الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1542

(2016/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل الأحداث/الحوادث العارضة/ المعلومات الحدسية

نسق تبادل الرسائل المتعلقة بمعلومات الدورة

التوصية ITU-T X.1542

الاتحاد الدولي للاتصالات

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
الدليل	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
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349-X.1340
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
أمن أشكال أخرى للحوسبة السحابية	X.1699-X.1680

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

التوصية ITU-T X.1542

نسق تبادل الرسائل المتعلقة بمعلومات الدورة

ملخص

في بيئة اليوم، تتعرض الشبكات الحاسوبية لتهديدات من داخل المنظمة ومن خارجها على السواء. وتقوم أنظمة جدران الحماية بتسجيل معلومات عن توصيلات لبروتوكول التحكم في الإرسال (TCP)/بروتوكول الإنترنت (IP) صادرة وواردة منتقاة.

ومع ذلك، فإن هذه الأنظمة المتاحة حالياً غير قابلة للتشغيل البيني بشكل عام لأن لكل نظام منها وظيفته الخاصة وآليات التحكم وأنساق تسجيل الدورات الخاصة به.

والحاجة الملحة التي تلمسها معظم الإدارات الأمنية حالياً هي الحفاظ على نسق متسق لتبادل معلومات الدورة عبر مختلف أنظمة جدران الحماية بل حتى عبر بنى تحتية مختلفة.

وتصف التوصية ITU-T X.1542 نموذج المعلومات الخاص بنسق تبادل الرسائل المتعلقة بمعلومات الدورة (SIMEF) وتوفر نموذج بيانات ذا صلة موصف بمخطط لغة الوسم الموسعة (XML). ويحدد النسق SIMEF تمثيلاً لنموذج بيانات من أجل تبادل المعلومات سجل الدورة لطبقة النقل فيما يتعلق بالإدارة الأمنية للشبكة المركزية ونظام تبادل المعلومات الأمنية. والمواصفة الخاصة بأي من بروتوكولات النقل خارج مجال تطبيق هذه التوصية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1542	2016-09-07	17	11.1002/1000/12852

مصطلحات أساسية

نموذج بيانات، تبادل الرسائل، أمن الشبكة، معلومات الدورة.

---

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بحرف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظة

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، كان 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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1542

نسق تبادل الرسائل المتعلقة بمعلومات الدورة

1 مجال التطبيق

تشرح هذه التوصية نسق تبادل الرسائل المتعلقة بمعلومات الدورة (SIMEF)، وهو نموذج بيانات لتمثيل معلومات الدورة الصادرة عن الأنظمة الأمنية مثل جدران الحماية مع شرح الأساس المنطقي لاستعمال هذا النموذج. ويقدم تنفيذ لنموذج البيانات بلغة الوسم القابلة للتوسيع (XML)، مع استنباط تعريف لنمط الوثيقة (DTD) باللغة XML وتقديم أمثلة كذلك.

2 المراجع

لا توجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

لا يوجد.

2.3 المصطلحات المعرَّفة في هذه التوصية

تُعرف هذه التوصية المصطلحين التاليين:

1.2.3 المحلل: المحلل هو نظام أمن للشبكة يكتشف الهجمات بتحليل معلومات الدورات الواردة والصادرة. وهو ينتج أيضاً سجلاً للدورة ويرسله إلى أنظمة إدارة الأمن.

2.2.3 معلومات الدورة: هي معلومات تتضمن دورة بروتوكول التحكم في الإرسال (TCP)/بروتوكول وحدات بيانات المستعمل (UDP) وخدمة التطبيق وكيانات الدورة كما يراها موردو معلومات الدورات. وتعرف الدورة بمجموعة الحركة التي تدار كوحدة للنقل. وتعرف دورات بروتوكول التحكم في الإرسال (TCP)/بروتوكول وحدات بيانات المستعمل (UDP) بشكل متفرد عن طريق متوالية من (عنوان بروتوكول الإنترنت للمصدر ومنفذ البروتوكولين UDP/TCP للمصدر وعنوان برتوكول الإنترنت ومنفذ البروتوكولين UDP/TCP للهدف).

ملاحظة – يستند هذا التعريف إلى المرجع [b-IETF RFC 2663].

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

BSD توزيع برمجية بيركلي *(Berkeley Software Distribution)*

CGI السطح البيني لبوابة مشتركة *(Common Gateway Interface)*

DTD تعريف نمط الوثيقة *(Document Type Definition)*

FTP بروتوكول نقل الملفات *(File Transfer Protocol)*

HTTP بروتوكول نقل النصوص المترابطة *(Hypertext Transfer Protocol)*

IP بروتوكول الإنترنت *(Internet Protocol)*

LAN شبكة محلية *(Local Area Network)*

MAC التحكم في النفاذ إلى الوسائط *(Media Access Control)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

NTP بروتوكول وقت الشبكة *(Network Time Protocol)*

POSIX سطح بيني محمول لنظام التشغيل *(Portable Operating System Interface)*

SIMEF نسق تبادل الرسائل المتعلقة بمعلومات الدورة *(Session Information Message Exchange Format)*

SNA معمارية شبكة مشتركة *(Shared Network Architecture)*

SNMP بروتوكول إدارة الشبكة البسيط *(Simple Network Management Protocol)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

UDP بروتوكول مخطط بيانات المستخدم *(User Datagram Protocol)*

UML لغة النمذجة الموحدة *(Unified Modelling Language)*

URL موقع موارد موحد *(Uniform Resource Locator)*

UTF نسق تحويل مجموعة رموز عالمية *(Universal character set Transformation Format)*

VPN شبكة خاصة افتراضية *(Virtual Private Network)*

XML لغة الوسم القابلة للتوسيع *(extensible Markup Language)*

5 الاصطلاحات

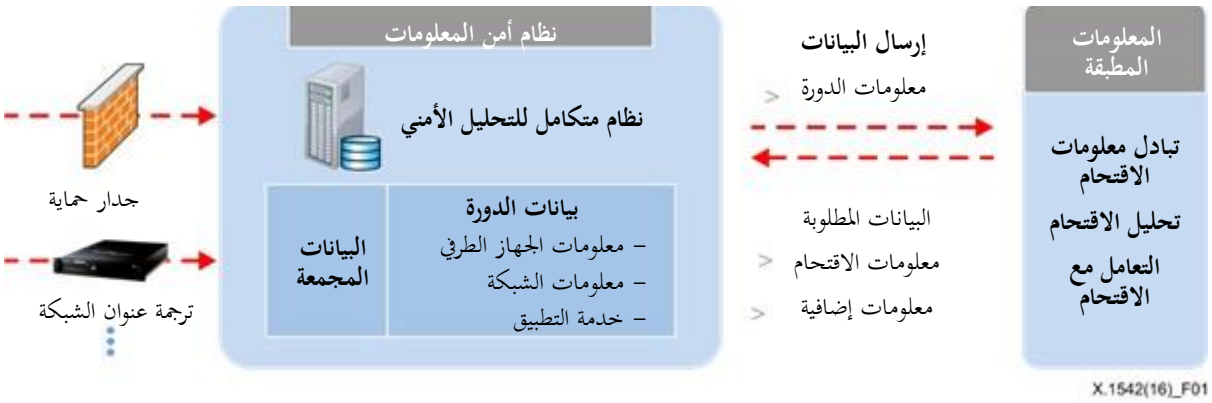
®UNIX علامة تجارية مسجلة للفريق المفتوح.

®POSIX علامة تجارية مسجلة لمعهد مهندسي الكهرباء والإلكترونيات.

6 لمحة عامة

تتعرض شبكات الحاسوب في بيئة الشبكات الحالية لتهديدات من داخل منظمة ومن خارجها على حد سواء. لذا، كُرست معظم أبحاث أمن الشبكات من أجل تطوير أنظمة متكاملة لإدارة أمن الشبكات وأدوات لمراقبة الشبكات تمكن منظمة من التقاط الرزم TCP/IP التي تمر عبر أجهزتها الشبكية ومشاهدة البيانات الملتقطة في شكل تتابع لمحادثات بين العملاء والمخدمات. وعلى سبيل المثال تقوم أنظمة جدران الحماية بتسجيل معلومات الدورة عن توصيلات لبروتوكول التحكم في الإرسال (TCP)/بروتوكول الإنترنت (IP) صادرة وواردة منتقاة.

ويُعرض في الشكل 1 المفهوم SIMEF. ويمكن جمع معلومات الدورة من أنظمة جدران الحماية ومن أجهزة ترجمة عنوان الشبكة (NAT) وما شابهها. ويوصف النسق SIMEF نموذج البيانات الذي يغطي التوصيلة الشبكية للعميل/المخدم وجهاز المستعمل النهائي وخدمة التطبيق. ويعرف النسق SIMEF نموذج البيانات وأصناف الرسائل ذات الصلة من أجل تبادل معلومات دورة طبقة النقل المهمة بالنسبة لأنظمة إدارة الأمن وأنظمة تبادل المعلومات. ويمكن أن يطبق على نظام تبادل معلومات الاقتحام.



الشكل 1 – مفهوم النسق SIMEF

7 التمثيل والتعريف

تستعمل هذه التوصية ثلاثة ترميزات: لغة النمذجة الموحدة (UML) لوصف نموذج البيانات واللغة XML لوصف الترميز المستخدم في وثائق النسق SIMEF والترميز SIMEF لتمثيل الوثائق ذاتها.

1.7 وثائق اللغة XML للنسق SIMEF

تشرح هذه الفقرة قواعد تنسيق الوثائق SIMEF XML. وقد وُرثت هذه القواعد بمعظمها من تلك الموضوعة لتحديد نسق وثائق XML. ويرد وصف لغة برمجة الوثائق SIMEF XML في الفقرتين من 1.1.7 إلى 2.1.7.

1.1.7 الإعلان XML

الوثائق SIMEF التي يتم تبادلها بين تطبيقات ممثلة للنسق SIMEF، يجب أن تبدأ بإعلان XML، ويجب أن تحدد إصدار اللغة XML المستعمل. ويوصى بمواصفة التشفير المستعمل.

ومن ثم، ينبغي للرسالة SIMEF أن تبدأ بالآتي:

```
<?xml version="1.0" encoding="UTF-8"?>
<simef: SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef"/>
```

ويمكن للتطبيقات المتمثلة للنسق SIMEF أن تختار حذف الإعلان XML داخلياً لتوفير مساحة، على أن يضاف نقاط عندما تكون الرسالة موجهة إلى مقصد آخر (متصفح ويب، مثلاً). ولا يوصى بهذه الممارسة ما لم تنفذ بدون فقدان كل من صيغة الرسالة ومعلومات التشفير.

لذلك، قد يقرر المنفذون أن يتفق المحللون والمدراء خارج النطاق على تعريف نمط خاص للوثيقة (DTD) يستعملونه لتبادل الرسائل (النمط القياسي كما هو معرف هنا، أو نمط مع تمديدات)، والقيام بعد ذلك بحذف تعريف نمط الوثيقة من الرسائل SIMEF. وطريقة التفاوض بشأن هذا الاتفاق تقع خارج نطاق هذه الوثيقة.

2.1.7 معالجة بيانات الرموز في النسق SIMEF

لدواعي إمكانية الحمل، لا ينبغي للتطبيقات المتمثلة للنسق SIMEF أن تستعمل، ولا للرسائل SIMEF أن تشفر، بتشفيرات رموز خلاف UTF-8 وUTF-16. واتساقاً مع المعيار XML، إذا لم يحدد التشفير لأي رسالة SIMEF، يُفترض التشفير UTF-8.

1.2.1.7 مراجع كيانات الرموز

يوصى بأن تستعمل التطبيقات المتمثلة للنسق SIMEF شكل مرجع الكيان من الرموز '&'، و'<'، و'>'، و'"'، و'' (علامة اقتباس واحدة) عند كتابة هذه الرموز في البيانات لتفادي أي إمكانية لسوء التفسير.

2.2.1.7 معالجة المساحات الفارغة

تدعم جميع عناصر النسق SIMEF النعت "xml:space".

3.2.1.7 اللغات في النسق SIMEF

تحدد التطبيقات المتمثلة للنسق SIMEF اللغة المشفر بها محتوياتها؛ وبوجه عام، يمكن تحقيق ذلك بتحديد النعت "xml:lang" لعنصر المستوى الأعلى وجعل بقية العناصر الأخرى "ترث" هذا التعريف.

2.7 أنماط البيانات SIMEF

داخل أي رسالة XML SIMEF، يجب التعبير عن جميع البيانات بنصوص نظراً إلى أن اللغة XML لغة تنسيق نصوص. وهي توفر تصنيف المعلومات من أجل نعوت الأصناف في نموذج البيانات. ولكل نمط بيانات في النموذج متطلبات تنسيق محددة في أي رسالة XML SIMEF؛ وتحدد هذه المتطلبات في هذه الفقرة.

1.2.7 الأعداد الصحيحة

تُمثل نعوت الأعداد الصحيحة بنمط البيانات INTEGER. ويجب أن تشفر بيانات الأعداد الصحيحة بالأساس 10 أو بالأساس 16. وفي تشفير الأعداد الصحيحة بالأساس 10 تستعمل الأرقام من '0' إلى '9' وإشارة اختيارية ('+' أو '–'). ومثال على ذلك "123"، "–456". وفي تشفير الأعداد الصحيحة بالأساس 16 تستعمل الأرقام من '0' إلى '9' والحروف من 'a' إلى 'f' (أو الحروف الكبيرة منها)، على أن تسبق بالرمزين "0x". ومثال على ذلك "0x1a2b".

2.2.7 الأعداد الحقيقية

نعوت الأعداد الحقيقية (الفاصلة المتحركة) تمثل البيانات REAL. وتشفير بيانات الأعداد الحقيقة بالأساس 10. وتشفير الأعداد الحقيقية هو تشفير دالة المكتبة "strtod" للمعيار 1003.1 [b-IEEE 1003.1] للسطح البيني لنظام التشغيل المحمول (POSIX): إشارة اختيارية ('+' أو '–') تليها سلسلة غير فارغة من الأرقام العشرية، تتضمن اختيارياً رمزاً للأساس، ثم يلي ذلك جزءاً أساسياً اختيارياً. ويتألف الجزء الأسّي من الحرف 'e' أو 'E' يليه إشارة اختيارية، ثم رقم عشري واحد أو أكثر. ومثال على ذلك "123.45e02" و"89e-03 ,–567" ويجب أن تدعم التطبيقات المتمثلة للنسق SIMEF رمزي الأساس '.' و',‘.

3.2.7 الرموز والسلاسل

تمثل النعوت ذات الرمز الواحد بنمط البيانات CHARACTER. وتمثل النعوت ذات الرمز المتعددة والمعروف طولها بنمط البيانات STRING. ولا توجد متطلبات تنسيق خاصة لبيانات الرموز والسلاسل، خلاف ضرورة استعمال مراجع الرموز من حين لآخر لتمثيل الرموز الخاصة.

1.3.2.7 مراجع كيانات الرموز

لبعض الرموز في الوثائق XML معاني خاصة في بعض السياقات. ولإدراج الرمز الفعلي ذاته في أي من هذه السياقات، يستعمل تتابع escape خاص، يطلق عليه مرجع الكيان.

وفيما يلي الرموز التي قد يلزم استعمال التتابع escape معها في بعض الأوقات مع مراجع الكيانات الخاصة بها:

الرمز	مرجع الكيان
&	&amp;
<	<
>	>
"	"
‘	'

2.3.2.7 مراجع شفرات الرموز

أي رمز يعرف بالمعيار [b-ISO/IEC 10646] والمعايير أحادية الشفرة يمكن إدراجه في أي وثيقة XML باستعمال مرجع للرمز. ويبدأ مرجع الرمز بالرمزين ’&‘ و’#‘ وينتهي بالرمز ’;‘. من بين هذه الرموز تُدخل شفرة الرمز.

وتدخل شفرة الرمز بين هذه الرموز ’x‘، فإنها تفسر بالنظام الستة عشري (الأساس 16)؛ وخلاف ذلك، فإنها تفسر بالنظام العشري (الأساس 10). فعلى سبيل المثال يشفر الرمز (&) كالتالي: &#38؛ أو &#x0026؛ ويشفر رمز أقل من (<) كالتالي &#60؛ أو &#x003C؛ وأي رمز من بايتة واحدة أو بايتتين أو أربع بايتات موصف في المعيار ISO/IEC 10646 والمعايير أحادية الشفرة يمكن إدراجه في أي وثيقة باستعمال هذه التقنية.

4.2.7 البايتات

تمثل البيانات الاثنينية بنمط البيانات BYTE (و[]BYTE). وتشفير البيانات الاثنينية في مجملها باستعمال الأساس 64.

5.2.7 الأنماط العددية

تمثل الأنماط العددية بنمط البيانات ENUM وتتألف من قائمة مرتبة من قيم مقبولة.

6.2.7 سلاسل التاريخ والتوقيت

تمثل سلاسل التاريخ والتوقيت بنمط البيانات DATETIME. وتحدد كل سلسلة من هذه السلاسل لخطة زمنية معينة؛ ولا تُدعم المديات الزمنية. وتنسق هذه السلاسل طبقاً لمجموعة فرعية من المعيار [b-ISO 8601:2014]، كما هو مبين أدناه. وتشفير مراجع القسام داخل الأقواس إلى فقرات المرجع [b-ISO 8601:2004].

7.2.7 الأختام الزمنية للبرتوكول NTP

تمثل الأختام الزمنية لبروتوكول وقت الشبكة (NTP) بنمط البيانات NTPSTAMP ويرد شرحها بالتفصيل في المعيار [b-IETF RFC 1305] والمعيار [b-IETF RFC 5905]. وأي خاتم زمني NTP عبارة عن عدد غير جبري بعلامة كسرية ثابتة من 64 بتة. ويقع الجزء الصحيح في البتات الاثنتين والثلاثين الأولى والجزء الكسري في البتات الاثنتين والثلاثين الثانية. وفي الرسائل SIMEF، تشفر الأختام الزمنية NTP كقيمتين ستة عشريتين كل منها من 32 بتة، يفصل بينهما فترة (’.‘). ومثال على ذلك، "0x12345678.0x87654321".

8.2.7 قوائم المنافذ

تمثل قوائم المنافذ بنمط البيانات PORTLIST وتتألف من قائمة من الأرقام (أعداد صحيحة فردية) التي يفصل بين كل رقمين فيها بفاصلة، ومديات (N-M تعني البوابات من N إلى M، حصراً). ويمكن استعمال أي توليفة من الأرقام والمديات في قائمة واحدة. ومثال على ذلك:

"5-25,37,42,43,53,69-119,123-514".

9.2.7 معرفات الهوية الفريدة

هناك نمطان من معرفات الهوية الفريدة يستعملان في هذه التوصية. ويمثل النمطان كلاهما بأنماط البيانات STRING. وتنفذ معرفات الهوية هذه كنعوت على العناصر XML ذات الصلة وينبغي أن يكون لها قيم فريدة كالتالي:

1 نعت صنف الجهاز "deviceid" (الفقرة 2.3.2.8)، إذا تحدد، يجب أن تكون له قيمة فريدة عبر جميع المحللات في بيئة الكشف عن الاقتحام.

2 والقيمة بالتغيب هي "0" تشير إلى أن المحلل لا يستطيع توليد معرفات هوية فريدة.

وإذ وُصِّف نعت "ident"، بعدة أصناف، يجب أن تكون له قيمة فريدة عبر جميع الرسائل المرسلة من المحلل الفردي. ويجب أن تكون قيمة النعت "ident" فريدة لكل توليفة خاصة من البيانات التي تعرف الكائن، وليس لكل كائن. ويجوز أن يكون للكائنات أكثر من قيمة واحدة للنعت "ident" تصاحبها. فعلى سبيل المثال، يكون لتعريف مضيف بالاسم قيمة واحدة، بينما يكون لتعريف هذا المضيف بالعنوان قيمة ثانية، وكذلك يكون لتعريف هذا المضيف بالاسم والعنوان معاً قيمة أخرى بعد.

والقيمة بالتغيب "0" تشير إلى أن المحلل لا يستطيع توليد معرفات هوية فريدة.

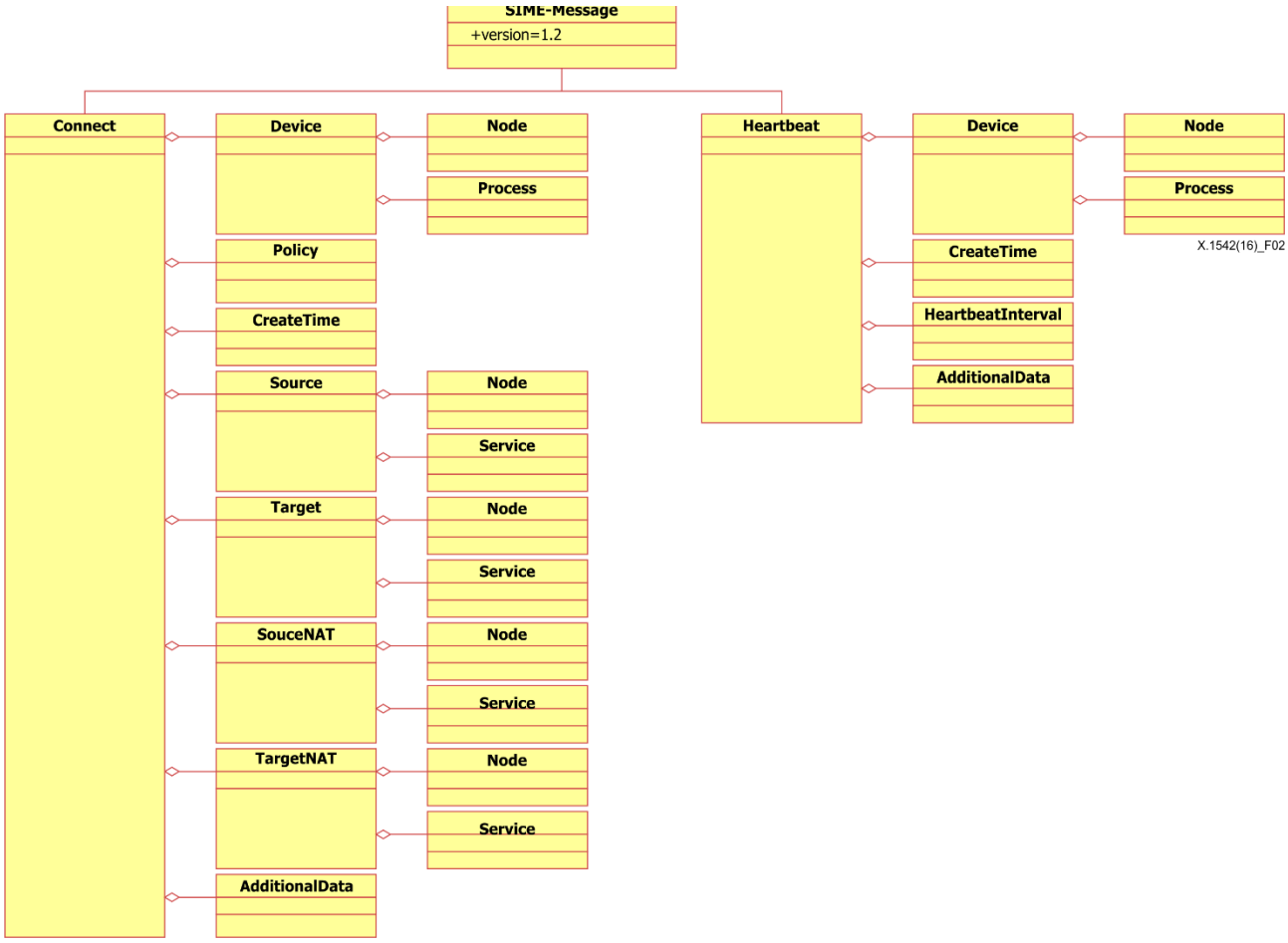
ومواصفة طرائق استحداث القيم الفريدة المتضمنة في هذه النعوت خارج نطاق هذه التوصية.

8 نموذج بيانات النسق SIMEF

يرد في هذه الفقرة بالتفصيل شرح المكونات الفردية لنموذج بيانات النسق SIMEF وتقدم مخططات لغة النمذجة الموحدة (UML) الخاصة بالنموذج لتوضيح علاقة المكونات ببعضها.

1.8 نظرة عامة لنموذج البيانات

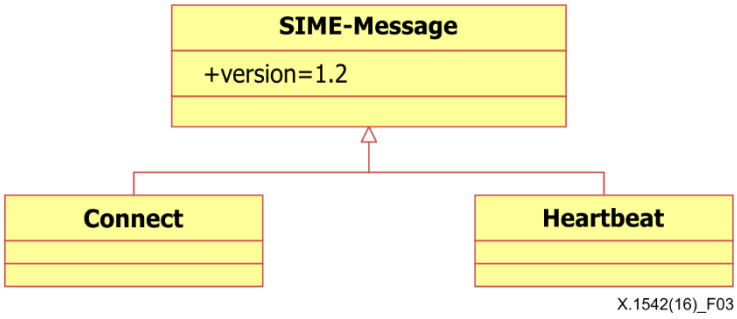
العلاقة بين المكونات الأساسية لنموذج البيانات مبينة في الشكل 2. وصنف المستوى الأعلى هو SIMEF-Message (الرسالة SIMEF)؛ وكل نمط من الرسائل صنف فرعي من صنف المستوى الأعلى هذا. وهناك نمطان من الرسائل يرد تعريفهما: Connects وHeartbeats. وتستعمل داخل كل رسالة أصناف فرعية لصنف الرسالة لتقديم المعلومات التفصيلية المنقولة في الرسالة. ولصنف الرسالة connect العديد من الأصناف الفرعية مثل Devices (الأجهزة) وPolicy (السياسة العامة) وSource (المصدر) وTarget (الهدف) وAdditionalData (البيانات الإضافية).



الشكل 2 – نموذج بيانات النسق SIMEF

1.1.8 أصناف النسق SIMEF

جميع رسائل النسق SIMEF عبارة عن حالات لصنف الرسالة SIMEF-Message؛ وConnect وHeartbeat (النبضات). ويرد وصف الصنفين كل على حدة في هذه الفقرة (انظر الشكل 3 والجدول 1 والجدول 2).



الشكل 3 – صنف المستوى الأعلى النموذج بيانات النسق SIMEF

الجدول 1 – نعوت أصناف النسق SIMEF

النعت	الاستعمال	نمط البيانات	الوصف
Version	ضروري	STRING	معلومات عن إصدار النسق SIMEF القيمة بالتغيب: 1.2

الجدول 2 – مكونات صنفَي النسق SIMEF

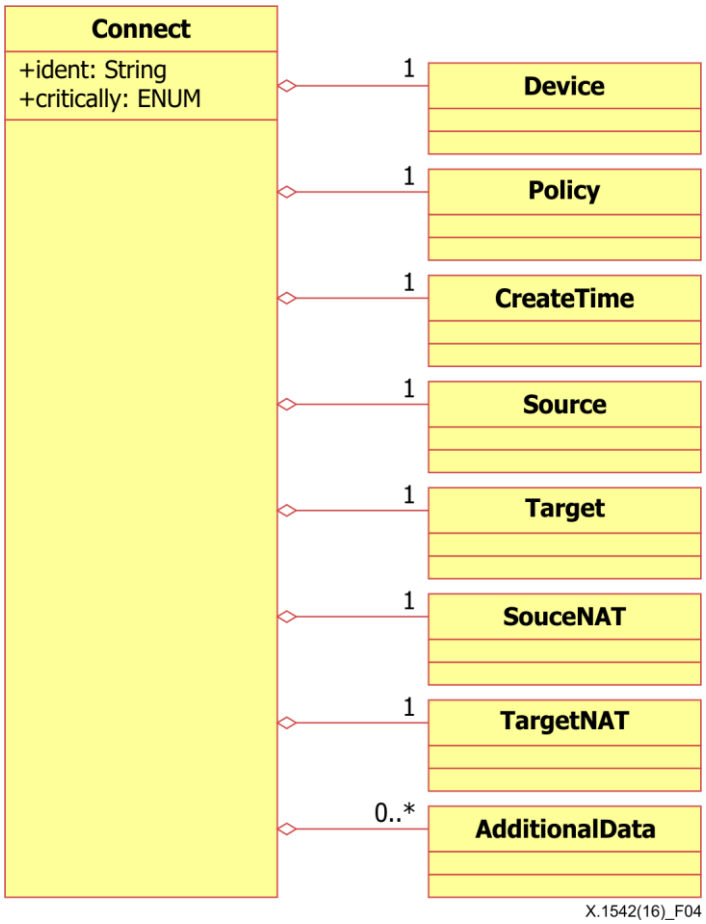
الصنفان	التجميع	نمط البيانات	الوصف
Connect	واحد (1) بالضبط		صنف معلومات الدورة
Heartbeat	صفر أو 1		صنف معلومات حالة النظام، تقديم اختياري

2.8 أصناف الرسائل

يرد وصف الأصناف الفردية في الفقرات من 1.2.8 إلى 4.2.8.

1.2.8 صنف Connect

الغرض من صنف Connect (التوصيل) تقديم معلومات الدورة. وهو يعبر عن نمط السجل المتولد بالتوصيل في جدار الحماية، كما أنه يعرض جميع المعلومات المتعلقة بمحاولات التوصيل بالداخل وكذلك بالخارج. انظر الجدول 3. ويبين الجدول 4 القيمة المسموح بها لنعوت الحراجة بصنف Connect. ويضم صنف Connect العديد من أصناف التجميع، كما هو مبين في الشكل 4. ويرد وصف أصناف التجميع نفسها في الجدول 5.



الشكل 4 – أصناف التجميع لصنف Connect

الجدول 3 – نعتا صنف Connect

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرفة هوية فريد لمعلومات النفاذ
criticality	اختياري	ENUM	تصنيف يتم حسب تقييم الحدث المتولد من التوصيل، القيمة بالتغيب: Unknown (غير معروف)

الجدول 4 – قيمة نعت criticality

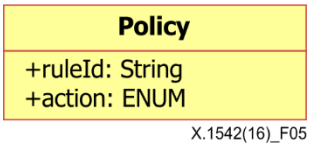
القيمة	مصطلحات أساسية	تعريف
0	unknown	عندما يجهل أثر الحدث أو يتعذر تحديده
1	normal	في حالة التوصيل العادي
2	suspicious	في حالة التوصيل المشتبه به
3	warning	عند احتمال أن يكون التوصيل إنذاراً
4	critical	إذا كان التوصيل خطير على الإجراء

الجدول 5 – مكونات صنف Connect

الصنف	التجميع	نمط البيانات	الوصف
Device	واحد (1) بالضبط		معلومات المحلل المولد لسجل
Policy	واحد (1) بالضبط		معلومات تحمل في المحلل للتوصيل
CreateTime	واحد (1) بالضبط	DATETIME	توقيت استحداث السجل
Source	واحد (1) بالضبط		مصدر الحدث المتسبب في التوصيل
Target	واحد (1) بالضبط		معلومات المقصد لحدث تسبب في توصيل
SourceNAT	واحد (1) بالضبط		معلومات ترجمة عنوان شبكة المصدر في حالة التسبب في التوصيل
TargetNAT	واحد (1) بالضبط		معلومات ترجمة عنوان شبكة المقصد في حالة التسبب في التوصيل
AdditionalData	صفر أو أكثر		معلومات إضافية يولدها الكاشف غير الموجود في الصنف الأخر

1.1.2.8 صنف Policy

يوفر صنف Policy (السياسة العامة) معلومات الإجراء الخاص ببيان كيفية التعامل مع الدورة في المحلل. انظر الشكل 5.



الشكل 5 – صنف Policy

وترد في الجدول 7، القيم المسموح بها لنعوت action في صنف Policy (انظر الجدول 6).

الجدول 6 – نعتا صنف Policy

النعت	الاستعمال	نمط البيانات	الوصف
ruleId	اختياري	STRING	معرفة الهوية الفريد للسياسة العامة لجدار الحماية المتولد بالتوصيل
action	اختياري	ENUM	تصنيف حسب جدار حماية العملية الناجمة عن التوصيل، القيمة بالتغيب: Unknown (غير معروف)

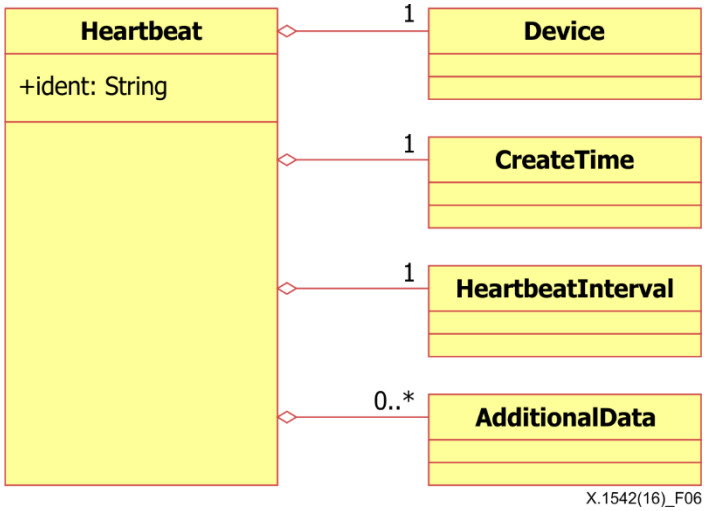
الجدول 7 – قيمة نعت action

القيمة	مصطلحات أساسية	التعريف
0	unknown	في حالة سلوك غير معروف
1	pass	في حالة السماح بالتوصيل
2	block	في حالة رفض التوصيل
3	protect	في حالة تجفير الرزمة المرسلة أو إدخال شفرة للتحقيق من السلامة (سجل شبكة خاصة افتراضية (VPN))
4	reject	في حالة رفض التوصيل. وبالتالي، تقدم رسائل أخطاء عند رفض النفاذ

2.2.8 صنف Heartbeat

تستعمل المحللات رسائل Heartbeat (النبضات) لبيان حالتها الآنية للمدراء. وتصميم النبضات بحيث ترسل على فترات منتظمة، كل 10 دقائق أو كل ساعة، مثلاً. ويشير استقبال رسالة نبضة من أي محلل للمدير أن المحلل سليم ويعمل؛ وعدم استلام هذه الرسالة (أو بصورة أكثر ترجيحاً فقدان عدد ما من رسائل النبضات المتعاقبة) يشير إلى أن المحلل تعرض للعطل أو توصيلية الشبكة تعرضت للعطل.

ويجب أن يدعم جميع المدراء استلام رسائل Heartbeat؛ ومع ذلك، فإن استعمال المحللات لهذه الرسائل أمر اختياري. وينبغي لمطوري برمجيات المدراء تمكين البرمجيات من التشكيل حسب كل محلل من أجل استعمال/عدم استعمال رسائل Heartbeat. وتتألف رسالة النبضة من العديد من أصناف التجميع، كما هو مبين في الشكل 6.



الشكل 6 – أصناف التجميع لصنف Heartbeat

وترد معلومات عن النعوت والمكونات الخاصة بصنف Heartbeat في الجدول 8 والجدول 9 على التوالي.

الجدول 8 – نعت صنف Heartbeat

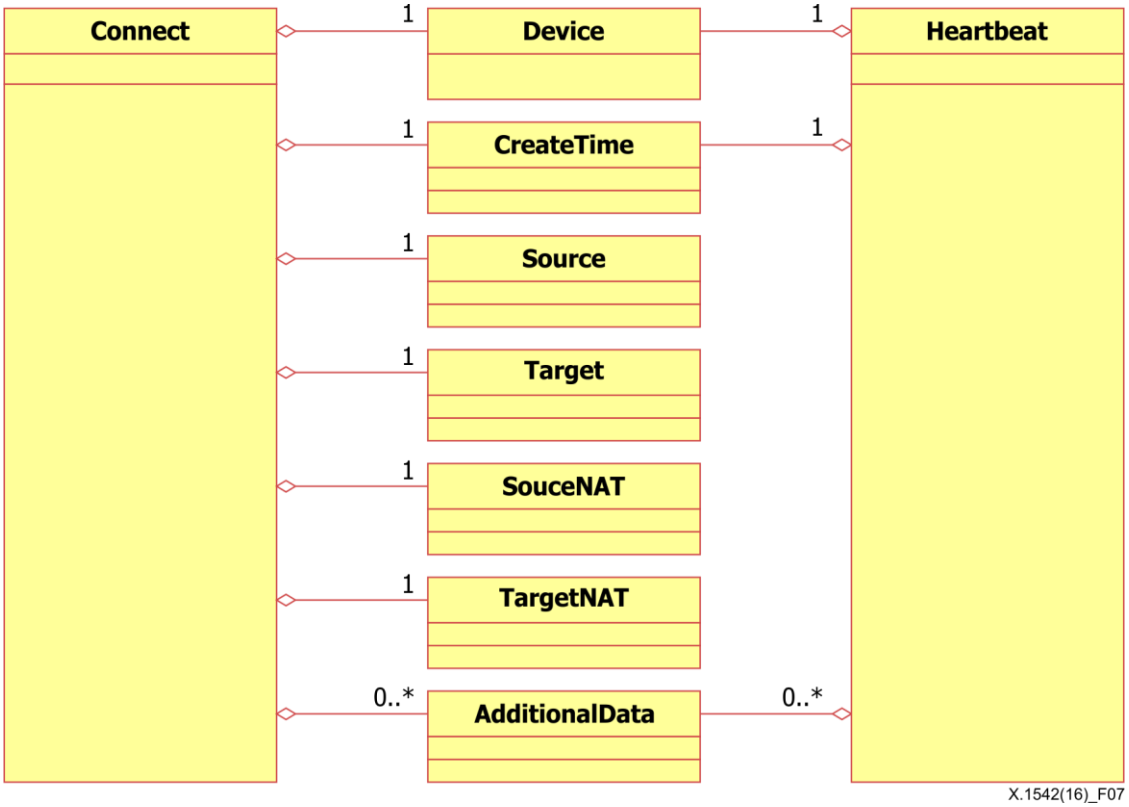
النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرفة هوية فريد للنبضة

الجدول 9 – مكونات صنف Heartbeat

الأصناف	التجميع	نمط البيانات	الوصف
Device	واحد (1) بالضبط		معلومات تعرف هوية المحلل المصدر للنبضة
CreateTime	واحد (1) بالضبط	DATETIME	توقيت استحداث النبضة
HeartbeatInterval	واحد (1) بالضبط	INTEGER	الفاصل الزمني (بالثواني) لتوليد النبضات
AdditionalData	صفر أو أكثر		معلومات يضيفها المحلل لا تلائم نموذج البيانات

3.2.8 الأصناف الأساسية

الأصناف الأساسية (Device وCreateTime وSource وTarget وSourceNAT وTargetNAT وAdditionalData) (الجهاز، وتوقيت الاستحداث، والمصدر والهدف، وترجمة عنوان شبكة المصدر، وترجمة عنوان شبكة الهدف، والبيانات الإضافية، على الترتيب) هي الأجزاء الرئيسية لصنفي التوصيل والنبضات، كما هو مبين في الشكل 7. ويرد وصف الأصناف الفردية في هذه الفقرة.

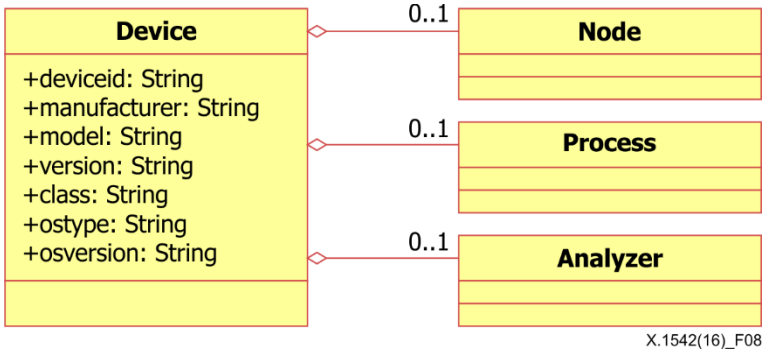


الشكل 7 – الأصناف الأساسية

1.3.2.8 صنف Device

يحدد صنف Device (الجهاز) المحلل الصادر منه رسالة Connect أو رسالة Heartbeat. ولا يمكن تشفير إلا جهاز واحد فقط لكل توصيل أو لكل نبضة ويجب أن يكون هذا الجهاز هو الجهاز الصادر منه التوصيل أو النبضات.

ويتألف صنف Device من ثلاثة أصناف للتجميع كما هو مبين في الشكل 8.



الشكل 8 – أصناف التجميع لصنف Device

ولصنف Device سبعة نعوت، على النحو المبيَّن في الجدول 10.

الجدول 10 – نعوت صنف Device

النعت	الاستعمال	نمط البيانات	الوصف
deviceid	اختياري	STRING	معرف هوية فريد للجهاز. إذا كان الجهاز يستعمل النعوت "ident" بشأن أصناف أخرى لتقديم معرفات هوية فريدة لهذه الكائنات، يجب أن يقدم أيضاً قيمة سارية للنعت "deviceid"
Manufacturer	اختياري	STRING	مصنع برمجيات و/أو عتاد الجهاز
Model	اختياري	STRING	اسم/رقم طراز برمجيات أو عتاد الجهاز
Version	اختياري	STRING	رقم إصدار برمجيات أو عتاد الجهاز
Class	اختياري	STRING	صنف برمجيات أو عتاد الجهاز
Ostype	اختياري	STRING	اسم نظام التشغيل
osversion	اختياري	STRING	إصدار نظام التشغيل

بالنسبة للنعت "ostype" للأنظمة المختلفة للمعيار POSIX 1003.1، فإن هذه القيمة هي التي تعاد في utsname.sysname بوساطة النداء uname() system، أو خرج الأمر "uname –s".

بالنسبة للنعت "osversion" للأنظمة المختلفة للمعيار POSIX 1003.1، فإن هذه القيمة هي التي تعاد في utsname.release بوساطة النداء uname() system أو خرج الأمر "uname –r".

محتوى النعوت "manufacturer" و"model" و"version" و"class" خاص بالبائع ولكن يمكن استعمالها معاً لتحديد أنماط مختلفة من المحللات.

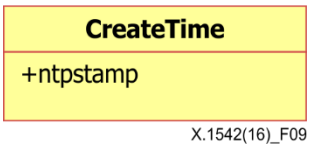
ويرد في الجدول 11 شرح أصناف التجميع التي تؤلف صنف Device.

الجدول 11 – مكونات صنف Device

الأصناف	التجميع	نمط البيانات	الوصف
Node	صفر أو واحد (1)		معلومات عن المستضيف أو الجهاز الموجود فيه المحلل (عنوان الشبكة، اسم الشبكة، وما إلى ذلك)
Process	صفر أو واحد (1)		معلومات عن العملية التي ينفذ فيها المحلل
Analyzer	صفر أو واحد (1)		معلومات عن المحلل التي يمكن أن تكون الرسالة مرت عبره

2.3.2.8 صنف CreateTime

يستعمل صنف CreateTime (توقيت الاستحداث) لبيان التاريخ والتوقيت الآنيين على الجهاز. إذا كان ينبغي استعمال فارق لضبط التوقيتات في العنصرين <CreateTime> و<NTP timestamps>، ينبغي أيضاً ضبط أختام توقيت البروتوكول NTP.



الشكل 9 – صنف CreateTime

ويعرض في الجدول 12 النعت الخاص بصنف CreateTime.

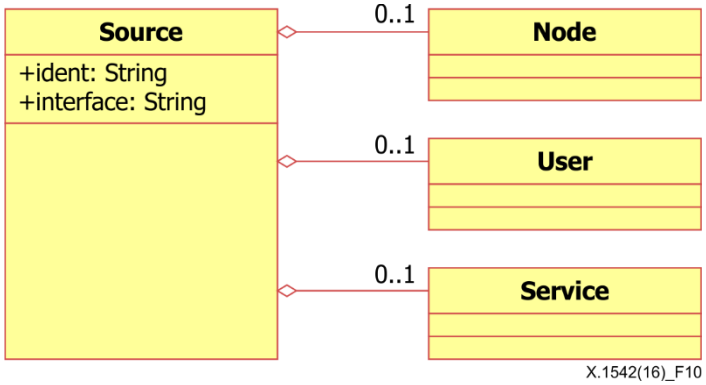
الجدول 12 – نعت صنف CreateTime

النعت	الاستعمال	نمط البيانات	الوصف
ntpstamp	مطلوب	ntpstamp	معلومات عن التوقيت الحالي على الجهاز

3.3.2.8 صنف Source

يحتوي صنف Source (المصدر) على معلومات عن المصدر المحتمل (المصادر المحتملة) للحدث (الأحداث) الذي (التي) يولد (تولد) دورة. وقد يكون للحدث الواحد أكثر من مصدر (كما هو الحال في هجمة رفض الخدمة الموزعة، مثلاً).

ويتألف صنف Source من ثلاثة أصناف للتجميع، كما هو مبين في الشكل 10.



الشكل 10 – أصناف التجميع للصنف Source

ويعرض في الجدول 13 نعتا صنف Source.

الجدول 13 – نعتا صنف Source

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرفة هوية فريد لهذا المصدر
Interface	اختياري	STRING	يمكن استعماله بواسطة جهاز قائم على الشبكة مع سطوح بينية متعددة لبيان السطح البيني الذي يُرى من عليه هذا المصدر

ويرد شرح أصناف التجميع التي تؤلف صنف Source في الجدول 14.

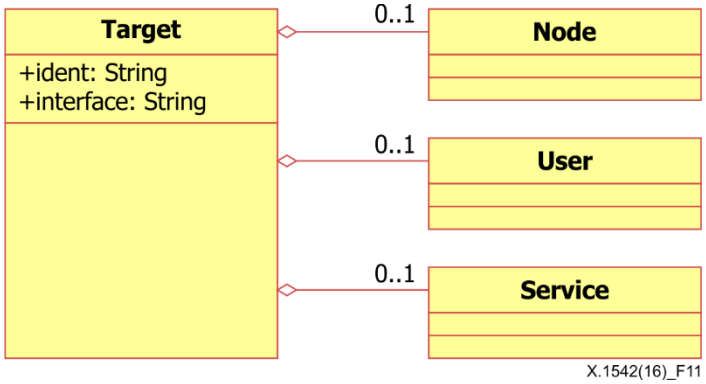
الجدول 14 – مكونات صنف Source

الأصناف	التجميع	نمط البيانات	الوصف
Node	صفر أو واحد (1)		معلومات عن المستضيف أو الجهاز الذي يعتقد أنه المتسبب في الأحداث (عنوان شبكة، اسم شبكة، وما إلى ذلك)
User	صفر أو واحد (1)		معلومات عن المستعمل الذي يعتقد أنه المتسبب في الحدث (الأحداث)
Service	صفر أو واحد (1)		معلومات عن خدمة الشبكة المشاركة في الحدث (الأحداث)

4.3.2.8 صنف Target

يتضمن صنف Target (الهدف) معلومات عن الهدف المحتمل (الأهداف المحتملة) للحدث (الأحداث) المولد (المولدة) للدورة. وقد يكون للحدث الواحد أكثر من هدف (كما في حالة كنس المنفذ، مثلاً).

ويتألف صنف Target من ثلاثة أصناف تجميع كما هو مبين في الشكل 11.



الشكل 11 – أصناف التجميع لصنف Target

يصنف Target نعتان على النحو المبيَّن في الجدول 15.

الجدول 15 – نعتا صنف Target

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد لهذا الهدف
Interface	اختياري	STRING	يمكن استعماله بواسطة جهاز قائم على الشبكة مع سطوح بينية متعددة لبيان السطح البيني الذي يُرى من عليه هذا الهدف

ويرد شرح أصناف التجميع التي يتألف منها صنف Target في الجدول 16.

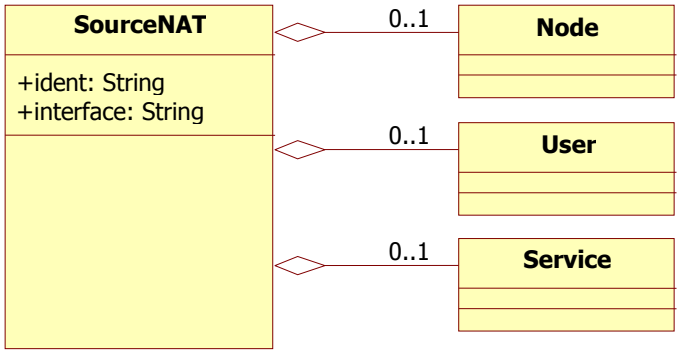
الجدول 16 – مكونات صنف Target

الأصناف	التجميع	نمط البيانات	الوصف
Node	صفر أو واحد (1)		معلومات عن المستضيف أو الجهاز الذي يجرى من عنده توجيه الحدث (الأحداث) (عنوان شبكة، اسم شبكة، وما إلى ذلك)
User	صفر أو واحد (1)		معلومات عن المستعمل الذي يجرى من عنده توجيه الحدث (الأحداث)
Service	صفر أو واحد (1)		معلومات عن خدمة الشبكة المشاركة في الحدث (الأحداث)

5.3.2.8 صنف SourceNAT

يتضمن صنف SourceNAT معلومات عن المصدر المحتمل (المصادر المحتملة) لحدث (أحداث) NAT الذي يولد (التي تولد) دورة. وقد يكون للحدث الواحد أكثر من مصدر يحول بواسطة NAT.

ويتألف صنف SourceNAT للمصدر من ثلاثة أصناف تجميع، كما يتضح من الشكل 12.



الشكل 12 – أصناف تجميع صنف SourceNAT

ولهذا الصنف نعتان على النحو المبيَّن في الجدول 17

الجدول 17 – نعتا صنف SourceNAT

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرفة هوية فريد للمصدر المحول بترجمة NAT
interface	اختياري	STRING	يمكن استعماله بواسطة جهاز قائم على الشبكة مع سطوح بينية متعددة لبيان السطح البيني الذي يرى منه تحويل هذا المصدر بترجمة NAT

ويرد شرح أصناف التجميع التي يتألف منها صنف SourceNAT في الجدول 18.

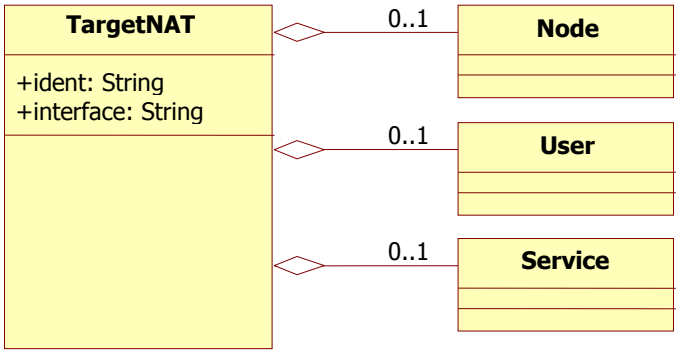
الجدول 18 – مكونات صنف SourceNAT

الأصناف	التجميع	نمط البيانات	الوصف
Node	صفر أو واحد (1)		معلومات عن المستضيف أو الجهاز الذي يعتقد أنه المتسبب في الأحداث (عنوان شبكة، اسم شبكة، وما إلى ذلك)
User	صفر أو واحد (1)		معلومات عن المستعمل الذي يعتقد أنه المتسبب في الحدث (الأحداث)
Service	صفر أو واحد (1)		معلومات عن خدمة الشبكة المشاركة في الحدث (الأحداث)

6.3.2.8 صنف TargetNAT

يتضمن هذا الصنف معلومات عن الهدف المحتمل (الأهداف المحتملة) لحدث (أحداث) ترجمة NAT الذي يولد (التي تولد) دورة. وقد يكون للحدث الواحد أكثر من هدف محول بواسطة ترجمة NAT.

ويتألف صنف TargetNAT من ثلاثة أصناف تجميع، كما هو مبين في الشكل 13.



الشكل 13 – أصناف التجميع لصنف TargetNAT

ولصنف TargetNAT نعتان على النحو المبيَّن في الجدول 19.

الجدول 19 – نعتا صنف TargetNAT

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد لهذا الهدف المحول بترجمة NAT
interface	اختياري	STRING	يمكن استعماله بواسطة جهاز قائم على الشبكة مع سطوح بينية متعددة لبيان السطح البيني الذي يرى منه هذا الهدف المحمول بترجمة NAT

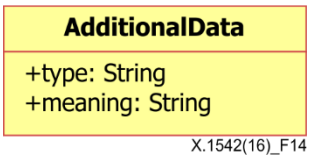
ويرد شرح أصناف التجميع التي يتألف منها صنف TargetNAT في الجدول 20.

الجدول 20 – مكونات صنف ترجمة عنوان شبكة الهدف

الأصناف	التجميع	نمط البيانات	الوصف
Node	صفر أو واحد (1)		معلومات عن المستضيف أو الجهاز الذي يجرى من عنده توجيه الحدث (الأحداث) (عنوان شبكة، اسم شبكة، وما إلى ذلك)
User	صفر أو واحد (1)		معلومات عن المستعمل الذي يجرى من عنده توجيه الحدث (الأحداث)
Service	صفر أو واحد (1)		معلومات عن خدمة الشبكة المشاركة في الحدث (الأحداث)

7.3.2.8 صنف AdditionalData

يستعمل صنف AdditionalData لتقديم معلومات يتعذر تمثيلها بنموذج بيانات النسق SIMEF. ويمكن استعمال هذا الصنف لتقديم البيانات الذرية (أعداد صحيحة، سلاسل، وما إلى ذلك) في الحالات التي تكون فيها حاجة إلى إرسال كم قليل فقط من البيانات الإضافية؛ ويمكن استعمالها أيضاً لتوسيع نموذج البيانات وتعريف نمط الوثيقة (DTD) لدعم إرسال بيانات مركبة (مثل رأسيات الرزم).



الشكل 14 – صنف AdditionalData

ولصنف البيانات الإضافية نعتان على النحو المبيَّن في الجدول 21.

الجدول 21 – نعتا صنف AdditionalData

النعت	الاستعمال	نمط البيانات	الوصف
type	مطلوب	ENUM	نمط بيانات يشرح معنى محتوى العنصر القيمة بالتغيب: string (سلسلة)
meaning	اختياري	STRING	سلسلة تشرح معنى محتوى العنصر

وتمثل أنماط صنف AdditionalData في الجدول 22 وتعرض القيم المسموح بها لهذا النعت في نفس الجدول.

الجدول 22 – قيم نعت النمط

القيمة	مصطلحات أساسية	التعريف
0	boolean	العنصر يحتوي على قيمة بولانية أي السلاسل "حقيقية" أو "كاذبة"
1	byte	محتوى العنصر بايتة وحيدة من 8 بتات
2	character	محتوى العنصر رمز وحيد
3	date-time	محتوى العنصر سلسلة بالتاريخ–التوقيت
4	integer	محتوى العنصر عدد صحيح
5	ntpstamp	محتوى العنصر خاتم توقيت للبروتوكول NTP
6	portlist	محتوى العنصر قائمة بالمنافذ
7	real	محتوى العنصر عدد حقيقي
8	string	محتوى العنصر سلسلة
9	Byte-string	محتوى العنصر [] بايتة
10	xml	محتوى العنصر بيانات موسومة باللغة XML

وقيم صنف AdditionalData هذه تعتمد على البائع/التنفيذ؛ وطريقة التأكد من فهم المدراء للسلاسل المرسلة من المحللات خارج نطاق هذه التوصية.

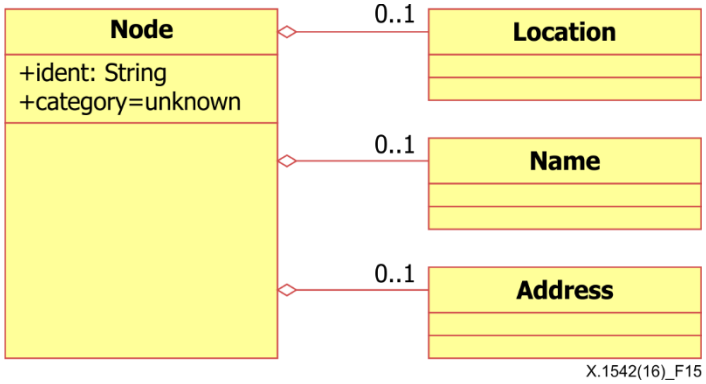
4.2.8 أصناف Support

تشكل أصناف Support (الدعم) الأجزاء الرئيسية للأصناف الأساسية ويتم تبادلها فيما بينها.

1.4.2.8 صنف Node

يستعمل صنف Node (العقدة) لتحديد المستضيفات وأجهزة الشبكة الأخرى (المسيرات والمبدلات وما إلى ذلك).

ويتألف صنف Node من ثلاثة أصناف تجميع، كما هو مبين في الشكل 15. وترد في الجدول 23 والجدول 24 والجدول 25 على التوالي النعوت، وقيمة نعت النمط، ومكونات صنف العقدة.



الشكل 15 – أصناف التجميع لصنف Node

الجدول 23 – نعتا صنف Node

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد للعقدة؛ انظر الفقرة 9.2.7
category	اختياري	ENUM	"الميدان" الذي استخرجت معلومات الاسم. القيمة بالتغيب = unknown (غير معروفة)

الجدول 24 – قيم نعت النمط

القيمة	مصطلحات أساسية	التعريف
0	Unknown	الميدان غير معروف أو غير ذي صلة
1	ads	خدمات الدليل المتقدمة للإصدار ويندوز 2000
2	afs	نظام أندرو للملفات (Transarc)
3	coda	نظام الملفات الموزع Coda
4	dfs	نظام الملفات الموزع (IBM)
5	dns	نظام أسماء الميادين
6	hosts	ملف المستضيفات المحلية
7	kerberos	ميدان كيربيروس
8	nds	خدمات الدليل الجديدة
9	nis	خدمات معلومات الشبكة (Sun)
10	nisplus	خدمات معلومات الشبكة القائمة (Sun)
11	nt	ميدان NT ويندوز
12	wfw	ويندوز لمجموعات العمل

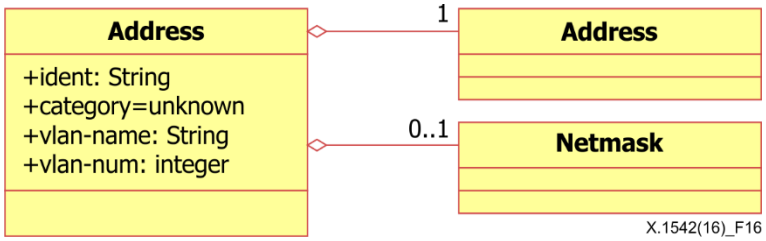
الجدول 25 – مكونات صنف Node

الأصناف	التجميع	نمط البيانات	الوصف
Location	صفر أو واحد (1)	STRING	موقع المعدة
Name	صفر أو واحد (1)	STRING	اسم المعدة. يجب أن تقدم هذه المعلومات عندما لا تقدم معلومات العنوان
Address	صفر أو أكثر		عنوان شبكة أو عتاد المعدة. ما لم يقدم اسم (أعلاه)، يجب تحديد عنوان واحد على الأقل.

2.4.2.8 صنف Address

يستعمل صنف Address (العنوان) لتمثيل عناوين الشبكات والعتاد والتطبيقات.

ويتألف صنف Address من صنف تجميع، كما هو مبين في الشكل 16.



الشكل 16 – صنفا تجميع صنف Address

وترد في الجدول 26 والجدول 27 والجدول 28 على التوالي، النعوت، وقيمة نعت النمط، ومكونات صنف العقدة.

الجدول 26 – نعوت صنف Address

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد للعنوان انظر الفقرة 9.2.7
category	اختياري	ENUM	نمط العنوان الممثل. وتعرض أدناه القيم المسموح بها لهذا النعت. القيمة بالتغيب: غير معروف
vlan-name	اختياري	STRING	اسم الشبكة المحلية (الشبكة المحلية الافتراضية) التي ينتمي إليها العنوان
Vlan-num	اختياري	INTEGER	رقم الشبكة المحلية (الشبكة المحلية الافتراضية) التي ينتمي إليها العنوان

الجدول 27 – قيم نعت النمط

القيمة	مصطلحات أساسية	التعريف
0	unknown	نمط العنوان غير معروف
1	atm	عنوان شبكة بأسلوب نقل غير متزامن
2	e-mail	عنوان بريد إلكتروني (المعيار [b-IETF RFC 2822])
3	lotus-notes	عنوان بريد إلكتروني Lotus Notes
4	Mac	عنوان التحكم في النفاذ إلى الوسائط
5	Sna	عنوان معمارية شبكة متقاسمة IBM
6	Vm	عنوان بريد إلكتروني (“PROFS”)
7	ipv4-addr	عنوان المضيف IPV4 بالترميز العشري المنقط (a.b.c.d)

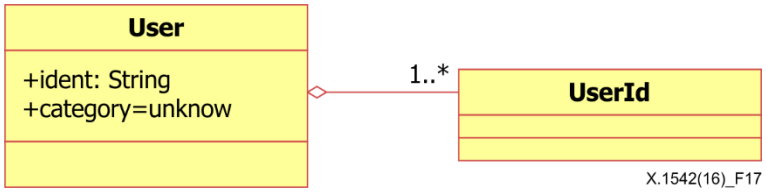
القيمة	مصطلحات أساسية	التعريف
8	ipv4-addr-hex	عنوان المضيف IPV4 بالترميز الستة عشري
9	ipv4-net	عنوان شبكة IPV4 بالترميز العشري المنقط، والخط المائل المامي وبتات الدلالة (a.b.c.d/nn)
10	ipv4-net-mask	عنوان الشبكة IPV4 بالترميز العشري المنقط مع الخط المائل الأمامي وقناع الشبكة بالترميز العشري المنقط (a.b.c.d./w.x.y.z)
11	ipv6-addr	عنوان المضيف IPv6
12	ipv6-addr-hex	عنوان المضيف IPv6 بالترميز الستة عشري
13	ipv6-net	عنوان الشبكة IPv6 بالخط المائل الأمامي وبتات الدلالة
14	Ipv6-net-mask	عنوان الشبكة IPv6 بالخط المائل الأمامي وقناع الشبكة

الجدول 28 – مكونات صنف Address

الأصناف	التجميع	نمط البيانات	الوصف
Address	واحد بالضبط	STRING	معلومات العنوان. يحدد نسق هذه البيانات نعت category
Netmask	صفر أو واحد (1)	STRING	قناع الشبكة للعنوان، حسب الاقتضاء.

3.4.2.8 صنف User

يستخدم صنف User (المستعمل) لوصف المستعملين. وهو يستخدم أساساً بوصفه صنف "حاوية" لصنف تجميع UserId، كما هو مبين في الشكل 17.



الشكل 17 – صنفا تجميع صنف User

وترد في الجدول 29 والجدول 30 والجدول 31 على التوالي، النعوت، وقيمة نعت النمط، ومكونات صنف العقدة.

الجدول 29 – نعتا صنف User

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد للمستعمل، انظر الفقرة 9.2.7.
category	اختياري	ENUM	نمط المستعمل الممثل. وترد أدناه القيم المسموح بها لهذا النعت. القيمة بالتغيب = unknown (غير معروف)

الجدول 30 – قيم نعت النمط

القيمة	مصطلحات أساسية	التعريف
0	unknown	نمط المستعمل غير معروف
1	application	مستعمل تطبيق
2	os-device	نظام تشغيل أو مستعمل جهاز

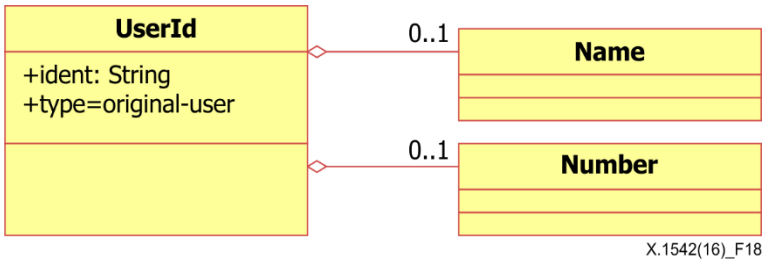
الجدول 31 – مكونات صنف User

الأصناف	التجميع	نمط البيانات	الوصف
UserId	واحد (1) أو أكثر		تعريف هوية مستعمل، كما هو مبين بنعت type الخاص به

1.3.4.2.8 صنف معرفة UserId

يوفر هذا الصنف معلومات محددة عن أي مستعمل. ويمكن استخدام أكثر من صنف UserId ضمن صنف User لبيان محاولات الانتقال من مستعمل لآخر أو تقديم معلومات كاملة عن امتيازات المستعمل (أو العملية).

ويتألف صنف UserId (معرف هوية المستعمل) من صنفين للتجميع، كما هو مبين في الشكل 18.



الشكل 18 – أصناف تجميع صنف UserId

وترد في الجدول 32 والجدول 33 على التوالي، النعوت، وقيمة نعت النمط، لصنف UserId.

الجدول 32 – نعوت صنف UserId

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد لمعرفة هوية المستعمل، انظر الفقرة 9.2.7.
type	اختياري	ENUM	نمط معلومات المستعمل الممثلة. وترد أدناه القيم المسموح بها لهذا. القيمة بالتغيب = مستعمل أصلي

الجدول 33 – قيم نعوت النمط

القيمة	مصطلحات أساسية	التعريف
0	current-user	معرف هوية المستعمل الحالي الذي يستخدمه المستعمل أو العملية
1	original-user	الهوية الفعلية للمستعمل أو العملية المبلغ عنها. وينبغي استعمال هذه القيمة بشأن الأنظمة التي (أ) تقوم بشكل ما من أشكال المراجعة و (ب) تدعم استخلاص معرف هوية المستعمل من تأشيرة "معرف هوية المراجعة".
2	target-user	معرف هوية المستعمل الذي يحاول المستعمل أو العملية أن يكونا عليه. وبتطبيق ذلك على أنظمة Unix مثلاً، عندما يحاول المستعمل استخدام "su" أو "rlogin" أو "telnet" وما إلى ذلك.

القيمة	مصطلحات أساسية	التعريف
3	user-privs	معرف هوية آخر للمستعمل أو العملية يمكنها استخدامه أو UserID مرتبط بتصريح الملف. عناصر متعددة لمعرف هوية المستعمل لهذا النمط يمكن استخدامها لتحديد قائمة الامتيازات.
4	current-group	معرف هوية المجموعة الحالي (إن وجد) الذي يستخدمه المستعمل أو العملية.
5	group-privs	معرف هوية آخر للمجموعة يمكن للمجموعة أو العملية استخدامه أو معرفة هوية مرتبط بتصريح الملف. فعلى سبيل المثال، في أنظمة Unix المقدمة بتوزيع برمجية بيركيلي (BSD)، تستخدم عناصر متعددة لمعرف UserID من هذا النمط لإدراج جميع معرفات هوية المجموعة على "group list" (قائمة المجموعات).
6	other-privs	لا تستخدم في سياق مستعمل أو مجموعة أو عملية، وتستخدم فقط في سياق الملف. وتصاريح الملفات التي تخصص للمستعملين لا تتفق لا مع تصاريح المستعملين أو المجموعات بشأن الملف.

وترد في الجدول 34 أصناف التجميع التي يتألف منها صنف UserId.

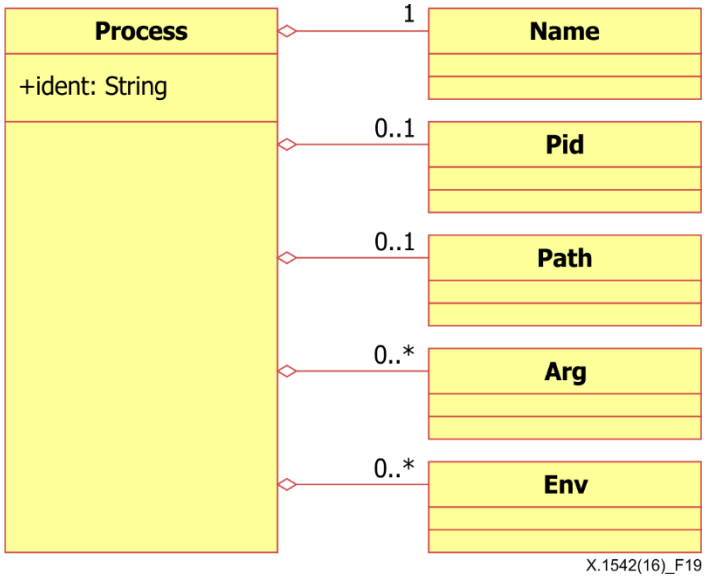
الجدول 34 – مكونات صنف UserId

الأصناف	التجميع	نمط البيانات	الوصف
Name	صفر أو واحد (1)	STRING	اسم مستعمل أو مجموعة.
Num	صفر أو واحد (1)	INTEGER	رقم مستعمل أو مجموعة

4.4.2.8 صنف Process

يستعمل صنف Process (العملية) لوصف العمليات الجاري تنفيذها على المصادر والأهداف والمحللات.

ويتألف صنف Process من خمسة نعوت تجميع، كما هو مبين في الشكل 19.



الشكل 19 – أصناف تجميع صنف Process

ولصنف Process نعت واحد (انظر الجدول 35).

الجدول 35 – نعت صنف Process

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرفة هوية فريد للعملية، انظر الفقرة 9.2.7.

وترد في الجدول 36 أصناف التجميع التي يتألف منها صنف Process.

الجدول 36 – مكونات صنف Process

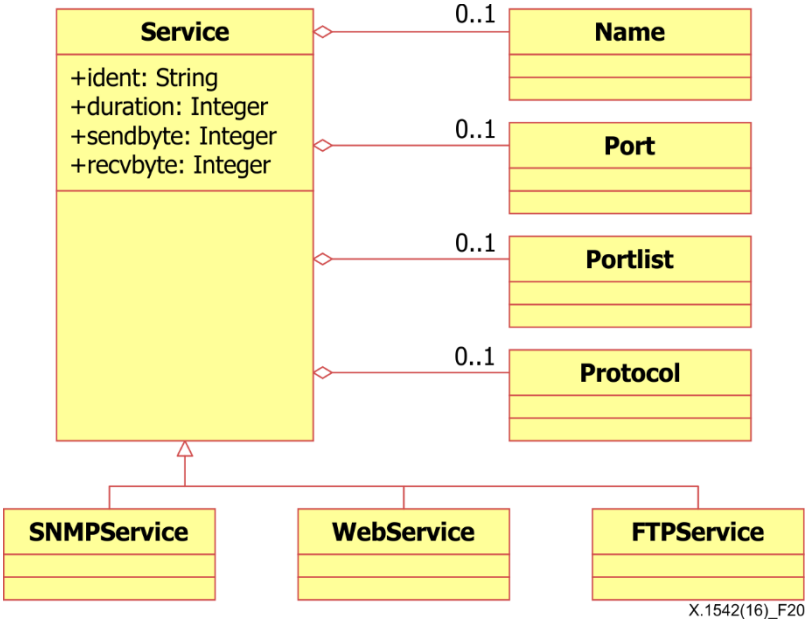
الأصناف	التجميع	نمط البيانات	الوصف
Name	واحد بالضبط	STRING	اسم البرنامج الجاري تنفيذه.
Pid	صفر أو واحد (1)	INTEGER	معرف هوية العملية الخاص بالعملية.
Path	صفر أو واحد (1)	STRING	المسار الكامل للبرنامج الجاري تنفيذه.
Arg	صفر أو واحد (1)	STRING	بند من خط الأوامر للبرنامج.
Env	صفر أو واحد (1)	STRING	سلسلة للبيئة المرتبطة بالعملية، تكون عادة بالنسق "VARIABLE=value"

وفي صنف Process، يكون نصف Name اسماً قصيراً، مع إمكانية تحديد بنود متعددة مع استعمالات متعددة للصنف arg (بند). ويمكن تحديد سلاسل بيئات متعددة مع استعمالات متعددة للصنف env (البيئة).

5.4.2.8 صنف Service

يصف صنف Service (الخدمة) خدمات الشبكة على المصادر والأهداف. ويمكنه تحديد الخدمات بالاسم والمنفذ وقائمة المنافذ والبروتوكول. وعندما تحدث خدمة في شكل صنف تجميع Source، يفهم أن الخدمة هي التي ينشأ عنها النشاط المعني؛ وأن الخدمة "مرفقة" بالعقدة وأن معلومات العملية والمستعمل مدرجة أيضاً في المصدر. وبالمثل، عندما تحدث الخدمة في شكل صنف تجميع Target يفهم أن الخدمة هي التي يوجه إليها النشاط المعني؛ وأن الخدمة "مرفقة" بالعقدة وأن معلومات العملية والمستعمل مدرجة أيضاً في الهدف. وإذا حدثت الخدمة في Source وTarget على السواء، ينبغي للمعلومات في الموقعين أن تكون واحدة. فإذا كانت المعلومات واحدة في الموقعين وكان المنفذون يرغبون في حملها في موقع واحد، ينبغي تحديدها كما لو كانت تجميعاً لصنف Target.

ويتألف صنف Service من أربعة أصناف تجميع، كما هو مبين في الشكل 20.



الشكل 20 – أصناف التجميع لصنف Service

ولصنف Service أربعة نعوت ترد في الجدول 37.

الجدول 37 – نعوت صنف Service

النعت	الاستعمال	نمط البيانات	الوصف
ident	اختياري	STRING	معرف هوية فريد للخدمة، انظر الفقرة 9.2.7
duration	اختياري	INTEGER	مدة التوصيل
sendbyte	اختياري	INTEGER	حجم البايتة المرسلة بعد التوصيل
recvByte	اختياري	INTEGER	حجم البايتة المستقبلة بعد التوصيل

وترد في الجدول 38 أصناف التجميع التي يتألف منها صنف Service.

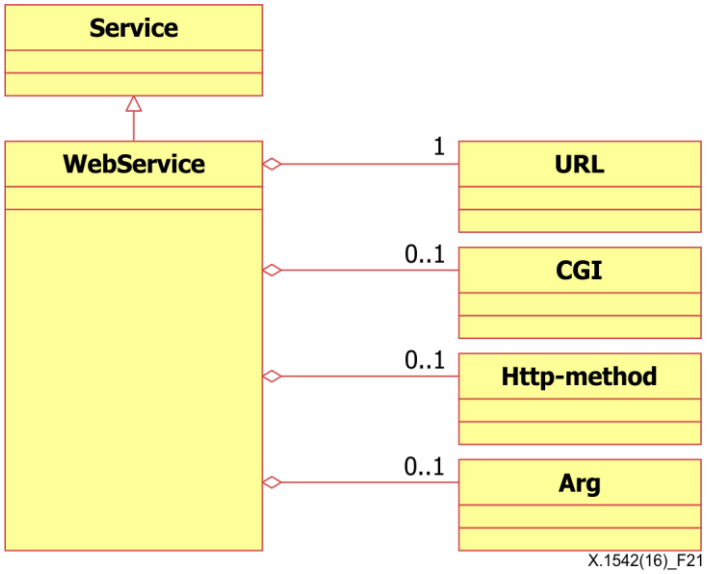
الجدول 38 – مكونات صنف Service

الصنف	التجميع	نمط البيانات	الوصف
Name	صفر أو واحد (1)	STRING	اسم الخدمة. ينبغي، متى كان ذلك ممكناً، استعمال الاسم المأخوذ من قائمة المنافذ معروفة جيداً صادرة عن هيئة تخصيص أرقام الإنترنت (IANA)
Port	صفر أو واحد (1)	INTEGER	رقم المنفذ المستعمل
Portlist	صفر أو واحد (1)	PORTLIST	قائمة بأرقام المنافذ المستعملة، انظر الفقرة 8.2.7 من أجل قواعد التنسيق
Protocol	صفر أو واحد (1)	STRING	معلومات إضافية عن البروتوكول المستعمل

1.5.4.2.8 صنف WebService

يحمل صنف WebService (خدمة الويب) معلومات إضافية تتعلق بحركة الويب.

ويتألف صنف WebService من أربعة أصناف تجميع، كما هو مبين في الشكل 21.



الشكل 21 – أصناف تجميع صنف WebService

وترد في الجدول 39 أصناف التجميع التي يتألف منها صنف WebService.

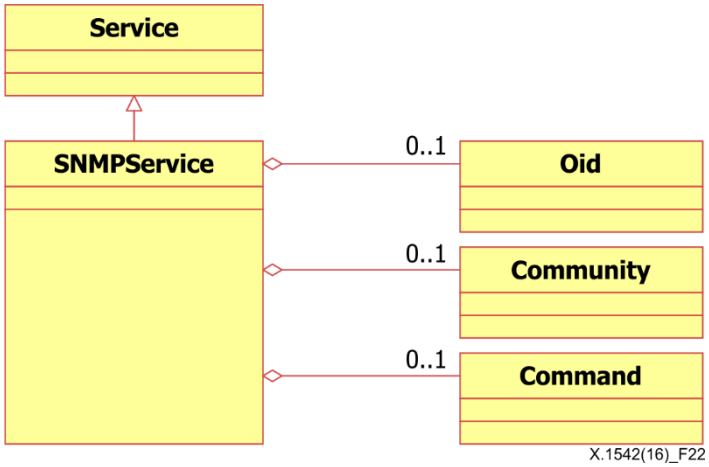
الجدول 39 – مكونات صنف WebService

الأصناف	التجميع	نمط البيانات	الوصف
URL	واحد (1) بالضبط	STRING	موقع الموارد الموحد (URL) في الطلب
CGI	صفر أو واحد (1)	STRING	السطح البيني للبوابة المشتركة (CGI) في الطلب، بدون بنود
Http-method	صفر أو واحد (1)	STRING	طريقة بروتوكول نقل النصوص المترابطة المستعملة في الطلب (GET ،PUT)
Arg	صفر أو واحد (1)	STRING	البنود المقدمة لنص السطح البيني

2.5.4.2.8 صنف SNMPService

يحمل صنف SNMPService (خدمة البروتوكول SNMP) معلومات إضافية تتعلق بحركة بروتوكول إدارة الحركة البسيط (SNMP).

ويتألف صنف SNMPService من ثمانية أصناف تجميه كما هو، مبين في الشكل 22.



الشكل 22 – أصناف التجميع لصنف SNMPService

وترد في الجدول 40 أصناف التجميع التي يتألف منها صنف SNMPService.

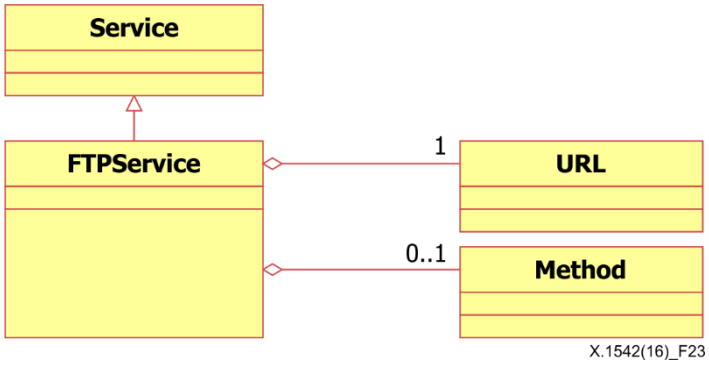
الجدول 40 – مكونات صنف SNMPService

الأصناف	التجميع	نمط البيانات	الوصف
Oid	صفر أو واحد (1)	STRING	معرف هوية الكائن في الطلب
Community	صفر أو واحد (1)	STRING	سلسلة مجتمع الكائن
Command	صفر أو واحد (1)	STRING	الأمر المرسل إلى مخدم البروتوكول SNMP (GET، SET، وما إلى ذلك)

3.5.4.2.8 صنف FTPService

يحمل صنف FTPService (خدمة البروتوكول FTP) معلومات إضافية تتعلق بحركة بروتوكول نقل الملفات (FTP).

ويتألف صنف FTPService من صنفين للتجميع، كما هو مبين في الشكل 23.



الشكل 23 – صنفا التجميع لصنف FTPService

ويرد في الجدول 41 صنفا التجميع المكونان لصنف FTPService.

الجدول 41 – مكونا صنف FTPService

الأصناف	التجميع	نمط البيانات	الوصف
URL	واحد (1) بالضبط	STRING	الموقع URL في الطلب.
Method	صفر أو واحد (1)	STRING	طريقة البروتوكول FTP المستعملة في الطلب (PUT، GET).

9 اعتبارات الأمن

تناقش هذه الفقرة الاعتبارات الأمنية التي يجب أن تؤخذ في الاعتبار من جانب منفذي النسق SIMEF.

وتشرح هذه التوصية نموذج المعلومات من أجل نسق تبادل الرسائل المتعلقة بمعلومات الدورة (SIMEF) وتقدم نموذج بيانات مصاحباً يرد توصيفه بمخطط اللغة XML. ويحدد النسق SIMEF تمثيلاً لنموذج بيانات من أجل تبادل معلومات سجل دورة طبقة النقل فيما يتعلق بالإدارة المركزية لأمن الشبكة ونظام تبادل معلومات الأمن.

وعلى الرغم من عدم وجود شواغل أمنية تتعلق مباشرة بنسق هذه البيانات، فإن البيانات نفسها يمكن أن تتضمن معلومات حساسة أمنياً قد تتطلب حماية سريتها و/أو سلامتها و/أو تيسرها.

وتقترح هذه التوصية ضرورة حماية الأنظمة المستعملة في جميع هذه البيانات وإرسالها ومعالجتها وتخزينها من الاستعمال غير المرخص مع حماية البيانات نفسها من النفاذ غير المرخص. ووسائل تحقيق هذه الحماية خارج نطاق هذه التوصية.

التذييل I

مثال على النسق SIMEF ومخططه

(لا يشكل هذا التذييل جزءاً من هذه الوثيقة)

يورد هذا التذييل مثالاً على مخطط باللغة XML للنموذج SIMEF. والأمثلة التالية عبارة عن المخططين XML وSYSLOG لتشفير معلومات الدورة في النموذج SIMEF.

I.1 مخطط النسق SIMEF

I.1.1 المخطط XML

```
<?xml version="1.0" encoding="UTF-8"?>

<simef:SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef/">
     <Connect ident="1008380" criticality="normal">
        <Device Deviceid="TTA-FW" model="FW1000">
           <Node>
              <Address category="ipv4-addr">
                <address>1.1.1.1</address>
              </Address>
           </Node>
        </Device>
        <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaa">
                  2010-08-18T15:41:28+00:00
           </CreateTime>
        <Policy Ruleid="45" action="pass"></Policy>
           <Source>
           <Node>
              <Address category="ipv4-addr">
                <address>2.2.2.2</address>
              </Address>
           </Node>
           <Service duration="9" size="144">
              <port>38168</port>
              <protocol>17</protocol>
           </Service>
        </Source>
        <Target>
           <Node>
              <Address category="ipv4-addr">
                <address>3.3.3.3</address>
              </Address>
           </Node>
           <Service duration="9" size="0">
              <name>dns</name>
              <port>53</port>
              <protocol>17</protocol>
           </Service>
        </Target>
        <Classification origin="vendor-specific">
           <name>45</name>
        </Classification>
     </Connect>
</simef:SIMEF-Message>
```

2.1.I المخطط SYSLOG

```
2014-03-18 15:41:28 Local0.Notice 1.1.1.1 TTA: TTA-FW device_id= TTA [Root]system-notification-00257(traffic):    start_time="2014-03-18    15:41:19"    duration=9 policy_id=45 service=dns proto=17 src zone=Untrust dst zone=Trust action=Permit sent=144 rcvd=0 src=2.2.2.2 dst=3.3.3.3 src_port=38168 dst_port=53 src-xlated ip=2.2.2.2   port=38168   dst-xlated   ip=3.3.3.3   port=53   session_id=1008380 reason=Close - AGE OUT<000>
```

2.I أمثلة للنسق SIMEF

1.2.I تصريح جدار الحماية

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008380" criticality="1">
              <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
                            </Address>
                     </Node>
              </Device>
              <Policy Ruleid="45" action="1"></Policy>
              <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                     2014-03-18T15:41:28+00:00
              </CreateTime>
              <Source>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>2.2.2.2</address>
                            </Address>
                     </Node>
                      <Service duration="9" size="144">
                            <port>38168</port>
                            <protocol>17</protocol>
                     </Service>
              </Source>
              <Target>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>3.3.3.3</address>
                            </Address>
                     </Node>
                     <Service duration="9" size="0">
                            <name>dns</name>
                            <port>53</port>
                            <protocol>17</protocol>
                     </Service>
              </Target>
              <Classification origin="2">
                     <name>45</name>
              </Classification>
       </Connect>
</SIMEF-Message>
```

2.2.I السجل الخاص بالشبكة VPN

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008057" criticality="1">
              <Device Deviceid="TTA-VPN" manufacturer="TTA" model="VPN1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
```

```
                        </Address>
                    </Node>
                </Device>
                <Policy ruleid="700" action="3"></Policy>
                <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
                    2014-03-19T12:51:22+00:00
                </CreateTime>
                <Source>
                    <Node>
                        <Address category="ipv4-addr">
                            <address>2.2.2.2</address>
                        </Address>
                    </Node>
                    <Service duration="41" size="16905">
                        <port>59078</port>
                        <protocol>TCP</protocol>
                    </Service>
                </Source>
                <Target>
                    <Node>
                        <Address category="ipv4-addr">
                            <address>3.3.3.3</address>
                        </Address>
                    </Node>
                    <Service duration="41" size="1448">
                        <name>junos-http</name>
                        <port>80</port>
                        <protocol>TCP</protocol>
                    </Service>
                </Target>
                <Classification origin="2">
                    <name>700</name>
                </Classification>
        </Connect>
</SIMEF-Message>
```

3.2.I سجل ترجمة عنوان الشبكة (NAT)

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
        <Connect ident="1009632" criticality="1">
                <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
                <Node>
                        <Address category="ipv4-addr">
                            <address>1.1.1.1</address>
                        </Address>
                    </Node>
                </Device>
                <Policy ruleid="57" action="1"></Policy>
                <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
                    2014-03-19T16:21:12+00:02
                </CreateTime>
                <Source>
                    <Node>
                        <Address ident="" category="ipv4-addr">
                            <address>2.2.2.2</address>
                        </Address>
                    </Node>
                    <Service duration="41" size="16905">
                        <port>59078</port>
                        <protocol>TCP</protocol>
                    </Service>
                </Source>
                <Target>
```

```
                <Node>
                        <Address ident="" category="ipv4-addr">
                                <address>3.3.3.3</address>
                        </Address>
                </Node>
                <Service duration="41" size="1448">
                        <name>junos-http</name>
                        <port>80</port>
                        <protocol>TCP</protocol>
                </Service>
        </Target>
        <SourceNat>
                <Node>
                        <name>trust</name>
                        <Address category="ipv4-addr">
                                <address>4.4.4.4</address>
                        </Address>
                </Node>
                <Service>
                        <port>59078</port>
                </Service>
        </SourceNat>
        <TargetNat>
                <Node>
                        <Address category="ipv4-addr">
                                <address>5.5.5.5</address>
                        </Address>
                </Node>
                <Service>
                        <port>80</port>
                </Service>
        </TargetNat>
    </Connect>
</SIMEF-Message>
```

بيبليوغرافيا

[b-ISO 8601:2004] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times.*

[b-ISO/IEC 10646] ISO/IEC 10646:2012, *Information technology – Universal Coded Character Set (UCS).*

[b-IEEE Std 1003.1] IEEE Std 1003.1-2008, *IEEE Standard for Information Technology – Portable Operating System Interface (POSIX(R)).*

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network time protocol (version 3): Specification, implementation*.

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP network address translator (NAT): Terminology and considerations*.

[b-IETF RFC 2822]) IETF RFC 2822 (2001), *Internet message format*.

[b-IETF RFC 5905] IETF RFC 5905 (2010), *Network time protocol version 4: Protocol and algorithms specification*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2017