service.	Classes mise en oeuvre par un opérateur pour offrir un service différencié à ses clients. Chacune des classes de service pouvant regrouper plusieurs classes de trafic du client.
Contrat de service.	Un « accord de service », ou « contrat de service », est un document contractuel établi entre un fournisseur et un client ou entre 2 fournisseurs, répondant à l'obligation d'information sur le niveau de qualité des services offerts/attendus. Le contrat de service est un outil de travail essentiel ; il spécifie notamment des informations sur la nature des flux échangés, leur volume et la priorité relative des flux. Il fait également apparaître les mentions suivantes : - le délai de mise en service ; - le niveau de qualité minimum garanti pour chacune des caractéristiques techniques essentielles définies dans l'offre, telles que le débit, la capacité ou toute autre caractéristique susceptible d'être mesurée ; - le délai de rétablissement du service lorsque celui-ci est interrompu ; - le nombre maximal de coupure par an et par mois, la durée maximale cumulée des incidents par an et par mois ; - le délai de réponse aux réclamations. Chaque information est fournie de façon précise et quantifiée dans l'unité appropriée. [Références : - périmètre des contrats de services applicables au sein du MINDEF, guide SCAT n° 16009 Ed 01 du 29 juin 2007 (n.i. BO) ; - arrêté du 16 mars 2006 (n.i. BO) relatif aux contrats de services de communications électroniques].
CS *Class Selector.*	Cf. DSCP
CTSIC	Commission Technique des Systèmes d'Information et de communication
DiffServ *Differentiated Services.*	Modèle défini par l'IETF visant à classer et regrouper les flux dans les classes de trafic et à affecter un comportement du réseau pour chacune de ces classes. Dans le modèle DiffServ, il n'y a aucune signalisation.

	L'information de QoS est portée par un champ dans l'en-tête IP, le champ DSCP.
DSCP *Differentiated Services CodePoint.*	Les 6 premiers bits du champ DS. A chaque valeur du DSCP correspondent une classe de trafic et un comportement (PHB) des routeurs vis-à-vis des flux de cette classe. La longueur du champ DSCP permet théoriquement de gérer au maximum 64 classes de trafic. [RFC 2474] prévoit, pour garantir une compatibilité avec les champs *precedence* utilisés auparavant, des *codepoints* appelés CS (*Class Selector*). Les CS sont de la forme xxx000. Le champ *precedence* occupant 3 bits, 8 valeurs (nommées CS0 à CS7) sont possible. La valeur 000000 étant réservée au *Best* effort.
EF Expedited Forwarding.	Cf. PHB
Elastique.	Une application élastique ne traite pas les informations immédiatement. Les informations reçues sont bufferisées, ce qui permet d'accepter une certaine variation de délai et d'éviter les pertes. Une telle application privilégie la bonne réception de toutes les données plutôt que l'utilisation immédiate de ces données. Exemples d'applications élastiques : transfert de fichier, messagerie, …
IETF Internet Engineering Task Force.	Organisme chargé de la standardisation de l'Internet.
Inélastique.	Ces applications nécessitent de disposer d'une faible variation de délai. Les informations reçues sont utilisées immédiatement après leur réception même si toutes les données n'ont pas été reçues. Parmi ces applications, certaines peuvent être en mesure de s'autoadapter aux conditions de trafic. Ce type d'applications nécessite généralement d'être associé à des mécanismes de contrôle d'admission. Exemples d'applications inélastiques : téléphonie, diffusion TV en direct, vidéo surveillance,
IPv4 Internet Protocol version 4.	Version actuelle du protocole IP.
IPv6 *Internet Protocol* version 6.	Version suivante du protocole IP, en cours de déploiement.
MPLS *Multi Protocol Label Switching.*	Protocole destiné à mettre en place de l'ingénierie de trafic dans un réseau afin d'apporter de la qualité de service tout en utilisant la bande passante de manière optimale. MPLS permet également de mettre en oeuvre des solutions de réseaux privés virtuels en cloisonnant les flux.
Noyau Dur.	Ensemble de capacités maîtrisées pour garantir, dans un contexte de menaces et à un moment donné, la liberté d'action et l'autonomie de décision du CEMA afin de commander et conduire les forces et garantir la posture nucléaire (1) doivent s'exercer au profit de trois grandes chaînes : nucléaire, renseignement et opération (comprenant entre autre l'OTIAD et les moyens de la PPS). Les abonnés « acteurs » de ces chaînes sont définis comme abonnés « noyau dur », les flux correspondant à ces chaînes sont définis comme flux « noyau dur ». L'identification des abonnés et flux « noyau dur » est du ressort de l'Etat Major des armées.
OTIAD.	Organisation Territoriale Interarmées de Défense
PHB *Per Hop Behavior.*	Comportement appliqué à un flux lors de la traversée d'un routeur. En plus du comportement initial Best effort du protocole IP (pour lequel le réseau fait de son mieux pour acheminer les paquets mais n'assure aucun traitement particulier), DiffServ introduit 2 PHB : - EF (*Expedited Forwarding*, [RFC 3246]) caractérise un PHB adapté au trafic à forte contrainte temporelle ; - AF (*Assured Forwarding*, [RFC 2597]) caractérise un PHB adapté au trafic sensible à la perte de paquet. Le taux de perte est fonction du niveau de priorité dans la classe.
PPS.	Posture Permanente de Sûreté
QoS *Quality of*	Service fourni par le réseau et destiné à appliquer aux flux utilisateurs des traitements appropriés à leur

Service /Qualité de Service.	nature technique et opérationnelle.
RFC *Request for comments.*	Documents techniques de référence de la communauté Internet.
SLA *Service Level Agreement.*	Cf contrat de service.
ToS *Type of Service.*	Champ de l'en-tête IP destiné à indiquer le niveau de priorité du paquet (3 bits) et à donner des préférences en termes de routage. Ce champ est peu utilisé ou de manière propriétaire. Il a été redéfini et est aujourd'hui généralement remplacé par le champ DS.
VoIP *Voice over IP.*	Voix sur IP.
VPN *Virtual Private Network.*	Réseau privé virtuel.

(1) Source : Rapport du groupe de travail « Identification d'un noyau dur des SIOC » de l'EMA.

ANNEXE II.

DIFFÉRENCES PAR RAPPORT A LA DIRECTIVE CTSIC DE 20014.

Le tableau suivant présente les différences de marquage DSCP entre la directive CTSIC de 2004 ([QOS]) et la présente directive.

TYPE DE FLUX.	MARQUAGE DSCP DIRECTIVE 2004.	NOUVEAU MARQUAGE.
Flux de services réseau vitaux.	CS7	CS6 (1)
Flux marqués EFx.	1 niveau de priorité opérationnelle	5 niveaux de priorité opérationnelle possibles (dont 3 réservés pour une future utilisation)
Flux marqués AFx.	3 niveaux de priorité opérationnelle	5 niveaux de priorité opérationnelle possibles (dont 2 réservés pour une future utilisation)
Flux de services communs (DNS, NTP, DHCP, etc.).	CS6	AF2x
Flux signalisation VoIP/visioconférence.	CS5	Marquage DSCP identique au flux data associé (EFx ou AF4x), CS5 sinon.

(1) La directive de 2004 ([QOS]) mentionnait les flux SSH pour l'administration à distance des équipements dans la classe de trafic « Services réseau vitaux » CS7. Ce type de flux est en réalité à rapprocher en termes de caractéristiques de la classe de trafic « Gestion » dont le marquage DSCP doit être CS2.