|  |  |
| --- | --- |
| **Assemblée mondiale de normalisation des télécommunications (AMNT-20)Genève, 1er-9 mars 2022** |  |
|  |  |
|  |  |
| SÉANCE PLÉNIÈRE | Document 10-F |
|  | Janvier 2022 |
|  | Original: anglais |
|  |
| Commission d'études 11 de l'UIT-T |
| Exigences de signalisation, protocoles, spécifications de test et lutte contre la contrefaçon des produits |
| rapport de la CE 11 de l'UIT‑T à l'assemblée mondiale de normalisation des télécommunications (AMNT‑20),partie iI: QUESTIONS DONT L'ÉTUDE EST PROPOSÉE AU COURS DE LA PROCHAINE PÉRIODE D'ÉTUDES (2022-2024) |

|  |  |
| --- | --- |
| **Résumé:** | La présente contribution contient le texte des Questions proposées par la Commission d'études 11 pour la prochaine période d'études qui sont soumises à l'Assemblée pour approbation. |
| **Contact:** | M. Andrey KUCHERYAVYPrésident de la CE 11 de l'UIT-TFédération de Russie | Tél.: 79213140320Courriel: akouch@mail.ru |

**Note du TSB:**

Le rapport de la Commission d'études 11 à l'AMNT‑20 est présenté dans les documents suivants:

Partie I: **Document 9** – Considérations générales

Partie II: **Document 10** – Questions qu'il est proposé d'étudier pendant la période d'études 2022‑2024

# 1 Liste des 14 Questions proposées par la Commission d'études 11

|  |  |  |
| --- | --- | --- |
| Numéro de la Question | Titre de la Question | Statut |
| A/11 | Architectures pour la signalisation et les protocoles destinées aux réseaux de télécommunication et lignes directrices pour les mises en œuvre | Suite de la Question 1/11 |
| B/11 | Exigences de signalisation et protocoles pour les services et les applications dans les environnements de télécommunication | Suite de la Question 2/11 |
| C/11 | Exigences de signalisation et protocoles pour les télécommunications d'urgence | Suite de la Question 3/11 |
| D/11 | Protocoles pour la commande, la gestion et l'orchestration des ressources de réseau | Suite de la Question 4/11 |
| E/11 | Exigences de signalisation et protocoles pour les passerelles de réseaux limitrophes dans le contexte de la virtualisation des réseaux et de l'intégration d'intelligence dans les réseaux | Suite de la Question 5/11 |
| F/11 | Protocoles prenant en charge les technologies de commande et de gestion pour les réseaux IMT-2020 et les réseaux ultérieurs | Suite de la Question 6/11 |
| G/11 | Exigences de signalisation et protocoles pour le rattachement au réseau et l'informatique en périphérie pour les réseaux futurs et les réseaux IMT-2020 et ultérieurs | Suite de la Question 7/11 |
| H/11 | Protocoles prenant en charge les réseaux de contenus répartis et les technologies des réseaux centrés sur les informations pour les réseaux futurs et les réseaux IMT-2020 et ultérieurs | Suite de la Question 8/11 |
| I/11 | Tests pour l'Internet des objets, ses applications et systèmes d'identification | Suite de la Question 12/11 |
| J/11 | Paramètres de surveillance pour les protocoles utilisés dans les réseaux émergents, y compris l'informatique en nuage et en périphérie, les réseaux pilotés par logiciel et la virtualisation des fonctions de réseau (SDN/NFV) | Suite de la Question 13/11 |
| K/11 | Tests de l'informatique en nuage, des réseaux pilotés par logiciel (SDN) et de la virtualisation des fonctions de réseau (NFV) | Suite de la Question 14/11 |
| L/11 | Lutte contre la contrefaçon et le vol d'équipements de télécommunication/TIC | Suite de la Question 15/11 |
| M/11 | Spécifications de tests pour les protocoles, les réseaux et les services prenant en charge les technologies émergentes, comportant notamment des évaluations comparatives | Suite de la Question 16/11 |
| N/11 | Lutte contre les logiciels de télécommunication/TIC contrefaits ou ayant subi une altération volontaire | Suite de la Question 17/11 |

# 2 Libellé des Questions

On trouvera dans la suite du présent document le texte proposé pour les Questions.

Question A/11

Architectures pour la signalisation et les protocoles destinées aux réseaux
de télécommunication et lignes directrices pour les mises en œuvre

(Suite de la Question 1/11)

### A.1 Motifs

De nombreux organismes et forums consacrés à la normalisation souhaitent que les réseaux puissent prendre en charge des services et ont élaboré à cette fin un certain nombre d'architectures. Il est notamment nécessaire de disposer d'un modèle d'architecture normalisé prenant en charge la signalisation des commandes dans les domaines de la voix et la vidéo sur réseaux LTE (VoLTE/ViLTE), de la virtualisation de réseau, de l'informatique en nuage, de l'apprentissage automatique (ML) et de l'intelligence artificielle (IA), de la technologie des registres distribués, des réseaux de distribution de clés quantiques (QKDN) et des technologies connexes, et d'autres technologies de télécommunication/TIC émergentes qui pourraient être exploitées dans le contexte des services IMT-2020, des réseaux IMT-2020 et des réseaux ultérieurs.

Un modèle de référence normalisé pour le plan de commande est nécessaire afin de constituer un ensemble d'interfaces permettant d'assurer l'interopérabilité entre les réseaux de télécommunication, entre les équipements de différents fournisseurs, entre les réseaux d'informatique en nuage, entre les réseaux virtualisés et les réseaux physiques, et entre des réseaux évoluant en différentes étapes comme les réseaux IMT-2020 et les réseaux ultérieurs.

Étant donné que l'UIT-T a élaboré les normes applicables aux réseaux publics existants, et en particulier aux services et aux protocoles de commande, il est prévu, au titre de cette Question, de définir les architectures de signalisation et de protocoles destinées aux réseaux de télécommunication exploitant des technologies émergentes telles que l'apprentissage automatique (ML) et l'intelligence artificielle (IA), la technologie des registres distribués, les réseaux de distribution de clés quantiques (QKDN) et les technologies connexes, etc. De plus, cette Question devrait permettre d'étudier les améliorations possibles de l'architecture de signalisation et de commande qui permettraient de prendre en charge le système de signalisation des réseaux ENUM répartis.

Une coopération avec les commissions d'études de l'UIT-T et d'autres organismes de normalisation est nécessaire afin de recueillir toutes les informations pertinentes auprès de ces organismes et de jouer un rôle important de coordination pour assurer l'interopérabilité à l'échelle mondiale.

Par ailleurs, les études menées et les résultats obtenus par divers organismes internationaux de normalisation ont abouti à différentes solutions en matière de convergence et d'interopérabilité en raison de l'évolution des protocoles dans les réseaux à commutation par paquets. C'est pourquoi les États Membres de l'UIT, et en particulier les pays en développement, ont indiqué qu'ils avaient besoin, pour bien comprendre les stratégies et les scénarios de déploiement de réseau et de service, de lignes directrices sur les mises en œuvre des protocoles de signalisation pour les réseaux et les services.

Le groupe chargé de cette Question mettra à jour les rapports techniques et lignes directrices existants sur la mise en œuvre de la signalisation et des protocoles destinés à aider les pays en développement. Il mettra aussi à jour les recommandations en vigueur relevant de cette Question, par exemple les Recommandations UIT-T Q.3030, Q.3040, Q.3050, Q.3051 et Q.3052.

### A.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

− Quelles améliorations faut-il apporter à l'architecture de signalisation et de commande pour modéliser le plan de commande destinés aux réseaux de télécommunication qui prennent en charge des technologies émergentes telles que le ML, l'IA, la technologie des registres distribués, les réseaux QKDN et les technologies connexes, et les technologies employées dans les réseaux IMT-2020 et ultérieurs, compte tenu des nouveaux services et des nouvelles applications ainsi que de tous les types de réseaux publics d'accès filaire et hertzien sur lesquels ces services sont susceptibles d'être fournis?

− Quelles améliorations faut-il apporter à l'architecture de signalisation et de commande pour prendre en charge le système de signalisation des réseaux ENUM répartis?

− Quelles améliorations faut-il apporter à l'architecture de signalisation et de commande pour prendre en charge la voix et la vidéo sur réseaux LTE (VoLTE/ViLTE) et les services IMT-2020, notamment le large bande mobile évolué (eMBB), les communications massives de type machine (mMTC) et les communications ultra‑fiables présentant un faible temps de latence (URLLC), ainsi que d'autres nouveaux services à valeur ajoutée?

− Quelles améliorations faut‑il apporter à l'architecture de signalisation et de commande pour garantir la sécurité de celles-ci et prendre en charge des services ou des applications d'intérêt général tels que le traitement des appels d'urgence, la portabilité des numéros, la confidentialité, etc.?

– Quelles activités sont nécessaires pour que l'UIT‑T et l'UIT‑D élaborent des lignes directrices communes sur différents aspects des stratégies et scénarios de déploiement de réseaux et de services afin de faciliter la mise en œuvre de protocoles de signalisation dans les réseaux et les services?

– Quels mécanismes de coordination sont nécessaires en ce qui concerne l'évolution de la signalisation et des protocoles pour les réseaux de télécommunication émergents en coopération avec les commissions d'études de l'UIT-T et avec d'autres organismes de normalisation?

### A.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

− Déterminer les exigences auxquelles l'architecture des protocoles de signalisation et de commande de réseaux de télécommunication à la fois génériques et indépendants de la technologie d'accès est censée répondre. Ces exigences devront sans doute être redéfinies à intervalles réguliers au fur et à mesure de l'évolution des technologies de télécommunication et de télématique, compte tenu des architectures des protocoles de signalisation et de commande disponibles à l'UIT‑T et dans d'autres organismes de normalisation.

− Recenser les modifications et améliorations à apporter à l'architecture des protocoles de signalisation et de commande pour que celle-ci respecte les exigences de l'architecture des réseaux émergents (notamment les services IMT-2020, les réseaux IMT-2020 et ultérieurs, etc.).

– Étudier l'architecture de signalisation et de commande pour modéliser le plan de commande des réseaux de télécommunication exploitant des technologies émergentes telles que le ML, l'IA, la technologie des registres distribués, les réseaux QKDN et les technologies connexes, et les technologies employées dans les réseaux IMT-2020 et ultérieurs.

– Recenser les améliorations à apporter à l'architecture des protocoles de signalisation et de commande pour prendre en charge le système de signalisation des réseaux ENUM répartis.

– Recenser les améliorations à apporter à l'architecture des protocoles de signalisation et de commande pour prendre en charge les réseaux de télécommunication évoluant vers des réseaux futurs.

− Recenser un ensemble d'interfaces pour lesquelles l'interopérabilité et l'interfonctionnement entre différents équipements de réseau est souhaitable et dont les exigences de signalisation détaillées doivent être étudiées et les protocoles de commande doivent être normalisés.

– Étudier et élaborer des lignes directrices communes sur différents aspects des stratégies et scénarios de déploiement de réseaux et de services pour faciliter la mise en œuvre de protocoles de signalisation dans les réseaux et les services, en particulier pour aider les pays en développement.

− Assurer la communication et la coopération entre les commissions d'études et les forums chargés de l'évolution de la signalisation et des protocoles pour les réseaux émergents.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### A.4 Relations

Recommandations

– Y.2012, Y.3015, Y.3510, Y.3104

Questions

– Toutes les Questions de la CE 11, en particulier celles relatives aux architectures et aux protocoles de signalisation

Commissions d'études

– CE 2: aspects des réseaux ENUM

– CE 13: architecture des réseaux existants et des réseaux émergents

– CE 15: transport

– CE 16: services et codage multimédias

– CE 17: cadre de sécurité

– CE 20: l'Internet des objets et ses applications

– CE 1 et CE 2 de l'UIT‑D

Autres organismes

– ATIS

– Broadband Forum

– CCSA

– ETSI

– IETF

– IEEE

– W3C

Grandes orientations du SMSI

– C2, C11

Objectifs de développement durable

– 9

Question B/11

Exigences de signalisation et protocoles pour les services et les applications dans les environnements de télécommunication

(Suite de la Question 2/11)

### B.1 Motifs

Avec l'augmentation constante du nombre de services et d'applications, la demande de renforcement des capacités des réseaux de télécommunication n'a cessé de croître. En outre, des technologies comme l'informatique en nuage, les mégadonnées, la technologie des registres distribués (DLT), l'apprentissage automatique et l'intelligence artificielle, les réseaux QKDN et les technologies connexes, et d'autres technologies et TIC émergentes vont favoriser l'apparition de nouveaux protocoles de signalisation qui permettront d'interconnecter les réseaux IMT-2020 et les réseaux ultérieurs et d'établir des communications adéquates entre eux. Ces technologies émergentes ainsi que l'évolution des technologies actuelles auront sans aucun doute une incidence sur la normalisation de la signalisation et des protocoles.

L'un des objectifs de l'évolution des réseaux de télécommunication est d'assurer, en toute sécurité, une vaste gamme de services allant de la téléphonie classique et des services intelligents à des services novateurs, comprenant des services de transmission audio, vidéo et de données et des services conversationnels, des services de streaming, des jeux interactifs, des systèmes de banque et de paiement mobiles, des applications de tierces parties, etc.

### B.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels protocoles de signalisation conviennent pour mettre en œuvre différents services et applications dans l'environnement de télécommunication émergent?

– Quels nouveaux protocoles et exigences de signalisation faut-il élaborer pour prendre en charge les services dans les réseaux de télécommunication évoluant vers des réseaux IMT‑2020 et ultérieurs?

– Quels nouveaux protocoles et exigences de signalisation faut-il élaborer pour prendre en charge des services et des applications fondés sur des technologies de télécommunication/TIC émergentes?

– Quels genres de technologies émergentes, par exemple des architectures et des mécanismes reposant sur des réseaux QKDN et les technologies connexes, sont nécessaires pour garantir la sécurité de la signalisation et des commandes, et en particulier du système de signalisation N° 7 (SS7) et des systèmes de signalisation émergents?

– Quels protocoles et exigences de signalisation faut-il élaborer pour prendre en charge les communications et les services de messagerie en temps réel?

– Quels nouveaux protocoles et exigences de signalisation faut-il élaborer pour prendre en charge la gestion des services de télécommunication?

– Quels nouveaux protocoles et exigences de signalisation sont nécessaires pour prendre en charge des services ou des applications d'intérêt général tels que les systèmes de banque et de paiement mobiles, la crypto‑monnaie, les communications d'urgence multimédias, la confidentialité, la portabilité de numéro, etc.?

### B.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Établir les exigences de signalisation et les protocoles nécessaires pour mettre en œuvre différents services et applications dans l'environnement de télécommunication.

– Établir les exigences de signalisation et les protocoles nécessaires pour prendre en charge de futurs services sur les réseaux de télécommunication évoluant vers des réseaux IMT-2020 et ultérieurs.

– Établir les exigences de signalisation et les protocoles nécessaires pour prendre en charge les services et applications fondés sur des technologies émergentes.

– Établir les exigences de signalisation et les protocoles nécessaires pour prendre en charge les communications et les services de messagerie en temps réel.

– Assurer la sécurité des réseaux de signalisation en s'appuyant sur des technologies émergentes, comme par exemple les réseaux QKDN et les technologies connexes.

– Établir les exigences de signalisation et les protocoles nécessaires pour prendre en charge la gestion des services de télécommunication.

− Élaborer des spécifications pour l'interfonctionnement entre les nouveaux protocoles et exigences de signalisation et les protocoles et exigences de signalisation existants.

− Établir les exigences de signalisation et les protocoles destinés à protéger l'intérêt général.

− Améliorer les protocoles de signalisation existants selon les besoins recensés.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### B.4 Relations

Recommandations

– Série Q.600, série Q.700, série Q.900, série Q.1900, série Q.2700, série Q.2900, série Q.3400, série Q.3500 et série Q.3600

Questions

– Toutes les Questions de la Commission d'études 11

Commissions d'études

– CE 2: aspects de gestion du réseau et communications d'urgence

– CE 13: exigences des services, architecture, informatique en nuage et aspects de mobilité

– CE 15: réseaux électriques intelligents

– CE 16: services et applications multimédias

– CE 17: aspects de sécurité

– CE 20: l'Internet des objets et ses applications

Autres organismes

– ARIB

– ATIS

– Broadband Forum

– CCSA

– ETSI

– IETF

– IEEE

– TIA

– TTA

– TTC

Grandes orientations du SMSI

– C2, C5, C11

Objectifs de développement durable

– 9

Question C/11

Exigences de signalisation et protocoles pour les télécommunications d'urgence

(Suite de la Question 3/11)

### C.1 Motifs

Dans l'environnement de réseau émergent, il sera nécessaire d'étudier l'incidence des technologies, capacités et services d'applications qui apparaissent (par exemple les réseaux IMT‑2020 et ultérieurs, la convergence des réseaux de Terre et à satellite, la voix et la vidéo sur LTE (VoLTE/ViLTE), les communications de machine à machine (M2M), l'Internet des objets (IoT), la technologie des registres distribués, l'apprentissage automatique et l'intelligence artificielle, les réseaux QKDN et les technologies connexes) sur les télécommunications d'urgence, et en particulier sur le service de télécommunications d'urgence (ETS). Il faudra également étudier comment certaines nouvelles technologies et certains nouveaux services d'applications peuvent être utilisés à l'appui des télécommunications d'urgence.

Il convient en outre de poursuivre les travaux sur les applications des télécommunications d'urgence, par exemple en améliorant les spécifications et les protocoles de signalisation pour la voix, la vidéo et les données,

Le groupe chargé de la Question est responsable de la mise à jour des capacités ETS existantes dans les Suppléments et Recommandations relevant de la CE 11, par exemple les Recommandations Q.931, Q.761, Q.762, Q.763, Q.764, Q.1902.1, Q.1902.3, Q.1902.4, Q.1950, Q.2630.3 et Q.2931, le Supplément 47 à la série Q, le Supplément 49 à la série Q concernant les informations propres au service ETS, et les Suppléments 53, 57, 61, 62, 63, 68, 69 et 70 à la série Q.

Le groupe chargé de la Question assurera la liaison avec les organismes de normalisation régionaux s'occupant des télécommunications d'urgence ou des capacités nécessaires à leur mise en œuvre, par exemple avec le 3GPP, qui est chargé des communications prioritaires; avec l'IETF, qui définit des solutions techniques pour limiter les encombrements afin de faciliter la mise en œuvre des communications prioritaires pour les utilisateurs des télécommunication d'urgence; ou encore avec l'IEEE, qui travaille sur la série de normes IEEE 802.11 à l'intention des utilisateurs des télécommunications d'urgence.

### C.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quelles améliorations faut-il apporter aux exigences de signalisation et aux protocoles pour prendre en charge les télécommunications d'urgence et les opérations de secours en cas de catastrophe dans les réseaux IMT-2020 et ultérieurs?

– Quels protocoles et exigences de signalisation faut-il définir pour prendre en charge les télécommunications d'urgence et les opérations de secours en cas de catastrophe, compte tenu de la convergence des réseaux de Terre et à satellite?

– Quelles Recommandations faut-il élaborer pour répondre à ces exigences lorsque ces travaux ne relèvent pas d'autres Questions de la Commission d'études?

– Quelles modifications convient-il de proposer aux plans d'ensemble des différentes Commissions d'études directrices afin de prévoir de nouvelles capacités, de mieux mettre en œuvre les capacités déjà normalisées ou de supprimer un contenu obsolète?

### C.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Analyser les capacités de télécommunications d'urgence qui ont été jugées prioritaires par les différentes Commissions d'études directrices afin de déterminer les tâches précises à ajouter aux programmes de travail pour les différentes Questions de la Commission d'études.

– Faire en sorte que les communications nécessaires aient lieu au niveau technique entre les responsables des Questions de la Commission d'études, afin que les travaux qu'ils effectuent pour mettre en œuvre les capacités de télécommunications d'urgence soient efficaces, cohérents et complets.

– Faire en sorte que les communications nécessaires aient lieu au niveau technique entre les responsables des Questions de la Commission d'études, les responsables des Questions d'autres Commissions d'études et d'autres groupes qui élaborent des normes relatives aux télécommunications d'urgence, comme cela est prévu dans les plans des différentes Commissions d'études directrices.

– Revoir les capacités associées au service ETS et aux communications des opérations de secours en cas de catastrophe définies dans les Recommandations relevant du domaine de responsabilité de la Commission d'études pour s'assurer qu'elles restent pertinentes et efficaces.

– Contribuer à l'élaboration et à la tenue à jour des plans qui relèvent de la responsabilité des différentes Commissions d'études directrices pour les télécommunications d'urgence, et proposer de nouveaux contenus lorsque cela semble approprié.

– Élaborer des Suppléments et des Recommandations pour définir des exigences de signalisation et des protocoles relatifs aux télécommunications d'urgence et aux opérations de secours en cas de catastrophe dans les réseaux IMT-2020 et ultérieurs.

– Élaborer des Suppléments et des Recommandations pour définir des exigences de signalisation et des protocoles relatifs aux télécommunications d'urgence et aux opérations de secours en cas de catastrophe, compte tenu de la convergence des réseaux de Terre et à satellite.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### C.4 Relations

Recommandations

– Les travaux à effectuer au titre de cette Question entrent dans le cadre défini par la Recommandation UIT-T Y.1271 et la Recommandation UIT-T Y.2205.

Questions

– Toutes les Questions de la CE 11

Commissions d'études

Les commissions d'études concernées sont les suivantes, en particulier pour ce qui est des Questions se rapportant expressément aux télécommunications d'urgence:

– CE 2 de l'UIT-T

– CE 9 de l'UIT-T

– CE 13 de l'UIT-T

– CE 16 de l'UIT-T

– CE 17 de l'UIT-T

– CE 20 de l'UIT-T

Autres organismes:

– ARIB

– ATIS

– IETF

– IEEE

– ETSI

– TIA

– TTA

– TTC

Grandes orientations du SMSI

– C2, C5

Objectifs de développement durable

– 9, 11, 13, 16

Question D/11

Protocoles pour la commande, la gestion et l'orchestration
des ressources de réseau

(Suite de la Question 4/11)

### D.1 Motifs

Les responsables de l'étude de cette Question ont élaboré un ensemble de Recommandations fondées sur des modèles de données et des exigences de signalisation et des protocoles qui concernaient la commande, la gestion et l'orchestration de ressources de réseaux supports. La normalisation de ces domaines devrait se poursuivre et s'étendre notamment aux réseaux pilotés par logiciel (SDN), à la virtualisation des fonctions de réseau (NFV), aux réseaux d'informatique en nuage, au découpage de réseau, aux réseaux IMT-2020 et ultérieurs, à la virtualisation des réseaux, au passage à l'IPv6 et aux réseaux futurs. Elle devrait s'étendre aussi à de nouveaux domaines d'études de l'UIT-T comme l'intelligence artificielle et l'apprentissage automatique, les réseaux fondés sur les mégadonnées, la technologie des registres distribués, l'informatique en nuage répartie, l'informatique en périphérie à accès multiple (MEC), les réseaux dédiés à la puissance de calcul et d'autres types de réseaux supports prenant en charge des technologies de l'information émergentes.

Le trafic produit par un nombre croissant de nouveaux services, par exemple les services issus des réseaux SDN et de la NFV, des réseaux d'informatique en nuage et d'autres réseaux supports prenant en charge des technologies de l'information émergentes présente un comportement très différent de celui du trafic produit par les services des réseaux de prochaine génération (NGN) classiques. L'architecture de commande de ce nouveau trafic pourrait donc devenir plus complexe. Les exigences de signalisation des réseaux supports sont étroitement liées aux mécanismes et protocoles de commande des ressources de réseau.

Recommandations en vigueur relevant de la Question: Q.1970, Q.1990, Q.2630, Q.2761-2764, Q.2920, Q.2931 et Q.2932.1, Q.3150/Y.1416, Q.3151/Y.1417, Q.3300, Q.3301.1, Q.3302.1, Q.3303.0, Q.3303.1, Q.3303.2, Q.3303.3, Q.3304.1, Q.3304.2, Q.Suppl.51, Q.Suppl.67, Q.3316, Q.3405, Q.3716, Q.3718, Q.3740, Q.3741.

### D.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

− Quels modèles de données et quels protocoles et exigences de signalisation sont nécessaires pour la commande, la gestion et l'orchestration des ressources de réseau faisant intervenir de nouveaux types de protocoles et de réseaux de transport (par exemple les réseaux d'informatique en nuage, les réseaux électriques intelligents, les réseaux futurs, les réseaux SDN et de la NFV, la virtualisation des réseaux, le découpage de réseau, l'informatique en périphérie à accès multiple (MEC) et les réseaux IMT‑2020 et ultérieurs)?

– Quels modèles de données et quels protocoles et exigences de signalisation sont nécessaires pour les réseaux fondés sur les mégadonnées et sur l'intelligence artificielle et l'apprentissage automatique?

– Quels modèles de données et quels protocoles et exigences de signalisation sont nécessaires pour la télémétrie des réseaux?

– Quels modèles de données et quels protocoles et exigences de signalisation sont nécessaires pour les réseaux fondés sur la technologie des registres distribués?

– Quels modèles de données et quels protocoles et exigences de signalisation sont nécessaires pour les réseaux d'informatique en nuage et l'informatique en nuage répartie?

– Quels modèles de données et quels protocoles et spécifications de signalisation sont nécessaires pour les réseaux dédiés à la puissance de calcul?

− Quelles nouvelles Recommandations sont nécessaires pour prendre en charge la commande des réseaux supports et des ressources dans de nouveaux domaines d'application comme les flux d'unidiffusion et de multidiffusion pour le service TVIP, les réseaux domestiques et la mobilité?

− Quelles nouvelles Recommandations sont nécessaires pour assurer la gestion du transfert intercellulaire aux fins de la mobilité?

− Quelles nouvelles Recommandations sont nécessaires pour assurer la sécurité de la commande et la signalisation des réseaux supports et des ressources?

− Quelle nouvelle architecture fonctionnelle et quelles améliorations des protocoles sont nécessaires pour assurer la commande des réseaux supports et des ressources pour les services et applications d'intérêt général, tels que le traitement des appels d'urgence et les secours en cas de catastrophe?

− Quelles nouvelles Recommandations sont nécessaires pour prendre en charge la signalisation des informations de qualité de service (QoS) et la gestion du trafic?

− Quelles améliorations faut-il apporter aux Recommandations existantes pour réaliser directement ou indirectement des économies d'énergie et utiliser efficacement les ressources dans le secteur des technologies de l'information et de la communication (TIC) ou dans d'autres secteurs?

− Quelles améliorations faut-il apporter aux nouvelles Recommandations pour réaliser ces économies d'énergie et utiliser efficacement les ressources?

– Quels sont les nouveaux services pour lesquels la mise en place du protocole IPv6 est une condition préalable nécessaire?

– Quelles nouvelles procédures de protocole sont nécessaires pour mettre en œuvre les nouveaux services précités?

– Quelles nouvelles Recommandations sur le modèle d'informations et le modèle de données sont nécessaires pour pouvoir collaborer avec la communauté "open source" émergente?

### D.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

− Établir des modèles de données ainsi que des exigences de signalisation et des protocoles pour les nouveaux services supports afin de prendre en charge le trafic de nouvelles applications reposant sur les architectures des réseaux futurs (SDN, NFV, virtualisation de réseau, réseaux MEC, découpage de réseau, réseaux d'informatique en nuage et informatique en nuage répartie, réseaux IMT-2020 et ultérieurs, etc.).

– Établir des modèles de données ainsi que des exigences de signalisation et des protocoles pour les réseaux fondés sur les mégadonnées et sur l'intelligence artificielle et l'apprentissage automatique.

– Établir des modèles de données ainsi que des exigences de signalisation et des protocoles pour la télémétrie des réseaux.

– Établir des modèles de données ainsi que des exigences de signalisation et des protocoles pour les réseaux d'informatique en nuage et l'informatique en nuage répartie.

– Établir des modèles de données ainsi que des exigences de signalisation et des protocoles pour les réseaux prenant en charge la technologie des registres distribués, et notamment pour les infrastructures de réseaux fiables décentralisées (DNI).

– Établir des modèles de données ainsi que des exigences de signalisation et des protocoles pour les réseaux dédiés à la puissance de calcul.

− Établir des exigences de signalisation et des protocoles pour la coordination du contrôle d'admission.

− Établir des exigences de signalisation et des protocoles pour la commande de support et de ressources et la gestion du trafic prenant en charge des flux d'unidiffusion/de multidiffusion pour le service de TVIP.

− Établir des exigences de signalisation et des protocoles pour les signaux liés à la qualité de service et la gestion du trafic.

− Établir des exigences de signalisation et des protocoles pour la commande de support et de ressources dans les réseaux domestiques.

− Établir des exigences de signalisation et des protocoles pour prendre en charge le transfert intercellulaire afin d'assurer une mobilité de session transparente.

− Établir des exigences de signalisation et des protocoles pour les interactions entre les domaines de commande de support et de ressources.

− Établir, avec les groupes chargés de Questions ou autres groupes des commissions d'études de l'UIT-T concernés, des spécifications d'interfaces avec les couches adjacentes.

− Améliorer les Recommandations existantes sur la commande de support et de ressources et sur la signalisation.

− Étudier et élaborer des Recommandations en vue de déterminer les spécifications des mécanismes de commande de support et de signalisation qui dépendent du service.

– Recenser les services pour lesquels de nouvelles procédures de protocole sont nécessaires pour le passage à l'IPv6.

– Définir de nouvelles procédures de protocole pour les services recensés ci-dessus.

– Établir des exigences de signalisation et des protocoles fondées sur un modèle d'informations et un modèle de données à mettre en œuvre ultérieurement par des moyens open source.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### D.4 Relations

Recommandations

– H.248, Q.1950, Y.1541, Y.1221, Y.2111, I.555, Q.1970, Q.1990, série Q.263x, série Q.29xx, Y.2121, Y.3300, série Y.35xx, Q.37xx-séries, Q.33xx-séries, Q.34xx‑séries

Questions

– Toutes les Questions de la CE 11

Commissions d'études

– CE 15: transport et technologies du réseau ASON, en particulier architectures des réseaux de transport, et gestion et commande des systèmes et équipements de transport

– CE 16: aspects multimédias

– CE 17: aspects de sécurité

– CE 13: SDN, NFV, réseaux d'informatique en nuage et informatique en nuage répartie, virtualisation de réseau, découpage de réseau, réseaux MEC, réseaux fondés sur les mégadonnées, réseaux fondés sur l'intelligence artificielle et l'apprentissage automatique, réseaux IMT-2020 et ultérieurs

Autres organismes

– 3GPP

– ETSI

– IEEE

– IETF

– TIA

– Linux Foundation Edge

– Linux Foundation Networking (LFN)

– Linux Foundation Hyperledger

– OpenStack

– Open Network Operating System

Grandes orientations du SMSI

– C2, C11

Objectifs de développement durable

– 9

Question E/11

Exigences de signalisation et protocoles pour les passerelles de réseaux limitrophes dans le contexte de la virtualisation des réseaux
et de l'intégration d'intelligence dans les réseaux

(Suite de la Question 5/11)

### E.1 Motifs

Les dispositifs et les fonctions de services destinés aux passerelles de réseaux limitrophes (BNG), qui constituent le fondement des réseaux d'accès utilisateurs et de la fourniture de services, sont en constante mutation grâce à de nouvelles technologies comme les réseaux SDN, la NFV, l'informatique en nuage, l'Internet des objets et l'intelligence artificielle, et surtout grâce au fait que l'architecture de réseau évolue vers la virtualisation, l'ouverture et l'intégration d'intelligence. Dès lors, pour s'adapter à cette évolution architecturale, il convient d'élaborer de nouvelles exigences de service, de nouvelles interfaces et de nouveaux protocoles de signalisation pour les BNG afin de pouvoir prendre en charge les services multiples. Il faut aussi améliorer les capacités des BNG pour garantir la qualité de service, la fiabilité et la sécurité dans le contexte de services supports multiples.

Lorsque les technologies SDN (réseaux pilotés par logiciel) et NFV (virtualisation des fonctions de réseau) sont introduites dans le réseau d'accès, il faut définir de nouvelles interfaces pour les capacités de réseau ouvert, ainsi qu'un nouveau protocole pour commander les dispositifs de transfert physique sous-jacents, une nouvelle procédure interactive de protocole pour la communication entre le contrôleur et les dispositifs de transfert, de nouveaux protocoles et de nouvelles procédures pour améliorer la fiabilité et l'utilisation des ressources, et il convient de distribuer de manière souple les politiques de l'utilisateur aux multiples passerelles BNG. De plus, de nouvelles procédures de protocole sont nécessaires pour pouvoir fournir rapidement les services sur les réseaux IP clients, desservir le client via de multiples passerelles de réseau large bande et fournir un service à valeur ajoutée (VAS) dans les réseaux ouverts.

L'architecture des réseaux des opérateurs évolue aussi progressivement avec l'apparition des technologies émergentes. Toute passerelle de réseaux limitrophes (BNG) doit être capable de prendre en charge les multiservices porteurs et des fonctions telles qu'un réseau fixe (par exemple un serveur d'accès distant à large bande (BRAS)), un réseau mobile (par exemple une passerelle PDN), une passerelle de service IoT, une passerelle de réseau espace-Terre, etc. Les fonctions d'une BNG peuvent être mises en œuvre en chargeant des fonctions de réseau virtuel sur une infrastructure de télécommunication en nuage virtualisée. Il convient d'étudier les spécifications fonctionnelles de la BNG au regard des différents scénarios, de la commande d'accès utilisateur, des procédures de distribution et de fourniture de services, du protocole de signalisation et du mécanisme de garantie de la qualité de service pour pouvoir planifier avec souplesse l'utilisation des ressources en présence de différentes exigences de performance de retransmission et de sécurité.

Par ailleurs, pour automatiser le réseau et planifier ses ressources de manière efficace et souple, il convient d'introduire une technologie d'intelligence artificielle dans le réseau. Il faut acquérir des données sur l'état de tout le réseau en temps réel à partir de ses principaux éléments (par exemple une BNG) pour pouvoir prendre une décision de commande intelligente et assurer ainsi une meilleure qualité de service. Il faut aussi définir le modèle de données, le processus d'interaction entre les données et le protocole de signalisation pour que l'entité prenant des décisions par intelligence artificielle puisse acquérir des données sur l'état du réseau en temps réel et pour acheminer la politique optimisée aux éléments du réseau (par exemple une BNG) afin d'assurer un support efficace des services utilisateurs.

### E.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels nouveaux protocoles et procédures faut-il définir pour permettre la fourniture rapide de services par des réseaux IP personnalisés qui exploitent des technologies émergentes (par exemple les réseaux SDN, la NFV, l'informatique en nuage, l'Internet des objets, l'intelligence artificielle, l'informatique en périphérie du réseau mobile (MEC), etc.)?

– Quels nouveaux protocoles et procédures faut-il définir pour pouvoir acheminer des services et des politiques à l'utilisateur par le biais de passerelles de réseau large bande exploitant des technologies émergentes?

– Quels nouveaux protocoles et procédures faut-il définir pour pouvoir utiliser des réseaux dédiés à la puissance de calcul parmi plusieurs passerelles de réseaux limitrophes?

– Quels nouveaux protocoles, interfaces et fonctions faut-il mettre en œuvre pour qu'une passerelle de réseaux limitrophes puisse prendre en charge des technologies émergentes?

– Quels nouveaux protocoles, interfaces et fonctions faut-il mettre en œuvre pour qu'une passerelle de réseaux limitrophes puisse prendre en charge la convergence de technologies prenant en charge des réseaux à accès multiples (notamment l'accès fixe, l'accès mobile, l'accès par l'Internet des objets et l'accès par technologies spatiales, etc.)?

– Quels nouveaux mécanismes, protocoles et procédures faut-il définir pour distribuer les politiques de l'utilisateur, pour contrôler l'accès de l'utilisateur et garantir à l'utilisateur une certaine qualité de service?

– Quels nouveaux protocoles et procédures faut-il définir pour pouvoir fournir un service à valeur ajoutée dans les réseaux ouverts?

– Quels nouveaux protocoles et procédures faut-il définir dans les passerelles BNG pour la prise en charge de services multiples?

– Quels nouveaux protocoles et procédures faut-il définir pour permettre une gestion des réseaux et une orchestration des ressources assistées par intelligence artificielle entre plusieurs passerelles de réseaux limitrophes?

– Quels nouveaux modèles de données, protocoles et processus d'interaction faut-il définir pour permettre à des entités décisionnelles fondées sur l'intelligence artificielle d'acquérir des données sur l'état du réseau en temps réel auprès des passerelles de réseaux limitrophes?

### E.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Élaborer des descriptions de service pour les services qui ne sont pas décrits par d'autres organismes de normalisation, et définir les termes selon les besoins.

– Définir de nouveaux protocoles et procédures pour pouvoir fournir rapidement des services sur les réseaux IP clients.

– Définir de nouveaux protocoles et procédures pour pouvoir desservir le client via de multiples passerelles de réseaux limitrophes exploitant des technologies émergentes.

– Définir de nouveaux protocoles et procédures pour permettre de créer un réseau dédié à la puissance de calcul parmi de multiples passerelles de réseaux limitrophes.

– Élaborer de nouveaux protocoles, exigences et fonctions permettant aux passerelles de réseaux limitrophes de prendre en charge des technologies émergentes (par exemple les réseaux SDN, la NFV, l'informatique en nuage, l'Internet des objets, l'intelligence artificielle, l'informatique en périphérie du réseau mobile (MEC), etc.).

– Élaborer de nouveaux protocoles, exigences et fonctions permettant aux passerelles de réseaux limitrophes de prendre en charge la convergence de technologies de réseau à accès multiples (notamment l'accès fixe, l'accès mobile, l'accès par l'Internet des objets et l'accès par technologies spatiales, etc.).

– Définir de nouveaux protocoles et procédures permettant aux passerelles de réseaux limitrophes d'améliorer l'utilisation des ressources des réseaux par des commandes de réseau intelligentes.

– Définir de nouveaux protocoles et procédures pour assurer la gestion et la distribution des politiques de l'utilisateur grâce aux technologies SDN.

– Définir de nouveaux protocoles et procédures permettant de fournir un service à valeur ajoutée dans les réseaux ouverts.

– Définir de nouveaux protocoles et procédures pour la prise en charge de services supports multiples sur les passerelles BNG.

– Élaborer une méthode et des spécifications de test pour tester la sécurité des procédures de protocole se rapportant aux services fournis par des passerelles de réseau large bande.

– Définir de nouveaux protocoles et procédures permettant une gestion des réseaux et une orchestration des ressources assistées par intelligence artificielle entre plusieurs passerelles de réseaux limitrophes.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### E.4 Relations

Recommandations

– Séries Q, Y et H

Questions

– Questions A/11, B/11 et D/11 sur le contrôle des politiques

– Questions C/11, G/11 et M/11

Commissions d'études

– CE 13 de l'UIT-T et autres Commissions d'études travaillant sur les réseaux NGN, les réseaux futurs, les réseaux IMT-2020 et les passerelles de réseau large bande

– CE 20 de l'UIT-T

Autres organismes

– Broadband Forum

– IETF

– ETSI

Open Source

– ONAP

Grandes orientations du SMSI

– C2

Objectifs de développement durable

– 9

Question F/11

Protocoles prenant en charge les technologies de commande et de gestion
pour les réseaux IMT-2020 et les réseaux ultérieurs

(Suite de la Question 6/11)

### F.1 Motifs

L'équipe responsable de cette Question a élaboré plusieurs protocoles prenant en charge des technologies de commande et de gestion telles que l'orchestration, le découpage de réseau, l'exposition des capacités de réseau, ou encore le recensement et la gestion des environnements de réseaux hétérogènes pour créer des réseaux IMT‑2020.

L'exploitation de l'intelligence artificielle (IA) pour automatiser les réseaux et intégrer de l'intelligence dans leur fonctionnement est un sujet majeur actuellement. Il convient de déterminer comment tirer parti de l'IA et des mégadonnées pour commander et gérer de manière intelligente des réseaux IMT-2020 et ultérieurs, afin que ces méthodes puissent être offertes rapidement sur le marché pour répondre à sa demande. Il faut notamment définir en priorité les protocoles permettant de prendre en charge une commande intelligente des réseaux IMT-2020 et ultérieurs et des mécanismes de pointe tels que les temps de réponse courts, une faible gigue et une faible perte de paquets, une largeur de bande garantie, un réseau de très grande envergure, une connectivité et une topologie souples, l'attribution et le partage de ressources et le découpage de réseau. Si les secteurs verticaux fournissent des spécifications précises, la gestion du plan utilisateur peut être améliorée pour optimiser le trajet vers l'utilisateur et répondre ainsi aux besoins de ces secteurs.

Par ailleurs, les protocoles concernant le système de gestion commun prenant en charge à la fois les réseaux fixes et mobiles sont également des questions importantes qu'il faudra examiner à l'avenir.

### F.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels protocoles et mécanismes faut-il définir pour combler les lacunes recensées par les organismes de normalisation concernés?

– Quels protocoles et mécanismes faut-il définir pour prendre en charge les scénarios de service, spécifications, capacités et architecture pour les réseaux IMT-2020 et ultérieurs définis par les commissions d'études pertinentes de l'UIT‑T et d'autres organismes de normalisation?

– Quels protocoles et mécanismes faut-il définir pour les technologies essentielles à la mise en place de réseaux IMT-2020 et ultérieurs, notamment les commandes intelligentes des réseaux de transport, l'orchestration, le découpage de réseau, l'optimisation du plan utilisateur, l'exposition des capacités de réseau, l'identification, l'authentification de dispositifs, la convergence fixe/mobile, la gestion de réseau dans les environnements de réseaux hétérogènes, etc.?

– Comment peut-on tirer parti des technologies émergentes, en particulier l'intelligence artificielle, les mégadonnées, les réseaux QKDN et les technologies connexes, dans les protocoles de commande et de gestion des réseaux IMT‑2020 et ultérieurs?

– Quels protocoles et mécanismes faut-il définir pour pouvoir offrir avec une performance élevée des fonctions comme le temps de latence ultra-faible et la haute fiabilité dans les réseaux IMT‑2020 et ultérieurs?

– Quels protocoles et mécanismes faut-il définir pour améliorer et renforcer les interfaces fondées sur les services qui sont destinées aux réseaux IMT‑2020 afin d'améliorer l'efficacité, la souplesse et l'intelligence de ces réseaux?

– Comment utiliser et exploiter les logiciels open source, en collaboration avec les organismes concernés, dans le contexte des technologies essentielles aux réseaux IMT‑2020 et ultérieurs afin de mettre en œuvre les nouvelles Recommandations?

### F.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Élaborer des Recommandations sur les protocoles et mécanismes concernant la commande des réseaux IMT-2020 et ultérieurs dotés de fonctionnalités évoluées, prenant en charge les réseaux de très grande envergure, une connectivité et une topologie souples, la convergence fixe/mobile, l'optimisation du plan utilisateur, etc.

– Élaborer des Recommandations sur les protocoles et mécanismes prenant en charge les réseaux IMT‑2020 et ultérieurs grâce à des technologies telles que le découpage de réseau, la virtualisation des ressources, l'orchestration, l'intelligence artificielle et les mégadonnées, les réseaux QKDN et les technologies connexes, etc.

– Élaborer des Recommandations sur les protocoles, et en particulier sur les mécanismes, concernant d'autres technologies essentielles pour les réseaux IMT-2020 et ultérieurs, notamment l'identification, l'authentification de dispositif, l'exposition des capacités de réseau, etc.

– Élaborer des Recommandations sur les protocoles, et en particulier sur les mécanismes, concernant le système de gestion commun destiné aux réseaux IMT-2020 et ultérieurs.

– Élaborer des Recommandations sur les protocoles, et en particulier sur les mécanismes, concernant les réseaux IMT‑2020 et permettant d'obtenir une performance élevée au regard de fonctions comme le temps de latente ultra-faible et la haute fiabilité.

– Élaborer des Recommandations sur les protocoles concernant les réseaux IMT‑2020 et ultérieurs pour améliorer et renforcer les interfaces fondées sur des services afin d'obtenir davantage d'efficacité, de souplesse et d'intelligence.

– Élaborer un supplément, un rapport technique et des lignes directrices sur les bonnes pratiques et les mises en œuvre des protocoles et mécanismes destinés aux réseaux IMT‑2020 et ultérieurs, notamment des logiciels open source, en collaboration avec les organismes concernés.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### F.4 Relations

Recommandations

– Séries Q et Y

Questions

– D/11, G/11, H/11, K/11

Commissions d'études

– Commission d'études 2 de l'UIT‑T

– Commission d'études 13 de l'UIT‑T

– Commission d'études 15 de l'UIT‑T

– Autres CE participant aux études relatives aux réseaux IMT-2020

Autres organismes

– UIT-R

– ETSI

– IETF

– IEEE

– 3GPP

Grandes orientations du SMSI

– C2, C5

Objectifs de développement durable

– 9, 17

Question G/11

Exigences de signalisation et protocoles pour le rattachement au réseau
et l'informatique en périphérie pour les réseaux futurs
et les réseaux IMT-2020 et ultérieurs

(Suite de la Question 7/11)

### G.1 Motifs

L'UIT-T a mené des études sur les exigences de signalisation et les protocoles destinés aux réseaux futurs. L'informatique en périphérie, qui est nécessaire pour l'intelligence artificielle, les mégadonnées ou encore la conduite autonome et les robots, est un sujet d'actualité depuis que les réseaux IMT‑2020 ont commencé à être commercialisés.

Les réseaux futurs et les réseaux IMT‑2020 feront appel à un large éventail de services (par exemple le multimédia, la télédétection, l'intelligence artificielle, les mégadonnées, la mobilité, les robots, etc.). Ils présenteront des éléments de convergence en raison de leur capacité de calcul élevée et des possibilités qu'ils offriront à l'informatique en périphérie dans le contexte de réseaux hétérogènes (par exemple des réseaux IMT‑2020, LTE, 3G, WLAN, BLE, LPWA, etc.), de systèmes à dispositifs multiples (par exemple des téléphones intelligents, des tablettes, des ordinateurs portables, des capteurs, des caméras de surveillance, etc.) et de l'informatique en nuage (par exemple l'informatique en nuage et en périphérie, l'informatique en nuage destinée au public, etc.) Leurs capacités pourront être combinées de manière dynamique à des fins de collaboration. Ces services constituent ce qu'on appelle "l'informatique en périphérie", et les protocoles de signalisation devraient permettre de relier la source et le dispositif pour réaliser ce type de fonctionnement. Différentes technologies seront nécessaires à cette fin, notamment l'authentification et la configuration fédérées pour un transfert dynamique des médias, l'attribution d'adresses IP par session et la configuration du terminal, la vérification de l'autorisation d'accès au réseau, la modification en cours de session de la connectivité de service, la commande de rattachement et l'attribution des ressources.

De plus, les réseaux IMT‑2020 permettent d'accélérer le trafic de paquets de données d'un facteur supérieur à dix par rapport à la 4G, tandis que l'informatique en périphérie réduit le temps de latence des transactions en recensant dans les réseaux IMT‑2020 les capacités informatiques les plus proches des utilisateurs mobiles finals. De ce point de vue, l'informatique en nuage est également importante car elle permet d'effectuer des transactions de données avec un temps de latence ultra‑faible et d'offrir les services requis avec un débit élevé (par exemple la réalité virtuelle ou la réalité augmentée, le streaming, l'industrie 4.0, les robots, l'Internet des objets, etc.) Ces procédures devront être conçues de manière à pouvoir prendre en compte différents services émergents comme la réalité virtuelle ou la réalité augmentée, les jeux en streaming, l'intelligence artificielle, les mégadonnées, la conduite autonome, les robots, etc.

Pour étendre autant que possible la polyvalence des services et la capacité des dispositifs, il faut également maximiser l'utilisation des ressources et les commandes fondées sur les connaissances. Il faut par conséquent examiner les aspects fondamentaux des réseaux futurs tels que la virtualisation et les réseaux pilotés par logiciel (SDN), l'informatique en périphérie intelligente (IEC), l'informatique en périphérie à accès multiples (MEC) et les services en nuage destinés aux réseaux d'accès.

###

### G.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quelles Recommandations nouvelles ou révisées sont nécessaires pour gérer la révision des exigences de signalisation et des protocoles pour la fonction NACF?

– Quelles nouvelles Recommandations sont nécessaires pour élaborer des exigences de signalisation et des protocoles permettant de prendre en charge le rattachement au réseau et les services informatiques en périphérie (intelligence artificielle, mégadonnées, mobilité, nuage en périphérie, etc.) dans le but d'offrir des services multi‑dispositifs, des interfaces et des connexions?

– Quels mécanismes associés sont nécessaires à la signalisation du rattachement et de l'informatique en périphérie pour garantir la sécurité des services multi‑dispositifs, des interfaces et des connexions?

– Quels mécanismes de commande sont nécessaires à la signalisation du rattachement et de l'informatique en périphérie pour prendre en charge la gestion de la mobilité et des ressources virtuelles?

– Quelle architecture fonctionnelle et quelles entités sont nécessaires au rattachement au réseau pour prendre en charge les réseaux futurs et les réseaux IMT-2020, notamment lorsque le réseau d'accès exploite les technologies SDN, NFV, IEC et MEC?

– Quelle architecture fonctionnelle et quelles entités sont nécessaires pour prendre en charge les services de streaming multi-interfaces, en particulier pour la signalisation et les protocoles de rattachement dans le réseau d'accès?

### G.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Conserver les Recommandations actuelles qui sont en cours d'étude au titre de la présente Question.

– Définir les exigences de signalisation et les protocoles nécessaires à la révision des exigences de signalisation et des protocoles à l'appui du rattachement au réseau et de l'informatique en périphérie.

– Définir les exigences de signalisation et les protocoles nécessaires à la prise en charge des procédures de rattachement et de l'informatique en périphérie pour les dispositifs multiples, les connexions multiples et les interfaces multiples dans le contexte des réseaux futurs (par exemple SDN, NFV) et des réseaux IMT-2020 et ultérieurs.

– Définir les exigences de signalisation et les protocoles pour la prise en charge des fonctions de la gestion de la mobilité et des ressources dans les réseaux d'accès comme dans les réseaux centraux.

– Définir les exigences de signalisation et les protocoles nécessaires à la prise en charge de différents systèmes efficaces de classification de trafic et de pilotage fondés sur des dispositifs qui exploitent la technologie MEC (par exemple une couche prenant en charge la technologie SDK, IEC, MEC, etc.), de réseaux centraux (par exemple le découpage de réseau, l'APN, etc.) et de gestion des équipements périphériques (par exemple le nuage en périphérie, etc.) pour garantir que l'on dispose de réseaux IMT‑2020 et ultérieurs à faible temps de latence.

– Définir les exigences de signalisation et les protocoles nécessaires à la prise en charge de la gestion de la mobilité et de la migration de services ou d'applications vers des environnements exploitant l'informatique et le nuage en périphérie, notamment en s'appuyant sur les attributions de puissance de calcul, les attributions de ressources dépendant de la mobilité et la tolérance aux pannes pour acheminer le trafic de la périphérie la plus proche dans les réseaux futurs et les réseaux IMT‑2020 et ultérieurs.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### G.4 Relations

Recommandations

– Recommandations de la série Y sur les spécifications et l'architecture pour les réseaux futurs et les réseaux IMT-2020 et ultérieurs

– Recommandations de la série Q sur les spécifications et les protocoles de signalisation, les mesures et les tests

Questions

– Questions A/11, B/11, D/11, M/11, F/11

Commissions d'études

– CE 13: spécifications et architecture pour les réseaux futurs et les réseaux IMT-2020 et ultérieurs, y compris la gestion de la mobilité et la virtualisation des ressources

– CE 16: services multimédias dans les environnements multi-dispositifs/interfaces/
connexion

– CE 20: services et protocoles M2M et IoT

– CE 17: sécurité et gestion de l'identité

Autres organismes

– ISO/CEI JTC1/WG7

– IETF

– OMA

– ETSI

Grandes orientations du SMSI

– C2

Objectifs de développement durable

– 9

Question H/11

Protocoles prenant en charge les réseaux de contenus répartis et les technologies des réseaux centrés sur les informations pour les réseaux futurs et les réseaux IMT-2020 et ultérieurs

(Suite de la Question 8/11)

### H.1 Motifs

Les nouveaux services et applications multimédias nécessitent différentes fonctions et fonctionnalités. Les fonctions de transport de type multidiffusion de bout en bout font partie des principales caractéristiques des applications multimédias ayant une capacité de communication multi-parties. Une série de Recommandations UIT‑T ont donc été élaborées sur les cadres et protocoles régissant la gestion de groupe et les communications de multidiffusion de bout en bout dans des environnements de réseau de multidiffusion IP et non IP. La collaboration avec l'ISO/CEI JTC 1/SC 6 a permis d'élaborer des textes normatifs communs sur les communications multi-parties, à savoir: série UIT-T X.606 | série ISO/CEI 14476, série UIT-T X.607 | série ISO/CEI 14476, série UIT-T X.608 | série ISO/CEI 14476, UIT-T X.602 | ISO/CEI 16513, série UIT-T X.603 | série ISO/CEI 16512, série UIT-T X.604 | série ISO/CEI 24793, UIT-T X.605 | ISO/CEI 13252. Ces Recommandations devront être régulièrement tenues à jour et pourront être actualisées pour répondre aux nouveaux besoins éventuels du marché.

Certains services multimédias répartis et conversationnels, par exemple la TVIP, l'affichage numérique, la vidéo à la demande, la téléprésence, le service de radiodiffusion personnelle, le streaming multimédia et d'autres nouveaux services de fourniture de contenus nécessitent une capacité de communication efficace dans différents environnements de réseau et doivent pouvoir prendre en charge des contenus enrichis comme la réalité augmentée et la réalité virtuelle, ou encore l'ultra-haute définition (4K, 8K). Les protocoles des réseaux de services répartis fondés sur la technologie d'homologue à homologue (P2P) peuvent constituer une solution intéressante pour la prise en charge de nouvelles applications qui nécessitent une capacité de communication très performante et modulable. La CE 11 élabore des Recommandations sur l'architecture et les protocoles de signalisation pour les communications sur les réseaux P2P gérés (MP2P); ces Recommandations peuvent s'appliquer aux communications multimédia de bout en bout, et en particulier aux services de streaming vidéo et de distribution de contenus. L'élaboration de Recommandations sur les protocoles pour les communications P2P hybrides (HP2P), qui se composent d'un réseau P2P maillé et d'un réseau P2P arborescent, a également débuté et va se poursuivre. Les protocoles de communication HP2P permettront de disposer de capacités de distribution d'informations efficaces et souples pour offrir des services liés à l'Internet des objets et des services exploitant la technologie des registres distribués. La série de Recommandations qui seront élaborées fourniront des solutions et des lignes directrices destinées aux vendeurs et aux fournisseurs souhaitant mettre en œuvre et déployer des services de distribution et de fourniture de contenus qui utilisent les technologies P2P.

Les réseaux centrés sur les informations (ICN) ont fait et continuent à faire l'objet d'études au sein de nombreuses organisations de normalisation, et notamment du Groupe de recherche de l'IETF sur les réseaux centrés sur les informations, qui étudie l'intégration des technologies ICN dans l'Internet existant dans le cadre de déploiements superposés (réseau ICN sur IP), de déploiements sous‑jacents (îlots ICN dans IP) ou d'un réseau ICN dans une infrastructure IP virtualisée. Ces approches sont décrites dans le Document RFC 8763. Les protocoles et les mécanismes pour la découverte, la distribution et la fourniture de contenus sur la base de la technologie ICN dans des

déploiements superposés, sous-jacents et de virtualisation IP constitueront de nouveaux sujets d'étude très importants pour la prise en charge des spécifications et des capacités connexes des réseaux IMT-2020 et ultérieurs.

Les Recommandations concernées par cette Question sont notamment les suivantes: X.601, X.602, X.603, X.603.1, X.603.2, X.604, X.604.1, X.604.2, X.605, X.606, X.606.1, X.607, X.607.1, X.608 et X.608.1, X.609, X.609.1, X.609.2, X.609.3, X.609.4, X.609.5, X.609.6, X.609.7, X.609.8, X.609.9, X.609.10, Q.4100-Q.4139 (pour les protocoles et la signalisation concernant les communications P2P).

### H.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quelles mises à jour ou améliorations faut-il apporter aux Recommandations existantes pour répondre aux nouveaux besoins du marché?

– Quelles Recommandations faut-il élaborer pour définir des protocoles pour la découverte, la distribution et la fourniture de contenus afin de prendre en charge les spécifications et les architectures fonctionnelles des réseaux existants, des réseaux futurs et des réseaux IMT‑2020 et ultérieurs?

– Quelles Recommandations faut-il élaborer pour définir des protocoles pour la découverte, la distribution et la fourniture de contenus sur la base de la technologie ICN dans les déploiements superposés, sous-jacents et de virtualisation IP qui sont pris en compte dans les réseaux futurs et les réseaux IMT-2020 et ultérieurs?

– Quels protocoles et mécanismes faut-il élaborer pour prendre en charge les communications P2P gérées et hybrides?

– Quels mécanismes et technologies essentielles faut-il définir pour mettre en œuvre des systèmes définis par les applications et compatibles avec tous les réseaux?

– Quels paramètres et interfaces de couche 4 faut-il définir respectivement pour la couche supérieure et inférieure?

### H.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Mettre à jour et améliorer les Recommandations de la série X.60x, y compris les normes relatives aux communications multi-parties dont le texte est commun avec des normes de l'ISO/CEI JTC 1/SC 6, pour répondre aux nouveaux besoins du marché.

– Élaborer des Recommandations sur des protocoles permettant de prendre en charge la découverte, la distribution et la fourniture de contenus pour les réseaux d'anciennes générations, les réseaux futurs et les réseaux IMT‑2020 et ultérieurs.

– Élaborer des Recommandations sur des protocoles permettant de prendre en charge la découverte, la distribution et la fourniture de contenus sur la base de la technologie des réseaux centrés sur les informations (ICN) dans les déploiements superposés, sous-jacents et de virtualisation IP qui sont pris en compte dans les réseaux IMT‑2020 et ultérieurs.

– Élaborer des Recommandations sur des protocoles et des mécanismes permettant de prendre en charge les communications P2P gérées et hybrides.

– Élaborer des Recommandations sur les protocoles permettant de prendre en charge les communications multimédias multi-parties de bout en bout, y compris les services et applications de radiodiffusion personnelle.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?Q=8/11>).

### H.4 Relations

Recommandations

– Recommandations de la série X sur les communications multimédias multi-parties

– Recommandations de la série Y et Suppléments sur la TVIP, la fourniture de contenus, les réseaux DSN, les réseaux futurs et les réseaux IMT-2020 et ultérieurs

– Recommandations de la série H sur les services et applications multimédias

– Recommandations de la série Q sur la signalisation, les protocoles, les mesures et les spécifications de test liés au domaine d'application de la Question

Questions

– Toutes les Questions de la CE 11

Commissions d'études

– CE 13 de l'UIT-T: réseaux futurs et réseaux IMT-2020 et ultérieurs

– CE 16 de l'UIT-T: applications et services multimédias

– CE 17 de l'UIT-T: questions de sécurité

Autres organismes

– ISO/CEI JTC1/SC6

– IETF, ICNRG

Grandes orientations du SMSI

– C2

Objectifs de développement durable

– 9

Question I/11

Tests pour l'Internet des objets, ses applications et systèmes d'identification

(Suite de la Question 12/11)

### I.1 Motifs

D'un point de vue général, l'Internet des objets (IoT) peut être considéré comme un projet ayant des répercussions sur les technologies et la société. Du point de vue de la normalisation technique, il peut être perçu comme une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques et virtuels) grâce à des technologies de l'information et de la communication interopérables, existantes ou en évolution. En exploitant des capacités d'identification, de saisie de données, de traitement et de communication, l'IoT tire pleinement parti des objets pour offrir des services à toutes sortes d'applications, tout en préservant le niveau de confidentialité nécessaire. Les concepts de société ubiquitaire, de réseau ubiquitaire et de ville ubiquitaire, pour ne citer que quelques exemples, ont été formulés dans la perspective d'un déploiement au niveau mondial des applications, services et technologies de l'Internet des objets, qui pourrait s'appuyer sur l'identification par radiofréquence (RFID), les réseaux de capteurs ubiquitaires (USN), les communications orientées machine (MOC), les communications de machine à machine (M2M), les communications par dispositif intelligent (SDC) et les services IoT fondés sur le nuage (CIS). La RFID a été normalisée par l'ISO/CEI JTC 1/SC 31, les technologies des réseaux de capteurs par l'ISO/CEI JTC 1/WG 7, les réseaux USN par la CE 20 de l'UIT-T, les communications MOC par la CE 13 de l'UIT-T, les communications M2M par l'UIT-T et l'ETSI, les communications SDC par la TIA et les services CIS par l'ETSI, l'OGC et le W3C.

NOTE 1 – Le terme "ubiquitaire" s'entend de la capacité de fournir tout service à tout moment, en tout lieu et au moyen de tout dispositif.

Tous ces mots clés correspondent à des cas d'utilisation analogues et à des fonctions identiques, mais ils renvoient à des technologiques différentes. On peut considérer l'IoT comme un cadre général recouvrant l'ensemble de ces mots clés, qui désignent eux-mêmes des technologies.

Étant donné l'étendue du concept d'IoT et sa possible association à de nombreuses technologies de base, il est nécessaire d'examiner les questions d'interopérabilité.

D'une manière générale, l'IoT offre divers nouveaux types de connectivité qui peuvent être utilisés dans différentes applications orientées client (réseaux de capteurs ubiquitaires volants (FUSN), réalité augmentée fondée sur l'IoT, etc.).

Par ailleurs, compte tenu du mécanisme d'authentification sécurisée utilisé par les technologies fondées sur l'IoT et des identités IoT, on peut considérer que l'IoT permet aussi de lutter contre la contrefaçon.

Dès lors, les tests applicables aux technologies et applications IoT sont de plus en plus importants aujourd'hui, en particulier au regard de l'interopérabilité des dispositifs IoT et de la confiance à l'égard des systèmes IoT utilisés.

Outre les applications IoT classiques, il est conseillé d'envisager des tests dans les domaines où les mises en œuvre de dispositifs IoT sont les plus nombreuses:

– Les villes intelligentes et durables.

– Les dispositifs à porter sur soi.

– L'Internet des objets industriel (IIoT).

– L'assistance à la conduite fondée sur le réseau pour les véhicules autonomes.

– Les réseaux de dispositifs volants fondés sur les aéronefs sans pilote.

En règle générale, il existe dans chacun de ces domaines différents scénarios pour connecter les dispositifs IoT à l'Internet, aux plates-formes en nuage et aux services à distance. De ce point de vue, il est très pertinent d'examiner les questions touchant aux procédures de test des dispositifs IoT.

### I.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels types de tests sont nécessaires pour les éléments de réseau IoT?

– Comment tester la sécurité des dispositifs IoT, compte tenu de leurs paramètres (par exemple la performance, la taille de la mémoire, la voie de communication, etc.)?

– Quelles séries de tests faut-il élaborer pour tester les procédures d'identification et d'authentification IoT?

– Comment tester les solutions techniques IoT à utiliser pour lutter contre la contrefaçon?

– Quelles nouvelles Recommandations faut-il élaborer afin de définir des mécanismes pour tester les applications IoT, y compris les aspects de sécurité et de confidentialité?

– Quelles nouvelles Recommandations faut-il élaborer pour définir des mécanismes de test de l'interopérabilité, des capacités et de la sécurité des systèmes d'identification IoT?

– Quels sont les scénarios de test à utiliser pour tester les dispositifs à porter sur soi?

– Quels sont les scénarios de test à utiliser pour tester le système IoT industriel (IIoT) et les dispositifs qui lui sont liés?

– Quelles séries de tests faut-il élaborer pour tester la méthodologie ou le mécanisme (les procédures) d'essai des technologies et protocoles de l'IoT et l'IIoT fondées sur l'analyse de prévisions?

– Quelles nouvelles Recommandations doivent être élaborées pour assurer l'interopérabilité, la compatibilité et la sécurité des dispositifs IoT à employer dans des villes intelligentes et durables?

– Quelles procédures de test doivent être élaborées à l'égard des technologies et des protocoles de l'IoT employés aux fins de l'assistance à la conduite fondée sur le réseau pour les véhicules autonomes?

### I.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Définir les séries de tests à utiliser pour tester les éléments de réseau IoT.

– Élaborer la méthodologie et les spécifications de test pour les essais relatifs à la sécurité de l'IoT.

– Élaborer des séries de tests pour tester les procédures d'identification et d'authentification IoT.

– Élaborer des séries de tests pour tester les solutions techniques IoT à utiliser pour lutter contre la contrefaçon.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester les applications IoT, y compris les aspects de sécurité et de confidentialité.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester l'interopérabilité, les capacités et la sécurité des systèmes d'identification IoT.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester les dispositifs à porter sur soi.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester l'Internet des objets industriel et les applications IIoT.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester les technologies et protocoles de l'IoT et l'IIoT fondées sur l'analyse de prévisions.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester les technologies et protocoles IoT à employer dans des villes intelligentes et durables.

– Élaborer la méthodologie ou le mécanisme à utiliser pour tester les technologies et protocoles de l'IoT employés aux fins de l'assistance à la conduite fondée sur le réseau pour les véhicules autonomes.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### I.4 Relations

Recommandations:

– Séries Q, Y, H, I, M et F

Questions:

– L/11; M/11

Commissions d'études:

– CE 2 de l'UIT‑T

– CE 5 de l'UIT‑T

– CE 13 de l'UIT‑T

– CE 16 de l'UIT‑T

– CE 17 de l'UIT‑T

– CE 20 de l'UIT‑T

Autres organismes:

– ETSI, et en particulier TC cyber

– IEEE

– IETF

– ISO/CEI JTC 1 (en particulier ISO/CEI JTC 1 TC27, JTC1 GT 7, ISO/CEI JTC 1/SC 6, ISO/CEI JTC 1/SC 31, ISO/CEI JTC 1/GT 10)

– OGC

– TIA

– W3C

Grandes orientations du SMSI:

– C5

Objectifs de développement durable

– 9

Question J/11

Paramètres de surveillance pour les protocoles utilisés dans les réseaux émergents, y compris l'informatique en nuage et en périphérie, les réseaux pilotés par logiciel et la virtualisation des fonctions de réseau (SDN/NFV)

(Suite de la Question 13/11)

### J.1 Motifs

Les réseaux émergents suivants ont été recensés et créés: réseaux futurs, Internet des objets (IoT), réseaux VoLTE/ViLTE, réseaux IMT-2020, etc. Pour réduire les investissements et les dépenses d'exploitation, les technologies SDN (réseaux pilotés par logiciel) et NFV (virtualisation des fonctions de réseau) ont été déployées dans les réseaux émergents afin de séparer commande et service, commande et support, matériel et logiciel.

Par ailleurs, l'informatique en nuage et l'informatique en périphérie commencent à faire partie des infrastructures du monde connecté. Dans ce nouvel environnement qui voit le jour, il faudrait offrir aux opérateurs et aux utilisateurs finals la possibilité de déterminer si les infrastructures qu'ils utilisent peuvent prendre en charge certains services et applications.

À mesure que l'intelligence artificielle parvient à maturité, elle commence à être exploitée dans les réseaux, notamment pour prendre des décisions de manière intelligente et faire des prévisions intelligentes pour les opérateurs et les entreprises actives sur l'Internet. Le choix des paramètres de surveillance, au sein des modèles de décision ou de prévision intelligentes, a une incidence considérable sur l'efficacité du réseau et en définitive sur l'expérience de l'utilisateur.

La normalisation de paramètres de système de surveillance pour les réseaux émergents, y compris l'informatique en nuage, permettra aux opérateurs, aux administrations et aux utilisateurs finals de disposer d'informations de surveillance compatibles et comparables entre les opérateurs de réseau, les fournisseurs de services et les utilisateurs finals. Elle pourrait également être utile pour résoudre des points de désaccord.

### J.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quel est l'ensemble minimal de paramètres à utiliser pour évaluer la performance du réseau?

– Quel est l'ensemble minimal de paramètres de surveillance à utiliser pour l'informatique en nuage et l'informatique en périphérie?

– Quel est l'ensemble minimal de paramètres de surveillance à utiliser pour les technologies NFV et SDN?

– Quel est l'ensemble minimal de paramètres de surveillance à utiliser pour les réseaux, applications et services émergents?

– Quels types de paramètres de surveillance faut-il utiliser pour les questions de sécurité?

– Quels types de paramètres de surveillance faut-il utiliser pour l'intelligence artificielle employée dans les réseaux, applications et services émergents?

– Quel est l'ensemble minimal de paramètres de surveillance à utiliser pour les réseaux, applications et services intelligents?

### J.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Définir un ensemble minimal de paramètres et une méthodologie de mesure de ces paramètres à utiliser pour évaluer la performance du réseau.

– Définir un ensemble minimal de paramètres et une méthodologie de mesure de ces paramètres à utiliser pour évaluer l'informatique en nuage et en périphérie.

– Définir un ensemble minimal de paramètres et une méthodologie de mesure de ces paramètres à utiliser pour évaluer les technologies NFV et SDN.

– Définir un ensemble minimal de paramètres et une méthodologie de mesure de ces paramètres à utiliser pour évaluer les réseaux, applications et services émergents.

– Étudier les types de paramètres de surveillance à utiliser pour les questions de sécurité.

– Étudier les types de paramètres de surveillance à utiliser pour l'intelligence artificielle appliquée aux réseaux, applications et services émergents.

– Étudier les types de paramètres de surveillance à utiliser pour les réseaux, applications et services intelligents.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### J.4 Relations

Recommandations

– Séries Q, Y, H, I, M, F et P de l'UIT‑T

Questions

– Questions A/11, B/11, D/11, G/11, I/11, K/11 et M/11

Commissions d'études

– CE 3 de l'UIT‑T: questions de politique générale et de réglementation

– CE 12 de l'UIT‑T: questions de qualité de service et de qualité d'expérience

– CE 13 de l'UIT-T: réseaux futurs, technologies SDN/NFV, informatique en nuage et architecture des réseaux émergents

– CE 16 de l'UIT-T: services et applications multimédias

– CE 17 de l'UIT‑T: questions de sécurité

– CE 20 de l'UIT‑T: IoT et ses applications

Autres organismes

– ETSI

– IEEE

– IETF

Grandes orientations du SMSI

– C2, C5

Objectifs de développement durable

– 9

Question K/11

Tests de l'informatique en nuage, des réseaux pilotés par logiciel (SDN)
et de la virtualisation des fonctions de réseau (NFV)

(Suite de la Question 14/11)

### K.1 Motifs

L'informatique en nuage est un modèle permettant d'offrir un accès par le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service. Un réseau piloté par logiciel est un ensemble de technologies permettant de programmer, d'orchestrer, de contrôler et de gérer des ressources de réseau de manière directe, ce qui facilite la conception, la fourniture et l'exploitation de services de réseau de façon dynamique et modulable. La virtualisation des fonctions d'un réseau s'entend du principe consistant à séparer les fonctions d'un réseau du matériel physique constituant celui-ci en utilisant une méthode d'abstraction virtuelle de ce matériel.

L'informatique en nuage, les SDN et la NFV sont des technologies émergentes qui sont abondamment utilisées dans différents scénarios. La conformité, l'interopérabilité et les essais comparatifs de ces technologies représentent des sujets d'importance majeure.

Dans le contexte de l'informatique en nuage, des SDN et de la NFV, les tests de conformité consistent à vérifier qu'une mise en œuvre donnée de ces technologies est conforme à une norme établie, par exemple une norme sur des spécifications fonctionnelles ou sur un protocole. Les tests d'interopérabilité consistent à déterminer si des entités associées à l'informatique en nuage, aux SDN et à la NFV sont capables d'interagir entre elles de la manière prévue. Les essais comparatifs servent quant à eux à mesurer la performance des mises en œuvre de ces technologies.

Au demeurant, de plus en plus de services, comme par exemple les SDN dans les réseaux étendus (SD-WAN), sont mis en œuvre au moyen de l'informatique en nuage, des SDN et de la NFV. Il faut donc envisager de tester aussi les services fondés sur ces technologies.

Il convient de travailler en coopération avec la CE 13 de l'UIT-T (la principale Commission d'études en matière d'informatique en nuage) pour tester l'informatique en nuage. Les activités de test débuteront une fois que la terminologie et l'architecture auront été définies par la CE 13.

### K.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quelles sont les exigences de l'informatique en nuage, des SDN et de la NFV en matière de conformité, d'interopérabilité et d'essais comparatifs?

– Quels types de séries de tests sont nécessaires pour tester l'informatique en nuage, les SDN et la NFV, notamment en termes de conformité, d'interopérabilité et d'essais comparatifs?

– Comment créer un système de test automatisé pour l'informatique en nuage, les SDN et la NFV afin d'améliorer l'efficacité des essais?

– Quels types de séries de tests sont nécessaires pour tester des services mis en œuvre au moyen de l'informatique en nuage, des SDN et de la NFV?

– Quelle collaboration est nécessaire pour réduire autant que possible la redondance des tâches avec les autres organismes de normalisation?

– Quelle collaboration est nécessaire pour faire appel à la communauté "open source"?

### K.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Recenser les exigences de l'informatique en nuage, des SDN et de la NFV en matière de conformité, d'interopérabilité et d'essais comparatifs.

– Élaborer des séries de tests permettant de tester l'informatique en nuage, les SDN et la NFV en termes de conformité, d'interopérabilité et d'essais comparatifs.

– Créer une méthodologie et un cadre de tests automatisés de l'informatique en nuage, des SDN et de la NFV.

– Élaborer des séries de tests permettant de tester les services mis en œuvre au moyen de l'informatique en nuage, des SDN et de la NFV.

– Mettre en place la collaboration nécessaire avec les organismes de normalisation, consortiums et forums extérieurs et les communautés "open source".

– Mettre à jour et améliorer les Recommandations relevant de la Question.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### K.4 Relations

Recommandations

– Séries Q, Y, H, I, M et F (en particulier les Recommandations relatives à l'informatique en nuage et aux tests)

Questions

– Toutes les Questions de la CE 11

Commissions d'études

– CE 2: aspects opérationnels

– CE12: qualité de service et qualité d'expérience

– CE 13: architecture des réseaux futurs et informatique en nuage

– CE 15: transport, accès et installations domestiques

– CE 16: services et applications multimédias

– CE 17: sécurité

Autres organismes

– ISO/CEI JTC 1 (et en particulier ISO/CEI JTC 1 SC 38)

– IETF

– ETSI NFV ISG

– IEEE

– OASIS

– NIST

– TM Forum

– ONF

Grandes orientations du SMSI

– C2, C5, C11

Objectifs de développement durable

– 9

Question L/11

Lutte contre la contrefaçon et le vol d'équipements de télécommunication/TIC

(Suite de la Question 15/11)

### L.1 Motifs

Les travaux menés au titre de cette Question ont été surtout consacrés à l'élaboration de Recommandations et de rapports techniques sur la lutte contre la contrefaçon d'équipements de télécommunication/TIC. Ces dernières années, avec l'utilisation croissante d'équipements de télécommunication/TIC dans la vie quotidienne, les problèmes liés à la vente, à la circulation et à l'utilisation de dispositifs de contrefaçon se sont multipliés sur la plupart des marchés et ont eu des conséquences néfastes pour les fabricants, les utilisateurs et les pouvoirs publics.

Un nombre considérable d'équipements de télécommunication/TIC contrefaits ont été découverts et ont posé des problèmes de sécurité nationale, de performance, de qualité de service et de pertes de revenus pour tous les acteurs du domaine. Cette situation a poussé les États Membres de l'UIT, en particulier les pays en développement, à examiner le problème et en particulier ses effets néfastes, et à étudier l'incidence positive éventuelle des mesures prises.

Par ailleurs, la demande de services, qui se traduit par la production et la mise à disposition d'un plus grand nombre d'équipements de télécommunication/TIC, a également engendré une augmentation du nombre d'équipements volés. Certains de ces équipements sont remis sur le marché après altération et modification de leur identité, contournant ainsi les mesures d'inscription d'identités sur liste noire mises en œuvre par les pouvoirs publics et les opérateurs de réseau mobile. En conséquence, en plus de leur engagement dans la lutte contre la contrefaçon d'équipements de télécommunication/TIC, la plupart des pays ont aussi mis en place des mesures contre le vol d'équipements de télécommunication/TIC, certaines de ces mesures visant à éviter que les équipements volés dont les identités ont été modifiées ne soient réactivés sur des réseaux et à gérer efficacement la situation.

La CE 11 a approuvé la Recommandation UIT‑T Q.5050 intitulée "Cadre pour des solutions permettant de lutter contre la contrefaçon de dispositifs TIC" et la Recommandation UIT‑T Q.5051 intitulée "Cadre pour la lutte contre l'utilisation de dispositifs mobiles volés"; elle a en outre entrepris d'examiner un certain nombre de nouveaux sujets.

Dans le cadre de l'UIT et dans le monde entier, des débats ont été menés pour déterminer si des tests de conformité et d'interopérabilité pouvaient contribuer à la lutte contre la contrefaçon d'équipements TIC. Dans la Résolution 188 (Rév. Dubaï, 2018) de l'UIT, la Conférence de plénipotentiaires, consciente du fait que la modification des dispositifs de télécommunication/TIC risquait de réduire l'efficacité des solutions adoptées par les pays pour lutter contre la contrefaçon, a invité les États Membres à prendre toutes les mesures nécessaires à cette lutte. Des identifiants uniques et persistants pourraient permettre de reconnaître les produits authentiques. Il convient en outre d'accorder une attention particulière au risque que la contrefaçon de dispositifs IoT se répande et aux problèmes qu'elle pourrait poser.

Par ailleurs, dans la Résolution 189 (Rév. Dubaï, 2018) de l'UIT sur la lutte contre le vol de dispositifs mobiles, la Conférence de plénipotentiaires a décidé d'étudier et d'encourager la mise au point de solutions et de moyens pour continuer de lutter contre le vol de dispositifs mobiles et prévenir ce phénomène, et elle a invité les États Membres à adopter les mesures nécessaires pour prévenir et repérer l'altération volontaire ainsi que la reproduction d'identifiants de dispositifs TIC mobiles et pour lutter contre ce phénomène, et à empêcher l'accès aux réseaux mobiles des dispositifs dont l'identifiant a été altéré volontairement ou reproduit.

La présente Question a pour objet d'examiner toutes les pistes possibles pour lutter contre le vol et la contrefaçon de dispositifs de télécommunication/TIC, particulièrement au regard de la gestion d'identité dans la chaîne logistique des produits, la traçabilité, la sécurité, la confidentialité et la confiance à l'égard des personnes et des réseaux. Une coopération entre les commissions d'études de l'UIT-T, entre l'UIT-T et l'UIT-D, ainsi qu'avec des organismes extérieurs à l'UIT (en particulier des organismes de normalisation) sera nécessaire en vue d'obtenir des informations complètes sur le sujet et de bien le comprendre; il sera notamment nécessaire d'organiser des séminaires ou ateliers en collaboration avec les parties prenantes. Une coordination entre les organisations concernées est également nécessaire à cette fin.

Le groupe chargé de cette Question mettra à jour les Recommandations Q.5050 et Q.5069 et le rapport technique TR-CF de l'UIT‑T.

### L.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels rapports techniques sont nécessaires pour faire mieux connaître le problème de la contrefaçon des équipements TIC et les dangers qui en résultent?

– Peut-on utiliser des tests de conformité et d'interopérabilité et des mécanismes d'évaluation pour lutter contre la contrefaçon d'équipements de télécommunication/TIC?

– Quelles technologies peut-on utiliser pour lutter contre la contrefaçon, l'altération et le vol d'équipements de télécommunication/TIC?

– Quels sont les cadres de gestion d'identité appropriés pour lutter contre la contrefaçon et le vol d'équipements de télécommunication/TIC dont l'identité est modifiée?

– Quelles nouvelles catégories de dispositifs de télécommunication/TIC faut-il prendre en compte dans la lutte contre la contrefaçon, et quel identifiant unique de dispositif pourrait être envisagé pour chaque catégorie?

– Quels types de recommandations, suppléments, rapports techniques et lignes directrices convient-il d'élaborer pour lutter contre la contrefaçon, l'altération et la modification d'équipements TIC et contre la duplication d'identifiants de dispositifs uniques?

– Quels types de recommandations, suppléments, rapports techniques et lignes directrices convient-il d'élaborer pour aider les Membres de l'UIT, en coopération avec le Secteur de l'UIT-D, à lutter contre la contrefaçon et à réduire l'utilisation d'équipements TIC volés?

– Quels recommandations, suppléments, rapports techniques et lignes directrices de l'UIT sont nécessaires à la gestion de la chaîne logistique (de la fabrication à la commercialisation, en passant par l'importation et la distribution) afin de renforcer la traçabilité, la sécurité, la confidentialité et la confiance à l'égard des personnes, des produits et des réseaux?

– Quels recommandations, suppléments, rapports techniques et lignes directrices de l'UIT sont pertinents pour lutter contre la contrefaçon d'équipements IoT et les dangers qui en résultent?

– Dans ce domaine, de quoi faut-il tenir compte pour réaliser directement ou indirectement des économies d'énergie dans le secteur des TIC ou dans d'autres secteurs?

### L.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Élaborer des recommandations, suppléments, rapports techniques et lignes directrices pour aider les Membres de l'UIT, en coopération avec le Secteur de l'UIT-D, à lutter contre la contrefaçon d'équipements de télécommunication/TIC et les dangers qui en résultent.

– Élaborer des recommandations, suppléments, rapports techniques et lignes directrices pour aider les Membres de l'UIT, en coopération avec le Secteur de l'UIT-D, à lutter contre la contrefaçon d'équipements IoT.

– Élaborer des recommandations, suppléments, rapports techniques et lignes directrices pour traiter le problème du vol d'équipements de télécommunication/TIC et aider les États Membres, en coopération avec le Secteur de l'UIT‑D, à mettre en place des solutions pour réduire l'utilisation d'équipements volés.

– Élaborer des recommandations, suppléments, rapports techniques et lignes directrices pour recenser de nouvelles catégories de dispositifs de télécommunication/TIC qui pourraient bénéficier de la lutte contre la contrefaçon, et déterminer quel identifiant unique de dispositif pourrait être envisagé pour chaque catégorie.

– Étudier des solutions pertinentes, y compris des cadres de gestion de l'identité, pour lutter contre la contrefaçon et le vol d'équipements de télécommunication/TIC dont l'identifiant unique a été modifié ou dupliqué.

– Déterminer quelles technologies pertinentes peuvent être employées dans la lutte contre la contrefaçon, la modification ou le vol d'équipements de télécommunication/TIC et les dangers qui en résultent.

– Organiser des ateliers et des manifestations dans les régions de l'UIT en coopération avec le Secteur de l'UIT-D pour promouvoir les travaux de l'UIT-T dans ce domaine et impliquer les parties prenantes.

– Étudier les solutions possibles en matière de tests de conformité et d'interopérabilité (C&I) pour lutter contre la contrefaçon et la modification d'équipements de télécommunication/TIC, compte tenu des activités de la CASC de l'UIT‑T.

– Étudier les résultats obtenus par différents organismes de normalisation internationaux et élaborer des spécifications techniques à utiliser dans les travaux de normalisation menés au titre de la Question.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### L.4 Relations

Résolutions

– Résolution 188 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires intitulée "Lutter contre la contrefaçon de dispositifs de télécommunication fondés sur les technologies de l'information et de la communication".

– Résolution 189 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires intitulée "Aider les États Membres à lutter contre le vol de dispositifs mobiles et à prévenir ce phénomène".

– Résolution 79 de la CMDT (Rév. Buenos Aires, 2017) intitulée "Rôle des télécommunications/technologies de l'information et de la communication dans la lutte contre la contrefaçon de dispositifs de télécommunication/d'information et de communication et le traitement de ce problème".

– Résolution 76 de l'AMNT (Rév. Hammamet, 2016) intitulée "Études relatives aux tests de conformité et d'interopérabilité, assistance aux pays en développement et futur programme éventuel de marque UIT".

– Résolution 96 de l'AMNT (Rév. Hammamet, 2016) intitulée "Études du Secteur de la normalisation des télécommunications de l'UIT visant à lutter contre la contrefaçon des dispositifs de télécommunication/technologies de l'information et de la communication".

– Résolution 97 de l'AMNT (Rév. Hammamet, 2016) intitulée "Lutter contre le vol de dispositifs de télécommunication mobiles".

Recommandations:

– UIT-T X.1255, UIT-T X.660, UIT-T Q.5050, UIT-T Q.5051

Questions

– Toutes les Questions de la CE 11, en particulier celles relatives aux architectures de commande et de signalisation, aux protocoles et aux tests de conformité et d'interopérabilité

Commissions d'études

– CE 2 de l'UIT-T

– CE 3 de l'UIT-T

– CE 5 de l'UIT-T

– CE 12 de l'UIT-T

– CE 13 de l'UIT-T

– CE 17 de l'UIT-T

– CE 20 de l'UIT-T

– CE 1 et CE 2 de l'UIT-D

Autres organismes

– ETSI

– CEI

– IEEE

– IETF

– ISO/CEI JTC 1

Grandes orientations du SMSI

– C2, C5, C11

Objectifs de développement durable

– 9

Question M/11

Spécifications de tests et évaluations comparatives concernant les protocoles,
les réseaux et les services prenant en charge les technologies émergentes

(Suite de la Question 16/11)

### M.1 Motifs

Aux termes de la Résolution 76 de l'AMNT – Études relatives aux tests de conformité et d'interopérabilité, assistance aux pays en développement et futur programme éventuel de marque UIT – il est décidé que la Commission d'études 11 de l'UIT T doit coordonner les activités menées par le Secteur en ce qui concerne le programme de l'UIT sur la conformité et l'interopérabilité (C&I) dans l'ensemble des commissions d'études et examiner les recommandations figurant dans le plan d'activité sur la conformité et l'interopérabilité pour la mise en œuvre à long terme du programme C&I.

L'UIT‑T produit actuellement un grand nombre de Recommandations. Pour parvenir à l'interopérabilité et à la conformité, un des aspects importants du Programme C&I de l'UIT concerne l'élaboration et la tenue à jour de cadres et de méthodologies de test.

Il est essentiel que les méthodologies concernant les tests de conformité et d'interopérabilité utilisées par toutes les commissions d'études qui s'intéressent aux tests soient harmonisées et cohérentes entre elles. Dans un souci d'interopérabilité à l'échelle mondiale, toutes les Recommandations de l'UIT‑T doivent être élaborées et actualisées en tenant compte des critères de conformité et d'interopérabilité, en fonction de la méthodologie utilisée.

Les tests de conformité ont pour objectif de déterminer si les spécifications énoncées dans une Recommandation sont complètement et correctement respectées dans une mise en œuvre donnée. Les tests d'interopérabilité, quant à eux, ont pour objectif de déterminer si deux mises en œuvre ou plus de la même Recommandation communiquent et échangent correctement des informations entre elles. En principe, toute mise en œuvre doit d'abord être testée au regard de la conformité avant d'être testée au regard de l'interopérabilité.

Les tendances récentes (par exemple les technologies de l'IMT‑2020 et de l'Internet des objets) peuvent modifier considérablement l'architecture de réseau existante et exiger une performance de réseau supérieure. Elles peuvent en outre avoir une incidence sur les spécifications des dispositifs terminaux, par exemple des équipements des locaux client (CPE), des unités mobiles, des téléphones, etc.

La plupart des opérateurs de télécommunication mettent actuellement en œuvre diverses nouvelles technologies, tout en passant des réseaux à commutation de circuits à des réseaux à commutation par paquets et en essayant de fournir leurs services selon le principe du "tout sur IP". En conséquence, les opérateurs se retrouvent confrontés à certains problèmes qui, en général, sont liés à la compatibilité et à l'interopérabilité des équipements TIC utilisés et à l'interconnexion des réseaux IP (par exemple 4G, IMT-2020), ces systèmes étant notamment utilisés pour des services en itinérance ou nomades. Ainsi, la fourniture de services de voix et vidéo sur LTE (VoLTE/ViLTE) en itinérance pose certains problèmes aux opérateurs en raison de l'absence de procédures d'itinérance convenues entre les parties prenantes, de divers scénarios possibles pour la mise en œuvre des services VoLTE/ViLTE et d'autres éléments non normalisés (par exemple ENUM, appel d'urgence, etc.). Des tests de conformité et d'interopérabilité des interfaces réseau-réseau (NNI) aux

Recommandations UIT-T peuvent aider les opérateurs à s'assurer que leurs solutions VoLTE/ViLTE sont prêtes pour l'interconnexion. Cette méthode fondée sur l'interconnexion peut aussi être utilisée pour les réseaux futurs en mode paquets, par exemple les réseaux IMT-2020 et ultérieurs.

D'une manière générale, l'évaluation comparative est une méthode couramment utilisée pour mesurer et apprécier des paramètres de signalisation par rapport à des objectifs théoriques de performance, qui devrait aider à assurer la fourniture du service de bout en bout et à garantir la fiabilité du réseau.

Dans le cas des réseaux IMT-2020, l'évaluation comparative ne se limite pas uniquement à la couche transport, mais s'applique aussi à la performance, la qualité et la fiabilité des plates‑formes virtuelles.

Il est important pour les opérateurs et leurs utilisateurs de pouvoir déterminer les valeurs de performance et de productivité du réseau au regard des services pour lesquels une certaine qualité est requise.

Ainsi, les systèmes de mesure de la performance relative à l'Internet, qui sont mis à la disposition du public sur l'Internet, ne fournissent pas des mesures fiables et comparables. Outre l'absence de mesures normalisées pour le débit Internet dans les Recommandations de l'UIT-T, les résultats de tests obtenus par les méthodes d'évaluation existantes peuvent varier d'une méthode à l'autre. Les résultats des tests dépendent évidemment des segments de réseau qui sont utilisés sur une connexion de bout en bout. En particulier, il est impossible de garantir que la connexion de bout en bout soit fondée uniquement sur le réseau d'un opérateur de télécommunication donné et n'emprunte pas d'autres segments de réseau pouvant appartenir à d'autres opérateurs.

La mise au point d'une méthode unifiée de mesure de la performance relative à l'Internet est importante pour tous les acteurs des TIC.

De plus, cette méthode normalisée pourra être utilisée pour la définition du *"Cadre pour la fourniture, sur les réseaux de données fixes et mobiles, de services TIC avec la qualité de service garantie et le débit binaire demandé" en vue de l'élaboration de mécanismes économiques et de modèles d'interaction efficaces dans la chaîne "opérateur-fournisseur-utilisateur*".

NOTE – Les paramètres et exigences de qualité de service et d'expérience, et notamment les indicateurs clés de performance des réseaux et des services sont définis par la CE 12 de l'UIT‑T et les organismes de normalisation connexes. La série Q.3900-Q.4099 (tests pour les réseaux de prochaine génération), la série Q.1912.x, la série X.290 (sauf X.292), les Suppléments X.Suppl.4 et X.Suppl.5 et la série Z.500 relèvent de cette Question.

### M.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quelle est la méthodologie permettant de tester les technologies émergentes?

– Quelles sont les Recommandations UIT‑T en vigueur qui comportent des séries de tests?

– Quelle est l'architecture du banc d'essai ou des installations d'essai à employer pour tester les technologies émergentes?

– Quelles technologies actuellement mises au point pour le marché des TIC nécessitent des tests de conformité et d'interopérabilité (compte tenu des besoins du marché)?

– Quels types de séries de tests sont nécessaires pour tester l'interconnexion des réseaux fondés sur le protocole IP (par exemple la 4G ou les réseaux IMT‑2020 et ultérieurs)?

– Quels types de plates-formes de service pourraient faire l'objet d'une évaluation comparative?

– Quels types de procédures de test pourraient être utilisés pour l'évaluation comparative?

– Quel type de trafic pourrait être simulé pour l'évaluation comparative?

– Quels objectifs théoriques doivent faire l'objet d'une évaluation comparative?

– Quelles procédures de test faut-il élaborer pour les paramètres de réseaux normalisés, et notamment pour ceux qui sont définis dans le cadre des mesures de performance liées à l'Internet (UIT-T Q.3960), par exemple le débit binaire de bout en bout à l'intérieur et à l'extérieur du réseau fixe et mobile de l'opérateur (c'est-à-dire entre les utilisateurs du réseau de l'opérateur et une ressource Internet particulière)?

– Comment les paramètres, les technologies et les services peuvent-ils faire l'objet de tests à distance?

– Quelles procédures faut-il élaborer pour mettre en œuvre des tests à distance?

– Quelle est l'architecture de réseau à utiliser pour les tests à distance?

– Quelle méthodologie faut-il employer pour tester des dispositifs mobiles IMT‑2020?

– Quelle méthodologie faut-il employer pour tester les services qui nécessitent un temps de réponse ultra-court?

### M.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Étudier la méthodologie permettant de tester les technologies émergentes.

– Recenser les Recommandations de l'UIT‑T en vigueur qui comportent des séries de tests.

– Déterminer l'architecture du banc d'essai ou des installations d'essai à employer pour tester les technologies émergentes.

– Recenser les technologies TIC axées sur le marché pour lesquelles des tests de conformité et d'interopérabilité sont nécessaires.

– Élaborer des séries de tests à employer pour tester l'interconnexion des réseaux fondés sur le protocole IP (par exemple la 4G ou les réseaux IMT‑2020 et ultérieurs).

– Déterminer les types d'équipements qui pourraient faire l'objet d'une évaluation comparative.

– Élaborer les procédures de test à employer dans les évaluations comparatives.

– Déterminer le type de trafic à simuler pour l'évaluation comparative.

– Définir les objectifs théoriques devant faire l'objet d'une évaluation comparative.

– Établir des procédures d'essai pour les paramètres de réseaux normalisés, et notamment pour ceux qui sont définis dans le cadre des mesures de performance liées à l'Internet (UIT‑T Q.3960), par exemple le débit binaire de bout en bout à l'intérieur et à l'extérieur du réseau fixe et mobile de l'opérateur (c'est-à-dire entre les utilisateurs du réseau de l'opérateur et une ressource Internet particulière).

– Déterminer les paramètres, les technologies et les services qui peuvent faire l'objet de tests à distance.

– Définir les procédures nécessaires pour mettre en œuvre des tests à distance.

– Définir l'architecture de réseau à utiliser pour les tests à distance.

– Élaborer une méthodologie (un guide) qui étendrait l'expérience actuelle et les méthodes de test aux réseaux IMT-2020.

– Définir la méthodologie permettant de tester des dispositifs IMT‑2020.

– Déterminer la méthodologie permettant de tester les services qui nécessitent un temps de réponse ultra‑court.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### M.4 Relations

Recommandations

– Séries Q, Y, H, G, E, I, M, P, X, Z et F

Questions

– Toutes les Questions de la CE 11 de l'UIT-T

Commissions d'études

– CE 13 de l'UIT-T: réseaux futurs (par exemple SDN, NFV), informatique en nuage, réseaux IMT‑2020, apprentissage automatique

– CE 15 de l'UIT-T: technologies de réseau central et de réseau d'accès

– CE 16 de l'UIT-T: services et applications multimédias et cybersanté

– CE 17 de l'UIT-T: langages de test, y compris la notation TTCN-3

– Toutes les autres CE de l'UIT-T qui participent aux activités en matière de conformité et d'interopérabilité, de réseaux IMT‑2020 et ultérieurs et d'apprentissage automatique

– CE 1 et CE 2 de l'UIT-D: centres de tests à distance

– CE 3 de l'UIT‑T: questions de politique générale

– CE 12 de l'UIT-T: paramètres et spécifications de qualité de service

Autres organismes

– ETSI (en particulier ETSI TC INT et ETSI TC NTECH)

– IETF

– IEEE

Grandes orientations du SMSI

– C5, C6

Objectifs de développement durable

– 9

Question N/11

Lutte contre les logiciels de télécommunication/TIC contrefaits
ou ayant subi une altération volontaire

(Suite de la Question 17/11)

### N.1 Motifs

Dans la Résolution 188 (Rév. Dubaï, 2018) de l'UIT, la Conférence de plénipotentiaires a reconnu que les dispositifs de télécommunication/TIC de contrefaçon avaient des incidences néfastes pour les gouvernements, les constructeurs, les fournisseurs et les consommateurs, et elle s'est déclarée consciente du fait que l'altération volontaire de ces dispositifs risquait de limiter l'efficacité des solutions adoptées par les pays pour lutter contre la contrefaçon. Elle a donc invité les États Membres à prendre toutes les mesures nécessaires pour lutter contre la contrefaçon de dispositifs de télécommunication/TIC.

Parallèlement, dans sa Résolution 96 (Hammamet, 2016), l'Assemblée mondiale de normalisation des télécommunications a reconnu que les dispositifs de télécommunication/TIC de contrefaçon ou ayant subi une altération volontaire pouvaient avoir des incidences néfastes sur la sécurité et le respect de la vie privée des utilisateurs, ainsi que pour les gouvernements, les constructeurs, les fournisseurs, les opérateurs et les consommateurs, en termes de perte de recettes, de dégradation de l'image de marque ou des droits de propriété intellectuelle et de la réputation, ou encore de perturbations des réseaux.

En outre, dans la Résolution 189 (Rév. Dubaï, 2018) de l'UIT sur la lutte contre le vol de dispositifs mobiles, la Conférence de plénipotentiaires a reconnu que le vol de ces dispositifs pouvait avoir des conséquences préjudiciables sur les données des utilisateurs ainsi que sur leur sentiment de sécurité et de confiance dans l'utilisation des technologies de l'information et de la communication (TIC). Elle a pris la résolution d'envisager et d'encourager l'élaboration de méthodes permettant de poursuivre la lutte et d'employer des moyens de dissuasion contre le vol de dispositifs mobiles, et elle a invité les États Membres à prendre les mesures nécessaires pour prévenir, mettre en évidence et limiter l'altération volontaire et la duplication des identifiants de dispositifs TIC mobiles.

Dans sa Résolution 97 (Hammamet, 2016), l'Assemblée mondiale de normalisation des télécommunications a reconnu que le vol de dispositifs mobiles appartenant à des utilisateurs pouvait conduire à une utilisation à des fins délictueuses des services et des applications de télécommunication/TIC et entraîner ainsi des pertes économiques pour le propriétaire et utilisateur légitime. Elle a affirmé qu'il était nécessaire de recenser les mesures techniques existantes et futures, tant du point de vue des logiciels que du matériel, propres à limiter les conséquences de l'utilisation de dispositifs mobiles volés.

La CE 11 de l'UIT-T a reçu des contributions de la part d'États membres de l'UIT et de Membres du Secteur qui ont conduit à l'approbation de la Recommandation UIT‑T Q.5050, intitulée "Cadre pour des solutions permettant de lutter contre la contrefaçon de dispositifs TIC", et de la Recommandation UIT‑T Q.5051, intitulée "Cadre pour la lutte contre l'utilisation de dispositifs mobiles volés". Par ailleurs, un certain nombre de nouveaux sujets d'étude ont été acceptés.

D'autre part, certaines contributions portaient sur la nécessité d'examiner de nouveaux scénarios, notamment les suivants:

i) L'altération volontaire du logiciel pilotant des dispositifs mobiles volés pour accéder sans autorisation aux données de l'utilisateur, avec toutes les conséquences que cela entraîne.

ii) Les dispositifs de réseau (par exemple des routeurs ou des commutateurs) contrefaits ou altérés pour donner accès de manière cachée au réseau de l'utilisateur et permettre de voler des données, ce qui entraîne des pertes de revenus.

iii) Les récepteurs de télévision payante dont le logiciel a été contrefait ou altéré pour permettre à des personnes n'ayant pas payé l'abonnement d'accéder sans autorisation aux données du fournisseur de contenu.

Il n'existe pas de solution simple à ce problème, car en général l'utilisateur d'équipements de télécommunication/TIC n'est pas conscient des vulnérabilités des dispositifs contrefaits ou du logiciel contrefait ou altéré. Il est donc essentiel de sensibiliser toutes les parties prenantes à cette question.

C'est pourquoi il est prévu d'étudier, au titre de la présente Question, les possibilités réelles de lutter contre les logiciels TIC contrefaits ou altérés. Une coopération entre les commissions d'études de l'UIT-T, entre l'UIT-T et l'UIT-D, ainsi qu'avec des organismes extérieurs à l'UIT (en particulier des organismes de normalisation) sera nécessaire pour obtenir des informations complètes sur le sujet et bien le comprendre, et il sera en particulier nécessaire d'organiser des séminaires ou ateliers en collaboration avec les parties prenantes. Une coordination entre les organisations concernées est également nécessaire à cette fin.

### N.2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels sont les effets néfastes, pour les parties prenantes, de l'emploi d'équipements de télécommunication/TIC contrefaits ou altérés ou de logiciels contrefaits ou altérés, et du détournement de données qui en résulte?

– Quel type d'effets néfastes l'emploi d'équipements de télécommunication/TIC contrefaits ou altérés ou d'équipements normaux mais dont le logiciel a été contrefait ou altéré pourrait avoir sur les parties prenantes (par exemple les utilisateurs et les fournisseurs de services), notamment au regard du détournement de données qui en résulte?

– Quels rapports techniques et lignes directrices sont nécessaires pour sensibiliser au problème d'altération des logiciels d'équipements de télécommunication/TIC ou de détournement de données de télécommunication/TIC et aux problèmes qui en résultent?

– Quels types de recommandations, suppléments, rapports techniques et lignes directrices devraient être élaborés pour aider les Membres de l'UIT, en coopération avec le Secteur de l'UIT‑D, à lutter contre la contrefaçon ou l'altération de logiciels d'équipements de télécommunication/TIC et le détournement de données, ainsi que contre les problèmes qui en résultent?

– Quels types de recommandations, suppléments, rapports techniques et lignes directrices devraient être élaborés pour faire diminuer le phénomène de détournement de données, notamment à l'égard des données stockées dans des équipements TIC et dans les contenus acheminés par les fournisseurs de services TIC?

– Quelles technologies et solutions peuvent être employées pour lutter contre la contrefaçon ou l'altération de logiciels d'équipements de télécommunication/TIC et contre les problèmes qui en résultent?

– Les systèmes d'évaluation de la conformité peuvent-ils être employés dans la lutte contre la contrefaçon ou l'altération de logiciels TIC?

### N.3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Étudier les effets néfastes, pour les parties prenantes, de l'emploi d'équipements de télécommunication/TIC contrefaits ou altérés ou de logiciels contrefaits ou altérés, et du détournement de données qui en résulte.

– Étudier les technologies et solutions pertinentes et appropriées pouvant être employées dans la lutte contre la contrefaçon ou l'altération de logiciels TIC et le détournement de données et d'autres conséquences néfastes qui en résultent.

– Élaborer des recommandations, suppléments, rapports techniques et lignes directrices pour aider les Membres de l'UIT, en coopération avec le Secteur de l'UIT‑D, à lutter contre la contrefaçon ou l'altération de logiciels TIC et le détournement de données, et contre les problèmes qui en résultent.

– Organiser des ateliers et des manifestations dans les régions de l'UIT, en coopération avec le Secteur de l'UIT-D, pour promouvoir les travaux de l'UIT-T dans ce domaine et impliquer les parties prenantes.

– Étudier les éventuels systèmes d'évaluation de la conformité pouvant être employés dans la lutte contre la contrefaçon ou l'altération de logiciels TIC et le détournement de données, compte tenu des activités de la CASC de l'UIT‑T.

– Étudier les résultats obtenus par divers organismes de normalisation internationaux et élaborer des spécifications techniques pour alimenter les travaux de normalisation menés au titre de la Question.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 11 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### N.4 Relations

Résolutions

– Résolution 188 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires intitulée "Lutter contre la contrefaçon de dispositifs de télécommunication fondés sur les technologies de l'information et de la communication".

– Résolution 189 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires intitulée "Aider les États Membres à lutter contre le vol de dispositifs mobiles et à prévenir ce phénomène".

– Résolution 96 de l'AMNT (Rév. Hammamet, 2016) intitulée "Études du Secteur de la normalisation des télécommunications de l'UIT visant à lutter contre la contrefaçon des dispositifs de télécommunication/technologies de l'information et de la communication".

– Résolution 97 de l'AMNT (Rév. Hammamet, 2016) intitulée "Lutter contre le vol de dispositifs de télécommunication mobiles".

Recommandations

– UIT-T X.1127, UIT-T Q.5050, UIT-T Q.5051

Questions

– Toutes les Questions de la CE 11, en particulier celles relatives aux commandes, aux architectures de signalisation, aux protocoles, aux tests de conformité et d'interopérabilité et à la lutte contre la contrefaçon et le vol de TIC

Commissions d'études

– CE 2 de l'UIT-T

– CE 3 de l'UIT-T

– CE 9 de l'UIT-T

– CE 13 de l'UIT-T

– CE 16 de l'UIT-T

– CE 17 de l'UIT-T

– CE 20 de l'UIT-T

– CE 1 et CE 2 de l'UIT-D

Autres organismes

– ETSI

– CEI

– IEEE

– IETF

– ISO/CEI JTC 1

Grandes orientations du SMSI

– C2, C5, C9, C11

Objectifs de développement durable

– 9

\_\_\_\_\_\_\_\_\_\_\_\_\_\_