الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2705
(2013/03)

السلسلة Y: البنية التحتية العالمية للمعلومات وجوانب بروتوكول الإنترنت وشبكات الجيل التالي

شبكات الجيل التالي – الأمـــن

متطلبات الأمن الدنيا للتوصيل البيني لخدمة الاتصالات في حالات الطوارئ (ETS)

التوصيـــة ITU-T Y.2705

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
نوعية الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الأمن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3499-Y.3000
الحوسبة السحابية	Y.3999-Y.3500

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T Y.2705

متطلبات الأمن الدنيا للتوصيل البيني لخدمة الاتصالات في حالات الطوارئ (ETS)

ملخص

خدمة الاتصالات في حالات الطوارئ (ETS) هي عبارة عن خدمة وطنية توفر خدمات اتصالات ذات أولوية للمستعملين المرخص لهم لخدمة الاتصالات في حالات الطوارئ عند وقوع كوارث وفي حالات الطوارئ. وتوفر التوصية ITU-T Y.2705 متطلبات الأمن الدنيا للتوصيل البيني بين شبكات خدمة الاتصالات في حالات الطوارئ. ويتيح هذا الأمر الفرصة لدعم هذه الخدمة بالحماية الأمنية المطلوبة بين مختلف الشبكات الوطنية عبر اتفاقات ثنائية و/أو متعددة الأطراف عند وقوع الكوارث وفي حالات الطوارئ.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2705	2013-03-01	13

المصطلحات الرئيسية

خدمة الاتصالات في حالات الطوارئ (ETS)، وأمن شبكات الجيل التالي والخدمات والقدرات ذات الأولوية.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

خدمة الاتصالات في حالات الطوارئ (ETS) هي عبارة عن خدمة وطنية توفر خدمات اتصالات ذات أولوية للمستعملين المرخص لهم لخدمة الاتصالات في حالات الطوارئ عند وقوع كوارث وفي حالات الطوارئ. ولئن كان تنفيذ خدمة الاتصالات في حالات الطوارئ شأناً وطنياً، فإن الكوارث/الطوارئ تتجاوز أحياناً الحدود الجغرافية، ومن ثم بات من المحتمل أن تُبرم البلدان/الإدارات اتفاقات ثنائية و/أو متعددة الأطراف للربط بين أنظمتها الخاصة بخدمة الاتصالات في حالات الطوارئ. وتتيح هذه الاتفاقات خدمات اتصالات ذات أولوية (بالصوت مثلاً والمراسلة والفيديو والبيانات) تندرج في إطار خدمة الاتصالات في حالات الطوارئ كي تدعمها مختلف الشبكات الوطنية الداخلة في اتفاقات ثنائية و/أو متعددة الأطراف في ظروف الكوارث والطوارئ.

وستعتمد سلامة خدمة الاتصالات في حالات الطوارئ (ETS) وسريتها وتيسّرها وسط الشبكات الوطنية الموصولة بينياً على أمن كل شبكة وطنية مشاركة في الاتصالات من طرف إلى طرف. ولتمكين الشبكات من ضمان أمن خدمات اتصالات الطوارئ من طرف إلى طرف بين مختلف الشبكات الوطنية (أي البلدان/الإدارات)، يلزم تحديد متطلبات للأمن من أجل التوصيل البيني لهذه الخدمات.

التوصيـــة ITU-T Y.2705

متطلبات الأمن الدنيا للتوصيل البيني لخدمة الاتصالات في حالات الطوارئ (ETS)

1 مجال التطبيق

توفر هذه التوصية متطلبات الأمن الدنيا للتوصيل البيني بين شبكات خدمة الاتصالات في حالات الطوارئ. ويشمل نطاق متطلبات الأمن حماية السلامة والسرية والتيسُّر لاتصالات هذه الخدمة عبر الحدود الشبكية (أي بين الشبكات الوطنية المختلفة).

والغرض من هذه التوصية هو توفير الحد الأدنى من متطلبات الأمن التي يُمكِن استخدامها لتسهيل دعم خدمة الاتصالات في حالات الطوارئ عبر الشبكات الموصولة بينياً على نحو مباشر أو غير مباشر.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T E.106] التوصية ITU-T E.106 (2003)، *الخطة الدولية لأولويات الطوارئ (IEPS) الخاصة بعمليات الإغاثة في حالات الكوارث.*

[ITU-T E.107] التوصية ITU-T E.107 (2007)، *خدمة اتصالات الطوارئ (ETS) وإطار التوصيل البيني للتطبيقات الوطنية للخدمة ETS.*

[ITU-T M.3342] التوصية ITU-T M.3342 (2006)، *مبادئ توجيهية لتعريف نماذج تمثيل اتفاق سوية الخدمة SLA.*

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2010)، *المتطلبات الوظيفية ومعمارية شبكات الجيل التالي.*

[ITU-T Y.2205] التوصية ITU-T Y.2205 (2011)، *شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية.*

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تعرِّف هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 التخويل [b-ITU-T X.800]: منح حقوق النفاذ، التي تشمل منح النفاذ بناءً على حقوق النفاذ.

2.1.3 التيسُّر [b-ITU-T X.800]: خاصية كون الشيء قابلاً للنفاذ والاستخدام بناءً على طلب من كيان مُخَوّل.

3.1.3 السرية [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مخولين أو لكيانات، أو عمليات غير مُخَوَّلَة.

4.1.3 سلامة البيانات [b-ITU-T X.800]: هي خاصية أن البيانات لم يطرأ عليها تغيير أو تدمير بصورة غير مخولة.

5.1.3 خدمة الاتصالات في حالات الطوارئ (ETS) [ITU-T E.107]: هي خدمة وطنية توفر للمستعملين المخوّلين أولوية الاتصالات إلى خدمة اتصالات الطوارئ في أوقات الكوارث وحالات الطوارئ.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلح التالي:

1.2.3 مقدم الخدمة: مقدم الخدمة هو مقدم لخدمة اتصالات عمومية مخول لتقديم خدمة الاتصالات في حالات الطوارئ (ETS).

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

ANI السطح البيني لشبكة التطبيق (*Application Network Interface*)

CVE مواطِن الضعف والتعرّض الشائعة (*Common Vulnerabilities and Exposures*)

CVE موطِن الضعف والتعرّض الشائع (*Common Vulnerability and Exposure*)

CVSS نظام تقييم مواطن الضعف الشائعة (*Common Vulnerability Scoring System*)

CWE تعداد مواطن الضعف الشائعة (*Common Weakness Enumeration*)

CYBEX تبادل معلومات الأمن السيبراني (*Cyber Security Information Exchange*)

DDoS الحرمان من الخدمة الموزع (*Distributed Denial of Service*)

DNS مخدّم اسم الميدان (*Domain Name Server*)

DoS الحرمان من الخدمة (*Denial of Service*)

DSCP نقطة شفرة الخدمات المتفاضلة (*Diffserv Code Point*)

ETS خدمة الاتصالات في حالة الطوارئ (*Emergency Telecommunications Service*)

IDS نظام كشف دخول الدخلاء (*Intrusion Detection system*)

IEPS الخطة الدولية لأولويات الطوارئ (*International Emergency Preference Scheme*)

IP بروتوكول الإنترنت (*Internet Protocol*)

IPS نظام منع دخول الدخلاء (*Intrusion prevention system*)

IPsec أمن بروتوكول الإنترنت (*IP Security*)

LAN شبكة محلية (*Local Area Network*)

NE عنصر شبكة *(Network Element)*

NGN شبكة الجيل التالي (*Next Generation Network*)

NNI سطح التماس بين شبكة وأخرى (*Network-Network Interface*)

PII المعلومات المحددة لهوية شخص (*Personally Identifiable Information*)

PSTN الشبكة الهاتفية العمومية التبديلية (*Public Switch Telephone Network*)

QoS جودة الخدمة (*Quality of Service*)

SLA اتفاق مستوى الخدمة (*Service Level Agreement*)

SNI السطح البيني لشبكة الخدمة (*Service Network Interface*)

UNI السطح البيني لشبكة المستخدم (*User Network Interface*)

5 الاصطلاحات

في هذه التوصية:

تكتب الحروف الأولى من المصطلح (Service Provider) بالخط الكبير في هذه التوصية لأن "مورد خدمة" هنا يشير إلى مورد خدمة اتصالات عمومية مخول بتقديم خدمة الاتصالات في حالات الطوارئ (ETS) (انظر القسم 1.2.3).

تُشير العبارات الرئيسية "يلزم"، متطلب يجب التقيّد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه التوصية.

والعبارة الرئيسية "يوصي بـ" تشير إلى مطلب "مُوصى به" وإن كانت ليست ضرورية بصورة مطلقة. وهكذا لا يتطلب الأمر وجود هذا الشرط لزعم المطابقة.

والعبارة الرئيسية "يحظر على" تشير إلى اشتراط يجب الالتزام الصارم به وعدم السماح بالحيد عنه وذلك لزعم التطابق مع هذه التوصية.

والعبارة الرئيسية "يمكن اختيارياً" تشير إلى مطلب اختياري مسموح به دون أن ينطوي بأي معنى على أنه موصى به. وليس المقصود من هذا المصطلح أن يشير ضمناً إلى أن تنفيذ المورّد يجب أن يوفر هذا الخيار، كما يمكن لهذه الخاصية أن تُفعَّل اختيارياً من جانب مُشغّل الشبكة/مقدم الخدمات. بل يعني أن المورد قد يختار إتاحة هذه الخاصية ويظل مع ذلك يزعم التطابق مع هذه المواصفة.

وفي متن هذه التوصية وملحقاتها، تصادف أحياناً عبارات "يتعين" و"يتعين ألا" و"ينبغي" و"يمكن"، وينبغي تأويلها لتفيد بالمعاني الآتية على التوالي: "يتعين" و"يحظر" و"يوصى" و"من الجائز". وإذ تظهر مثل هذه العبارات أو المصطلحات الرئيسية في تذييل أو في مادة محددة صراحة على أنها "إعلامية"، تفسَّر على أنه ليس وراءها أي قصد معياري.

6 التهديدات والمخاطر الأمنية

قد تُستهدف الاتصالات في حالة الطوارئ (ETS) بهجمات تُخلّ بالأمن السيبراني بسبب الطبيعة الحرجة لهذه الاتصالات. يُرجى الرجوع إلى التوصيات [ITU–T E.107] و[ITU–T Y.2205] و[ITU–T Sup57 b–] للاطلاع على تعريف الاتصالات في حالة الطوارئ ومعلومات عنها. والتهديدات أو الأعمال المؤذية الساعية لتعطيل خدمة الاتصالات في حالة الطوارئ أو إساءة استخدامها أو التلاعب بها أو إلحاق الضرر بها خلاف ذلك قد تأتي من مجموعة متنوعة من المصادر، بما فيها الشبكات الموصولة بينياً. فعلى سبيل المثال، قد تُستهدف الاتصالات في حالة الطوارئ بهجمات تُخل بالأمن السيبراني لأسباب من قبيل:

- تعطيل قدرة طواقم التعافي من الكوارث على التواصل
- الحصول على معلومات حساسة عن طريق التنصت على مكالمات/دورات خدمة الاتصالات في حالة الطوارئ (ETS).

ويُنظر إلى تهديد كثغرة أمنية أو نقطة ضعف محتملة إذا كان استغلاله يؤثر سلباً على تيسر الاتصالات في حالة الطوارئ أو على سلامتها أو سريتها.

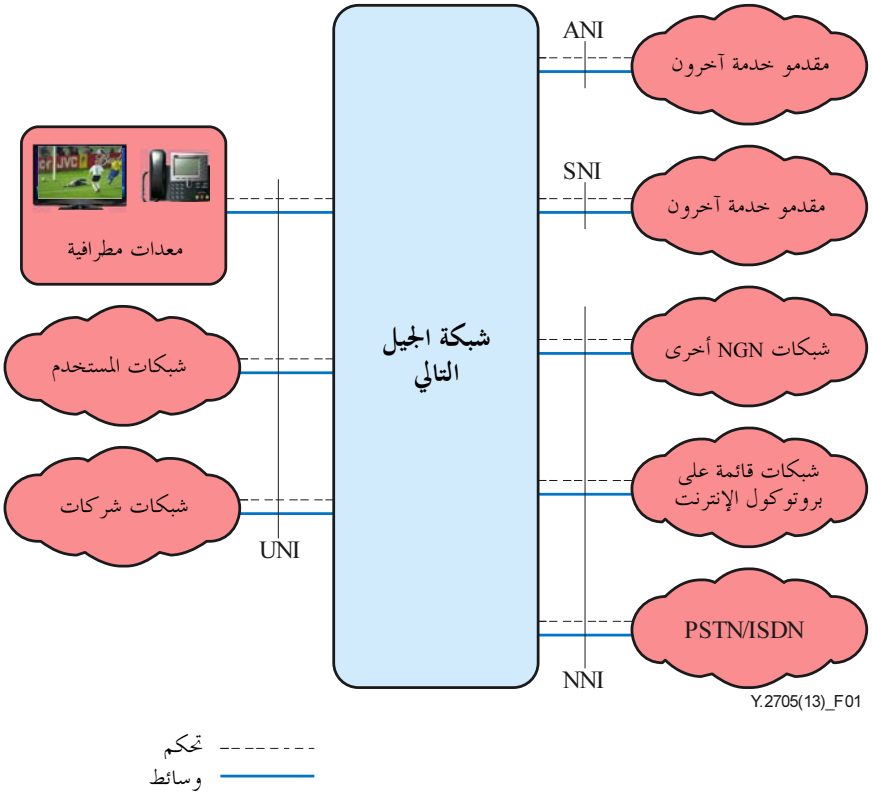
وتركز هذه التوصية أساساً على التهديدات المتعلقة بالتوصيل البيني لشبكات خدمة الاتصالات في حالة الطوارئ (ETS). وعلى سبيل المثال لا الحصر، تشمل التهديدات المتعلقة بالتوصيل البيني للشبكات ما يلي:

- تهديد عام من التوصيل البيني: ثغرات أمنية أو مواطن ضعف محتملة ترتبط بتوصيل الشبكة (مثل شبكة الجيل التالي) مع غيرها من الشبكات المدارة وغير المدارة، مثل شبكة الإنترنت العامة.
- تهديد مرده التصميم والتنفيذ: ثغرات أمنية أو مواطن ضعف محتملة في معمارية التوصيل البيني للشبكات وتصاميم التنفيذ.
- تهديد من الإدارة والتشغيل ومن الداخل: ثغرات أمنية أو مواطن ضعف محتملة في وظائف القيادة والسيطرة لخدمة الاتصالات في حالة الطوارئ (ETS) وبنيتها التحتية الأساسية.

- تهديد من النقل والمرافق: ثغرات أمنية أو مواطن ضعف محتملة ترتبط بشبكة النقل الأساسية (على سبيل المثال، التسيير، استنساخ الشبكة، التنوع والمرونة)، ونظم الدعم (على سبيل المثال، الطاقة والبيئة)، والحماية المادية لموجودات الشبكة.

7 المعمارية المرجعية لأمن التوصيل البيني لخدمة الاتصالات في حالة الطوارئ (ETS)

تعتمد هذه التوصية على نموذج المعمارية الوظيفية وتوصيلية الشبكة المحدد في التوصية [ITU–T Y.2012].



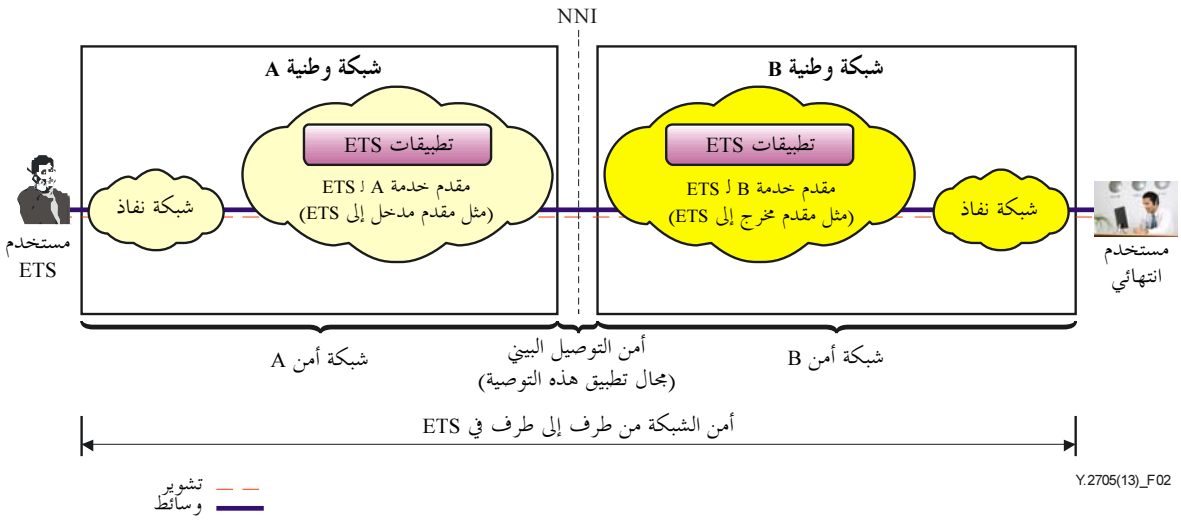
الشكل 1 – التوصيلية مع شبكة الجيل التالي [ITU–T Y.2012]

إن السطوح البينية ذات الصلة بالتوصيلات البينية هي التالية:

- السطح البيني لشبكة التطبيق (ANI)
- السطح البيني لشبكة الخدمة (SNI)
- سطح التماس بين شبكة وأخرى (NNI).

يرجى الرجوع إلى التوصية [ITU-T Y.2012] للاطلاع على أوصاف السطوح البينية ANI وSNI وNNI.

للسماح للشبكات المختلفة بدعم خدمة الاتصالات في حالة الطوارئ (ETS) عبر حدود الشبكة، هناك حاجة إلى إجراءات أمنية محددة لحماية سلامة خدمة الاتصالات في حالات الطوارئ وسريتها وتيسُّرها ضمن كل شبكة وطنية وعبر التوصيل البيني للشبكات الوطنية.



الشكل 2 – أمن الشبكة من طرف إلى طرف في تطبيقات خدمة الاتصالات في حالة الطوارئ (ETS)

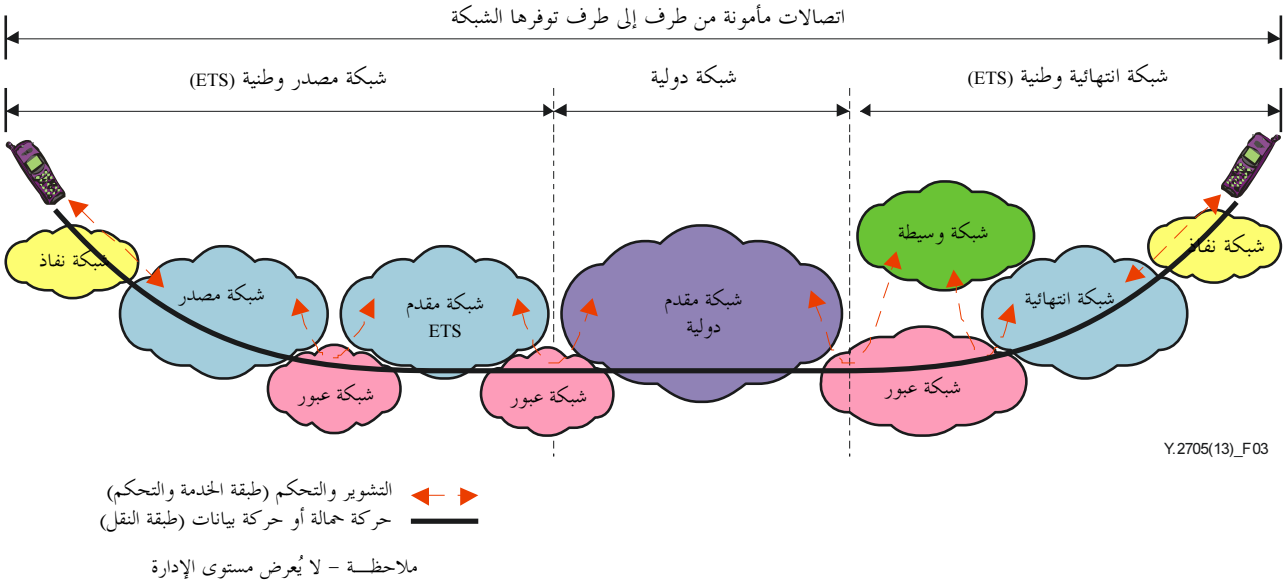
يبين الشكل 2 أن الأمن من طرف إلى طرف لخدمة الاتصالات في حالة الطوارئ (ETS) العابرة لشبكات متعددة (للشبكتين الوطنيتين A وB) سوف يعتمد على تدابير الأمن المتخذة في فُرادى الشبكات وعلى الحماية الأمنية للتوصيل البيني لشبكتين.

ويبين الشكل 2 أن تركيز هذه التوصية ينصبُّ على تأمين التوصيل البيني لخدمة الاتصالات في حالة الطوارئ.

8 أهداف الأمن ومبادئه التوجيهية في التوصيل البيني لخدمة الاتصالات في حالة الطوارئ

1.8 الأهداف العامة

يتمثل الهدف العام في توفير شبكة حماية الأمن من طرف إلى طرف لخدمة الاتصالات في حالة الطوارئ (ETS) التي يمكن أن تعبر ميادين الشبكات الوطنية والدولية (أي البلدان/الإدارات) لمورّدي شبكة مختلفين، وحيث كل شبكة مسؤولة عن الأمن داخل الميدان الخاص بها على أساس كل قفزة على حدة.



الشكل 3 – مثال اتصال من طرف إلى طرف عبر حالات تنفيذ وطنية مختلفة لخدمة الاتصالات في حالة الطوارئ (ETS)

يبيّن الشكل 3 خدمة اتصالات في حالة الطوارئ (ETS) من طرف إلى طرف (مثل الاتصالات ذات الأولوية عبر الصوت أو الفيديو أو البيانات أو الرسائل) تصدر وتنتهي في شبكتين وطنيتين مختلفتين. ويوضح المثال أن الاتصالات ذات الأولوية في حالة الطوارئ من طرف إلى طرف يمكن أن تعبر العديد من مقاطع الشبكة والميادين الإدارية (مثل شبكة النفاذ وشبكة المصدر وشبكة مقدم خدمة الاتصالات في حالة الطوارئ وشبكة الموردين الدوليين والشبكة الوسيطة والشبكة الانتهائية). والهدف العام هو لكل شبكة موصولة بينياً على طول مسير الاتصالات في حالة الطوارئ من طرف إلى طرف هو توفير الحماية الأمنية اللازمة داخل الميدان الخاص بها بما في ذلك التوصيل البيني بالشبكة المجاورة بحيث لا تُمس سلامة خدمة الاتصالات في حالات الطوارئ وسريتها وتيسُّرها من طرف إلى طرف.

2.8 مبادئ توجيهية عامة

ينبغي إرساء مقاربة ومنهجية منظمتين وتنفيذهما بين كل شبكتين موصولتين بينياً في خدمة الاتصالات في حالة الطوارئ (ETS) عن طريق استخدام اتفاقات مستوى الخدمة (SLA). وينبغي أن يشمل ذلك ما يلي:

1) تقييم المخاطر الأمنية: تقييم المخاطر التي تتهدد موجودات خدمة الاتصالات في حالة الطوارئ (ETS)، وتحليل التهديدات ونقاط الضعف المتعلقة بالتوصيل البيني لخدمة الاتصالات في حالة الطوارئ. فمن الأهمية بمكان أن يجري تقييم المخاطر الأمنية بشكل دوري، وعند إدخال التغييرات، والجديد من التكنولوجيا أو الخدمات أو التطبيقات.

2) معمارية الأمن وحلوله: وضع سياسة أمنية وتصميم معمارية الأمن وتوصيف الحلول للتخفيف من التهديدات المنظورة لخدمة الاتصالات في حالة الطوارئ (ETS). ويشمل ذلك إبرام اتفاقات مستوى الخدمة اللازمة الثنائية أو متعددة الأطراف لتحقيق الأمن (راجع [ITU-T M.3342] و[b-TMF GB917] للحصول على معلومات أوفى عن اتفاقات مستوى الخدمة). وتشمل مجالات المعالجة: السياسات الأمنية والمتطلبات وتصميم المعمارية والوعي الظرفي وأدوات الطب الشرعي، وأمن البنية التحتية ليصار إلى تضمينها في اتفاقات مستوى الخدمة بشأن التوصيل البيني.

3) تنفيذ الأمن: تنفيذ ونشر المعمارية والحلول الأمنية استناداً إلى اتفاقات مستوى الخدمة الثنائية أو متعددة الأطراف، حسب الاقتضاء، لأمن التوصيل البيني لخدمة الاتصالات في حالة الطوارئ.

4) العمليات الأمنية: ينبغي تحديد وتنفيذ التدابير التشغيلية لإدارة الحلول الأمنية للتوصيل البيني لخدمة الاتصالات في حالة الطوارئ. ومثال ذلك: إدارة التهديدات من المطلعين على الشؤون الداخلية، وإدارة المعلمات القابلة للتشكيل، والقيم الافتراضية، والقدرة على التعافي وعمليات تدارك الأعطال، واختبار أمن خدمة الاتصالات في حالة الطوارئ (ETS)، وتسجيل وتدقيق الحوادث ذات الصلة بأمن خدمة الاتصالات في حالة الطوارئ.

3.8 الأهداف والمتطلبات الشائعة

تعرض هذه الفقرة متطلبات وأهداف شائعة.

R–1 على مقدِّم الخدمة حماية الاتصالات في حالة الطوارئ من التدخلات (مثل الالتقاط والاختطاف وإعادة الاستعراض) التي من شأنها أن تمس بصحة خدمة الاتصالات في حالة الطوارئ (ETS) وبسلامتها وسريتها وتيسُّرها، وفقاً للممارسات الأمنية الفضلى المتاحة تجارياً، أثناء مرور حركة هذه الخدمة في ميدان مقدم الخدمة.

وفي المتطلب أعلاه، الميدان هو "مقطع الشبكة" المادي أو المنطقي الذي يمارس فيه مقدم الخدمة السيطرة الإدارية والتشغيلية الكاملة، وكذلك تصريف الأمور والصيانة والأمن.

ويُتوقع أن يدعم مقدمو الخدمة مجموعة واسعة من الأدوات والقدرات الأمنية ويستخدموها لحماية خدمة الاتصالات في حالة الطوارئ والشبكة بالكامل وجميع التطبيقات المدعومة. ومن المهم أن تُتّخذ التدابير المناسبة لضمان ألا يؤثر استخدام هذه القدرات الأمنية سلباً على أداء خدمة الاتصالات في حالة الطوارئ وألا يتسبَّب بأي إخلال أمني غير مقصود بهذه الخدمة.

R–2 يتعين ألا يتداخل استخدام مقدِّم الخدمة للآليات الأمنية (مثل نظام لكشف التسلل ونظام منعه [IDS/IPS] والتجفير) مع آليات المعاملة ذات الأولوية المستخدمة لدعم خدمة الاتصالات في حالة الطوارئ (ETS) (يرجى الرجوع إلى [ITU-T Y.2205] للاطلاع على تعريف ووصف آليات المعاملة ذات الأولوية).

O–1 يُستحسن أن يشمل استخدام مقدم الخدمة لأدوات وقدرات الأمن، التدابير المناسبة لتقليل الآثار السلبية على جودة خدمة الاتصالات (QoS) في حالة الطوارئ (عن طريق التسبب بتأخير لا داعي له، على سبيل المثال).

4.8 الاستيقان في خدمة الاتصالات في حالة الطوارئ وتخويلها والتحكم في النفاذ إليها

تشمل هذه الفقرة ما يلي:

- الاستيقان من مستخدمي خدمة الاتصالات في حالة الطوارئ وتخويلهم
- استيقان مستخدمي خدمة الاتصالات في حالة الطوارئ من مقدمي هذه الخدمة وتخويلهم
- الاستيقان من مصادر البيانات في خدمة الاتصالات في حالة الطوارئ
- الاستيقان والتخويل المتبادل بين مقدمي خدمة الاتصالات في حالة الطوارئ.

1.4.8 الاستيقان المتبادل

الاستيقان هو عملية التحقق من هوية طرف يشارك في شكل ما من أشكال الاتصال. ويضمن الاستيقان صلاحية الهوية المزعومة للكيانات المشاركة في الاتصالات (مثل شخص أو جهاز أو خدمة أو تطبيق) ويضمن بأن أي كيان لا يحاول التنكر في غير هويته الحقيقية أو استظهار اتصال سابق دون تخويل.

إن خدمة الاتصالات في حالة الطوارئ (ETS) من طرف إلى طرف يمكن أن تنطوي على العديد من مقاطع الشبكة والميادين الإدارية (مثل شبكة المصدر وشبكة النفاذ وشبكة مقدم خدمة الاتصالات في حالة الطوارئ والشبكة الوسيطة وشبكة النفاذ الانتهائية). وعند تلقي حركة خدمة الاتصالات في حالة الطوارئ، يُلزم مقدم الخدمة بالتحقق من صحة المصدر وتخويله (شبكة مثلاً) من الحركة الواردة. وعند تسليم حركة خدمة الاتصالات في حالة الطوارئ، يُلزم مقدم الخدمة بالتحقق من صحة وتخويل الكيان الذي يسلمه حركة شبكة الجيل التالي (شبكة مثلاً). وفي الوقت الحاضر، لا يمكن التحقق من علاقات الثقة الأمنية للتوصيل البيني إلا من خلال التوصيل البيني المادي المباشر بين اثنتين من الشبكات الموصولة بينياً.

R–3 يتعين على مقدمي الخدمة أن يستيقنوا من بعضهم بعضاً لتبادل (أي تسليم أو استلام) حركة خدمة الاتصالات في حالة الطوارئ (ETS). وهذا يشمل أي حركة تبادل تشوير أو وسائط لتلك الخدمة بين مقدمي خدمة عبر السطوح البينية NNI أو ANI أو SNI.

ويمكن تحقيق ذلك من خلال التحقق من التوصيل البيني المادي المباشر واتفاقات مستوى الخدمة (SLA).

ملاحظـــة – ليس القصد هنا الاستيقان من كل مكالمة/دورة، بل القصد هو التعريف بمفهوم آليات تقوم بالاستيقان حسب الحاجة أو بشكل دوري.

2.4.8 التحكّم في النفاذ

تدعو الضرورة لتدابير التحكم في النفاذ للحماية ضد استخدام موارد الشبكة دون تخويل، بما في ذلك استخدام الموارد بطريقة غير مخوّل بها. ويضمن التحكم في النفاذ أن يقتصر النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات على المخوَّل له بذلك من الأشخاص أو الأجهزة.

ويشير التحكم في النفاذ عند سطح التماس بين شبكة وأخرى (NNI) إلى قدرة الشبكة المتلقية على قبول أو رفض حركة واردة محددة من شبكة مجاورة وتقييد نفاذ الكيانات خارج الشبكة إلى الموارد ضمن الشبكة.

R–4 يتعين على مقدم الخدمة وضع قواعد وإنفاذ تدابير التحكم في النفاذ للحماية من الاتصالات غير المخولة في حالة الطوارئ عبر سطوح التماس بين شبكة وأخرى. وعلى وجه التحديد، ينبغي لمقدمي الخدمة ألا يسمحوا بعبور

الاتصالات لسطح التماس بين شبكة وأخرى إلا لتلك التي تجريها كيانات الشبكة (NEs) ذات الهوية المحددة والتخويل المسبق (من خلال اتفاقيات مستوى الخدمة مثلاً).

R–5 عند تلقي حركة تشوير خدمة الاتصالات في حالة الطوارئ (ETS) من مقدم خدمة آخر، يتعين على مقدم الخدمة التحقق من علاقات الثقة بينه وبين مقدم الخدمة الذي يتلقى منه الحركة.

R–6 عند تلقي حركة وسائط خدمة الاتصالات في حالة الطوارئ (ETS) من مقدم خدمة آخر، يتعين على مقدم الخدمة التحقق من علاقات الثقة بينه وبين مقدم الخدمة الذي يتلقى منه الحركة.

R–7 عند تسليم حركة تشوير خدمة الاتصالات في حالة الطوارئ (ETS) إلى مقدم خدمة آخر، يتعين على مقدم الخدمة التحقق من علاقات الثقة بينه وبين مقدم الخدمة الذي يسلمه الحركة.

R–8 عند تسليم حركة وسائط خدمة الاتصالات في حالة الطوارئ (ETS) إلى مقدم خدمة آخر، يتعين على مقدم الخدمة التحقق من علاقات الثقة بينه وبين مقدم الخدمة الذي يسلمه الحركة.

ملاحظـــة – ليس القصد الضمني مما ورد أعلاه أن يجري التحقق من كل مكالمة/دورة.

التخويل هو منح امتيازات تشمل منح النفاذ استناداً إلى امتيازات النفاذ. ويُمنح التخويل إلى كيان ما، بعد التحقق بواسطة عملية استيقان وتحكم في النفاذ.

R–9 إن مقدم الخدمة مُلزَم بتوفير الحماية الأمنية لمنع النفاذ غير المخول إلى خدمة الاتصالات في حالة الطوارئ.

وتشمل الوسائل التي يمكن بها تحقيق المتطلَب R–9، على سبيل المثال لا الحصر، الوسائل التالية (حسب الاقتضاء):

- الاستيقان من المستخدمين النهائيين والمعدات في الاتصالات في حالة الطوارئ وتخويلهم
- الاستيقان من مصادر البيانات في الاتصالات في حالة الطوارئ وتخويلها (مصدر الرسالة أو مصدر البيانات، على سبيل المثال)
- القدرات الأمنية للحماية من النفاذ غير المخول به إلى معلومات وموارد خدمة الاتصالات في حالة الطوارئ (على سبيل المثال، معلومات المستخدم في مخدمات الاستيقان ونظم الإدارة).

وينطوي التحكم في النفاذ إلى النظام على تدابير أمنية لمنع النفاذ غير المخول به إلى عناصر الشبكة وأنظمتها ونقاط النفاذ المرتبطة بها. وهناك تهديدات ترتبط بالنفاذ غير المخول به إلى عناصر الشبكة وأنظمتها الداعمة لخدمة الاتصالات في حالة الطوارئ (ETS). ولذلك، يجب وضع تدابير مناسبة للتحكم في النفاذ ومنع النفاذ غير المخول به، ويجب إنفاذها.

R–10 يتعين على مقدمي الخدمة وضع قواعد وإنفاذ تدابير التحكم في النفاذ لمنع النفاذ غير المخول به إلى عناصر الشبكة وأنظمتها الداعمة لخدمة الاتصالات في حالة الطوارئ. وهذا يشمل الحماية الأمنية للنفاذ المنطقي والمادي.

R–11 يتعين على مقدمي الخدمة الحماية من النفاذ غير المخول به إلى بيانات وموارد خدمة الاتصالات في حالة الطوارئ (أي يتعين على مقدم الخدمة ألا يسمح إلا للجهات الإدارية المخولة بالنفاذ إلى بيانات ETS ومواردها [مثل الملفات وأجهزة القيادة والبرمجيات] ضمن عناصر الشبكة وأنظمتها الداعمة لهذه الخدمة).

5.8 سلامة خدمة الاتصالات في حالة الطوارئ (ETS)

تشمل هذه الفقرة ما يلي:

- حماية سلامة تشوير خدمة الاتصالات في حالة الطوارئ
- حماية سلامة وسائط خدمة الاتصالات في حالة الطوارئ.

1.5.8 سلامة التشوير

يجب حماية تشوير الاتصالات في حالة الطوارئ بين الشبكات من الالتقاط والإفساد والتلاعب (من قبيل الحذف أو الإنشاء أو إعادة الاستعراض).

R–12 يتعين على مقدمي الخدمة حماية سلامة كل حركة تشوير اتصالات في حالة الطوارئ العابرة للسطوح البينية NNI وANI وSNI .

وتشمل الإجراءات التي يمكن اتخاذها لحماية سلامة حركة تشوير الاتصالات في حالة الطوارئ، على سبيل المثال لا الحصر، ما يلي:

أ) التدابير الأمنية المادية (على سبيل المثال، الحماية المادية لعناصر الشبكة ووسط الإرسال ومرافقه، وإنفاذ التدابير المناسبة للتحكم في النفاذ)

ب) حماية بالتجفير

ج) وضع متطلبات السلامة المناسبة والأهداف المحددة لها في اتفاقات مستوى الخدمة، وإنفاذها

د) مراقبة سلامة تشكيلات سطح التماس بين شبكة وأخرى (NNI).

2.5.8 سلامة الوسائط

يجب حماية وسائط الاتصالات في حالة الطوارئ بين الشبكات من الالتقاط والإفساد والتلاعب (من قبيل الحذف أو الإنشاء أو إعادة الاستعراض).

R–13 يتعين على مقدم الخدمة حماية سلامة كل حركة وسائط خدمة الاتصالات في حالة الطوارئ (ETS) العابرة للسطوح البينية NNI أو SNI.

وتشمل الإجراءات التي يمكن اتخاذها لحماية سلامة حركة الوسائط، على سبيل المثال لا الحصر، ما يلي:

أ) التدابير الأمنية المادية (على سبيل المثال، الحماية المادية لعناصر الشبكة ووسط الإرسال ومرافقه، وإنفاذ التدابير المناسبة للتحكم في النفاذ)

ب) حماية بالتجفير

ج) وضع متطلبات السلامة المناسبة والأهداف المحددة لها في اتفاقات مستوى الخدمة، وإنفاذها

د) مراقبة سلامة تشكيلات سطح التماس بين شبكة وأخرى (NNI).

6.8 سرية الاتصالات في حالة الطوارئ وحماية المعلومات المحددة لهوية شخص

يتعين أن توفر الاتصالات في حالة الطوارئ عبر السطوح البينية NNI وANI وSNI حماية السرية لمنع الكيانات غير المخولة من الحصول على معلومات حساسة. وهذا يشمل حماية السرية لما يلي:

- التشوير والتحكم في خدمة الاتصالات في حالة الطوارئ (ETS)
- الحركة الحاملة لخدمة الاتصالات في حالة الطوارئ (على سبيل المثال، الصوت أو الفيديو أو البيانات)
- المعلومات المحددة لهوية شخص (PII).

1.6.8 سرية التشوير

يتعين على مقدمي الخدمة حماية تشوير خدمة الاتصالات في حالة الطوارئ المدعوم عبر السطوح البينية NNI أو ANI أو SNI من النفاذ غير المخول. ويجب أن تحمى معلومات التشوير من التنصت لتقليل فرصة تحليل حركة التشوير الذي يفشي معلومات حساسة يمكن إساءة استخدامها (على سبيل المثال، أنماط الاتصال، ومعلومات عن الموقع، وهوية المستخدمين).

R–14 يتعين على مقدمي الخدمة حماية سرية كل تشوير خدمة الاتصالات في حالة الطوارئ عبر السطوح البينية NNI أو ANI أو SNI.

وتشمل الإجراءات التي يمكن اتخاذها لحماية سرية حركة التشوير والوسائط، على سبيل المثال لا الحصر، ما يلي:

أ) التدابير الأمنية المادية (على سبيل المثال، الحماية المادية لعناصر الشبكة ووسط الإرسال ومرافقه، وإنفاذ التدابير المناسبة للتحكم في النفاذ)

ب) حماية بالتجفير

ج) وضع متطلبات السرية المناسبة والأهداف المحددة لها في اتفاقات مستوى الخدمة، وإنفاذها.

وفيما ترتبط حماية السرية بآليات التجفير في كثير من الأحيان، فليس المقصود ضمناً بالمتطلب الوارد في هذه الفقرة أن الأساليب التجفيرية يجب أن تُستخدم في جميع السيناريوهات أو لجميع انسيابات التشوير من طرف إلى طرف. إنما القصد من هذا المتطلب هو أن مقدمي الخدمة يجب أن يوفروا وينفذوا التدابير اللازمة لضمان حماية اتصالات التشوير عبر السطوح البينية NNI وANI وSNI من التنصّت. وهذا يعني أنه يجب فحص كل توصيل بيني لتحديد الآليات المناسبة للاستخدام لتوفير حماية السرية، على النحو الذي تمليه سياسة الأمن. على سبيل المثال، قد يتسنى توفير حماية السرية من خلال استخدام عملية مادية وما يرتبط بها، حسب التشكيلات المعمارية والمادية للتوصيل البيني وفق بروتوكول الإنترنت (سيناريو الوصلة المادية المخصصة مثلاً).

2.6.8 سرية الوسائط

يجب حماية تدفقات الوسائط (على سبيل المثال، الصوت والفيديو والبيانات) من النفاذ غير المخول لأن التنصّت على تدفقات وسائط خدمة الاتصالات في حالة الطوارئ (ETS) يمكن أن يفشي تكشّف معلومات أمنية حساسة (أي منقولة في اتصالات الوسائط).

R–15 يتعيّن على مقدم الخدمة حماية سرية كل حركة وسائط خدمة الاتصالات في حالة الطوارئ (ETS) العابرة للسطوح البينية NNI أو SNI.

وتشمل الإجراءات التي يمكن اتخاذها لحماية سرية حركة الوسائط، على سبيل المثال لا الحصر، ما يلي:

أ) التدابير الأمنية المادية (على سبيل المثال، الحماية المادية لعناصر الشبكة ووسط الإرسال ومرافقه، وإنفاذ التدابير المناسبة للتحكم في النفاذ)؛

ب) حماية بالتجفير؛

ج) وضع متطلبات السرية المناسبة والأهداف المحددة لها في اتفاقات مستوى الخدمة، وإنفاذها.

3.6.8 حماية المعلومات المحددة لهوية شخص (PII)

يجب حماية المعلومات المحددة لهوية شخص (PII) المرتبطة بخدمة الاتصالات في حالة الطوارئ (ETS) من الرصد أو الكشف غير المخول بهما (على سبيل المثال، هويات المستخدم النهائي لخدمة الاتصالات في حالة الطوارئ، وهويات الكيانات التي تجري اتصالات فيما بينها، ومعلومات الاشتراك بهذه الخدمة وموقع المستخدم النهائي لها).

R–16 يتعين على مقدم الخدمة السماح لفئة مختارة من مستخدمي خدمة الاتصالات في حالة الطوارئ باستخدام هذه الخدمة مع إغفال هوياتهم.

R–17 يتعين على مقدم الخدمة حماية سرية هويات فئة مختارة من مستخدمي خدمة الاتصالات في حالة الطوارئ.

R–18 يتعين على مقدم الخدمة حماية سرية موقع فئة مختارة من مستخدمي خدمة الاتصالات في حالة الطوارئ.

وهناك حاجة للحماية من الرصد غير المخول به لمعلومات استخدام خدمة الاتصالات في حالة الطوارئ (مثل أنماط الاستخدام كحجم حركة هذه الخدمة والمواقع والوقت والتردد وما إلى ذلك). وهذا يشمل الدعم واستخدام القدرات الأمنية لحماية المعلومات الحساسة المستمدة من رصد أنشطة الشبكة مثل المواقع التي زارها المستخدم النهائي على شبكة الإنترنت وموقعه الجغرافي، وعناوين IP وأسماء مخدّم اسم الميدان (DNS) المسندة إلى الأجهزة في شبكة مقدم الخدمة.

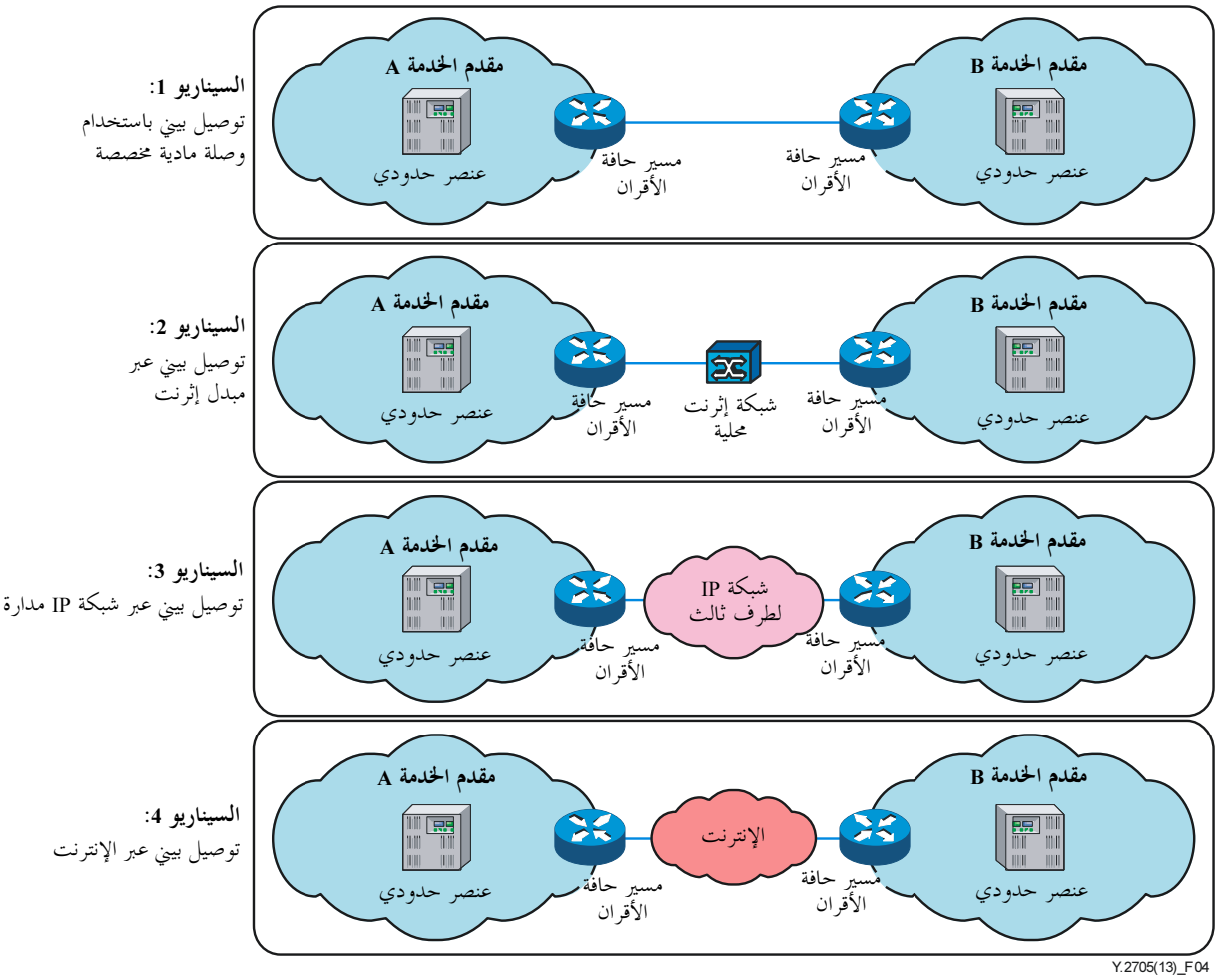
O–2 يُستحسن أن يوفر مقدم الخدمة حماية لمعلومات استخدام خدمة الاتصالات في حالة الطوارئ من الرصد أو الكشف غير المخول بهما (على سبيل المثال، أنشطة الشبكة مثل المواقع التي زارها مستخدم هذه الخدمة على شبكة الإنترنت، أو عناوين IP الخاصة به، أو أنماط الاستخدام كحجم حركة هذه الخدمة والمواقع والوقت والتردد).

7.8 نقل بروتوكول الإنترنت بين الشبكات

1.7.8 اعتبارات عامة

إن التوصيل البيني لمقدمَّي خدمة اثنين وفق بروتوكول الإنترنت (IP) لكليهما سيمتلك اختلافات توصيلية معمارية ومادية تترتب عليها آثار أمنية مختلفة.

وستعتمد سلامة هذا التوصيل البيني وتيسره على عوامل مثل المعمارية والاتصال المادي واتفاقات مستوى الخدمة.



الشكل 4 – تشكيلات التوصيل البيني من بروتوكول الإنترنت (IP) إلى بروتوكول الإنترنت (IP)

يُظهر الشكل 4 مجموعة من التشكيلات المحتملة للتوصيل البيني من بروتوكول الإنترنت (IP) إلى بروتوكول الإنترنت (IP):

1 توصيل بيني باستخدام وصلة مادية مخصصة: في هذه التشكيلة، تُستخدم وصلة مادية مخصصة لتوصيل مسيّر حافة الأقران لمقدم الخدمة A إلى مسيّر حافة الأقران لمقدم الخدمة B.

2 توصيل بيني عبر مبدّل إثرنت: في هذه التشكيلة، يوصل مسيّر حافة الأقران لمقدم الخدمة A بمسيّر حافة الأقران لمقدم الخدمة B عبر مبدّل إثرنت لشبكة محلية (LAN).

3 توصيل بيني عبر شبكة IP مدارة: في هذه التشكيلة، يقام توصيل بيني وفق بروتوكول الإنترنت لمقدم الخدمة A ومقدم الخدمة B عبر شبكة IP مدارة. وقد تكون هذه شبكة IP مدارة لطرف ثالث يقدم الخدمة.

4 توصيل بيني عبر الإنترنت: في هذه التشكيلة، يُقام توصيل بيني وفق بروتوكول الإنترنت لمقدم الخدمة A ومقدم الخدمة B عبر شبكة الإنترنت المفتوحة.

وهناك مدلولات أمنية مختلفة لخدمة الاتصالات في حالة الطوارئ (ETS) لكل من السيناريوهات المبينة في الشكل 4.

ولا توجد شروط أو قيود موضوعة في هذه الوثيقة فيما يتعلق بالتوصيل البيني وفق بروتوكول الإنترنت المستخدم لتوصيل مقدم الخدمة بينياً. والهدف العام هو أنه يتعين على مقدمي الخدمة القيام، بناءً على تشكيلة IP إلى IP محددة، بدعم وتنفيذ التدابير الأمنية المناسبة لحماية التوصيل البيني والحيلولة دون وقوع أي تأثيرات على الخدمات من خلال التنازلات التوفيقية في التوصيل البيني وفق بروتوكول الإنترنت.

R–19 يتعين على مقدم الخدمة حماية شبكة نقل بروتوكول الإنترنت بين شبكتي مقدمي خدمة موصولتين بينياً من التدخلات (مثل الالتقاط والاختطاف وإعادة الاستعراض) التي من شأنها أن تمس بصحة خدمة الاتصالات في حالة الطوارئ (ETS) وبسلامتها وسريتها وتيسرها، وفقاً للممارسات الأمنية الفضلى المتاحة تجارياً.

ولتلبية هذا المتطلب، ينبغي لمقدم الخدمة وضع وإنفاذ قواعد لحماية شبكة نقل بروتوكول الإنترنت بين شبكتي مقدمي خدمة موصولتين بينياً، وتوثيق هذه القواعد في اتفاقات مستوى الخدمة.

R–20 يتعيّن على مقدم الخدمة حماية سلامة آليات أولوية حركة بروتوكول الإنترنت وقدراتها الوظيفية وبيانات البروتوكول المصاحبة (مثل نقاط شفرة Diffserv) المستخدمة لدعم خدمة الاتصالات في حالة الطوارئ عبر التوصيل البيني لشبكة بروتوكول الإنترنت بين مقدمي خدمة.

ملاحظـــة – وهذا يشمل حماية سلامة البيانات المشكِّلة المتعلقة بخدمة الاتصالات في حالة الطوارئ أو المعلمات المتعلقة بالتوصيل البيني وفق بروتوكول الإنترنت وكذلك أي تقابل ينطوي عليه الأمر (على سبيل المثال، نقاط شفرة Diffserv على أساس الخطة المستخدمة في التوصيل البيني لفرادى مقدمي الخدمة).

CR–1 وإذا ما عبر تشوير خدمة الاتصالات في حالة الطوارئ مقطعاً غير موثوق في شبكة نقل بروتوكول الإنترنت (كنقل بروتوكول الإنترنت من خلال طرف ثالث)، يتعين على مقدم الخدمة استخدام التجفير (على سبيل المثال، IPsec) لحماية السلامة والسرية.

CR–2 وإذا ما عبرت وسائط خدمة الاتصالات في حالة الطوارئ مقطعاً غير موثوق في شبكة نقل بروتوكول الإنترنت (كنقل بروتوكول الإنترنت من خلال طرف ثالث)، يتعين على مقدم الخدمة استخدام التجفير (على سبيل المثال، IPsec) لحماية السلامة والسرية.

2.7.8 استخدام التجفير

يتعين ألا يتدخل استخدام آليات أمنية (كالتجفير) أو يحجب المعلومات عن آليات معاملة الأولوية.

وتنطبق المتطلبات التالية عند استخدام أنفاق IPsec لحركة خدمة الاتصالات في حالة الطوارئ بين الشبكات (أي عبر السطوح البينية NNI وANI وSNI):

R–21 يتعيّن على مقدم الخدمة وضع وإنفاذ قواعد لملء وحماية سلامة المعلومات ذات الأولوية (على سبيل المثال، قيم نقطة شفرة الخدمات المتفاضلة (DSCP)) عند استخدام أنفاق أمن بروتوكول الإنترنت (IPsec) لحركة خدمة الاتصالات في حالة الطوارئ بين الشبكات. وعلى وجه التحديد، يتعين تضمين اتفاقات مستوى الخدمة قواعد بشأن كيفية ملء قيم نقطة شفرة الخدمات المتفاضلة من الرأسية الداخلية عند نقطة الدخول إلى أمن بروتوكول الإنترنت، ويتعين إنفاذ هذه القواعد للسماح بمعاملة الأولوية بين نقاط الدخول والخروج في أمن بروتوكول الإنترنت.

8.8 تيسُّر خدمة الاتصالات في حالة الطوارئ (ETS)

1.8.8 الهدف العام

لضمان تيسّر أكبر لخدمة الاتصالات في حالة الطوارئ، يجب أن تبقى أعطال كل نظام في هذه الخدمة (يدعمها) طفيفاً، ويجب أن تكون استعادة الخدمة سريعة (حالما يقع انقطاع أو عطل). وينبغي أن تُحتسب الأعطال الناجمة عن التنازلات التوفيقية من أجل الأمن لدى التخطيط والتصميم الكلي لتيسر خدمة الاتصالات في حالة الطوارئ. وفيما يلي الهدف العام لتيسر خدمة الاتصالات في حالة الطوارئ في سياق الأمن:

O–3 يُستحسن أن يحتسب مقدمو الخدمة الأعطال المحتملة أو انقطاعات الخدمة بسبب الأحداث الأمنية التي تؤثر على التوصيلات البينية للشبكات في التخطيط والتصميم الكلي من طرف إلى طرف لتيسر خدمة الاتصالات في حالة الطوارئ (أي مكالمات/دورات هذه الخدمة العابرة لشبكات مقدمي خدمة متعددين). وهذا يشمل تدابير لتحقيق التدارك السريع للأعطال الناجمة عن الأحداث الأمنية.

2.8.8 حماية التيسُّر

تجب حماية خدمة الاتصالات في حالة الطوارئ من الحرمان من الخدمة (DoS)، والحرمان الموزع من الخدمة (DDoS)، وأنواع أخرى من الهجمات التي يمكن أن تؤثر على تيسر خدمة الاتصالات في حالة الطوارئ. ويشمل ذلك الحماية من الهجمات التي تؤثر على تيسر هذه الخدمة لفرادى مستخدميها أو جماعاتهم أو مستخدميها في موقع معين (مثل موقع شبكة مؤسسة وكالة حكومية) أو مستخدميها في منطقة جغرافية أو إقليمية مستهدفة، أو الهجمات التي تؤثر على تيسر هذه الخدمة ككل.

R–22 يتعين على مقدم الخدمة أن يحمي تيسر خدمة الاتصالات في حالة الطوارئ (على سبيل المثال، من الحرمان من الخدمة (DoS)، والحرمان الموزع من الخدمة (DDoS)، وأنواع أخرى من الهجمات التي يمكن أن تؤثر على تيسر هذه الخدمة) وفقاً للممارسات الأمنية الفضلى المتاحة تجارياً. ويتعين أن يشمل ذلك الحماية من الحرمان من الخدمة (DoS)، والحرمان الموزع من الخدمة (DDoS)، وأنواع أخرى من الهجمات التي يمكن أن تؤثر على تيسر خدمة الاتصالات في حالة الطوارئ لفرادى مستخدميها أو جماعاتهم أو مستخدميها في موقع معين (مثل موقع شبكة مؤسسة وكالة حكومية) أو مستخدميها في منطقة جغرافية أو إقليمية مستهدفة، أو الهجمات التي تؤثر على تيسر هذه الخدمة ككل.

وتشمل الإجراءات التي يمكن اتخاذها لحماية تيسُّر خدمة الاتصالات في حالة الطوارئ، على سبيل المثال لا الحصر، ما يلي:

أ) استخدام آليات التحكم في الدخول والتضييق عليه

ب) استخدام أدوات ووظائف التخفيف من الحرمان من الخدمة (DoS)، والحرمان الموزع من الخدمة (DDoS)

ج) استخدام أنظمة كشف التسلل وأنظمة منع التسلل (IDS/IPS)

د) استخدام أدوات مراقبة الأمن

هـ) استخدام أدوات الوعي الظرفي.

R–23 يتعين أن يشمل استخدام مقدمي الخدمات الأمنية لأدوات وقدرات حماية التيسُّر (على سبيل المثال، آليات التعامل مع الحرمان من الخدمة (DoS)، والحرمان الموزع من الخدمة (DDoS)) التدابير المناسبة لمنع الحرمان غير المقصود من المكالمات/الدورات المشروعة في خدمة الاتصالات في حالة الطوارئ (كحظر أو منع إكمال مكالمة/دورة مشروعة في خدمة الاتصالات في حالة الطوارئ أو نبذ رزمها المشروعة).

9.8 أمن الإدارة والعمليات

يغطي هذا القسم بعض المواضيع المتعلقة بما يلي:

- أمن عمليات إدارة (على سبيل المثال، المعلمات القابلة للتشكيل والافتراضية المتصلة بتوفير التوصيل البيني لخدمة الاتصالات في حالة الطوارئ (ETS))،
- تسجيل الأحداث ذات الصلة بالأمن في خدمة الاتصالات في حالة الطوارئ،
- تنبيهات وإنذارات عندما تقع الخروقات الأمنية أو يُحتمل أن تكون قد وقعت.

1.9.8 سلامة بيانات خدمة الاتصالات في حالة الطوارئ

يجب توفير حماية سلامة البيانات المخزنة لخدمة الاتصالات في حالة الطوارئ لمنع أي تلف أو التلاعب في البيانات يؤثر على سلامة هذه الخدمة أو تيسُّرها.

R–24 يتعين على مقدم الخدمة حماية سلامة البيانات المزودة من خدمة الاتصالات في حالة الطوارئ. وهذا يشمل أي بيانات تخص هذه الخدمة، مثل بيانات الاشتراك المزودة.

2.9.8 المعلمات القابلة للتشكيل والقيم الافتراضية

تتعدد التهديدات الأمنية المتعلقة بإدارة المعلمات القابلة للتشكيل والقيم الافتراضية التي تحددها منافذ البيع وتوريد المعدات. فعلى سبيل المثال، لا بد من تعديل القيم الافتراضية لمختلف المعلمات القابلة للتشكيل عن الصيغة المسلَّمة من منفذ البيع، لتلبية متطلبات مقدم الخدمة. ويجب تخصيص المعلمات القابلة للتشكيل على الوجه الصحيح وتحديثها بحيث يمكن أن تعمل بصورة مرضية. ويجب أن يخوَّل هذا المسؤول البشري بشكل مناسب لأداء إدارة الأمن.

R–25 يُلزم مقدم الخدمة بوضع وإنفاذ قواعد لإدارة المعلمات القابلة للتشكيل والقيم الافتراضية في سياق دعم خدمة الاتصالات في حالة الطوارئ. ويتعين تنفيذ تدابير التحكم في النفاذ وإنفاذها بحيث يقتصر تنفيذ هذه المهام على المسؤول المخول فحسب (أي يحرم جميع المستخدمين الآخرين هذا الإذن).

3.9.8 إدارة التهديدات داخلية المصدر

قد يتمكّن فرد ما (على سبيل المثال، موظف أو مقاول أو عامل آخر) أن يتصرف بصفة إدارية غير مخوَّلة أو يسيء استخدام صفته الإدارية عند نفاذه إلى عناصر الشبكة وأنظمة دعم خدمة الاتصالات في حالة الطوارئ. لذلك، هناك حاجة للحد من التهديدات داخلية المصدر.

R–26 يتعين على مقدم الخدمة وضع وتنفيذ عمليات أمنية للحد من التهديدات داخلية المصدر لخدمة الاتصالات في حالة الطوارئ.

وقد تشمل الأساليب التي يمكن النظر فيها للتخفيف من هذه التهديدات ما يلي:

- ضوابط الاستيقان وإسناد الامتيازات حسب الأدوار والفصل بين الوظائف، وأساليب النفاذ المأمون في النفاذ إلى النظام عن بعد ومن حامل الأجهزة ومن المركبات وبصورة مؤتمتة؛
- تسجيل الأحداث الأمنية المتعلقة بالإجراءات الإدارية؛
- فرز معلومات خدمة الاتصالات في حالة الطوارئ وتطبيقاتها، والنفاذ إلى نظم وتطبيقات مشتركة؛
- تدقيق البيانات المشكَّلة في عناصر الشبكة وقواعد بياناتها (على سبيل المثال، البيانات الوصفية للاشتراكات) لتسجيل التغييرات غير المخولة وفضحها.

4.9.8 التعاون في تبادل معلومات الأمن السيبراني

ينبغي لمقدمي الخدمة إقامة علاقات تعاونية مع الشركاء لتبادل المعلومات بشأن أحداث الأمن السيبراني (بما في ذلك تبادل المعلومات في الوقت الفعلي خلال الهجمات ضد الأمن السيبراني). ويمكن لتبادل المعلومات بشأن حوادث الأمن السيبراني أن يعود بالمنافع المتبادلة، ويمكن الاستفادة منه لتوقع التهديدات التي تتعرض لها خدمة الاتصالات في حالة الطوارئ مما يجعل مقدم الخدمة في وضع يمكنه من اتخاذ تدابير مضادة فعالة.

O–4 يستحسن أن يضع مقدم الخدمة وينفذ عمليات إدارية وتشغيلية تكفي لتوفير علاقات تعاونية لتبادل المعلومات والتشارك فيها بشأن أحداث الأمن السيبراني. وينبغي أن تأخذ العمليات وظائف التحليل في الاعتبار لجعل المعلومات مفيدة كمدخل إلى إجراءات الأمن والتدابير المضادة لحماية خدمة الاتصالات في حالة الطوارئ.

يرجى الرجوع إلى التوصيات التالية لقطاع تقييس الاتصالات للحصول على معلومات بشأن تبادل معلومات الأمن السيبراني:

- [b-ITU-T X.1500]
- [b-ITU-T X.1500.1]
- [b-ITU-T X.1520]
- [b-ITU-T X.1521]
- [b-ITU-T X.1524]
- [b-ITU-T X.1570]

5.9.8 إدارة الاستجابة لمقتضيات الحوادث والتعافي من الأحداث الأمنية

يعتمد تيسُّر خدمة الاتصالات في حالة الطوارئ على الإجراءات التشغيلية القائمة للتعافي من الحوادث الأمنية واستعادة الخدمة منها. فمن الأهمية بمكان أن تكون هذه الإجراءات محددة بوضوح وموثقة ومنفذة. وهذا يشمل السياسات والممارسات اللازمة للتدارك واستعادة الخدمة ضمن ميدان مقدِّم الخدمة وعبر ميادين التوصيل البيني والخدمات بين الشبكات. وتدعو الضرورة لحماية إجراءات التشغيل والتوثيق والتنفيذ من المتسللين والتهديدات داخلية المصدر.

R–27 يُلزم مقدم الخدمة بتوثيق خطة الاستجابة لمقتضيات الحوادث والتعافي موضحاً السياسات والإدارة، والخطوات التنفيذية والعمليات والإجراءات التي ينطوي عليها التعافي من الحوادث الأمنية واستعادة الخدمة. وهذا يشمل السياسات والممارسات اللازمة للتدارك واستعادة الخدمة ضمن ميدان مقدم الخدمة وعبر ميادين التوصيل البيني والخدمات بين الشبكات.

ببليوغرافيا

[b-ITU-T Q-Sup.57] ITU-T Q-series Recommendations – Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-ITU-T X.1500.1] Recommendation ITU-T X.1500.1 (2012), *Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures.*

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system.*

[b-ITU-T X.1524] Recommendation ITU-T (2012), *Common weakness enumeration*.

[b-ITU-T X.1570] Recommendation ITU-T X.1570 (2011), *Discovery mechanisms in the exchange of cybersecurity information*.

[b-TMF GB917] GB 917 (2012), *SLA Management Handbook, Release 3.1,* TM Forum.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	**البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2013