الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1210

(2014/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

نظرة عامة على آليات تصحيح أخطاء الأمن المستند إلى المصدر في الشبكات القائمة على بروتوكول الإنترنت

التوصيـــة ITU-T X.1210

الاتحاد الدولي للاتصالات ITU

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أشكال أخرى لأمن الحوسبة السحابية	X.1699–X.1680

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

نظرة عامة على آليات تصحيح أخطاء الأمن المستند إلى المصدر في الشبكات القائمة على بروتوكول الإنترنت

ملخص

توفر التوصية ITU-T X.1210 آليات لتصحيح أخطاء الأمن المستند إلى المصدر من أجل المسائل المتعلقة بالأمن، فضلاً عن معايير الاختيار والمبادئ التوجيهية الأمنية الأساسية لآليات تصحيح الأخطاء.

ويشمل تصحيح أخطاء الأمن المستند إلى المصدر في الشبكات القائمة على بروتوكول الإنترنت تقنيات تُستخدم لاكتشاف المعلومات التقنية المتعلقة بنقاط الدخول إلى الشبكة أو مسيرات أو مسيرات جزئية أو مصادر لرزمة أو رزم تسبب حدثاً إشكالياً في الشبكة، وذلك لأغراض تطبيق تدابير تخفف منه عموماً.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1210	2014-01-24	17	11.1002/1000/12043

* للنفاذ إلى هذه التوصية، اطبع العنوان الإلكتروني http://handle.itu.int/ في حقل العنوان لمتصفح الإنترنت لديك، متبوعاً بمعرف الهوية الفريد للتوصية. ومثال ذلك http://handle.itu.int/11.1002/1000/11830-en.

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

نظرة عامة على آليات تصحيح أخطاء الأمن المستند إلى المصدر في الشبكات القائمة على بروتوكول الإنترنت

1 مجال التطبيق

توفر هذه التوصية نظرة عامة عن آليات تصحيح أخطاء الأمن المستند إلى المصدر، ومعايير التقييم، والمبادئ التوجيهية الأمنية الأساسية لآليات تصحيح الأخطاء.

ويمتثل من يطبقون ويستخدمون هذه التوصية لجميع القوانين واللوائح التنظيمية والسياسات الوطنية والإقليمية السارية المفعول.

2 المراجع

لا توجد.

3 التعاريف

1.3 المصطلحات المعرفة في توصيات أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الحرمان من الخدمة [b-ITU-T X.800]: منع نفاذ مخول به إلى الموارد أو تأخير عمليات حرجة من حيث الوقت الذي تستغرقه.

2.1.3 ميدان الأمن [b-ITU-T T.411]: مجموعة الموارد التي تخضع لسياسة أمنية واحدة.

3.1.3 التهديد [b-ITU-T X.800]: خرق أمني محتمل.

2.3 المصطلحات المعرفة في هذه التوصية

لا توجد.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

AS	نظام مستقل ذاتياً *(Autonomous system)*
BGP	بروتوكول بوابة الحدود *(Border Gateway Protocol)*
DoS	حرمان من الخدمة *(Denial-of-Service)*
ICMP	بروتوكول رسالة التحكم في الإنترنت *(Internet Control Message Protocol)*
IP	بروتوكول الإنترنت *(Internet Protocol)*
IPFIX	تصدير معلومات تدفق بروتوكول الإنترنت *(IP Flow Information Export)*
IPv4/v6	الإصدار الرابع/السادس من بروتوكول الإنترنت *(Internet Protocol version 4/version 6)*
ISP	مقدِّم خدمة الإنترنت *(Internet Service Provider)*
RID	الدفاع بين الشبكات في الوقت الفعلي *(Real-time Inter-network Defence)*
TCP	بروتوكول التحكم في الإرسال *(Transmission Control protocol)*

5 الاصطلاحات

لا توجد.

6 نظرة عامة على آليات تصحيح أخطاء الأمن المستند إلى المصدر

إن تصحيح أخطاء الأمن المستند إلى المصدر في الشبكات القائمة على بروتوكول الإنترنت (IP) ينطوي عموماً على عملية تقنية و/أو إدارية من أجل التحديد الموثوق لمصدر رزمة أو رزم بروتوكول الإنترنت التي يمكن أو لا يمكن أن تحمل عنوان بروتوكول الإنترنت الصحيح من المرسل، أو للمسيرات أو جزء من المسيرات التي تنتج مشكلات أمنية.

ويمكن أن تستخدم آليات تصحيح أخطاء الأمن المستند إلى المصدر لتحديد الموقع الفعلي أو المنطقي لمثل هذه الأحداث المنطوية على مشكلات أمنية في الوقت الفعلي بمساعدة من عناصر الشبكة مثل المسيّرات أو الحواسيب المضيفة في الشبكة.

وتناقش أدناه آليات تصحيح المشكلات الأمنية في الشبكات القائمة على بروتوكول الإنترنت.

1.6 تصحيح أخطاء الأمن المستند إلى المصدر باختبار الوصلة

يمكن أن يبدأ التصحيح من المسيّر الأقرب إلى الجهة المتضررة فتُختبر وصلاتها باتجاه المصدر على نحو تفاعلي إلى أن يتمكن مقدمو خدمة الإنترنت من تحديد أي من هذه الوصلات تستخدم في حمل حركة الجهة المخالِفة. ومن الناحية المثالية، يعاد هذا الإجراء بشكل متكرر على المسيّر باتّجاه المصدر حتى يتم تحديد مصدر المشكلة الأمنية.

وتفترض هذه التقنية أن المشكلة الأمنية تظل قائمةً حتى الانتهاء من إجراءات تصحيح الأخطاء. وعلى هذا النحو، لا يُعتد بهذه التقنية في الهجمات التي تُكتشف بعد وقوعها، أو الهجمات التي تُشن على نحو متقطع، أو الهجمات التي تعدل سلوكها رداً على تصحيح أخطاء الأمن.

وتدارك أخطاء المدخلات هو أحد سبل تنفيذ آلية اختبار الوصلة. وتوجد هذه الميزة بالفعل في كثير من المسيّرات فتسمح لمدير النظام بتحديد وصلات الشبكة الواردة إلى رزم محددة. فإذا عرف مشغِّل المسيّر الخصائص المحددة لحركة هجوم (وتسمى توقيع الهجوم)، يصبح حينها من الممكن تحديد وصلة الشبكة الواردة على المسيّر.

2.6 تصحيح أخطاء الأمن المستند إلى المصدر بشبكة غطائية حاسوبية

إن آلية الإحالة إلى ثقب أسود [b-IETF RFC 3882] هي تقنية تشغيلية تستخدم نفقاً في شكل بالوعة ينفَّذ في جميع نقاط الدخول المحتملة التي يمكن للهجمات أن تمر عبرها إلى المقصد/النظام المستقل ذاتياً (AS) المستهدف بالهجوم. وباستخدام بروتوكول بوابة الحدود (BGP) [b-IETF RFC 4271]، يمكن إحالة الحركة المتجهة نحو الحاسوب المضيف المهاجَم/المستهدَف إلى ثقب أسود، أي إسقاطها من الشبكة، أو إعادة تسييرها إلى مسير خاص (نفق) حيث يمكن لجهاز التقاط الحركة للتحليل، ثم إسقاطها.

3.6 تصحيح أخطاء الأمن المستند إلى المصدر بالسبر

إن بروتوكول رسالة التحكم في الإنترنت (ICMP) للإصدار الرابع من بروتوكول الإنترنت (IPv4) [b-IETF RFC 792]، وللإصدار السادس منه (IPv6) [b-IETF RFC 4443]، كانا وسيظلان إحدى أكثر آليات تصحيح الأخطاء فائدةً للشبكات القائمة على بروتوكول الإنترنت. ويرد عدد من الأدوات ضمن أنظمة التشغيل الشائعة التي تستخدم بروتوكول رسالة التحكم في الإنترنت، ومن هذه الأدوات المسبار ومرتسم المسير، من أجل إجراء تصحيح الأخطاء من طرف إلى طرف، أو على مستوى الوصلة.

4.6 تصحيح أخطاء الأمن المستند إلى المصدر بالتسجيل وأخذ العينات

يمكن أن يوفر أخذ عينات التدفق آلية مفيدة لتصحيح الأخطاء في الإشكالات الأمنية ضمن الشبكات القائمة على بروتوكول الإنترنت. ويمكن للمشغلين أن يلجؤوا إلى أخذ عينات التدفق sFlow [b-IETF RFC 3176]، أو أخذ عينات التدفق NetFlow [b-IETF RFC 3954] أو تصدير معلومات تدفق بروتوكول الإنترنت (IPFIX) [b-IETF RFC 5655]، مع مراعاة معايير أخذ عينات التدفق المعتمدة في المسيّرات المطبقة.

5.6 تصحيح أخطاء الأمن المستند إلى المصدر عبر الأنظمة المستقلة ذاتياً

عندما يتسع نطاق المشكلات الأمنية ليمتد عبر أنظمة مستقلة ذاتياً، يمكن للمشغلين الاعتماد على أدوات تصحيح الأخطاء على أساس السبر (انظر الفقرة 3.6) وأجهزة السبر على الخط التي تتوفر على شبكة الإنترنت، من قبيل المرآة (Looking Glass [b-LG]). وفي المستقبل، قد يتمكن المشغلون من تسهيل تبادل المعلومات من أجل أدوات أكثر تقدماً لتصحيح الأخطاء عبر أنظمة مستقلة ذاتياً، ومثال ذلك باستخدام الدفاع بين الشبكات في الوقت الفعلي (RID) [b-IETF RFC 6045].

7 المبادئ التوجيهية الأمنية الأساسية لآليات تصحيح أخطاء الأمن المستند إلى المصدر

ترد فيما يلي المبادئ التوجيهية الأمنية الأساسية لآليات تصحيح أخطاء الأمن المستند إلى المصدر:

- ينبغي تصميم آليات تصحيح أخطاء الأمن المستند إلى المصدر لتكون متينة وقادرة على استيعاب مختلف المقاييس وعلى النهوض من العثرات.
- ينبغي نشر آليات تصحيح أخطاء الأمن المستند إلى المصدر وتشغيلها عبر ميادين متعددة يدير كل منها مشرف مسؤول عن الأمن (أي تصحيح الأخطاء بين الأنظمة المستقلة ذاتياً).
- ينبغي تنفيذ آليات تصحيح أخطاء الأمن المستند إلى المصدر في أحد نمطي نماذج النشر: نموذج النشر المركزي أو نموذج النشر الموزع.
- ينبغي لآليات تصحيح أخطاء الأمن المستند إلى المصدر أن توفر اكتشاف المعلومات التقنية المتعلقة بنقاط الدخول إلى الشبكة أو مسيرات أو مسيرات جزئية أو مصادر لرزمة أو رزم تسبب حدثاً إشكالياً في الشبكة، وذلك لأغراض تطبيق تدابير تخفف منه عموماً.
- ينبغي تقييم آليات تصحيح أخطاء الأمن المستند إلى المصدر وفقاً لمعايير الأمن التي يرد وصفها في الفقرة 8 لاختيار المناسب من هذه الآليات.
- ينبغي للسطح البيني لآليات تصحيح أخطاء الأمن المستند إلى المصدر عبر أنظمة مستقلة ذاتياً أن يوفر السرية والاستيقان من أصل البيانات وسلامة المعلومات المتبادلة بين مختلف الميادين الأمنية، ويمكن أن يتيح تيسر آلية لتصحيح الأخطاء.

8 معايير لتقييم آليات تصحيح الأخطاء المستند إلى المصدر

توصِّف المعايير التي يمكن استخدامها لتقييم آليات تصحيح الأخطاء على النحو التالي:

- درجة مشاركة مقدم خدمة الإنترنت (ISP): درجة مشاركة مقدم خدمة الإنترنت عندما يقوم مشرف لدى مقدم خدمة الإنترنت بتحديد تصحيح الأخطاء. وتفترض معظم آليات تصحيح الأخطاء محدودية مرافق مقدمي خدمة الإنترنت المهيأة لتمكين تصحيح الأخطاء. ومن شأن مخطط مثالي لتصحيح الأخطاء أن يتطلب مستوى منخفضاً من مشاركة مقدم خدمة الإنترنت.
- عدد الرزم المطلوبة لتصحيح الأخطاء: عدد الرزم التي يستخدمها المشرف في تحديد مصدر المشكلة الأمنية فور اكتشاف هذه المشكلة.
- فعالية التنفيذ الجزئي: درجة فعالية تصحيح الأخطاء عند تنفيذ مخططه جزئياً لدى مقدم خدمة إنترنت واحد. وتتراوح الفعالية بين العجز وبين تحديد الهوية تحديداً مجدياً.
- المعلومات الخدمية للمعالجة من أجل تصحيح الأخطاء: مقدار المعلومات الخدمية للمعالجة في عنصر الشبكة الوسيط أو في الحاسوب المضيف الذي يُحتمل تضرره. ويُفضل مخطط مثالي لتصحيح الأخطاء بالحد الأدنى من المعلومات الخدمية للمعالجة في عنصر الشبكة الوسيط أو في الحاسوب المضيف المتضرر.

- درجة زيادة عرض النطاق: المقدار الإضافي من الحركة اللازمة لتصحيح الأخطاء. وينبغي لآلية تصحيح الأخطاء المرغوبة أن تتطلب زيادة في عرض النطاق بالحد الأدنى أو ألا تتطلب أي زيادة.
- متطلبات الذاكرة: مقدار الذاكرة الإضافية المطلوبة في عناصر الشبكة أو مخدّم مخصص لتصحيح الأخطاء. وفيما لا تحبَّذ الذاكرة الإضافية في عنصر الشبكة، يمكن تقبل ذاكرة إضافية في المخدّم المخصص. ومن شأن آلية تصحيح الأخطاء المثالية أن تتطلب كمية محدودة من الذاكرة الإضافية في مخدّم مخصص دون ذاكرة إضافية في عناصر الشبكة.
- متانة تصحيح الأخطاء: قدرة آلية تصحيح الأخطاء على تحقيق نتائج أداء مجدية حتى لو خُربت بعض عناصر الشبكة المشاركة في تصحيح الأخطاء. ويقع التخريب نتيجة لأخطاء ناشئة من سوء تشكيل عنصر الشبكة أو من برمجية تصحيحية غير مناسبة.
- السعة الاستيعابية: مقدار التشكيل الإضافي الذي يجرى على عناصر الشبكة الأخرى والمطلوب لإضافة عنصر شبكة واحد. وهذا يشير إلى مدى السهولة التي يمكن بها توسيع مخطط تصحيح الأخطاء. وتُعتبر السعة الاستيعابية جيدة إذا كان عنصر الشبكة المضاف حديثاً يتطلب التشكيل وحده، وتعتبر رديئة إذا تطلبت إضافة عنصر شبكة واحد التشكيل الكامل لبقية عناصر الشبكة. وينبغي أن تكون آلية تصحيح الأخطاء المثالية قابلة للتوسعة.
- عدد الوظائف اللازمة لتنفيذ تصحيح الأخطاء: مقدار الوظائف الإضافية المطلوبة لتنفيذ مخطط معين لتصحيح الأخطاء.
- القدرة على التعامل مع مشكلات أمنية ضخمة على مستوى الشبكة بأكملها: قدرة نظام تصحيح الأخطاء على إبراز مدى نجاح مخطط تصحيح الأخطاء في التعرف على المشكلات الأمنية على مستوى الشبكة بأكملها. وينبغي لمخطط تصحيح الأخطاء المثالي أن يحدد أي مشكلة أمنية بما في ذلك هجمات الحرمان من الخدمة الموزع (DDoS).
- القدرة على استكشاف الرزم المحوَّرة: قدرة نظام تصحيح الأخطاء على تحديد مصدر المشاكل حتى عند وقوع تحوير للرزم. وتحوير الرزم يعني تعديلها عند إعادة تسييرها. ومن بين التحويرات الشائعة ترجمة عنوان الشبكة، حيث يغيَّر عنوان مصدر الرزمة و/أو الرزم و/أو مقصدها.

بيبليوغرافيا

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

[b-ITU-T T.411] Recommendation ITU-T T.411 (1993), *Information technology – Open Document Architecture (ODA) and interchange format: Introduction and general principles*.

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[b-IETF RFC 3176] IETF RFC 3176 (2001), *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

[b-IETF RFC 3882] IETF RFC 3882 (2004), *Configuring BGP to Block Denial-of-Service Attacks*.

[b-IETF RFC 3954] IETF RFC 3954 (2004), *Cisco Systems NetFlow Services Export Version 9*.

[b-IETF RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4)*.

[b-IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[b-IETF RFC 5655] IETF RFC 5655 (2009), *Specification of the IP Flow Information Export (IPFIX) File Format*.

[b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*.

[b-LG] BGP Looking Glass, http://www.lookinglass.org/

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، 2015