الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2205

(2011/05)

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

شبكات الجيل التالي – الجوانب الخاصة بالخدمة:
قدرات ومعمارية الخدمات

شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية

التوصيـــة ITU-T Y.2205

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وجوانب متعلقة ببروتوكول 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
جودة الخدمة وأداء الشبكة	Y.1599–Y.1500
التشوير	Y.1699–Y.1600
الإدارة والتشغيل والصيانة	Y.1799–Y.1700
الترسيم	Y.1899–Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099–Y.2000
جودة الخدمة والأداء	Y.2199–Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	**Y.2249–Y.2200**
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات وشبكات الجيل التالي	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
الشبكات الذكية الشمولية	Y.2699-Y.2600
الأمن	Y.2799–Y.2700
التنقلية المعممة	Y.2899–Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3099-Y.3000

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

التوصيـــة ITU-T Y.2205

شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية

ملخص

تحدد هذه التوصية الاعتبارات التقنية التي يمكن استخدامها اختيارياً في شبكات الجيل التالي (NGN) بهدف تمكين اتصالات الطوارئ (ET). كما تتناول بإيجاز المبادئ التقنية التي ينطوي عليها دعم هذه الاتصالات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2205	2008-09-12	13
2.0	ITU-T Y.2205	2011-05-20	13

مصطلحات أساسية

معمارية، إنذار مبكر (EW)، اتصالات طوارئ، خدمة اتصالات طوارئ (ETS)، شبكة الجيل التالي (NGN)، اتصالات تفضيلية، الاتصالات ذات الأولوية، جودة الخدمة (QoS)، اتصالات الإغاثة وقت الكوارث (TDR).

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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/.

© ITU 2012

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق 1

2 المراجع 1

1.2 قطاع تقييس الاتصالات (ITU-T) 1
2.2 فريق مهام هندسة الإنترنت (IETF) 3
3.2 المعهد الأوروبي لمعايير الاتصالات (ETSI) 4
4.2 منتدى النطاق العريض 4

3 التعاريف 4

1.3 مصطلحات معرَّفة في أماكن أخرى 4
2.3 مصطلحات معرَّفة في هذه التوصية 4

4 المختصرات 5

5 وصف اتصالات الطوارئ (ET) والإنذار المبكر 7

1.5 معلومات عامة 7
2.5 اتصالات الطوارئ 8
3.5 الإنذار المبكر 9

6 اعتبارات عامة متعلقة باتصالات الطوارئ والإنذار المبكر 9

7 المتطلبات والمقدرات الوظيفية العامة 10

1.7 اتصالات الطوارئ 10
2.7 الإنذار المبكر 11

8 المبادئ التوجيهية والمتطلبات العامة للأمن 12

1.8 المبادئ التوجيهية العامة 12
2.8 المتطلبات العامة 12

9 آليات ومقدرات دعم اتصالات الطوارئ في الشبكات NGN 13

1.9 معلومات عامة 13
2.9 طبقة الخدمة 18
3.9 طبقة النقل 20
4.9 دعم تكنولوجيا النفاذ إلى الشبكة NGN 22

10 دعم الاتصالات في حالات الطوارئ من طرف إلى طرف 27

11 آليات ومقدرات توفير بعض جوانب الإنذار المبكر في الشبكات NGN 29

1.11 معلومات عامة 29
2.11 بروتوكول الإنذار المشترك (CAP) 29
3.11 إجراءات تسجيل التفرعات في إطار تفرع معرّف الشيء المنبه 30

12 أولوية ترميم الخدمة 30

الصفحة

13 تبديل الحماية وترميمها 31

1.13 اعتبارات عامة 31
2.13 معماريات حماية التراتب الرقمي المتزامن (SDH) 32
3.13 شبكة النقل البصرية (OTN) 32
4.13 تبديل الحماية الخطية للإثرنت 32
5.13 تبديل الحماية الحلقية للإثرنت 33
6.13 تبديل الحماية الخطية لشبكات نقل تبديل الوسم بعدة بروتوكولات (T-MPLS) 33
7.13 تبديل حماية أسلوب النقل غير المتزامن (ATM) 33
8.13 تبديل الحماية لشبكات تبديل الوسم بعدة بروتوكولات (MPLS) 34

التذييل I – فئات اتصالات الطوارئ 35

1.I اتصالات الطوارئ من فرد إلى سلطة 35
2.I اتصالات الطوارئ من فرد إلى فرد 35
3.I اتصالات الطوارئ من سلطة إلى سلطة 35
4.I اتصالات الطوارئ من سلطة إلى فرد 36

التذييل II – أمثلة لاستعمال أنظمة الإنذار المبكر 37

1.II نموذج الدفع 37
2.II نموذج الجذب 37

التذييل III – مثال عن تدفقات النداء/الدورة لخدمة اتصالات الطوارئ (ETS) في شبكات الجيل التالي (NGN) 38

بيبليوغرافيا 40

مقدمة

تقدم التوصية [ITU-T Y.1271] متطلبات شبكات اتصالات الطوارئ (ET) ومقدراتها. وقد ينجم عن تشغيل الاتصالات ذات الأولوية، استناداً إلى هذه المتطلبات وعلى النحو الذي تنتهجه سلطات تنسيق عمليات الإغاثة وقت الكوارث باستعمالها لشبكات الاتصالات العمومية، خلق آليات جديدة وتشغيل بين الآليات القائمة و/أو إعادة استعمالها. وينبغي أن تحظى اتصالات الطوارئ بمعاملة تفضيلية في خدمات الشبكات العمومية العادية. ويُستخدم مصطلح الاتصالات التفضيلية في بعض توصيات قطاع تقييس الاتصالات ليشمل الخدمات التي تتطلب معالجتها الأولوية. والاتصالات في حالات الطوارئ هي إحدى فئات الخدمات التي تُعتبر حائزة على معاملة تفضيلية. ويُستخدم مصطلحا الاتصالات التفضيلية والاتصالات في حالات الطوارئ كمترادفين.

وإضفاء صفة الأولوية على الاتصالات في حالات الطوارئ ليس جديداً؛ فالشبكات العاملة بتبديل الدارات تمارسه منذ سنوات وبصورة أساسية فيما يتعلق بالنداءات الصوتية (مثال ذلك [ITU-T E.106]). غير أن الطرائق التقنية المستخدمة في دعم هذه المتطلبات الأساسية المتعلقة باتصالات الطوارئ في بيئة الشبكات NGN تتطور. وطرائق الأولوية التقليدية في الدارات التبديلية لا تصلح بالضرورة للشبكات NGN بسبب الاختلافات الأساسية القائمة بين الاتصالات العاملة بتبديل الدارات والاتصالات العاملة بتبديل الرزم.

وتعرض التوصية [ITU-T Y.1271] المتطلبات والمقدرات الوظيفية عموماً كما تعرض المصطلحات النظرية بصرف النظر عن التكنولوجيا المستخدمة.

ونظراً إلى أن شبكات الجيل التالي تقوم على أساس تكنولوجيا تبديل الرزم التي تختلف أساساً عن تكنولوجيا تبديل الدارات، فمن الضروري دراسة القضايا التقنية والحلول الممكنة التي يمكن استخدامها من أجل تحقيق المقدرات الوظيفية لاتصالات الطوارئ في الشبكات NGN.

وتحدد هذه التوصية الاعتبارات التقنية التي يمكن استخدامها في الشبكات NGN من أجل توفير اتصالات الطوارئ، وتقدم المبادئ ذات الصلة التي تنطوي عليها.

التوصيـــة ITU-T Y.2205

شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية

1 مجال التطبيق

تحدد هذه التوصية الاعتبارات التقنية التي يمكن استخدامها في شبكات الجيل التالي (NGN) بهدف دعم اتصالات الطوارئ (ET). وإضافة إلى ذلك، تتناول بإيجاز المبادئ التقنية التي ينطوي عليها دعم اتصالات الطوارئ. كما تحدد أيضاً المواصفات والمقدرات الوظيفية المتعلقة باتصالات الطوارئ والتي لم تتطرق إليها التوصية [ITU-T Y.2201] في سياق الشبكات NGN المحددة في التوصية [ITU-T Y.2001] والواردة بمزيد من التفاصيل في التوصية [ITU-T Y.2011].

وتضم اتصالات الطوارئ (بما فيها تحديد بعض جوانب الإنذار المبكر (انظر الشكل 1)) ما يلي:

- اتصالات طوارئ من فرد إلى سلطة، مثل نداءات إلى مقدمي خدمات الطوارئ؛
- اتصالات طوارئ من سلطة إلى سلطة؛
- اتصالات طوارئ من سلطة إلى فرد، مثل خدمات التبليغ المجتمعية.

ويقدم التذييل I مزيداً من المعلومات عن فئات اتصالات الطوارئ المذكورة أعلاه.

وهناك أيضاً بعض المواصفات والمقدرات الخاصة بالإنذار المبكر. أما المقدرات الخاصة باتصالات الطوارئ الموجهة من فرد إلى سلطة فلا تتناولها هذه التوصية بالدراسة وتبقى خارج مجال تطبيقها.

ويمكن استخدام بعض الأساليب التقنية الموصوفة هنا لاتصالات الطوارئ من فرد إلى سلطة أو من فرد إلى فرد، ولكن هذه التوصية لا تتناول هذه الفئات.

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.

1.2 قطاع تقييس الاتصالات (ITU-T)

[ITU-T E.106] التوصية ITU-T E.106 (2003)، *الخطة الدولية للأولويات في حالات الطوارئ (IEPS) من أجل عمليات الإنقاذ 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 G.808.1] التوصية ITU-T G.808.1 (2010)، *تبديل الحماية التنوعية – تسجيل خطي وحماية الشبكة الفرعية.*

[ITU-T G.841] التوصية ITU-T G.841 (1998)، *أنماط وخصائص معماريات حماية شبكات التراتب الرقمي المتزامن (SDH).*

[ITU-T G.842] التوصية ITU-T G.842 (1997)، *التشغيل البيني لمعماريات حماية شبكة التراتب الرقمي المتزامن.*

[ITU-T G.873.1] التوصية ITU-T G.873.1 (2006)، *شبكة النقل البصري (OTN): الحماية الخطية.*

[ITU-T G.983.1] التوصية ITU-T G.983.1 (2005)، *أنظمة النفاذ البصرية عريضة النطاق المعتمدة على الشبكات البصرية المنفعلة (PON).*

[ITU-T G.8031] التوصية ITU-T G.8031/Y.1342 (2009)، *تبديل الحماية الخطية في الإثرنت.*

[ITU-T G.8032] التوصية ITU-T G.8032/Y.1344 (2010)، *تبديل الحماية الحلقية في الإثرنت.*

[ITU-T G.8131] التوصية ITU-T G.8131/Y.1382 (2007)، *تبديل الحماية الخطية لشبكات نقل تبديل الوسم متعدد البروتوكولات (MPLS-TP).*

[ITU-T H.248.1] التوصية ITU-T H.248.1 (2005)، *بروتوكول التحكم في البوابة: الصيغة 3.*

[ITU-T H.248.81] التوصية ITU-T H.248.81 (2011)، *بروتوكول التحكم في البوابة: المبادئ التوجيهية لاستخدام مبين النداء ومبين الأولوية للخطة الدولية للأولويات في حالات الطوارئ (IEPS) ضمن البيانات الوصفية للتوصية ITU-T H.248.*

[ITU-T H.323] التوصية ITU-T H.323 (2009)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*

[ITU-T H.460.4] التوصية ITU-T H.460.4 (2007)، *تعيين أولوية النداءات والشبكة القطرية/الدولية لتحديد مصدر النداء بالنسبة إلى مصدر النداءات ذات الأولوية H.323.*

[ITU-T I.630] التوصية ITU-T I.630 (1999)، *تبديل حماية أسلوب النقل غير المتزامن (ATM).*

[ITU-T J.260] التوصية ITU-T J.260 (2005)، *متطلبات الاتصالات التفضيلية على الشبكات IPCablecom.*

[ITU-T J.261] التوصية ITU-T J.261 (2009)، *إطار تنفيذ الاتصالات التفضيلية في الشبكات PCablecom وIPCablecom2.*

[ITU-T J.262] التوصية ITU-T J.262 (2009)، *مواصفات الاستيقان في الاتصالات التفضيلية عبر الشبكات IPCablecom2.*

[ITU-T J.263] التوصية ITU-T J.263 (2009)، *مواصفات الأولوية في الاتصالات التفضيلية عبر الشبكات IPCablecom2.*

[ITU-T Q.812] التوصية ITU-T Q.812 (2004)، *البيانات العامة لبروتوكول الطبقة العليا في السطحين البينيين Q وX.*

[ITU-T Q.1741.6] التوصية ITU-T Q.1741.6 (2009)، *مراجع IMT-2000 من أجل الصيغة 8 للشبكة المركزية لنظام الاتصالات العالمية المتنقلة (UMTS) المشتَق من النظام العالمي للاتصالات المتنقلة (GSM).*

[ITU-T Q.3303.3] التوصية ITU-T Q.3303.3 (2008)، *بروتوكول التحكم في الموارد رقم 3 – بروتوكول السطح البيني Rw الواقع بين الكيان المادي لتقرير السياسة (PD-PE) والكيان المادي لإنفاذ السياسة (PD–PE) (السطح البيني): القطر.*

[ITU-T Q.3321.1] التوصية ITU-T Q.3321.1 (2010)، *بروتوكول التحكم في الموارد رقم 1، الإصدار 2 – بروتوكول السطح البيني Rs الواقع بين كيانات التحكم في الخدمة والكيان المادي لتقرير السياسة المتبعة.*

[ITU-T Q-Sup.57] الإضافة 57 إلى سلسلة التوصيات ITU-T Q (2008)، *متطلبات التشوير لدعم خدمة الاتصالات في حالات الطوارئ (ETS) ضمن شبكات بروتوكول الإنترنت.*

[ITU-T X.660] التوصية المعيار الدولي ISO/IEC 9834-1 | ITU-T X.660 (2008): 2008، *تكنولوجيا المعلومات – التوصيل البيني في الأنظمة المفتوحة (OSI) – إجراءات التشغيل لسلطات التسجيل OSI: الإجراءات العامة والقيم العليا لتفرعات المعرفات الدولية.*

[ITU-T X.674] التوصية ITU-T X.674 (2011)، *إجراءات تسجيل التفرعات في إطار فرع معرّف الأغراض التنبيهي.*

[ITU-T X.1303] التوصية ITU-T X.1303 (2007)، *بروتوكول الإنذار الموحد (CAP 1.1).*

[ITU-T Y.110] التوصية ITU-T Y.110 (1998)، *مبادئ البنية التحتية العالمية للمعلومات ومعمارية الإطار.*

[ITU-T Y.1271] التوصية ITU-T Y.1271 (2004)، *إطار (أُطُر) متطلبات ومقدرات الشبكة اللازمة لتوفير اتصالات الطوارئ عبر الشبكات المتطورة بتبديل الرزم.*

[ITU-T Y.1541] التوصية ITU-T Y.1541 (2006)، *أهداف أداء الشبكة للخدمات القائمة على بروتوكول الإنترنت.*

[ITU-T Y.1720] التوصية ITU-T Y.1720 (2006)، *تبديل حماية شبكات تبديل الوسم بعدة بروتوكولات (MPLS).*

[ITU-T Y.2001] التوصية ITU-T Y.2001 (2004)، *نظرة عامة على شبكات الجيل التالي.*

[ITU-T Y.2011] التوصية ITU-T Y.2011 (2004)، *المبادئ العامة والنموذج المرجعي العام لشبكات الجيل التالي.*

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

[ITU-T Y.2111] التوصية ITU-T Y.2111 (2008)، *وظائف التحكم في الموارد والقبول في شبكات الجيل التالي.*

[ITU-T Y.2171] التوصية ITU-T Y.2171 (2006)، *سويات أولوية مراقبة القبول في شبكات الجيل التالي.*

[ITU-T Y.2172] التوصية ITU-T Y.2172 (2007)، *درجات أولوية ترميم الخدمة في شبكات الجيل التالي.*

[ITU-T Y.2201] التوصية ITU-T Y.2201 (2009)، *متطلبات ومقدرات شبكات الجيل التالي في قطاع تقييس الاتصالات.*

[ITU-T Y.2701] التوصية ITU-T Y.2701 (2007)، *المتطلبات الأمنية من شبكات الجيل التالي الإصدار 1.*

[ITU-T Y.2702] التوصية ITU-T Y.2702 (2008)، *متطلبات الاستيقان والتخويل في شبكات الجيل التالي الإصدار 1.*

[ITU-T Y.2704] التوصية ITU-T Y.2704 (2010)، *آليات وإجراءات الأمن لشبكات الجيل التالي.*

[ITU-T Y.2720] التوصية ITU-T Y.2720 (2009)، *إطار إدارة الهوية في شبكات الجيل التالي.*

[ITU-T Y.2721] التوصية ITU-T Y.2721 (2010)، *متطلبات وحالات استخدام إدارة الهوية في شبكات الجيل التالي.*

[ITU-T Y.2722] التوصية ITU-T Y.2722 (2011)، *آليات إدارة الهوية في شبكات الجيل التالي.*

2.2 فريق مهام هندسة الإنترنت (IETF)

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[IETF RFC 3168] IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

[IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior)*.

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*.

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[IETF RFC 4340] IETF RFC 4340 (2006), *Datagram Congestion Control Protocol (DCCP)*.

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*.

[IETF RFC 4542] IETF RFC 4542 (2006), *Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite*.

[IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.

[IETF RFC 5865] IETF RFC 5865 (2010), *A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic*.

3.2 المعهد الأوروبي لمعايير الاتصالات (ETSI)

[ETSI TS 183 017] ETSI TS 183 017 V3.2.1 (2010), TISPAN *Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification*.

4.2 منتدى النطاق العريض

[BBF TR-058] Broadband Forum TR-058 (2003), *Multi-Service Architecture and Framework Requirements*.

[BBF TR-059] Broadband Forum TR-059 (2003), *DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*.

[BBF TR-101] Broadband Forum TR-101 (2011), *Migration to Ethernet-Based DSL Aggregation*.

3 التعاريف

1.3 مصطلحات معرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في أماكن أخرى:

1.1.3 تنبيه [ITU-T X.674]: رسالة تحذير أو إنذار بشأن خطر محدق أو مشكلة وشيكة.

2.1.3 وكالة تنبيه [ITU-T X.674]: جهة وطنية أو إقليمية أو دولية مسؤولة عن إدارة التنبيهات.

3.1.3 خدمة اتصالات الطوارئ (ETS) [ITU-T E.107]: خدمة وطنية توفر أولوية الاتصالات للمستخدمين المخوّلين باستعمال خدمة اتصالات الطوارئ في أوقات الكوارث وحالات الطوارئ.

4.1.3 شبكة الجيل التالي (NGN) [ITU-T Y.2001]: شبكة تقوم على أساس الرزمة ويمكنها تقديم خدمات الاتصالات والاستفادة من النطاق العريض المتعدد وتكنولوجيات النقل التي تتسم بجودة الخدمة وتكون فيها الوظائف المتصلة بالخدمة مستقلة عن التكنولوجيات الأساسية المتصلة بالنقل. وتتيح هذه الشبكة نفاذ المستخدمين دون عوائق إلى الشبكات ومقدمي الخدمات المتنافسين و/أو الخدمات التي يختارونها. وهي تدعم التنقلية العامة التي تسمح بتقديم الخدمات إلى المستخدمين بشكل متسق في آن واحد في كل مكان.

2.3 مصطلحات معرَّفة في هذه التوصية

تستعمل هذه التوصية المصطلحات التالية:

1.2.3 اتصالات الطوارئ (ET): أي خدمة طوارئ تتطلب معالجة خاصة من الشبكة NGN مقارنةً بالخدمات الأخرى. وتضم خدمات الطوارئ الحكومية المخولة وخدمات السلامة العامة.

2.2.3 الاتصالات التفضيلية: فئة من الخدمات تتيح الأسبقية في النفاذ إلى موارد شبكة الاتصالات و/أو استخدامها.

3.2.3 اتصالات الإغاثة وقت الكوارث (TDR): خدمة اتصالات دولية ووطنية لأغراض الإغاثة وقت الكوارث، وتستخدم مرافق الشبكات المتقاسمة الدولية الدائمة العاملة أو مرافق الشبكات المؤقتة التي يتم إنشاؤها خصيصاً للاتصالات TDR أو مرافق من النوعين معاً.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

AAA الاستيقان والتخويل والمحاسبة (*Authentication, Authorization, and Accounting*)

AF وظيفة التطبيق (*Application Function*)

ANMS نظام إدارة عقدة النفاذ (*Access Node Management System*)

APS تبديل الحماية التلقائي (*Automatic Protection Switching*)

AQM الإدارة الفاعلة لطابور الانتظار (*Active Queue Management*)

ASN نفاذ إلى خدمة الشبكة (*Access Service Network*)

ASN.1 نظام الترميز التركيبي المجرد رقم 1 (*Abstract Syntax Notation One*)

BNG بوابة الشبكة عريضة النطاق (*Broadband Network Gateway*)

BS محطة القاعدة (*Base Station*)

CAC التحكم في قبول النداء (*Call Admission Control*)

CAP بروتوكول التنبيه المشترك (*Common Alerting Protocol*)

CPE معدات مبنى العميل (*Customer Premises Equipment*)

DCCP بروتوكول التحكم في ازدحام البيانات (*Data Congestion Control Protocol*)

DoS حرمان من الخدمة (*Denial of Service*)

DSCP نقاط شفرة الخدمات المتفاضلة (*Diff-Serv Code Points*)

DSLAM معدد النفاذ إلى الخط الرقمي للمشترك (*Digital Subscriber Line Access Multiplexer*)

EAS نظام تنبيه للطوارئ (*Emergency Alert System*)

ECN تبليغ صريح بازدحام (*Explicit Congestion Notification*)

EF إرسال سريع (*Expedited Forwarding*)

E-MTA مكيف مدمج لمطاريف متعددة (*Embedded Multi-Terminal Adapter*)

ENI التنفيذ الوطني لخدمة اتصالات الطوارئ (*ETS National Implementation*)

ET اتصالات طوارئ (*Emergency Telecommunications*)

ETH شبكة طبقة الإثرنت (*Ethernet Layer Network*)

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

EW إنذار مبكر (*Early Warning*)

GETS خدمة اتصالات طوارئ حكومية (*Government Emergency Telecommunications Service*)

IEPS خطة تفضيل الطوارئ الدولية (*International Emergency Preference Scheme*)

IP بروتوكول الإنترنت (*Internet Protocol*)

ISDN شبكة رقمية متكاملة الخدمات (*Integrated Services Digital Network*)

LAN شبكة محلية (*Local Area Network*)

LSP مسير تبديل الوسم (*Label Switched Path*)

MDF إطار التوزيع الرئيسي (*Main Distribution Frame*)

MMPS خدمة متعددة الوسائط ذات أولوية (*Multimedia Priority Service*)

MPS خدمة متعددة الوسائط ذات أولوية (*Multimedia Priority Service*)

MPLS تبديل الوسم بعدة بروتوكولات (*Multiprotocol Label Switching*)

MS قسم تعدد الإرسال (*Multiplex Section*)

NID جهاز الربط البيني مع الشبكة (*Network Interface Device*)

NOAA الإدارة الوطنية لدراسة المحيطات والغلاف الجوي (*National Oceanic and Atmospheric Administration*)

NGN شبكة الجيل التالي (*Next Generation Network*)

ODUk وحدة البيانات k في القناة البصرية (*Optical Channel Data Unit k*)

OLT انتهائية خط بصري (*Optical Line Termination*)

OMCI السطح البيني للإدارة والتحكم في انتهائية شبكة بصرية (*ONT Management and Control Interface*)

ONT انتهائية شبكة بصرية (*Optical Network Termination*)

OTN شبكة نقل بصرية (*Optical Transport Network*)

P-CSC-FE الكيان الوظيفي للتحكم في دورة نداء بالوكالة (*Proxy Call Session Control Functional Entity*)

PCC التحكم في السياسة المتبعة والترسيم (*Policy and Charging Control*)

PDP نقطة اتخاذ القرار (*Policy Decision Point*)

PEP نقطة إنفاذ السياسة المتبعة (*Policy Enforcement Point*)

PF وظيفة سياسة متبعة (*Policy Function*)

PHB السلوك لكل قفزة (*Per Hop Behaviour*)

PIN رقم تعريف الهوية الشخصي (*Personal Identification Number*)

PLMN شبكة اتصالات متنقلة برية عمومية (*Public Land Mobile Network*)

PON شبكة بصرية منفعلة (*Passive Optical Network*)

POTS خدمة هاتف عادية (*Plain Old Telephone Service*)

PSAP نقطة مسؤولة عن السلامة العامة (*Public Safety Answering Point*)

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

RACF وظيفة التحكم في الموارد والقبول (*Resource and Admission Control Function*)

RPH رأسية أولوية المورد (*Resource Priority Header*)

RSVP بروتوكول حجز الموارد (*Resource ReSerVation Protocol*)

QoS جودة الخدمة (*Quality of Service*)

SAME تشفير رسائل منطقة محدَّدة (*Specific Area Message Encoding*)

SCF وظيفة التحكم في الخدمة (*Service Control Function*)

SDH تراتب رقمي متزامن (*Synchronous Digital Hierarchy*)

SIP بروتوكول استهلال الدورة (*Session Initiation Protocol*)

SLA اتفاق مستوى الخدمة (*Service Level Agreement*)

SNC توصيلة شبكة فرعية (*SubNetwork Connection*)

SNCP حماية توصيلة شبكة فرعية (*SubNetwork Connection Protection*)

SS7 نظام التشوير رقم 7 (*Signalling System No.7*)

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

TDM تعدد إرسال بتقسيم الزمن (*Time Division Multiplexing*)

TDR اتصالات الإغاثة وقت الكوارث (*Telecommunications for Disaster Relief*)

T-MPLS نقل تبديل الوسم بعدة بروتوكولات (*Transport MPLS*)

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

UE معدات المستخدم (*User Equipment*)

UN/ISDR الاستراتيجية الدولية للحد من الكوارث (*United Nations International Strategy for Disaster Reduction*)

USI سطح بيني شامل للخدمات (*Universal Services Interface*)

VC قناة افتراضية (*Virtual Channel*)

VLAN شبكة محلية افتراضية (*Virtual LAN*)

VoIP نقل الصوت باستخدام بروتوكول الإنترنت (*Voice over IP*)

VP مسير افتراضي (*Virtual Path*)

W-CDMA نفاذ متعدد عريض النطاق بتقسيم شفري (*Wideband Code Division Multiple Access*)

WPS خدمة لا سلكية ذات أولوية (*Wireless Priority Service*)

xDSL أي من تنويعات الخط الرقمي للمشترك (*Any variant of Digital Subscriber Line*)

XML لغة شرحية قابلة للتوسيع (*Extensible Markup Language*)

XSD تعريف دلالات اللغة الشرحية القابلة للتوسيع (*XML Schema Definition*)

5 وصف اتصالات الطوارئ (ET) والإنذار المبكر

1.5 معلومات عامة

تستعمل هذه التوصية المصطلحات التالية:

- اتصالات الطوارئ (ET)
- خدمة اتصالات الطوارئ (ETS)

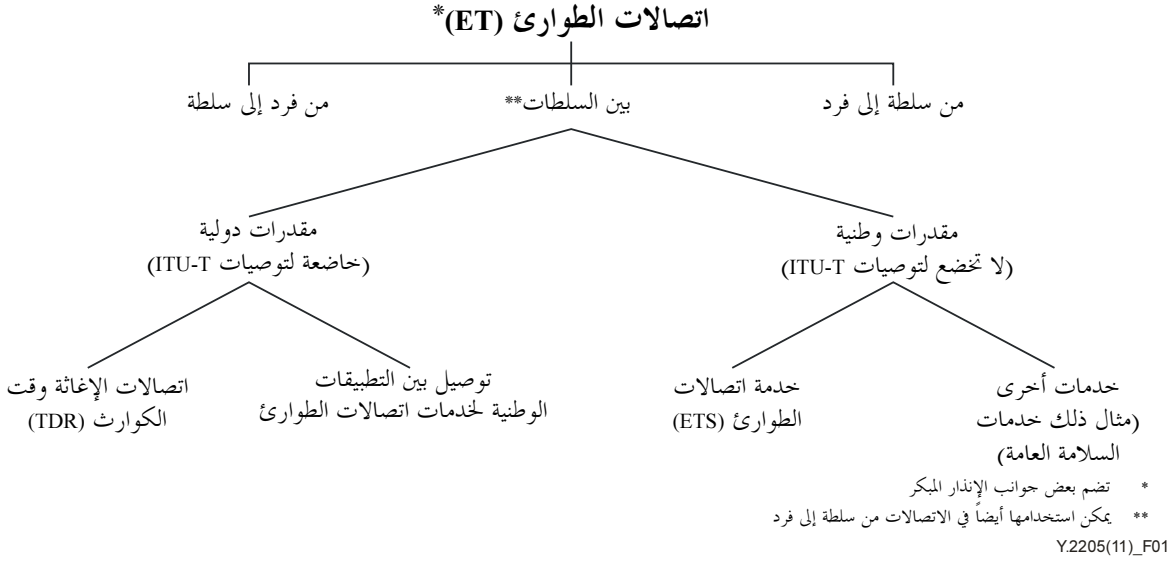
- اتصالات الإغاثة وقت الكوارث (TDR)
- إنذار مبكر (EW)

ومن المهم الاتفاق على الاستخدامات المختلفة لهذه المصطلحات وفهمها. ولهذه الغاية، تستخدم هذه المصطلحات على النحو التالي:

- ET: تسمية شاملة لأي خدمة طوارئ تتطلب معالجة خاصة من الشبكة NGN مقارنةً بالخدمات الأخرى.
- ETS: يستخدم هذا المصطلح وفقاً لتعريفه في التوصية [ITU-T E.107].
- TDR: التسمية النوعية لمقدرة اتصالات تستخدم لأغراض الإغاثة وقت الكوارث.
- EW: التسمية النوعية لجميع أنواع أنظمة الإنذار المبكر ومقدراته وخدماته.

ويمكن ترتيب هذه المكونات في شكل تفريع تكون فيه الاتصالات ET أصل جميع الأنشطة. ويبيِّن الشكل 1 أدناه استعمال المصطلحات والعلاقات فيما بينها.

وكما لوحظ في مقدمة بعض توصيات قطاع تقييس الاتصالات، على وجه التحديد منها سلسلة توصيات قطاع تقييس الاتصالات J.26x، يستخدم مصطلح الاتصالات التفضيلية ليشمل الخدمات التي تتطلب معالجة خاصة بالنسبة إلى الخدمات الأخرى. وباستثناء سياق سلسلة التوصيات J.26x، لا يشار إلى مصطلح الاتصالات التفضيلية في هذه التوصية. ويشمل مصطلح الاتصالات التفضيلية في سلسلة توصيات قطاع تقييس الاتصالات J.26x، خدمة اتصالات الطوارئ واتصالات الإغاثة وقت الكوارث والإنذار المبكر.



الشكل 1 – إطار علاقات المصطلحات المتعلقة باتصالات الطوارئ

2.5 اتصالات الطوارئ

تعني اتصالات الطوارئ (ET) أي خدمة طوارئ تتطلب معالجة خاصة من الشبكة NGN مقارنةً بالخدمات الأخرى. وهي تضم خدمات الطوارئ المخول لها من الحكومة وخدمات السلامة العامة. وفيما يلي أمثلة محددة للخدمات التي تشملها اتصالات الطوارئ:

1) اتصالات الإغاثة وقت الكوارث (TDR)

الاتصالات TDR هي مقدرة اتصالات دولية ووطنية لأغراض الإغاثة وقت الكوارث. وبإمكان الاتصالات TDR أن تستعمل مرافق الشبكة الدولية الدائمة المتقاسمة العاملة أو مرافق الشبكة المؤقتة المنشأة خصيصاً للاتصالات TDR أو تجمع بين النوعين في استعمالاتها.

2) خدمة اتصالات الطوارئ (ETS)

الخدمة ETS خدمة وطنية توفر للمستخدمين المخولين اتصالات ذات أولوية في الخدمة ETS في أوقات الكوارث وحالات الطوارئ. ويرد وصف الخدمة ETS في التوصية [ITU-T E.107]. وتقدم التوصية المذكورة إرشادات تستخدم في تمكين الاتصالات بين إحدى التطبيقات الوطنية (ENI) للخدمة ETS وغيرها من هذه التطبيقات (من سلطة إلى سلطة).

3) خدمات السلامة العامة وخدمات الطوارئ الوطنية/الإقليمية/المحلية

من أمثلة خدمات الطوارئ الأخرى خدمات السلامة العامة وخدمات الطوارئ الوطنية والإقليمية والمحلية. وهي خدمات متخصصة بمجالات الطوارئ على الصعيد الوطني والإقليمي والمحلي وبالسلامة العامة. وتتحدد خدمات الطوارئ هذه على الصعيد الوطني أو الإقليمي أو المحلي وتخضع للتقييس الوطني أو الإقليمي.

3.5 الإنذار المبكر

تعرّف الاستراتيجية الدولية لدى الأمم المتحدة للحد من الكوارث (UN/ISDR)، في تقرير صادر في سبتمبر 2006 [b-UN Global Survey] رُفع إلى الأمين العام للأمم المتحدة بشأن "الدراسة الاستقصائية العالمية لنظم الإنذار المبكر"، التي تصف الإنذار المبكر بأنه "قيام هيئات محددة بتوفير معلومات مفيدة في الوقت المناسب تساعد أشخاصاً معرضين للخطر على اتخاذ إجراءات من شأنها أن تجنبهم الخطر أو الحد منه والتأهب للاستجابة الملائمة". ويقدم تقرير الأمم المتحدة هذا تقديراً للمقدرات والثغرات والفرص المتاحة بهدف بناء نظام عالمي شامل للإنذار المبكر لجميع الأخطار الطبيعية.

6 اعتبارات عامة متعلقة باتصالات الطوارئ والإنذار المبكر

قبل إصدار التوصية [ITU-T Y.1271]، كانت مواصفات مقدرات اتصالات الطوارئ تتناول بصورة رئيسية الشبكات العاملة بتبديل الدارات مثل الشبكة الهاتفية العمومية التبديلية (PSTN).

وكانت هذه المواصفات تستند إلى بعض خصائص الشبكات العاملة بتبديل الدارات وتستفيد منها، مثل:

- التحكم في القبول باستعمال اقتران وثيق بين موارد التشوير وموارد الوسائط؛
- إرسال بمعدل بتات ثابت لمجمل حركة الوسائط التي تتطلب عرض نطاق موحد؛
- عرض نطاق محجوز لكل تدفق؛
- فصل حركة التحكم عن حركة البيانات.

وهذه الخصائص غير متوفرة بالضرورة في الشبكات الراهنة بتبديل الرزم على أساس الخدمة قدر المستطاع، حيث:

- تميل شبكات تبديل الرزم إلى اللجوء إلى تقاسم الموارد وإلى استعمال صفوف الانتظار لتسهيل مرور الحركة بالرشقات، ويحقق الجمع بين النوعين عادة على أساس الخدمة قدر المستطاع؛
- قد يكون التحكم في القبول صعباً، إذ هناك تطبيقات عديدة لا تذكر متطلبات عروض نطاقها، وليس من اقتران بين التشوير والوسائط؛
- تضم التطبيقات والخدمات متطلبات عرض نطاق متغيرة ويمكنها إرسال البيانات من خلال تسوية المعدلات دينامياً؛
- تتقاسم تدفقات رزم مختلفة عرض نطاق متعدد الإرسال إحصائياً؛
- يمكن للتحكم في الموارد وحركة البيانات أن يتقاسما نفس موارد الشبكة.

وقد تتنافس الرزم في الشبكات NGN بتبديل الرزم للحصول على عرض نطاق شريطة عدم وجود تدابير خاصة معاكسة. وفي مستوى النقل في حد ذاته لا يمكن رفض الرزم أو إخضاعها للمراقبة بسهولة. وإضافة إلى ذلك، تختلف هندسة حركة شبكة قائمة على الرزم اختلافاً كبيراً عن شبكة تبديل الدارات من حيث الطرائق المعيارية المقبولة عالمياً. وقد يتأثر "تدفق"

معين من الرزم بتدفقات أخرى منها لدى استخدامها لنفس المورد إلا عندما تتخذ الشبكة NGN تدابير خاصة متاحة ومناسبة لمنع ذلك. ومن ناحية أخرى قد يكون الفصل بين الخدمة والنقل في شبكة NGN مفيداً للحصول على مقدرات خدمة طوارئ أكثر مرونة وتنوعاً.

وتدل هذه الشروط على أن إقامة مقدرات اتصالات الطوارئ ليست عملية فورية أو تلقائية أو سهلة كما لا يمكن الانتقال بسهولة من سياق شبكات تبديل الدارات. وهناك فروق صغيرة أخرى بين الشبكات بتبديل الدارات والشبكات بتبديل الرزم وبين تكنولوجيات الرزم المختلفة تؤثر على تنفيذ مختلف المواصفات المحددة في التوصية [ITU–T Y.1271].

وبناءً على ذلك، ترمي التوصية الحالية إلى عرض الخصائص والآليات التي يمكن استعمالها في شبكة NGN بهدف تسهيل مواصفات اتصالات الطوارئ وبعض جوانب الإنذار المبكر. ولكن عند النظر في بروتوكولات الاتصالات في حالات الطوارئ وفي آلياتها والدعم المقدم لها، من المستحسن تجنب إدخال خصائص أو متطلبات لأنها قد تضيف المزيد من التعقيدات دون فائدة ذات شأن. ويجب توخي الحذر من خلال الأخذ في الاعتبار النفقات العامة المتكبدة في استهلاك الموارد وغيرها من الآثار، قبل إضافة ميزات جديدة "ذات أولوية" مثلاً.

7 المتطلبات والمقدرات الوظيفية العامة

تضم المتطلبات والمقدرات الوظيفية تلك المحددة في التوصيتين [ITU–T Y.1271] و[ITU–T Y.2201] المتعلقة بالشبكات NGN، وتلك الواردة في "الدراسة الاستقصائية العالمية لأنظمة الإنذار المبكر" الصادرة عن الأمم المتحدة والمتصلة بتطور الشبكات NGN [b–UN Global Survey].

1.7 اتصالات الطوارئ

يدرج الجدول 1 المتطلبات والمقدرات الوظيفية لاتصالات الطوارئ.

الجدول 1 – قائمة بالمتطلبات والمقدرات الوظيفية لاتصالات الطوارئ

المتطلبات والمقدرات الوظيفية لاتصالات الطوارئ
تعزيز معالجة الأولويات
أمن الشبكات
سرية الموقع
القدرة على ترميم تشغيل الشبكة
توصيلية الشبكة
قابلية التشغيل البيني
التنقلية
تغطية في آن واحد في كل مكان
القدرة على البقاء/التحمل
إرسال في الوقت الفعلي من أجل توفير: المهاتفة/النص في الوقت الفعلي والفيديو/التصوير (في حال تيسر عرض نطاق)
إرسال في غير الوقت الفعلي من أجل: رسائل/تدفقات في غير الوقت الفعلي (صوتية/فيديوية)
عرض نطاق قابل للتعديل
الموثوقية/التيسر

والغرض من ذلك هو ضمان تيسُّر خدمة الاتصالات الحرجة بصورة موثوقة للمستخدمين المخولين، كالأشخاص المشاركين في اتصالات الطوارئ مثلاً. وتضع التوصية [ITU-T Y.1271] "إطار (أطر) متطلبات ومقدرات الشبكة اللازمة لتأمين اتصالات الطوارئ عبر الشبكات المتطورة بتبديل الدارات وبتبديل الرزم".

وفيما يتعلق بخدمتي الفيديو والتصوير، ينبغي مراعاة تيسّر عرض النطاق (شكل المورد مثلاً).

ويمكن تقسيم وظائف الشبكة الخاصة بالاتصالات في حالات الطوارئ إلى الفئات التالية: خدمة الاستدعاء والاستيقان والتخويل ومعاملة الأولوية من طرف إلى طرف والتوصيل البيني للشبكات والعمل ما بين البروتوكولات.

ويتعلق استدعاء الخدمة بتفاعل المستخدم مع عنصر المستخدم (الهاتف على سبيل المثال) ومع الشبكة بمعلومات تشير إلى طلب خدمة اتصالات طوارئ من شبكة مقدم الخدمة. وتختلف نُهُج إقرار الطلب، ومنها ترتيبات الاشتراك. إذ تُستخدم معلومات الاشتراك لتخويل بعض طلبات الخدمة.

يؤدي مقدم الخدمة الاستيقان والتخويل لقبول أو رفض نفاذ المستخدم إلى الخدمة المطلوبة للاتصالات في حالات الطوارئ ويُتوقع للتخويل بحد ذاته أن يتم في الشبكة المركزية.

أما المعاملة ذات الأولوية من طرف إلى طرف فهي مجموعة من المقدرات التي تستخدمها الشبكة (أو الشبكات) في توفير احتمال كبير لإنشاء الخدمة والحفاظ عليها من شبكة المنشأ إلى شبكة الانتهاء وأي شبكات عبور بينهما. وتستمر المعاملة ذات الأولوية بدءاً من استدعاء الخدمة حتى تسليمها. وترد المعاملة ذات الأولوية فيما تقوم به عناصر الشبكة الداعمة للخدمة من التحكم في القبول وتوزيع موارد الشبكة ونقل التشوير والرزم الحاملة للوسائط.

ولا بد من التوصيل البيني للشبكات والعمل البيني للبروتوكولات من أجل دعم المعاملة ذات الأولوية من طرف إلى طرف لنقل التشوير والوسائط العابر لشبكات متعددة تعود لموردين مختلفين يستخدمون تكنولوجيات مختلفة. فعلى سبيل المثال، يمكن أن تختلف مستويات الأولوية على اختلاف التكنولوجيا المستخدمة في شبكات متعددة، وقد تدعو الحاجة لإقامة تقابل بين المستوى المحدد في تكنولوجيا ما وأخرى.

2.7 الإنذار المبكر

تحتاج أنظمة الإنذار المبكر لنظام اتصالات ناجع وموثوق ومتين. وفيما يلي بعض الأهداف التي تتوخاها أنظمة الإنذار المبكر في سياق اتخاذها من شبكات الجيل التالي نظاماً للاتصالات:

- توفير مقدرات تعمل بصورة دائمة وفعالة ومتينة ومتيسرة في كل دقيقة من كل يوم؛
- توفير مقدرات الاتصالات الضرورية للإرسال في الوقت الفعلي (مثل معلومات عن هزات أرضية أو مستوى مياه البحر)؛
- الاستناد إلى معايير متفق عليها دولياً؛
- ضمان سلامة أنظمة الإنذار المبكر وسلامة وصحة الرسائل (أي ضمان اقتصار الإرسال على الرسائل المخولة)؛
- حصر تقديم رسائل الإنذار بالذين يمكن أن يتضرروا بكارثة وشيكة وتجنب الرسائل عديمة النفع وغير الهادفة. (رسائل إلى أشخاص غير معنيين مثلاً و/أو رسائل لا تتضمن معلومات حيوية مفيدة).

ولحصر تقديم رسائل الإنذار بالذين يمكن أن يتضرروا بكارثة وشيكة، يمكن أن تتخذ أنظمة الإنذار المبكر أهدافاً أخرى تتعلق باصطفاء الرسائل بحيث تستهدف فئة مختارة من:

- مجموعة من المستخدمين؛
- مناطق أو غير ذلك.

(شكل من أشكال "الإذاعة الخلوية" مثلاً).

8 المبادئ التوجيهية والمتطلبات العامة للأمن

1.8 المبادئ التوجيهية العامة

يمكن للهجمات السيبرانية أن تستهدف ما يُستخدم لدعم اتصالات الطوارئ من عناصر الشبكة وأنظمتها ومواردها وبياناتها وخدماتها. وستعتمد سلامة وسرية وتيسر اتصالات الطوارئ، لا سيما حين تعرّضها لهجوم، على خدمات وممارسات الأمن التي تنفذ في شبكات الجيل التالي وعلى المقدرات الأمنية (مثل وظيفتي الاستيقان من المستخدم وتخويله) المنفذة كجزء من خدمة التطبيق في الاتصالات في حالات الطوارئ. وتشمل المبادئ التوجيهية العامة التي يتعين النظر فيها لدى التخطيط لأمن اتصالات الطوارئ (على سبيل الذِكر لا الحصر) ما يلي:

- جميع جوانب الاتصالات في حالات الطوارئ بما فيها التشوير والتحكم، والحمالة/الوسائط، والبيانات والمعلومات ذات الصلة بالإدارة (مثل معلومات البيانات العامة للمستخدم) يجب أن تكون محمية ضد التهديدات الأمنية. ويمكن أن تظهر التهديدات الأمنية ضد اتصالات الطوارئ في مختلف الطبقات (مثل طبقات النقل أو التحكم في الخدمة أو دعم الخدمة) وفي قطاعات الشبكة المختلفة (أي السطوح البينية للنفاذ والشبكة الأساسية والتوصيل البيني).
- وضع وإنفاذ السياسات والممارسات الأمنية الخاصة بخدمات الاتصالات في حالات الطوارئ. وينبغي تحديد وتنفيذ مقدرات التخفيف الكفيلة بتوفير حماية ضد التهديدات الأمنية المختلفة. وعلى وجه التحديد، ينبغي تحديد وتنفيذ مقدرات التخفيف والممارسات الأمنية للاتصالات في حالات الطوارئ بما يفوق تلك اللازمة لخدمات التطبيق العامة. وهذا يشمل السياسات الأمنية لحماية بيانات الإدارة والمعلومات المخزنة (مثل معلومات البيانات العامة للمستخدم) المتعلقة بالاتصالات في حالات الطوارئ.
- إجراءات التنفيذ والاستخدام المتبعة للاستيقان من المستخدمين أو الأجهزة أو المستخدمين والأجهزة معاً ولتخويلهم من أجل الحماية ضد النفاذ غير المخول إلى الموارد والخدمات والمعلومات المرتبطة بالاتصالات في حالات الطوارئ (مثل معلومات المستخدم في مخدّمات الاستيقان وأنظمة الإدارة). فعلى سبيل المثال، ينبغي تنفيذ وظيفتي الاستيقان والتخويل لمنع استخدام المستخدمين غير المخولين للموارد المخصصة للاتصالات في حالات الطوارئ درءاً للحرمان من الخدمة (DoS) وغيره من أنواع الهجمات.
- المسؤولية داخل كل شبكة ضمن ميدانها عن أمن الاتصالات العابرة للعديد من ميادين موردي الشبكات بحيث يمكن تأمين الاتصالات من طرف إلى طرف. وبما أن الاتصالات في حالات الطوارئ يمكن أن تشمل الاتصالات العابرة لميادين سياسات أمنية مختلفة لموردي الشبكات الوطنية والدولية (أي بلدان/إدارات)، فإن الحاجة تدعو لإنشاء وتنفيذ مقدرات علاقات ثقة وأساليب وإجراءات للتعرف على حركة اتصالات الطوارئ وإدارة هوية واستيقان من المستخدمين والشبكات عبر ميادين متعددة لإدارة الشبكة.

ويمكن الاطلاع على معلومات أوفى في المعيار [b-ATIS-1000010].

2.8 المتطلبات العامة

إن توصيات الأمن [ITU–T Y.2701] و[ITU–T Y.2702] و[ITU–T Y.2704] وتوصيات إدارة الهوية (IdM) [ITU–T Y.2720] و[ITU-T Y.2721] و[ITU-T Y.2722] لها صلة بأمن الاتصالات في حالات الطوارئ.

1.2.8 التحكم في النفاذ

يتعين عدم السماح إلا للمستخدمين المخولين بالنفاذ إلى اتصالات الطوارئ وأي موارد مرتبطة بها. ويجب منع أي نفاذ غير مخول به من قبل الدخلاء المنتحلين لصفة مخولة.

2.2.8 الاستيقان

إن ضرورة الحماية الأمنية تدعو لآليات ومقدرات للتعرف على مستخدمي أو أجهزة اتصالات الطوارئ أو كليهما معاً، وللاستيقان منهم وتخويل نفاذهم إلى اتصالات الطوارئ، حسب مقتضى الحال على أساس السياسة المتبعة[1] ومستوى الضمان لخدمة معينة (مثل خدمة الصوت أو البيانات أو الفيديو).

3.2.8 السرية والخصوصية

تدعو الضرورة لحماية سرية وخصوصية اتصالات الطوارئ ومعلومات المستخدم النهائي. ويشمل ذلك حماية سرية وخصوصية التشوير والتحكم وحركة الحمالة في اتصالات الطوارئ، ومعلومات المستخدم النهائي (مثل معلومات الهوية والاشتراك والموقع) ونشاطه حسب مقتضى الحال.

4.2.8 أمن الاتصالات

تدعو الضرورة لحماية اتصالات الطوارئ من التدخلات (كمنع الاعتراض غير القانوني أو الاختطاف أو إعادة التشغيل للتشوير أو لحركة الحمالة).

5.2.8 سلامة البيانات

تدعو الضرورة لحماية سلامة الاتصالات في حالات الطوارئ (كالحماية ضد ما هو غير مخول من تعديل أو حذف أو إنشاء أو إعادة تشغيل). وهذا يشمل حماية سلامة معلومات الاتصالات في حالات الطوارئ وأي بيانات تشكيل (كوسم الأولوية ومعلومات الأولوية المخزنة في وظائف قرار السياسة المتبعة ومستوى أولوية المستخدم وما إلى ذلك).

6.2.8 التيسُّر

يجب حماية تيسر الاتصالات في حالات الطوارئ. وعلى وجه التحديد، يجب أن تكون الاتصالات في حالات الطوارئ والموارد المرتبطة بها محمية ضد أي حرمان من الخدمة (DoS) وغيره من أشكال الهجمات.

9 آليات ومقدرات دعم اتصالات الطوارئ في الشبكات NGN

1.9 معلومات عامة

من أهم خصائص الشبكات NGN قدرتها على فصل التحكم في الخدمة/التطبيق عن النقل، الأمر الذي يتيح تقديم وتطوير كل من خدمات التطبيق وخدمات النقل بصورة منفصلة ومستقلة. وتتخذ عملية الفصل شكل مجموعتين أو طبقتين منفصلتين من الوظائف. تكون وظائف النقل في طبقة النقل، أما وظائف التحكم في الخدمة المتصلة بالتطبيقات، مثل المهاتفة، فتكون في طبقة الخدمة. ولكل طبقة عموماً مجموعتها الخاصة من الأدوار والفعاليات والميادين الإدارية (انظر التوصية [ITU–T Y.110]). والأدوار المشاركة في توفير الخدمة مستقلة عن تلك المشاركة في توصيلية النقل. ويمكن من وجهة نظر تقنية معالجة كل طبقة على حدة. وتضطلع وظائف التحكم في الموارد والقبول (RACF) بدور الحكم بين هاتين الطبقتين فيما يتعلق بالحجز (والتفاوض) المتعلق بنوعية الخدمة في معمارية الشبكة NGN. وتحدد التوصية [ITU-T Y.2111] المعمارية والمتطلبات الوظيفية الخاصة بوظائف التحكم في الموارد والقبول في شبكات الجيل التالي التي قد تستدعي عدداً من تكنولوجيات النفاذ والنقل والنفاذ الأساسي والميادين المتعددة. وتستند قرارات الوظيفة RACF المتعلقة بنوعية الخدمة إلى الاتفاقات SLA وأولوية الخدمة ومواصفات المستخدم وقواعد سياسة مشغل الشبكة وتيسر الموارد في شبكات النفاذ والشبكات المركزية على حد سواء. ويجب تحديد هوية مستخدمي اتصالات الطوارئ وإعطائهم الأولوية في قبول الوظيفة RACF لهم بعد الاستيقان من هويتهم وتخويلهم.

[1] تشمل السياسة المتبعة في هذا السياق جميع السياسات المرعية كتلك المتأتية عن قرارات مورد شبكة الجيل التالي أو المتطلبات التنظيمية أو القواعد الحكومية الأخرى.

وفي حال فصل حركة اتصالات الطوارئ عن حركة الاتصالات العادية في الشبكة NGN، يجب توفير علامات تمييز ملائمة تُعرف أيضاً بالواسمات. ويستخدم في هذا السياق مصطلح وسم (الحركة).

وفي معمارية بروتوكولات الشبكة NGN متعددة الطبقات (طبقة نقل وطبقة خدمات) ومن حافة إلى حافة (مقطع شبكة نفاذ ومقطع شبكة مركزية)، تظهر الواسمات بأشكال مختلفة في طبقات البروتوكول المختلفة رأسياً (تفاعل بين طبقات البروتوكول المختلفة) وأفقياً (تفاعل بين عناصر شبكة الاتصال) على حد سواء. وتنقل الواسمات في رزم تشوير و/أو تدرج داخل رأسية رزمة بيانات من أجل تحديد نداءات أو دورات اتصالات الطوارئ ووسمها. والواسمات المستخدمة في تحديد نداءات أو دورات و/أو حركة اتصالات الطوارئ ووسمها خاصة بالبروتوكول. ويجب وضع جدول تقابل ملائم بين الواسمات وتشغيلها في مختلف البروتوكولات من أجل إجراء معالجة خاصة (أولوية أو أسبقية مثلاً) من طرف إلى طرف لجميع جوانب نداء/دورة اتصالات الطوارئ (أي التحكم في النداء/الدورة، حركة وسيط وإدارة). وعلى سبيل المثال، توضع المعلومات المتوفرة في رأسية أولوية موارد البروتوكول SIP والمستخدمة في طبقة التحكم لتحديد أولوية النداء أو الدورة في جدول تقابل مع الشفرات Diff-serv (DSCP) المناسبة من أجل وسم حركة اتصالات الطوارئ في طبقة الشبكة IP. وبنفس الطريقة تتم مقابلة الشفرات DSCP في الطبقة 3 مع معلمات الأولوية الخاصة بالشبكات VLAN أو شبكات الإثرنت في الطبقة 2 وذلك في بروتوكول النقل. ويتحدد البروتوكول SIP في الوثيقة [IETF RFC 3261] وفي الصيغ المحدَّثة منها [b-IETF RFC 3265] و[b-IETF RFC 3853] و[b-IETF RFC 4320] و[b-IETF RFC 4916] و[b-IETF RFC 4032] و[b-IETF RFC 5027].

وتنزع الخدمات في طبقة الخدمة إلى استعمال مجموعة خاصة معينة من البروتوكولات. لذلك تختلف التقنيات المستخدمة في الخدمات المختلفة لاتصالات الطوارئ باختلاف الخدمات المعنية ومقدرات البروتوكولات الخاصة بتلك الخدمات.

ويمكن استعمال بروتوكول الإنترنت (IP) في طبقة النقل. ويمكن أن يتغاير إصدار بروتوكول الإنترنت من مزود إلى آخر، وقد تتطلب التوصيلية من طرف إلى طرف التكيف مع الإصدارات المختلفة بتغليف إصدار ضمن آخر. بيد أن ذلك ينبغي ألا يؤثر على نقل المعلومات المتصلة بخدمة الاتصالات في حالات الطوارئ.

وعلاوةً على ذلك، قد تختلف البروتوكولات المستخدمة في البُنى التحتية للنفاذ المحلي (الميل الأخير) عن تلك المستخدمة في البُنى التحتية المركزية. فقد تكون البُنى التحتية للنفاذ المحلي سلكية (نفاذ ثابت) أو لا سلكية أو خليطاً من النوعين.

وهكذا قد يمر مسير معين من طرف إلى طرف في نداء أو دورة اتصالات طوارئ بعدد كبير من تكنولوجيات النقل.

وستبيِّن فقرات لاحقة الخصائص المختلفة ومقدرات التكنولوجيات المختلفة التي يمكن استخدامها لتسهيل وضع مواصفات اتصالات الطوارئ.

ونظراً لأن طبقة النقل تستعمل البروتوكول IP (وعدداً من البروتوكولات ذات الصلة)، وبروتوكولات نقل يحددها الفريق IETF، فمن المستحسن استعمال المقدرات الوظيفية النافذة المحددة من قِبل هذا الفريق والمتعلقة باستخدامها في اتصالات الطوارئ. وستناقش هذه المقدرات في فقرات لاحقة.

ومن المهم التمييز بين المواصفات (RFC) التي يضعها الفريق IETF وبين نشرها في الإنترنت وفي سياق شبكة NGN. وفي الحالتين تعتمد المواصفات المستخدمة فعلياً على ما نشره المزوّد المعني بالأمر. ولكن بما أن الإنترنت لا تقع داخل نطاق تطبيقات القطاع ITU-T، فلا يمكن وضع أي افتراضات بشأن نوعية الخدمة أو المقدرات في مسيرات الإنترنت، كما هو مبين في الوثيقة [b- IETF RFC 4190][2]. وبالمقابل، هناك مواصفات أكثر صرامة لاتصالات الطوارئ الدولية في الشبكات NGN

[2] جاء في الوثيقة [b-IETF RFC 4190] ما يلي:

"كان من الثابت أثناء تطور الإنترنت أن توفير أفضل خدمة ممكنة هو نموذج الخدمة الافتراضي"؛

و"ينبغي ألا تعتمد الاتصالات ETS بين الميادين على توفير خدمة دائمة في كل مكان أو حتى على دعم واسع المدى على طول المسير بين الطرفين."

التي تستخدم البروتوكول IP وتقع ضمن صلاحيات قطاع تقييس الاتصالات ويمكن صياغتها في توصيات تصدر عن هذا القطاع وتخصص لاستعمالات مزوّدي الشبكات NGN.

وتصف الوثيقة [IETF RFC 4542] حلولاً ممكنة بشأن "خدمة إنترنت ذات أفضلية لحالات الطوارئ". وينطبق عدد كبير من المفاهيم الواردة في الوثيقة المذكورة على خدمة اتصالات الطوارئ (ETS) في سياق الشبكات NGN.

وفي شبكة NGN تضم طبقتين مستقلتين للخدمات والنقل، يتأثر نجاح اتصال الطوارئ بالعوامل التالية:

'1' تحديد حركة اتصالات الطوارئ ووسمها؛

'2' سياسة التحكم في القبول؛

'3' سياسة توزيع عرض النطاق؛

'4' استيقان وتخويل مستخدمي اتصالات الطوارئ المشروعين.

1.1.9 معالجة ذات أولوية

تشكل المعالجة ذات الأولوية عموماً عنصراً رئيسياً في اتصالات الطوارئ التي تعتبر تحديداً أكثر أهمية من خدمات الاتصالات العادية. وعندما تستهلك الخدمات العادية الغالبية العظمى من موارد الشبكة المحدودة، فإن اتصالات الطوارئ مضطرة إلى التنافس للحصول على نفس هذه الموارد، مما قد يؤثر سلباً على هذه الاتصالات. ولذا، ينبغي التفكير في بعض الوسائل التي تعطي الأولوية لمعالجة اتصالات الطوارئ نسبةً إلى الاتصالات العادية. ويعني ذلك بالدرجة الأولى:

أ) التعرّف على المستخدمين المخولين لاتصالات الطوارئ؛

ب) ضمان أولوية الخدمة لمستخدمي اتصالات الطوارئ المخولين.

وفي معمارية الشبكة NGN ذات الطبقات حسب تعريفها الوارد في التوصية [ITU-T Y.2012]، ينبغي أن يكون مؤشر الأولوية المرسل من وظيفة التحكم في الخدمة (SCF) إلى وظيفة التحكم في الموارد والقبول (RACF) قادراً على بيان مستويات الأولوية للمستخدمين من أجل إتاحة تطبيق سياسات مختلفة والتمييز بين الأنماط المتعددة لتطبيقات الأولوية. وعلى سبيل المثال، يمكن تزويد موظفي المستشفيات بمستوى أولوية أدنى من ذلك المخصص لمنسِّقي عمليات الإسعاف في قسم الطوارئ.

2.1.9 تعرّف الهوية والاستيقان والتخويل والتحكم في النفاذ

من الضروري منع النفاذ غير المخوَّل به إلى الخدمات والموارد المخصصة لاتصالات الطوارئ، من جانب المقتحمين مثلاً الذين ينتحلون هويات مستخدمين مخولين. وبالتالي لا بد من توفير آليات ومقدرات وظيفية من شأنها استيقان النفاذ المخول به لمستخدمي اتصالات الطوارئ والأجهزة، أو لأي توليف بين المستخدم والجهاز حسب الاقتضاء، مع مراعاة سياسة الخدمة المعنية (ETS وTDR مثلاً).

ومن الضروري التعرّف على طلبات نداء أو دورة اتصالات الطوارئ (من خلال مواصفات خاصة بالمراقمة أو إدخال البيانات أو مواصفات المستخدم أو الاشتراك مثلاً). وينبغي لمزودي الشبكات NGN أن يسرّعوا الاستيقان من مستخدمي اتصالات الطوارئ المخولين. ويلزم استعمال آليات وطرائق خاصة للاستيقان والتخويل استناداً إلى سياسة اتصالات الطوارئ المعنية (مثل استعمال رقم تعرف هوية شخصي (PIN) ومواصفات مستخدم ومواصفات اشتراك).

ومن أمثلة نُهُج استيقان وتخويل خدمة اتصالات الطوارئ ETS التي يرد وصفها في التذييل II للتوصية [ITU-T Y.2702] ما يلي:

أ) استعمال رقم تعرُّف الهوية الشخصي (PIN): يستخدم هذا النهج الرقم PIN لاستيقان وتخويل المستخدم. ونتعرف في هذا النهج هوية المستخدم وليس جهاز المستخدم. ولذلك فهو يُستعمل عادة في الحالات التي يمكن فيها للمستخدم تفعيل الخدمة ETS من أي جهاز.

ب) استعمال جانبية الاشتراك/الخدمة: تُستخدم في هذا النهج جانبية خدمة مطراف المستخدم للدلالة على الاشتراك في الخدمة ETS. ويجري استيقان مطراف المستخدم والتعرُّف إلى جانبية خدمة المستخدم كجزء من إجراءات

التسجيل المعتادة لدى مقدم خدمة NGN (أي مقدم خدمة ETS). وعندما يبادر المستخدم بطلب، فإن التحقق من جانبية خدمة المستخدم يحدد ما إذا كان المستخدم مخول له باستعمال الخدمة ETS أم لا. وبالتالي يلبَّى طلب الخدمة ETS إذا تأكدت صحة اشتراك الخدمة ETS من جانب مطراف المستخدم.

ج) استعمال مجموع الرقم PIN وجانبية الخدمة: يمكن أيضاً استخدام نهج الجمع بين الرقم PIN وجانبية الخدمة لاستيقان كل من المستخدم وجهاز المستخدم بغية توفير قدر أعلى من الكفالة.

د) استعمال علامات أمن خاصة وقياسات حيوية: إضافة إلى النُّهج الموصوفة أعلاه، يمكن استعمال نُهج أكثر تطوراً باستعمال علامات الأمن الخاصة بمقدرات القياس الحيوي لاستيقان وتخويل مستخدمي الخدمة ETS ومطاريفها وذلك بغية توفير مستوى أعلى من كفالة تحقق الهوية.

وبعد إجراء الاستيقان والتخويل للمستخدم أو جهاز المستخدم أو للاثنين معاً استناداً إلى السياسة المعمول بها، يتعيَّن وسم نداء/دورة اتصالات الطوارئ والإشارة إليه في اتجاه الشبكات التالية. وبعد إجراء الاستيقان والتخويل أيضاً، يجب إعطاء الأولوية إلى جميع جوانب نداء أو دورات اتصالات الطوارئ والتشوير/التحكم والحركة الحاملة وأي إدارة مستخدمة.

كما يتعيَّن أن يؤخذ في الاعتبار الاستيقان والتخويل فيما يتعلق بتحويل واستقبال نداءات/دورات اتصالات الطوارئ بين مزودي الشبكات NGN مع مراعاة البيئة متعددة المزودين والفصل بين خدمتي التحكم والنقل. وينبغي أن يستند استيقان مزودي الشبكات NGN والتخويل لهم بتحويل واستقبال نداءات/أو دورات اتصالات طوارئ إلى الاتفاقات SLA وإلى السياسات المعمول بها.

ويمكن الاستفادة من مقدرات إدارة الهوية (الواردة في التوصيات [ITU–T Y.2720] و[ITU–T Y.2721] و[ITU–T Y.2722]) لزيادة الثقة في معلومات الهوية في تطبيقات الاتصالات في حالات الطوارئ. وترد في التذييل III للتوصية [ITU–T Y.2721] أمثلة عن حالات استخدام إدارة الهوية المتصلة بخدمة الاتصالات في حالات الطوارئ (ETS). وتصف هذه الأمثلة كيفية استخدام مقدرات إدارة الهوية لدعم تطبيقات خدمة الاتصالات في حالات الطوارئ، وتغطي المواضيع التالية:

- ضمان الاستيقان باستخدام الجمع بين الجهاز والمستخدم (كترابط الاستيقان من المستخدم والجهاز).
- الاستيقان المعزز من مستخدمي خدمة اتصالات الطوارئ في خدمات الجيل التالي ذات الأولوية (مثل استخدام الأمارات والشهادات الرقمية والتعرف على الصوت والقياسات الحيوية).
- الاستيقان من الطرف المتصل ومن مصادر اتصالات البيانات (كضمان مصادر الرسائل والبيانات).
- تعرف هوية مقدمي الخدمة والاستيقان منهم في بيئة يتعدد فيها المقدمون (ومثال ذلك، تعرف هوية النفاذ وهوية موردي المحتوى ومقدمي خدمة الشبكة).
- تسجيل الدخول لمرة واحدة وتسجيل الخروج لمرة واحدة (ومثال ذلك، النفاذ إلى تطبيقات متعددة دون الحاجة لتقديم ثبوتيات فردية لكل تطبيق).

3.1.9 اعتبارات تتعلق بالتحكم من أجل ترجيح احتمال القبول

يكمن دور وظيفة التحكم في الموارد والقبول (RACF) في إتاحة التحكم في نوعية الخدمة (QoS) بحيث يضم قبول الموارد وحجزها إذا أراد مزود الخدمة ذلك. وفي هذا الصدد قد يكون من الضروري، أثناء تزايد طلب المستخدمين على الخدمة، رفض بعض الطلبات. ولولا هذا الرفض يتعذر على الشبكات NGN أن تضمن نوعية الخدمة في حالات الطوارئ على أتم وجه. وتنطوي عمليات نوعية الخدمة وعلاقتها مع الوظيفة RACF على تخويل يستند إلى مواصفات المستخدم والاتفاقات على مستوى الخدمة (SLA) وقواعد السياسة الخاصة التي يتبعها المشغل ودرجة أولوية الخدمة وتيسُّر موارد النقل في شبكات النفاذ والشبكات المركزية. وتفترض هذه التوصية ضرورة تزويد الوظيفة RACF بالقدرة على تصنيف طلبات الخدمة حسب ترتيب درجة أولويتها، وذلك باستعمال أولوية الخدمة (فالشبكة التي ترفض باستمرار طلبات مخول لها في حالة ازدحام مؤقت تعطي زبائنها نوعية خدمة سيئة إذ إن الزبائن مضطرون دوماً لإعادة تقديم طلباتهم). ولهذا السبب تؤكد هذه التوصية على أن

أولوية الخدمة عامل رئيسي لا بد من مراعاته في طريقة برمجة صفوف انتظار توزيع الموارد والقرار العام في القبول. وتناقش لاحقاً آليات إنفاذ هذه الوظيفة.

وأهم متطلبات الوظيفة RACF معالجة طلبات نوعية الخدمة المخول لها باستعمال مواصفات المستخدم ودرجة الأولوية. وينبغي خصوصاً أن يستعمل التحكم في القبول معلومات أولوية الخدمة لإدارة هذه الأولوية. وثمة طرائق مختلفة يمكن استخدامها في مراعاة أولوية خدمة التحكم في القبول حسب الموارد.

ومن الطرائق الممكنة تحديد عتبة قبول أعلى فيما يتعلق بحركة اتصالات الطوارئ، مما يتيح قبول مزيد من طلبات الأولوية عندما ترفض الطلبات العادية. وفي الحقيقة تزيد هذه الطريقة مؤقتاً من استعمال موارد الشبكة. ولكن نظراً لغزارة موارد الشبكة NGN وتحرير بعض الموارد بصورة طبيعية في أي فترة زمنية ملموسة (بحكم انتهاء دورات أخرى)، فإن النظام يستعيد مقدرة حركته اليومية المفترضة للتشغيل. وإضافة إلى ذلك، وبافتراض أن مقدار الحركة ذات الأولوية ضئيل نسبياً، وأن الشبكات نادراً ما تعمل أو لا تعمل أبداً باستطاعتها الكاملة 100 في المائة، يتضح أن العتبة الأعلى لقرار قبول الحركة ذات الأولوية لا يشكل أي خطر على عمل الشبكة إجمالاً أو على نوعية خدمة أي حركة أخرى.

وهنالك أنظمة للتحكم في القبول تقوم على عمليات الحجز ولا تسمح بطلب الخدمة إلا عندما يتوفر عرض النطاق المطلوب. وفي هذه الحالة، ينبغي لطريقة خدمة آليات البرمجة أن تعتبر أولوية الخدمة عنصراً رئيسياً.

وأخيراً، هناك آليات أخرى من أجل تفادي آليات التحكم في القبول (مثل تفادي الحركة ذات الأولوية للوظيفة RACF). وتجري كتابة مثال عن هذه الآلية ضمن فريق مهام هندسة الإنترنت (IETF).

1.3.1.9 التحكم في قبول النداء (CAC)

التحكم CAC هو مجموعة إجراءات وسياسات تتخذها الشبكة في مرحلة إقامة النداء أو الدورة ترمي إلى قبول خدمة ما أو رفضها استناداً إلى الأداء المطلوب ومعايير الأولوية وتيسر الموارد اللازمة.

والتحكم CAC في الشبكات التقليدية PSTN/ISDN يعني ببساطة إتاحة دارة ما أو عدم إتاحتها حسب التخويل. كما أن تخصيص الإدارة يفترض تعريفا تيسر المسير وعرض النطاق اللازم. وتبعاً لتيسر معلومات حالة الشبكة المتعلقة بأوضاع الدارات (قنوات النطاق الصوتي)، يمكن لشبكة PSTN/ISDN أن:

أ) تحوِّل نداءات الطوارئ على مسيرات محجوزة خصيصاً لحركة الطوارئ (إن وجدت)؛

ب) تنتظر تيسر دارة (دخول في صف انتظار).

ونظراً لعدم وجود مسيرات منفصلة أو معلومات عن حالة الدارات في شبكات بروتوكول الإنترنت، فإن التخويل بالدخول إلى الشبكة لا يكفي لضمان تيسر المسير من طرف إلى طرف أو عرض النطاق من طرف إلى طرف وهما شرطان ضروريان لنداء/دورة ما. ففي شبكات بروتوكول الإنترنت، لا يكاد يملك العنصر الداخل أي معلومات عن الظروف التي تحيط بالشبكة خارج مجاله. وبالتالي فإن التحكم CAC في العنصر الداخل إلى شبكة غير كافٍ لضمان تيسر المسير من طرف إلى طرف إن لم تضف إليه آليات أخرى.

وثمة نتيجة أخرى هي أن العنصر الخارج من الشبكة غير مزود بأي تحكم في العنصر البعيد الداخل إلى الشبكة والذي يحاول إقامة نداء/دورة أو بأي معلومات عنه. غير أن عنصراً خارجاً من شبكة PSTN/ISDN قادر على التحكم في العنصر الداخل الذي يحاول إقامة نداء/دورة، وذلك باستعمال آليات التشوير المصاحبة.

وتحدد التوصية [ITU-T Y.2171] مستويات لأولوية التحكم في القبول فيما يتعلق بخدمات الاتصالات التي تطلب الدخول إلى الشبكة وخصوصاً في حالات الطوارئ حيث قد تستنفد موارد الشبكة. وهي توصي تحديداً بثلاثة مستويات لأولوية التحكم في قبول الخدمات التي تطلب الدخول إلى شبكة NGN. ويُوصى بمستوى الأولوية 1 (وهو الأعلى) لاتصالات الطوارئ (بما فيها الخدمة ETS) في الشبكات NGN. وتتمتع الحركة ذات مستوى الأولوية هذا بأعلى درجات أولوية لقبولها في الشبكة NGN.

2.9 طبقة الخدمة

1.2.9 معلومات عامة

تمتلك البلدان خدمة ETS أو هي بصدد إنشائها من أجل التمكّن من معالجة الحركة المخول لها على أساس الأولوية لدعم عمليات الإغاثة في حالات الطوارئ ووقت الكوارث داخل حدودها الوطنية. ولكن قد تقع حالات أزمة يضطر فيها مستخدم الخدمة ETS في بلد ما إلى الاتصال بمستخدمين موجودين في بلد آخر. وفي هذه الحالة، من الضروري للنداء/الدورة ETS التي تبدأ في بلد ما أن تتلقى معاملة ذات أولوية من طرف إلى طرف، أي معاملة ذات أولوية في بلدَي المنشأ والمقصد. وقد يتطلب ذلك توصيلاً بين الخدمتين ETS الوطنيتين عبر شبكة دولية توفر مقدرات معاملة ذات أولوية أو تنقل الحركة ذات الأولوية بشفافية بين البلدين.

وتعرض الفقرات التالية عدداً من آليات البروتوكول المستخدمة في الدلالة على أولوية المعالجة والحصول عليها في مستوى التحكم في الخدمة في سياق الشبكة NGN بتبديل الرزم. وتبيّن أيضاً قابلية تطبيق آليات البروتوكول هذه على الخدمة ETS. ومقدرات البروتوكول هذه ضرورية للتطبيقات الدولية في سياق الاتصالات بين تطبيقات الخدمة ETS الوطنية عبر الشبكة الدولية (مثال ذلك التوصيل بين تطبيقي خدمة ETS وطنيين).

2.2.9 أولوية موارد البروتوكول SIP

تضيف الوثيقة [IETF RFC 4412] رأسيتين إلى بروتوكول استهلال الدورة (SIP) هما حقل أولوية الموارد وحقل القبول بأولوية الموارد، وتحدد إجراءات استعمالهما. ويمكن لوكلاء مستخدمي البروتوكول SIP استعمال حقل الرأسية 'أولوية الموارد' بما فيها بوابات ومطاريف الشبكة الهاتفية التبديلية العمومية (PSTN) والخدمات المخوَّلة SIP من أجل التأثير على معالجة الطلبات SIP.

وحرصاً على توفير التكافؤ مع بعض الأنظمة الراهنة، يمكن توفير الأولوية المناسبة لعدد من الأنظمة "المعيارية" المختلفة من خلال تحديد "حيِّز الأسماء" الملائم للنظام المعني وعدد مستويات الأولوية في ذلك النظام. وتحدد الوثيقة [IETF RFC 4412] حيّز الاسم وعدد مستويات الأولوية المصاحب له لاستعمالها في الخدمة ETS.

حيّز الاسم	عدد المستويات
ets	5
wps	5

وتحمل جميع النداءات/الدورات في بيئة الإنترنت حيّز الاسم "ets" مع 5 مستويات أولوية تحيل إلى درجة الأهمية في طبقة التطبيق (ضمن عناصر البروتوكول SIP). وتخصص لنداءات/دورات الخدمة ETS الداخلة التسمية "ets" في الرأسية 'أولوية موارد'. ويمكن التعرف على نداءات/دورات الخدمة ETS من خلال وجود قيمة حيّز الاسم "ets" في رأسية 'أولوية موارد' رسالة البروتوكول SIP وتُعطى أولوية "مرتفعة" لحجز/تخصيص الموارد بحيث تحظى بمعاملة تفضيلية في طبقة النقل. وثمة تسمية أخرى لحيّز أسماء مشابه "wps" مرفق بخمسة مستويات أولوية لتوزيع النداءات/الدورات حيث الموارد محدودة أو مزدحمة كما هو الحال في النفاذ الراديوي إلى الشبكات اللاسلكية.

3.2.9 الخطة الدولية للأولوية في حالات الطوارئ (IEPS)

تصف التوصية [ITU-T E.106] المواصفات الوظيفية والخصائص والنفاذ والإدارة التشغيلية في الخطة IEPS. وتتيح الخطة IEPS التشغيل بين مختلف التطبيقات الوطنية لخطط الأولوية/الأسبقية وتوفر أيضاً المعاملة التفضيلية من طرف إلى طرف للنداءات الهاتفية والبيانات المخول لها في النطاق الضيق.

ويتحدد نطاق تطبيق التوصية [ITU-T E.106] ضمن سياق الشبكات PSTN أو ISDN أو PLMN. وتوفر الخطة IEPS أولوية المعالجة لخدمة المهاتفة الدولية للمستخدمين المخولين عبر شبكات الاتصالات المعدّة لهذا الغرض. لذلك يمكن استخدام الخطة IEPS استناداً إلى اتفاقات ثنائية أو متعددة الأطراف بين البلدان/الإدارات، في سيناريو توصيل بين تطبيقات الخطة IEPS الوطنية.

4.2.9 بروتوكولات التحكم في الأنظمة ITU-T H.323

تعرض هذه الفقرة البروتوكولات المستخدمة في النظام ITU–T H.323 لتوفير اتصالات الأولوية.

وتحدد التوصية [ITU–T H.460.4] تخصيص أولوية النداء وتعرف هوية البلد/الشبكة الدولية مصدر النداء في النداءات ITU–T H.323 ذات الأولوية. وتتيح معلمة تخصيص أولوية النداء ITU–T H.460.4 مؤشر نداء الأولوية وخمسة مستويات لها.

وتعرِّف التوصية [ITU-T H.248.1] البروتوكولات المستخدمة بين عناصر بوابة متعددة الوسائط مفككة مادياً تُستعمل وفقاً للمعمارية المحددة في التوصية [ITU–T H.323]. وتعرِّف هذه التوصية [ITU–T H.248.1] أيضاً مؤشر نداء الخطة IEPS ودلالة الأولوية في خدمات الطوارئ المخول لها حكومياً (مثل ETS). وينقل مؤشر النداء ETS دلالة الأولوية بين جهاز التحكم ووظائف البوابة. وتنقل دلالة الأولوية مستويات الأولوية بين جهاز التحكم ووظائف البوابة، كما أن مؤشر الأولوية H.248 يوفر 16 مستوى من مستويات الأولوية. ويلبي مؤشر النداء IEPS ومؤشر الأولوية متطلبات ETS من حيث بيان سياق IEPS وحمل مستوى الأولوية، على التوالي. وفيما يتعلق بخدمات السلامة العامة، تحدد التوصية [ITU–T H.248.1] مؤشر الطوارئ من أجل نقل دلالة الأولوية بين جهاز التحكم ووظائف البوابة.

وتوفر التوصية [ITU-T H.248.81] مبادئ توجيهية بشأن استخدام مؤشر النداء IEPS ومؤشر الأولوية ITU–T H.248 في البيانات الوصفية لأنظمة ITU-T H.323 وشبكات الجيل التالي دعماً للخدمات ذات الأولوية (مثل ETS).

5.2.9 القطر

يدعم بروتوكول القطر (Diameter) [IETF RFC 3588] الاستيقان والتخويل والمحاسبة (AAA) لوظائف وتطبيقات الشبكة كالنفاذ إلى الشبكة وتنقلية بروتوكول الإنترنت.

والقصد من أزواج قيم النعوت (AVP) التالية هو أن تُستخدم في بروتوكول القطر دعماً للخدمات ذات الأولوية (مثل ETS):

- MPS – معرف الهوية.
- الحجز – الأولوية.
- الأولوية – المستوى (كجزء من زوج قيمتي النعتين الاحتفاظ بالتوزيع – الأولوية (ARP)).
- الدورة – الأولوية.

ويعرّف مشروع شراكة الجيل الثالث (3GPP) زوج قيمتي النعتين MPS – معرف الهوية في المواصفة [b–3GPP TS 29.214]. ويُستخدم هذا الزوج لوسم خدمة ذات أولوية (مثل طلب ETS/MPS) عبر السطح البيني Rx. ويحوي زوج قيمتي النعتين MPS – معرف الهوية الصيغة الوطنية لاسم الخدمة ذات الأولوية.

ويُعرّف المعهد الأوروبي لمعايير الاتصالات (ETSI) زوج قيمتي النعتين، الحجز – الأولوية في المواصفة [ETSI TS 183 017]. وتوصّف التوصيتان [ITU–T Q.3321.1] و[ITU–T Q.3303.3] استخدام زوج قيمتي النعتين، الحجز – الأولوية عبر السطحين البينيين Rs وRw لوظيفة التحكم في الموارد والقبول (RACF) [ITU–T Y.2111]، على التوالي، دعماً للخدمات ذات الأولوية. وبالمثل، فإن مواصفة مشروع [b-3GPP TS 29.214]، (السياسة المتبعة والتحكم في الترسيم عبر النقطة المرجعية Rx) و[ITU–T Q.1741.6] توصّف زوج قيمتي النعتين، الحجز – الأولوية عبر السطح البيني Rx للسياسة المتبعة والترسيم (PCC) دعماً للخدمات ذات الأولوية (مثل ETS). ويدعم زوج قيمتي النعتين، الحجز – الأولوية 16 مستوى أولوية يمكن استخدامها لطلب معاملة الأولوية. ويتزايد ترتيب الأولويات وفق القيم ما بين 0 و15، حيث تأتي "15" في المرتبة العليا و"0" في المرتبة الدنيا. ويشمل زوج قيمتي النعتين الحجز – الأولوية قيمة أولوية المستخدم.

ويعرّف مشروع 3GPP زوج قيمتي النعتين الأولوية – المستوى (كجزء من زوج قيمتي النعتين الاحتفاظ بالتوزيع - الأولوية (ARP)) في المواصفة [b-3GPP TS 29.212] (السياسة المتّبعة والتحكم في الترسيم عبر النقطة المرجعية Gx) و[ITU-T Q.1741.6]. وتوصّف التوصية [ITU-T Q.1741.6] زوج قيمتي النعتين الأولوية – المستوى عبر السطح البيني Gx للسياسة المتّبعة والترسيم (PCC) دعماً للخدمات ذات الأولوية (مثل ETS). ويدعم زوج قيمتي النعتين، الأولوية – المستوى 15 مستوى أولوية يمكن استخدامها لطلب

معاملة الأولوية. ويتناقص ترتيب الأولويات وفق القيم ما بين 1 و15 حيث تأتي "1" في المرتبة العليا و"15" في المرتبة الدنيا. وتُخصص قيم الأولوية 1 إلى 8 للخدمات المخولة بتلقي معاملة أولوية (مثل ETS، MPS). أما قيمة الأولوية "0" فهي قيمة احتياط وتُعامل على أنها خطأ منطقي إذا وردت. ويعبر زوج قيمتي النعتين الأولوية – المستوى قيمة أولوية المستخدم.

ويعرّف مشروع 3GPP زوج قيمتي النعتين الدورة – الأولوية في المواصفة [b-3GPP TS 29.229] (السطحان البينيان Cx وDx على أساس بروتوكول القطر؛ تفاصيل البروتوكول) و[ITU-T Q.1741.6]. وتوصّف هذه المواصفة استخدام زوج قيمتي النعتين الدورة – الأولوية عبر السطحين البينيين Cx وDx دعماً للخدمات ذات الأولوية (مثل ETS). وبالمثل، توصّف المواصفة [b–3GPP TS 29.329] (السطح البيني Sh على أساس بروتوكول القطر؛ تفاصيل البروتوكول) و[ITU–T Q.1741.6] استخدام زوج قيمتي النعتين الدورة – الأولوية عبر السطح البيني Sh دعماً للخدمات ذات الأولوية. ويدعم زوج قيمتي النعتين الدورة – الأولوية 5 مستويات أولوية يمكن استخدامها لطلب معاملة الأولوية عبر السطوح البينية Cx وDx وSh. ويتناقص ترتيب الأولويات وفق القيم ما بين 0 و4 حيث تأتي "0" في المرتبة العليا و"4" في المرتبة الدنيا.

3.9 طبقة النقل

1.3.9 معلومات عامة

تستند الحاجة إلى ترتيبات خاصة (مثل الاتفاقات SLA) من أجل معالجة اتصالات الطوارئ في شبكة NGN ذات حجم وتصميم مناسبين إلى افتراض أن موارد الشبكة غير كافية لحجم الحركة التي تقدمها الشبكة وأن حركة اتصالات الطوارئ في مثل هذه الظروف قد تُرفض أو تتأخر كثيراً و/أو تضطرب إلى درجة يتعذر عندها استعمالها أو أنها تستبعد نهائياً. وعندما يتجاوز حجم الحركة المستقبلة، في نموذج مصمم إحصائياً لهذه الغاية أو على أساس أفضل خدمة ممكنة، استطاعة عنصر شبكة استقبال معينة (مسيّر IP مثلاً) والاستطاعة الخارجة المتاحة لهذا العنصر فإن الإمكانية الوحيدة أمام عنصر الشبكة هذا هو استبعاد الحركة الفائضة. وذلك يعني أن اتصالات الطوارئ يمكن استبعادها شأنها شأن الاتصالات العادية إن لم تتخذ تدابير تفضيلية خاصة بشأنها (على النحو المحدد في اتفاق مستوى الخدمة (SLA) مثلاً). وقد وفر منتدى إدارة الحركة (TM) إرشاداً بشأن مواصفة وإدارة اتفاقات مستوى الخدمة (SLA) [b-TM Forum GB917]، ونظر بوجه خاص في كيفية تطبيق هذا الإرشاد على خدمة الاتصالات في حالات الطوارئ (ETS).

ويُوصى أحياناً بتقنية زيادة حجم الموارد كحلٍّ. بيد أن زيادة حجم الموارد قد لا تكون ممكنة ولا عملية في الكثير من الأحيان. والأمر الأكثر أهمية هو أن بعض حالات الطوارئ قد تنجم عن إتلاف أو تردي متعمد أو عفوي لأجزاء من الشبكة، مما يستبعد إمكانية زيادة حجم الموارد في أي مسيرات أو عناصر قد تتيسر في الحالات العادية. وهكذا فإن لتقنية زيادة حجم الموارد تأثيراً سلبياً. ولكي تكون شبكة NGN قادرة على معالجة جميع أنواع اتصالات الطوارئ في ظروف معاكسة، لا بد من توفير وسائل خاصة من شأنها أن تتيح معالجة تفضيلية لحركة اتصالات الطوارئ.

وتقدم الفقرات التالية عدداً من الآليات المستخدمة للحصول على أولوية المعالجة عند مستوى النقل في سياق الشبكة NGN بتبديل الرزم.

2.3.9 التحكم في عرض النطاق باستعمال البروتوكول RSVP

لعل هناك آلية في شبكات بروتوكول الإنترنت قادرة على إعطاء ما يكافئ (نوعاً ما) توزيع عرض نطاق استناداً إلى الدارات، وهذه الآلية تستعمل بروتوكول الإنترنت (IP) لتوزيع وحجز عرض النطاق. وهي متوفرة في شكل إجراء يحدده فريق المهام IETF في بروتوكول حجز الموارد (RSVP) الوارد في المعيار [IETF RFC 2205] وفي تحديثاته [b-IETF RFC 2750] و[b-IETF RFC 3936] و[b-IETF RFC 4495].

ومعلمات التحكم في الموارد، وهي ضرورية لبروتوكول استهلال الدورة (SIP) في طبقة الخدمة لاستخدامها مع البروتوكول RSVP (طبقة النقل)، واردة في المعيار [IETF RFC 3312]. وذلك يتيح استعمال التشوير RSVP قبل إجراءات

التشوير SIP و/أو أثناءها و/أو بالتداخل معها. وترد بعض الأمثلة على ذلك في التذييل A للمعيار [IETF RFC 4542]. بيد أن المعيار [IETF RFC 4542] يستخدم تقنية الاستباق.

ويعكف فريق مهام هندسة الإنترنت (IETF) حالياً على تطوير توسعات البروتوكول RSVP التي يمكن استعمالها لتأمين مقدرة أولوية القبول في طبقة الشبكة بغية زيادة احتمال إنشاء الدورة في دورات معينة أثناء ازدحام الشبكة. وهي تحدد توسعات RSVP جديدة لزيادة احتمال إكمال النداء دون اللجوء إلى الاستباق. وتستخدم تقنيات المقدرات المصمَّمة في شكل نماذج توزيع عرض نطاق من أجل الوفاء بشروط "أولوية القبول" التي تتطلبها شبكة اتصالات طوارئ تستعمل البروتوكول RSVP. وتوصّف هذه التوسعات خصوصاً عنصرين جديدين لسياسة البروتوكول RSVP يتيحان نقل "أولوية القبول" في رسائل تشوير RSVP بحيث تستطيع عقد البروتوكول RSVP اتخاذ قرارات التحكم بالقبول استناداً إلى عرض النطاق مع مراعاة درجة أولوية قبول النداء.

3.3.9 تنظيم طوابير الانتظار باستعمال الخدمات المتفاضلة

تقدم الوثيقة [IETF RFC 4594] جدولاً توصي به للتقابل بين أصناف الخدمات وشفرات الخدمات المتفاضلة (DSCP). ويعرض الشكل 3 في الوثيقة المذكورة جدول تقابل بين صنف الإرسال السريع وتطبيقات المهاتفة، مما يتيح للرزم IP أن تضم قيمة شفرة DSCP موزعة على صنف الإرسال المسرّع.

وعلاوةً على ذلك، توصي التوصية [ITU-T Y.1541] بوسم (وضع علامة) الحركة الصوتية في الرزم IP بالشفرة DSCP المكافئة للإرسال السريع. وتضمن عناصر الشبكة (أجهزة التسيير) في طبقة النقل التي تستقبل الرزم الموسومة بالإرسال السريع (EF) تسليماً في حينه للحركة المستعجلة نسبةً إلى الحركة غير المستعجلة وذلك باستخدام أسلوب الإرسال السريع المحدد للشفرة EF والمعرّف في المعيار [IETF RFC 3246].

غير أن الشفرة EF مستخدمة في حركة المهاتفة العادية. ولذا قد يكون من الضروري التمييز بطريقة ما بين حركة المهاتفة في حالات الطوارئ وحركة المهاتفة في غير حالات الطوارئ. انظر الفقرة التالية.

4.3.9 الشفرة DSCP للإرسال السريع في الحركة ذات القدرة المقبولة

تعرّف الوثيقة [IETF RFC 5865] شفرة VOICE-ADMIT DSCP لصنف الحركة الخاضع للتحكم في قبول النداء (CAC) والشامل لحركة خدمة الاتصالات في حالات الطوارئ (ETS). وهذا يتيح حركة في الوقت الفعلي تتوافق مع أسلوب الإرسال السريع بالقفزات الذي يستعمل إجراء CAC الذي يشمل الاستيقان والتخويل وقبول القدرة (انظر الفقرتين 1.3.9 و2.3.9 أعلاه) على عكس صنف الحركة في الوقت الفعلي الذي يتوافق مع أسلوب الإرسال السريع بالقفزات والذي لم يخضع لإجراء قبول القدرة.

5.3.9 التبليغ الصريح بالازدحام (ECN)

تعرّف الوثيقة [IETF RFC 3168] معمارية التبليغ الصريح بالازدحام (ECN) ذات الطبقة المزدوجة على أنها معمارية تعمل في طبقة الشبكة (أي بروتوكول الإنترنت) وطبقة النقل (مثل بروتوكول التحكم في الإرسال (TCP)). وهي تهدف لتوفير ملاحظات مشوّرة صريحة في الوقت المناسب إلى مصدر الازدحام باتجاه المقصد، بأدنى حد من، أو بدون، فقدان رزم، وبالتالي بالحد الأدنى من انقطاع التدفقات. وتنجَز هذه المعلومات المشوّرة بواسطة عقد وسيطة تدعم الإدارة الفاعلة لطابور الانتظار (AQM) التي تسم الرزم بتبليغ بازدحام وتعيد تسييرها باتجاه المقصد بدلاً من إسقاط الرزمة. ثم تعيد نقطة نهاية التدفق مؤشر إخطاري (أي تبليغ صريح بازدحام) إلى المصدر عبر بروتوكول نقل الطبقة العليا. وقد وسعت الوثيقة [IETF RFC 4340] دعم التبليغ الصريح بالازدحام (ECN) ليشمل بروتوكول التحكم في ازدحام البيانات (DCCP).

وفي حالة بروتوكولي TCP وDCCP كليهما، يحرك التبليغ الصريح بالازدحام (ECN) خوارزميات تراجع كامنة تتسم بالشفافية بالنسبة إلى التطبيقات. وتتمثل المنفعة العامة لهذه الميزة في جعل التطبيقات أكثر انسجاماً مع الشبكات، وفي خفض الحمولة المعروضة مما يفسح بالمجال أمام المزيد من المستخدمين/التطبيقات لاستخدام الشبكة. وفي سيناريو شفافية التطبيق هذا،

لا يحابي التبليغ الصريح بالازدحام (ECN) مستخدمي خدمة الاتصالات في حالات الطوارئ (ETS) مقارنةً بعموم المستخدمين، بل إنه يسهل استمرار استخدام موارد الشبكة من قبل مستخدمي خدمة الاتصالات في حالات الطوارئ وعموم المستخدمين على السواء.

ويعكف فريق عمل الشبكات لدى فريق مهام هندسة الإنترنت (IETF) حالياً على دراسة كيف يمكن استخدام التبليغ الصريح بالازدحام لتدفقات بروتوكول الوقت الفعلي (RTP) العاملة عبر بروتوكولي UDP/IP والتي تستخدم بروتوكول التحكم في النقل في الوقت الفعلي (RTCP) كآلية إخطار. ويتمثل الحل في موافاة المرسل بواسطة بروتكول RTCP بوسوم الازدحام من التبليغ الصريح بالازدحام (ECN)، والتحقق من الخصائص الوظيفية لهذا التبليغ من طرف إلى طرف وكيفية البدء باستخدام التبليغ الصريح بالازدحام. وقد أُعدت الدراسات لدى فريق مهام هندسة الإنترنت لتضيف دعم التبليغ الصريح بالازدحام إلى التطبيقات في الوقت الفعلي (مثل الصوت والفيديو) باستخدام بروتوكولي RTP/RTCP. وفي هذه الحالة، يُتاح التبليغ عن الازدحام إلى التطبيقات التي قد تختلف ردودها على التبليغ. ويُتوقع أن يحذو الرد الغيابي حذو بروتوكولي TCP وDCCP حيث يخفض التطبيق الحمل المقدم على الشبكة.

4.9 دعم تكنولوجيا النفاذ إلى الشبكة NGN

1.4.9 معلومات عامة

ثمة طرائق تكنولوجية متعددة للنفاذ إلى شبكات الجيل التالي (NGN). فهذا النفاذ، وفقاً للتوصية [ITU–T Y.2012]، يضم وظائف تعتمد على تكنولوجيا النفاذ، فيما يتعلق مثلاً بالتكنولوجيا W–CDMA والنفاذ xDSL. وتبعاً للتكنولوجيا المستخدمة في النفاذ إلى خدمات الشبكات NGN تضم شبكة النفاذ الوظائف التالية:

1) النفاذ إلى الكبل؛
2) النفاذ إلى الخطوط xDSL؛
3) النفاذ اللاسلكي (مثل المعيارين [b–IEEE 802.11] و[b–IEEE 802.16] والنفاذ 3G RAN)؛
4) النفاذ بالليف البصري.

ويحتاج توفير اتصالات الطوارئ أيضاً إلى ترتيبات خاصة في جزء النفاذ إلى الشبكة NGN. وتفترض الحاجة إلى الترتيبات الخاصة أن موارد النفاذ محدودة على غرار موارد الشبكة المركزية. ولذا فإن حركة اتصالات الطوارئ تتأثر تبعاً لمقدار الحركة المرسلة إلى جزء شبكة النفاذ (كأن ترفض أو تتأخر كثيراً و/أو تضطرب بحيث تصبح غير قابلة للاستخدام أو تُستبعد).

وبناءً على ذلك، ينبغي توفير وسائل خاصة تؤمن معالجة تفضيلية لحركة اتصالات الطوارئ في جزء النفاذ إلى الشبكة NGN لتمكين الشبكة NGN من معالجة جميع أنواع حالات الطوارئ في الظروف الصعبة. ويتطلب ذلك آليات ومقدرات منها:

- التعرف على حركة اتصالات الطوارئ؛
- النفاذ التفضيلي/ذو الأولوية إلى الموارد/المرافق؛
- التسيير التفضيلي/ذو الأولوية لحركة اتصالات الطوارئ؛
- إنشاء تفضيلي/ذو أولوية لدورات/نداءات اتصالات الطوارئ.

وإذ تحظى الاتصالات في حالات الطوارئ بمعاملة ذات أولوية، تؤخذ الجوانب التالية بعين الاعتبار: تصنيف أو وسم حركة المعاملة ذات الأولوية، والتشوير لإنشاء المسير الناقل لهذه الحركة وآليات تشمل سياسات دعم الأولوية المطلوبة. وهناك جوانب غير مقيّسة مثل انتقاء الآليات والسياسات والتطبيقات المرتبطة بها، ويمكن أن تختلف تبعاً لخصوصيات المناطق.

2.4.9 النفاذ اللاسلكي

يتعيَّن على شبكات النفاذ اللاسلكي أن توفر آليات ومقدرات خاصة من شأنها تأمين معالجة تفضيلية/ذات أولوية لنداءات أو دورات اتصالات الطوارئ. ويمكن استعمال الآليات والمقدرات التكنولوجية لتأمين المعالجة التفضيلية/ذات الأولوية. ويضم ذلك آليات ومقدرات منها:

- التعرّف على حركة اتصالات الطوارئ: أي تعرف هوية اتصالات الطوارئ المخول لها ووسمها.
- النفاذ التفضيلي/ذو الأولوية إلى الموارد/المرافق: ويسهِّل ذلك تسليم طلب اتصالات طوارئ إلى شبكة NGN عندما تكون موارد النفاذ المتيسرة قليلة.
- التسيير التفضيلي/ذو الأولوية لحركة اتصالات الطوارئ: ويضم عناصر مثل تنظيم صفوف انتظار الموارد المتيسرة والإعفاء من بعض وظائف الشبكة الإدارية التقييدية وحجز بعض المسيرات/الطرق لاتصالات الطوارئ.
- الإنشاء التفضيلي/ذو الأولوية لدورات أو نداءات اتصالات الطوارئ.

1.2.4.9 النظام العالمي للاتصالات المتنقلة (UMTS) والتطور في المدى البعيد (LTE)

يرد في المواصفة [b-3GPP TS 22.153] توصيف خدمة الأولوية وخدمة أولوية الوسائط المتعددة في أنظمة 3GPP. وقد حدد مشروع 3GPP خدمة الأولوية وخدمة أولوية الوسائط المتعددة في أنظمة 3GPP. وتتيح خدمة الأولوية وخدمة أولوية الوسائط المتعددة للمستعملين المرخص لهم أن يحصلوا على نفاذ ذي أولوية إلى أقرب قنوات راديوية متيسرة (مهاتفة أو إرسال بيانات) قبل غيرهم من المستعملين في الظروف التي يحبط فيها الازدحام محاولات النداء. وتضمن خدمة الأولوية تقدُّم نداء الأولوية وإكماله كي تضمن نداء أولوية "من طرف إلى طرف" بين الشبكات المتنقلة، ومن الشبكات المتنقلة إلى الشبكات الثابتة ومن الشبكات الثابتة إلى الشبكات المتنقلة. وتؤمن خدمة أولوية الوسائط المتعددة تقدُّم أولوية دورات الوسائط المتعددة وإكمالها كي تضمن دورات الوسائط المتعددة ذات الأولوية "من طرف إلى طرف" بما فيها الدورات بين الشبكات المتنقلة ومن شبكة متنقلة إلى شبكة ثابتة ومن شبكة ثابتة إلى شبكة متنقلة.

واستناداً إلى المواصفة [b–3GPP TS 22.153]، فإن مشروع 3GPP بصدد وضع المرحلة الثانية من التقرير التقني بشأن تحسينات خدمة أولوية الوسائط المتعددة (MPS) [b–3GPP TR 23.854] لتحديد التغييرات على مواصفات 3GPP في المرحلة الثانية القائمة (ومثالها المواصفات [b–3GPP TS 23.401] و[b–3GPP TS 23.203] و[b–3GPP TS 23.328] و[b–3GPP TS 23.272]) دعماً لخدمة أولوية الوسائط المتعددة (MPS)، بما فيها النظام الفرعي متعدد الوسائط لبروتوكول الإنترنت (IMS) وجوانب التحكم في السياسة المتّبعة والترسيم (PCC). والقصد من هذا التقرير التقني هو توضيح المتطلبات المعمارية وتدفقات النداء أو الدورة لخدمة أولوية الوسائط المتعددة (MPS). واستناداً إلى متطلبات المرحلة الثانية من مشروع 3GPP، ستوصَّف التغييرات على مواصفات 3GPP في المرحلة الثالثة القائمة دعماً لخدمة أولوية الوسائط المتعددة (MPS) في تكنولوجيات النفاذ إلى النظام العالمي للاتصالات المتنقلة (UMTS) والتطور في المدى البعيد (LTE).

2.2.4.9 معيار الصيغة المثلى للتطور والبيانات (EV-DO)

كشأن المرحلة الأولى من مشروع شراكة الجيل الثالث (3GPP)، وصَّفت المرحلة الثانية من المشروع (3GPP2) خدمة أولوية الوسائط المتعددة (MMPS) لأنظمة 3GPP2. وهذه المواصفة هي [b–3GPP2 S.R0117-0]. وترد في معايير السطح البيني لشبكة أنظمة 3GPP2 بضع مقدرات من قبيل تحديث مستويات أولوية الحمالة، ويمكن استخدام هذه المقدرات لتوفير خدمة أولوية الوسائط المتعددة. وبالمثل ترد في معايير السطح البيني على الهواء لأنظمة 3GPP2 بضع مقدرات من قبيل التنظيم في طابور الانتظار، ويمكن استخدام هذه المقدرات لتوفير خدمة أولوية الوسائط المتعددة.

3.2.4.9 النفاذ إلى شبكة WiMAX

تعرّف الوثيقة [b–WFM Stage1–r1] متطلبات المرحلة الأولى لخدمة الاتصالات في حالات الطوارئ (ETS) عبر شبكات WiMAX في الإصدار 1.6 استناداً إلى السطح البيني على الهواء الوارد في المعيار [b–IEEE 802.16] عام 2009. وتعزز

الوثيقة [b–WFM Stage1–r2] الإصدار 1.6 من متطلبات المرحلة الأولى لخدمة الاتصالات في حالات الطوارئ (ETS) عبر شبكات WiMAX كي يدعم الإصدار 2.0 السطح البيني على الهواء الوارد في المعيار [b–IEEE 802.16].

وتوصّف الوثيقة [b-WFM Stage2-a1] المرحلة الثانية من إطار حل شبكة WiMAX لخدمة اتصالات الطوارئ في الإصدار 1.6 دعماً لمتطلبات المرحلة الأولى. ويتناول الإطار ما تبادر به الشبكة من مؤشر أولوية ومعالجة أولويات في معمارية الاستيقان والتخويل والمحاسبة (AAA). وفي الإصدار 2.0، يجري وضع إطار لخدمة الاتصالات في حالات الطوارئ (ETS) على أساس معمارية التحكم في السياسة المتبعة والترسيم (PCC) وآليات الأولويات التي تطلقها معدات المستخدم.

وتوصّف الوثيقة [b-WFM Stage3-a1] المرحلة الثالثة من إجراءات ورسائل شبكة WiMAX في الإصدار 1.6 دعماً لمؤشر الأولوية ومعالجة الأولويات على أساس إطار حل المرحلة الثانية. ويضاف حقل مؤشر الأولوية إلى معلمة واصف جودة الخدمة في رسائل بروتوكولي نصف القطر (RADIUS) والقطر (Diameter) ضمن شبكة WiMAX. كما يرد في هذه الوثيقة وصف إجراءات بيان الأولوية لمعمارية الاستيقان والتخويل والمحاسبة (AAA) التي تستهلها الشبكة، فضلاً عن آليات معالجة الأولوية في محطة القاعدة (BS) وبوابة النفاذ إلى خدمة الشبكة (ASN) والكيانات الوظيفية لشبكة خدمة التوصيلية (CSN). أما المجالات الرئيسية لدعم خدمة الاتصالات في حالات الطوارئ (ETS) في شبكة WiMAX فهي كما يلي:

1) بعد أول دخول لجهاز مستخدم إلى شبكة WiMAX لارتباطه باشتراك في الشبكة لمصلحة الاتصالات في حالات الطوارئ (ETS)، تعبر مؤشرات الأولوية المرتبطة بأوائل تدفقات الخدمة من مخدم الاستيقان والتخويل والمحاسبة (AAA) إلى بوابة النفاذ إلى خدمة الشبكة (ASN) ثم إلى محطة القاعدة (BS). وتطبق محطة القاعدة معاملة الأولوية على توزيع المورد وجدولته الزمنية في تدفقات الخدمة ذات الأولوية.

2) بعد أن يستدعي جهاز المستخدم خدمة الاتصالات في حالات الطوارئ (ETS)، تعبر مؤشرات الأولوية المرتبطة بتدفقات الخدمة من وظيفة التطبيق (AF) إلى مخدم وظيفة الاستيقان والتخويل والمحاسبة (AAA)/السياسة المتبعة (PF) ثم إلى بوابة النفاذ إلى خدمة الشبكة (ASN) ثم إلى محطة القاعدة (BS). وتطبق محطة القاعدة معاملة الأولوية على توزيع المورد وجدولته الزمنية في تدفقات الخدمة ذات الأولوية.

3) وعند التمرير، يُحتفظ بمؤشرات أولوية جهاز المستخدم المرتبطة بتدفقات الخدمة لتمرَر من محطة القاعدة المخدمة إلى محطة القاعدة المستهدفة ضمن بوابة النفاذ إلى خدمة الشبكة (ASN) ومن بوابة ASN المخدمة إلى بوابة ASN المستهدفة. وتطبق محطتا القاعدة معاملة الأولوية على توزيع المورد وجدولته الزمنية في جميع تدفقات الخدمة ذات الأولوية خلال إعداد التمرير وتنفيذه.

4) وعند استدعاء جهاز مستخدم في وضع الراحة، تعبر مؤشرات الأولوية المرتبطة بتدفقات الخدمة من بوابة النفاذ إلى خدمة الشبكة (ASN) مع وظيفة مسير البيانات إلى مركز مراقب الاستدعاء ثم إلى محطة القاعدة. وتطبق محطة القاعدة معاملة الأولوية على توزيع المورد وجدولته الزمنية في تدفقات الخدمة ذات الأولوية ضمن رسائل الاستدعاء الإذاعية. ورداً على الاستدعاء ذي الأولوية، عندما يدخل جهاز المستخدم الشبكة، تتعرف محطة القاعدة على نداء اتصالات الطوارئ الوارد ذي الأولوية وتعامل جهاز المستخدم معاملة الأولوية في الخروج من وضع الراحة وكذلك في إضافة/تغيير تدفق خدمة نداء اتصالات الطوارئ إلى الجهاز الانتهائي للمستخدم.

ويجري تطوير إجراءات ورسائل إضافية للمرحلة 3 من خدمة الاتصالات في حالات الطوارئ (ETS) من أجل الإصدار 2.0 الذي يشمل مؤشر ومعاملة الأولوية لقياس المدى ولإنشاء تدفق خدمي وللسطح البيني الشامل للخدمات (USI).

3.4.9 النفاذ الثابت

يتعين على شبكات النفاذ الثابت أن تقدم آليات ومقدرات خاصة للمعالجة التفضيلية/ذات الأولوية لنداءات أو دورات اتصالات الطوارئ المرخص بها. ويمكن استعمال الآليات والمقدرات المحددة تكنولوجياً (مثل النظام [b–802.1p] مع الخطوط xDSL وIPCablecom وIPCable 2) لتأمين المعالجة التفضيلية/ذات الأولوية. وذلك يتضمن آليات ومقدرات منها:

- التعرّف على حركة اتصالات الطوارئ: أي تعرّف هوية اتصالات الطوارئ المخول لها ووسمها.
- النفاذ التفضيلي/ذو الأولوية إلى الموارد/المرافق: أي تسهيل تسليم طلب اتصالات الطوارئ إلى شبكة NGN عندما تكون موارد النفاذ المتيسرة قليلة.
- التسيير التفضيلي/ذو الأولوية لحركة اتصالات الطوارئ: ويضم عناصر مثل تنظيم طوابير انتظار الموارد المتيسرة والإعفاء من بعض الوظائف الإدارية التي تقيّد الشبكة وحجز بعض الطرق/المسيرات لاتصالات الطوارئ.
- الإنشاء التفضيلي/ذو الأولوية لنداءات/دورات اتصالات الطوارئ.

ويرد وصف الاعتبارات الخاصة بكل تكنولوجيا في الفقرات الفرعية التالية.

1.3.4.9 النفاذ إلى شبكة IPCablecom

تعرف التوصية [ITU-T J.260] متطلبات خدمة الاتصالات التفضيلية في الشبكات IPCablecom. وتعرّف التوصية [ITU–T J.261] إطار وضع المواصفات لدعم هذه المتطلبات عبر شبكات IPCablecom وIPCablecom 2 على حد سواء. ويتناول الإطار مجالين رئيسيين هما الأولوية والاستيقان. وتُحدد مجالات أخرى مثل التزويد وقابلية الترميم في المراجعات المستقبلية. ويحدَد الإطار ليشمل الجانبين المشتركين كليهما فضلاً عن الاختلافات الناتجة عن المعماريات المستخدمة في شبكات IPCablecom وIPCablecom 2 (القائمة على النظام الفرعي متعدد الوسائط لبروتوكول الإنترنت (IMS)). وهذه الشبكات شبكات رزم لها خصائص نوقشت في الفقرة 6 مثل تقاسم الموارد في حركة البيانات والتحكم. ويصنف الإطار الوارد في التوصية [ITU-T J.261] متطلبات الأولوية في التوصية [ITU-T J.260] من حيث التشوير والوسم والآليات.

وتعرّف التوصية [ITU-T J.262] مواصفة دعم متطلبات الاستيقان في شبكات IPCablecom 2. وتتضمن التوصية [ITU–T J.262] أمثلة تدفق لبيان تبادل الرسائل في سيناريوهات مختلفة تقابل الاستيقان القائم على رقم تعريف الهوية الشخصي (PIN) واستخدام رأسية أولوية موارد بروتوكول استهلال الدورة (SIP)، ومن هذه السيناريوهات: إجراء وكيل المستخدم لمكالمة VoIP إلى مستخدم PSTN باستعمال رقم PIN، وإجراء وكيل المستخدم لمكالمة VoIP إلى وكيل مستخدم VoIP باستعمال رقم PIN واشتراك قائم على الاستيقان.

وتعرّف التوصية [ITU-T J.263] مواصفة دعم تشوير الأولوية للمعاملة التفضيلية باستخدام رأسية أولوية موارد بروتوكول استهلال الدورة (SIP) [IETF RFC 4412]. ويرد خياران في المواصفة: (1) يبادر وكيل المستخدم (UA) بطلب يتضمن رأسية المورد – الأولوية؛ (2) بناءً على المعلومات الواردة في الطلب، تدرج وظيفة التحكم في دورة النداء بالوكالة (P–CSC–FE) القيمة المناسبة لمستوى الأولوية في رأسية المورد – الأولوية. أما قيم حيّز الاسم ومستوى الأولوية التي يتعين استخدامها في مناطق مختلفة، فهي ترد كملحقات بالتوصية [ITU-T J.263]. وفي بعض المناطق، يلزم دعم القيم المعرفة في المواصفة [IETF RFC 4412]. وتصف التوصية [ITU-T J.263] أيضاً العلاقة مع تدفقات الخدمة التي جرى إعدادها خلال تزويد المكيف المدمج متعدد المطاريف (E–MTA) في طبقة DOCSIS MAC لتعكس معلمات جودة الخدمة المطلوبة للاتصالات تفضيلية. ولا توجد آلية وسم محددة لنقل البيانات لأن بروتوكول الوقت الفعلي (RTP) لا يتضمن وسوم تشير إلى الأولوية. وتُدعم آليات تفعيل الأولوية لحجز الموارد والقيام بالتحكم في القبول بضبط البوابات المعرفة كجزء من جودة الخدمة الدينامية (DQoS) في شبكة IPCablecom.

2.3.4.9 النفاذ إلى شبكة xDSL

يرد في التقرير التقني [BBF TR-101] وصف لمعمارية مرجع تجميع الخط الرقمي لمشترك (DSL) القائم على الإثرنت. والتحكم في السياسة المتبعة في شبكة النفاذ إلى DSL يقوم على المواصفات الواردة في التقارير التقنية [BBF TR–058] و[BBF TR–059].

والنهج الأساسي لتوفير مقدرات خدمة اتصالات الطوارئ (ETS) في شبكة النفاذ إلى DSL يتمثل في استخدام المقدرات القائمة لجودة الخدمة لتوفير الأولوية لنداءات أو دورات خدمة اتصالات الطوارئ. وينفرد مخدّم السياسة المتبعة/نقطة اتخاذ قرار السياسة المتبعة (PDP) في هذا النهج بكونه الجهاز "المتنبه إلى خدمة اتصالات الطوارئ" الذي يضع الأولوية المناسبة الواجب تطبيقها على المقدرات القائمة لجودة الخدمة في بوابة الشبكة عريضة النطاق (BNG).

ونظراً للطبيعة غير المانعة لجهاز الربط البيني مع الشبكة (NID) وإطار التوزيع الرئيسي (MDF)، لا لزوم لميزات خدمة اتصالات الطوارئ (ETS) في عناصر الشبكة هذه. ويزوّد عرض النطاق ويثبَّت بين NID ومعدّد النفاذ إلى الخط الرقمي للمشترك (DSLAM) الذي يُصمم أيضاً بحيث لا يكون مانعاً. ومن ثم فإن النهج الذي يقع الاختيار عليه يستخدم مقدرات جودة الخدمة في بوابة الشبكة عريضة النطاق (BNG) للتحكم في تدفق البيانات من خلال معدد النفاذ إلى الخط الرقمي للمشترك ولضمان ألا تتسبب الحركة بازدحام معدد النفاذ هذا.

وقد صُممت وظيفة تجميع الإثرنت لنقل كل حركة بين BNG وDSLAM وبالتالي فهي عنصر غي مانع.

أما بوابة النفاذ إلى معدات مباني العملاء (CPE) فيمكن أن تكون متنبهة أو غير متنبهة إلى خدمة اتصالات الطوارئ (ETS). فإن كانت متنبهة إليها، أمكنها تنظيم أولويات حركة خدمة اتصالات الطوارئ لضمان الإرسال إلى شبكة النفاذ إلى DSL ولضمان عدم ازدحام معدد النفاذ إلى الخط الرقمي للمشترك (DSLAM).

ويتولى مخدّم السياسة المتبعة/نقطة اتخاذ قرار السياسة المتبعة (PDP) مسؤولية توفير السياسات الملائمة لحركة خدمة اتصالات الطوارئ (ETS) إلى BNG. وفي خدمة اتصالات الطوارئ، ينفذ مخدّم السياسة المتبعة/نقطة اتخاذ قرار السياسة المتبعة سياسات التحكم في القبول ليرجح بدرجة عالية احتمال نجاح نداء أو دورة خدمة اتصالات الطوارئ. وتؤثر السياسات المتبعة في إنشاء نداء أو دورة خدمة اتصالات الطوارئ والحفاظ عليهما وإنهائهما عبر شبكة النفاذ إلى DSL وصولاً إلى شبكة مبنى العميل. ويُفترض أن مخدّم السياسة المتبعة/نقطة اتخاذ قرار السياسة المتبعة سيتلقى طلب نداء أو دورة خدمة اتصالات الطوارئ من شبكات الجيل التالي (ومثالها، الكيان الوظيفي للتحكم في دورة نداء بالوكالة (P–CSC–FE)). وسيرسل مخدّم السياسة المتبعة/نقطة اتخاذ قرار السياسة المتبعة (PDP) إشعاراً بتلقي الطلب مشفوعاً بالمعلومات المناسبة عن خدمة اتصالات الطوارئ (ETS) وسيكلف بوابة الشبكة عريضة النطاق (BNG) بإيلاء أولوية على النحو المناسب.

وتقوم بوابة الشبكة عريضة النطاق (BNG) بمسؤولية توفير الأولوية لحركة خدمة اتصالات الطوارئ (ETS). وتطبق هذه البوابة التعليمات الواردة من مخدّم السياسة المتبعة/نقطة اتخاذ قرار السياسة المتبعة (PDP) عند تلقي وإنشاء الموارد المناسبة للتعامل مع نداء أو دورة خدمة اتصالات الطوارئ. وهي تطبق معاملة الأولوية، التي تتضمن وسم رزم الحمالة لتعامَل معاملة الأولوية لدى الإرسال إلى بوابة النفاذ إلى معدات مباني العملاء (CPE) وإلى الشبكة الإقليمية عريضة النطاق.

3.3.4.9 النفاذ إلى شبكة الألياف البصرية (FTTx)

يرد في التوصية [ITU-T G.983.1] وصف المعمارية المرجعية للنفاذ البصري إلى الشبكة البصرية المنفعلة (PON). وتحيل المعمارية المرجعية إلى نظام إدارة عقدة النفاذ (ANMS) للتحكم في انتهائية الخط البصري (OLT) وانتهائية الشبكة البصرية (ONT). ويوفر نظام إدارة عقدة النفاذ الخصائص الوظيفية لنقطة اتخاذ قرار السياسة المتبعة (PDP) التي تطبقها نقاط إنفاذ السياسة المتبعة (PEP) الواقعة في انتهائية الخط البصري (OLT) وانتهائية الشبكة البصرية (ONT).

لا يوجد اليوم أي تحكم مباشر في السياسة المتبعة أو إنفاذ لها ضمن شبكة النفاذ البصرية. بيد أن إيلاء الأولوية لخدمة اتصالات الطوارئ (ETS) في التعامل مع إعداد نداء أو دورة في شبكة النفاذ البصرية سيتطلب من نظام إدارة عقدة النفاذ (ANMS) أن يدعم وظائف تحكم دينامي في السياسة المتبعة. والنهج الأساسي لتوفير مقدرات خدمة اتصالات

الطوارئ (ETS) في شبكة النفاذ البصرية يتمثل في استخدام المقدرات القائمة لجودة الخدمة لتوفير الأولوية لنداء أو دورة خدمة اتصالات الطوارئ. وينفرد نظام إدارة عقدة النفاذ (ومثاله، مخدم السياسة المتبعة) في هذا النهج بكونه الجهاز "المتنبه إلى خدمة اتصالات الطوارئ" الذي يضع الأولوية المناسبة الواجب تطبيقها على المقدرات القائمة لجودة الخدمة في انتهائية الخط البصري (OLT) وانتهائية الشبكة البصرية (ONT). وتشوَّر سياسة خدمة اتصالات الطوارئ عبر السطح البيني Q3 (على النحو الموصّف في التوصية [ITU–T Q.812]) مع انتهائية الخط البصري، وتنعكس هذه السياسة من انتهائية الخط البصري إلى انتهائية الشبكة البصرية عبر السطح البيني لإدارة انتهائية الشبكة البصرية والتحكم فيها (OMCI).

ويتولى نظام إدارة عقدة النفاذ (ANMS) مسؤولية توفير السياسة الملائمة لحركة خدمة اتصالات الطوارئ (ETS) إلى انتهائية الخط البصري (OLT). وفي خدمة اتصالات الطوارئ، ينفذ نظام إدارة عقدة النفاذ (ANMS) سياسات التحكم في القبول ليرجح بدرجة عالية احتمال نجاح نداء/دورة خدمة اتصالات الطوارئ. وتؤثر السياسات المتبعة في إنشاء نداء/دورة خدمة اتصالات الطوارئ والحفاظ عليهما وإنهائهما ضمن شبكة النفاذ البصرية. ويتخذ نظام إدارة عقدة النفاذ القرارات النهائية بشأن السياسة المتبعة ويوفر ما يكفي من المعلومات لقيام انتهائية الخط البصري (OLT) وانتهائية الشبكة البصرية (ONT) بتشغيل التحكم في الموارد في خدمة اتصالات الطوارئ. ويُفترض أن نظام إدارة عقدة النفاذ سيتلقى طلب نداء/دورة خدمة اتصالات الطوارئ من شبكات الجيل التالي (ومثالها، الكيان الوظيفي للتحكم في دورة نداء بالوكالة (P–CSC–FE)). وسيرسل نظام إدارة عقدة النفاذ إشعاراً بتلقي الطلب مشفوعاً بالمعلومات المناسبة عن خدمة اتصالات الطوارئ (ETS) انتهائية الخط البصري (OLT) بإيلاء أولوية على النحو المناسب.

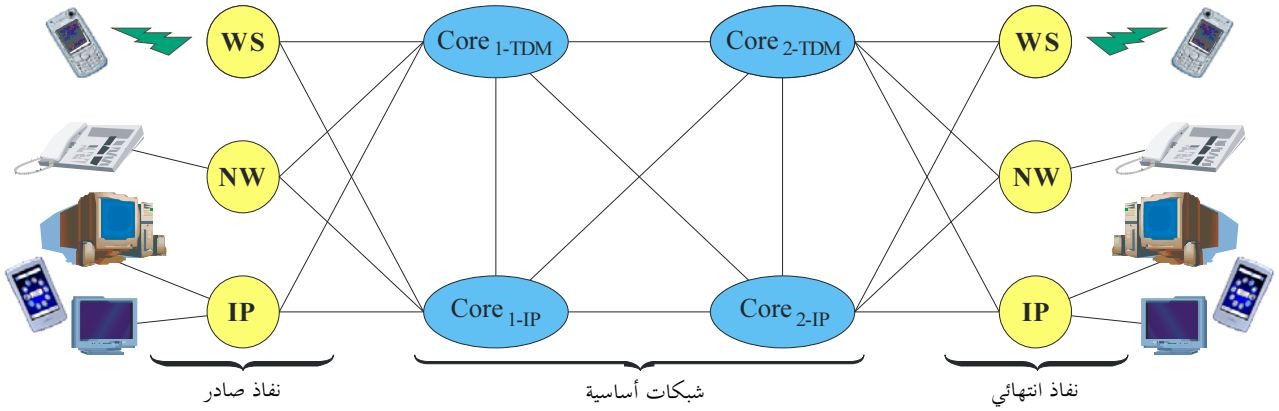
وقد صُممت انتهائية الخط البصري (OLT) وانتهائية الشبكة البصرية (ONT) لتنقلا كل حركة خدمة اتصالات الطوارئ (ETS). فتتولى انتهائية الخط البصري مسؤولية توفير الأولوية لحركة خدمة اتصالات الطوارئ. وتطبق هذه الانتهائية التعليمات الواردة من نظام إدارة عقدة النفاذ (ANMS) عند حجز وإنشاء الموارد المناسبة للتعامل مع نداء أو دورة خدمة اتصالات الطوارئ. وهي تطبق معاملة الأولوية، التي تتضمن وسم رزم الحمالة لتعامَل معاملة الأولوية لدى الإرسال.

10 دعم الاتصالات في حالات الطوارئ من طرف إلى طرف

يبين الشكل 2 مصفوفة نداء أو دورة من طرف إلى طرف لدعم مختلف تدفقات النداء أو الدورة في خدمة اتصالات الطوارئ (ETS). وهو يوضح النداءات أو الدورات:

- الصادرة والمنتهية بواسطة نفاذ بروتوكول الإنترنت (ومثاله الكبل وDSL) ونفاذ الخط السلكي ضيق النطاق (مثل هاتف النظام العادي القديم (POTS)) والنفاذ اللاسلكي (مثل هاتف GSM وCDMA)؛
- والعابرة من خلال الشبكات الأساسية العاملة على بروتوكول الإنترنت وعلى تبديل الدارات (تعدد الإرسال بتقسيم زمني (TDM)).

ويتطلب دعم خدمة الاتصالات في حالات الطوارئ من طرف إلى طرف عملاً بينياً للمعلومات الخاصة بهذه الخدمة ما بين ميدان تكنولوجيا بروتوكول الإنترنت وميادين التكنولوجيا الأخرى (مثل ميادين TDM السلكية واللاسلكية). ويشمل ذلك العمل البيني اللازم النداء/الدورة من طرف إلى طرف في خدمة اتصالات الطوارئ الذي يمكن أن يعبر ميادين تكنولوجيا مختلفة تظهر في الشكل 2. فعلى سبيل المثال، يتعين تشوير المعلومات الخاصة بخدمة اتصالات الطوارئ (ETS) (مثل وسم نداء خدمة اتصالات الطوارئ ومستوى الأولوية) على امتداد سطح التماس بين شبكة وأخرى (NNI) والذي يتوسط موردي شبكات الجيل التالي الموصولة بينياً.



WS: نفاذ لا سلكي
NW: نفاذ خط سلكي ضيق النطاق

ملاحظة: الشبكة الأساسية هي الشبكة المستيقنة أو شبكة العبور أو كلتاهما معاً.

Y.2205(11)_F02

الشكل 2 – مصفوفة نداء/دورة من طرف إلى طرف

ويمكن الاطلاع على السيناريوهات المرتبطة بالشكل 2 في المعيار [b–ATIS–1000010] الذي يحدد تحدد الإجراءات والمقدرات اللازمة لدعم خدمة اتصالات الطوارئ (ETS) ضمن شبكات مقدمي الخدمة القائمة على بروتوكول الإنترنت وفيما بينها. وفيما يلي سيناريوهات النداء أو الدورة الممكنة على أساس المصفوفة الظاهرة في الشكل 2:

- نفاذ صادر إلى الشبكة الأساسية 1
  - نفاذ صادر بخط سلكي إلى الشبكة الأساسية العاملة على بروتوكول الإنترنت
  - نفاذ صادر لا سلكي إلى الشبكة الأساسية العاملة على بروتوكول الإنترنت
  - نفاذ صادر وفق بروتوكول الإنترنت إلى الشبكة الأساسية العاملة على بروتوكول الإنترنت
  - نفاذ صادر وفق بروتوكول الإنترنت إلى الشبكة الأساسية متعددة الإرسال بتقسيم زمني (TDM)
- شبكة الأساس 1 إلى شبكة الأساس 2
  - الشبكة الأساسية متعددة الإرسال بتقسيم زمني (TDM) إلى الشبكة الأساسية العاملة على بروتوكول الإنترنت
  - الشبكة الأساسية العاملة على بروتوكول الإنترنت إلى الشبكة الأساسية متعددة الإرسال بتقسيم زمني (TDM)
  - شبكة الأساس 1 العاملة على بروتوكول الإنترنت إلى شبكة الأساس 2 العاملة على بروتوكول الإنترنت
- شبكة الأساس 2 إلى نفاذ إلى المقصد
  - الشبكة الأساسية العاملة على بروتوكول الإنترنت إلى نفاذ إلى المقصد بخط سلكي
  - الشبكة الأساسية العاملة على بروتوكول الإنترنت إلى نفاذ لا سلكي إلى المقصد
  - الشبكة الأساسية العاملة على بروتوكول الإنترنت إلى نفاذ إلى المقصد وفق بروتوكول الإنترنت
  - الشبكة الأساسية متعددة الإرسال بتقسيم زمني (TDM) إلى نفاذ إلى المقصد وفق بروتوكول الإنترنت

ويتطلب إنشاء النداء أو الدورة في خدمة اتصالات الطوارئ (ETS) لبروتوكولات التشوير اللازمة التي تنقل المعلومات المطلوبة الدالة على الطبيعة الحرجة لخدمة اتصالات الطوارئ. ولدعم معاملة الأولوية من طرف إلى طرف، من المهم أن يُدعم تقابل معلومات الأولوية تسهيلاً للعمل بين البروتوكولات المختلفة المستخدمة داخل الشبكة (ومثال ذلك، العمل البيني البروتوكولي ما بين التحكم في النداء أو الدورة والتحكم في الحمالة) أو بين مختلف أنواع الشبكات (ومثال ذلك، العمل البيني للتحكم في النداء أو الدورة بين شبكتين) بما في ذلك الشبكة الهاتفية العمومية التبديلية. وبالمثل، فمن الأهمية بمكان

السماح بتقابل معلومات الأولوية تسهيلاً للعمل البيني السلس بين أنواع النقل المختلفة، أي أنواع الوسائط. وبدون مثل هذا العمل البيني/التقابل، قد يتعذر تحقيق معاملة الأولوية من طرف إلى طرف.

ويحضر قطاع تقييس الاتصالات حالياً توجيهات بشأن التقابل اللازم لنعوت بروتوكول التشوير (المعلومات ذات الأولوية في خدمة اتصالات الطوارئ (ETS)) لدعم صحيح الإنشاء والقبول لخدمة اتصالات الطوارئ في مختلف البروتوكولات "الأفقية" (مثل ISUP وSIP وITU–T H.225.0) و"العمودية" (مثل ITU–T H.248.0 والقطر).

وتوفر الإضافة 57 إلى سلسلة التوصيات ITU-T Q [ITU–T Q-Sup.57] متطلبات التشوير لدعم مقدرات تفضيلية ضمن شبكات بروتوكول الإنترنت في خدمة اتصالات الطوارئ (ETS). ويرد في التذييل III مثال عن تدفق النداء من الإضافة [ITU–T Q-Sup.57] يبين الاستيقان الناجح من النداء أو الدورة وإنشائهما في خدمة اتصالات الطوارئ (ETS).

11 آليات ومقدرات توفير بعض جوانب الإنذار المبكر في الشبكات NGN

1.11 معلومات عامة

يمكن أن تُصنف أنظمة الإنذار المبكر في فئتين: نموذج الدفع ونموذج الجذب.

يقوم نموذج "الدفع" على أساس تسجيل المشاركين معلومات الاتصال بهم (مثل العناوين الإلكترونية) لدى خدمة مركزية. وعند وقوع حدث ما يتم إبلاغه لهؤلاء المشاركين المسجلين مع احتمال مزيد من الإشارات إلى معلومات إضافية. ومن أهم عناصر التصميم المعماري لهذا النموذج هو وجود سلطة مركزية تقوم بتحديد ضرورة توزيع هذه المعلومات وما يترتب على ذلك. وتكمن قوة هذا النموذج في أنه يأخذ على عاتقه مهمة مراقبة الأحداث مما يساعد المستعملين على الاستمرار في أعمالهم بصورة عادية وعدم الانشغال بمراقبة احتمال وقوع الكوارث أو حالات الطوارئ.

ويمثل نموذج الدفع آلية توزيع من "نقطة" إلى "عدة نقاط"، وهو نشيط في طبقة الخدمة وطبقة النقل على حد سواء (تعدد التوزيع مثلاً).

أما نموذج "الجذب" فهو عكس نموذج الدفع من حيث إنه يقوم على أساس تبادل معلومات من نمط أسئلة وأجوبة. وينبغي للمشاركين في كلا النموذجين أن يتسجلوا إفرادياً لكنهم مسؤولون في نموذج الجذب عن مراقبة المعلومات والحصول عليها. وتكمن فائدة هذا النظام في أن المعلومات لا ترد إلا عند الحاجة إليها أو عند طلبها.

وبإيجاز، تستعمل أنظمة الإنذار التطبيقات الراهنة والمقدرات الأساسية المتوفرة في شبكات بروتوكول الإنترنت. وإضافة نموذج الجذب أو الدفع تجعل هذه الأنظمة أكثر ملاءمة لاحتياجات المستعملين وتوقعاتهم. ويمكن أيضاً استعمال تطبيقات كل نوع بالموازاة مع الآخر: فنموذج الدفع يؤمن المراقبة التلقائية الدورية مع التبليغ، بينما يقوم نموذج الجذب بالحصول على معلومات محددة حسب الطلب.

وترد أمثلة لنموذجي الدفع والجذب في التذييل II.

2.11 بروتوكول الإنذار المشترك (CAP)

تصف هذه الفقرة بروتوكول الإنذار المشترك (CAP) المحدد في التوصية [ITU-T X.1303] والذي يمكن استخدامه في تطبيقات الإنذار المبكر. ويستخدم هذا البروتوكول لغة شرحية قابلة للتوسيع (XML) ويوفر أنساقاً معيارية لتبادل البيانات في المعلومات المهيكلة.

وتحدد التوصية [ITU-T X.1303] نسقاً عاماً لتبادل إنذارات الطوارئ لجميع الأخطار والإنذارات الموجهة للجمهور وذلك عبر جميع أنواع الشبكات. ويتيح البروتوكول CAP توزيع رسائل إنذار متسقة في أنظمة إنذار مختلفة كثيرة في نفس الوقت، مما يزيد من فعالية الإنذار ويسهِّل مهمته. كما أن البروتوكول CAP ييسِّر كشف النماذج الناشئة للإنذارات المحلية المختلفة مما قد يشير مثلاً إلى خطر خفي أو عمل عدائي. ويتيح البروتوكول CAP أيضاً نموذجاً معيارياً لرسائل إنذار فعَّالة تستند إلى أفضل الممارسات التي تحددها البحوث الأكاديمية والخبرات المستقاة من الواقع العملي.

ويقدم البروتوكول CAP نسق رسالة مفتوح غير مسجل الملكية يصلح لجميع أنواع الإنذارات والتبليغات. ولا يرتبط بأي تطبيق معين أو طريقة اتصالات معينة. ويتواءم نسق البروتوكول CAP مع التقنيات الناشئة مثل خدمات شبكة الويب أو خدمات الويب السريعة لقطاع تقييس الاتصالات ومع الأنساق الراهنة بما فيها تشفير رسالة منطقة معينة (SAME) المستعملة للاتصالات الراديوية لأحوال الطقس في الإدارة الوطنية لدراسة المحيطات والغلاف الجوي (NOAA) في الولايات المتحدة الأمريكية ولنظام الإنذار في حالات الطوارئ (EAS)، وتقدم مقدرات محسنة منها:

- استهداف جغرافي مرن يستخدم أشكال خطوط الطول/العرض وأشكال فراغية أخرى ثلاثية الأبعاد؛
- مراسلة متعددة اللغات ومتعددة الفئات المقصودة؛
- فترات فعلية ونهايات موقوتة أو مؤجلة؛
- وظائف محسنة لتحديث الرسائل وحذفها؛
- توفير نماذج معيارية لرسائل الإنذار الكاملة والفعالة؛
- المواءمة مع التحفير الرقمي ووظيفة التوقيع؛
- خدمة الصور الرقمية والإشارات الصوتية الرقمية.

ويتيح البروتوكول CAP تقليص التكاليف والحد من تعقيد التشغيل من خلال الاستغناء عن سطوح بينية لبرمجيات مختلفة تفصيلاً لتناسب العديد من موارد الإنذار وأنظمة التوزيع لجميع الأخطار. كما يمكن التحويل ما بين نسق الرسالة CAP والأنساق "الأصلية" لجميع أنواع تكنولوجيا التحسس والإنذار مما يشكل أساساً "لشبكة إنترنت للإنذار" وطنية ودولية مستقلة تكنولوجياً.

ويكافئ البروتوكول CAP المحدد في التوصية [ITU-T X.1303] بروتوكول الإنذار المشترك V1.1 لدى المنظمة OASIS على الصعيد التقني ويتواءم معه. كما وصّفت منظمة OASIS بروتوكول CAP V1.2 الذي يورد تحديثات للبروتوكول CAP V1.1.

وتضم التوصية [ITU-T X.1303] مواصفة ترميز ASN.1 مكافئة تتيح تشفير بتات متراصاً واستعمال الترميز ASN.1 وكذلك أدوات تعريف مخطط لغة XML (XSD) من أجل صياغة رسائل CAP ومعالجتها. وتتيح هذه التوصية للأنظمة الراهنة مثل النظام ITU–T H.323 تشفير الرسائل CAP ونقلها وفك تشفيرها بسهولة أكبر.

3.11 إجراءات تسجيل التفرعات في إطار تفرع معرّف الشيء المنبه

إن التوصية [ITU–T X.674] بشأن إجراءات تسجيل التفرعات في إطار تفرع معرّف الشيء المنبه تنص على تسجيل تفرعات معرّف الشيء (OID) لتحديد هوية أنواع مختلفة من التنبيهات ووكالات التنبيه. وعلى وجه التحديد، فهي توصّف إجراءات تسجيل التفرعات لتحديد (جميع أنواع) التنبيهات ووكالات التنبيه الواقعة تحت تفرع معرّف الشيء المنبه {joint-iso-itu-t(2) alerting(49)} وفقاً للتوصية [ITU–T X.660].

وتسهل التوصية [ITU-T X.674] توزيع معرفات الأشياء واستخدامها لتحديد هوية وكالات التنبيه (ومثالها، وكالات التنبيه التي تعينها الدول الأعضاء في المنظمة العالمية للأرصاد الجوية (WMO)).

ملاحظـــة – تحتفظ المنظمة العالمية للأرصاد الجوية بسجل سلطات التنبيه. ويمكن الاطلاع عليه عبر العنوان الإلكتروني: http://www-db.wmo.int/alerting/authorities.html.

12 أولوية ترميم الخدمة

عند حدوث عطل أو انقطاع في الشبكة، تتعرض الخدمات الحساسة (مثل خدمات الطوارئ) إلى الانقطاع وقد تحتاج إلى درجة أكبر من احتمال الترميم عما هو في الخدمات الأخرى. وتحدد التوصية [ITU–T Y.2172] ثلاثة مستويات أولوية

لترميم الخدمات في الشبكة NGN. وتبيِّن استخدام تصنيفات الأولوية هذه في رسائل التشوير على نحو يتيح للخدمة المعنية أن تقيم النداء أو الجلسة بدرجة أولوية الترميم المطلوبة، مما يزيد من احتمال ترميم الخدمات الحساسة مقارنة بالخدمات الأخرى.

13 تبديل الحماية وترميمها

1.13 اعتبارات عامة

يرد في التوصية [ITU-T G.808.1] وصف لعدد من المفاهيم العامة المشتركة للعديد من تكنولوجيات النقل. وتُحدَّد في هذه التوصية عدة قضايا هامة يتعين النظر فيها لدى توفير الحماية لحركة الاتصالات في حالات الطوارئ.

1.1.13 الحماية الفردية

ينطبق مفهوم الحماية الفردية على تلك الحالات التي يستفاد فيها من حصر الحماية في جزء من إشارات الحركة التي تحتاج إلى موثوقية عالية.

2.1.13 الحماية الجماعية

تسمح هذه الحماية بتبديل الحماية من خلال معالجة حزمة منطقية من كيانات النقل ككيان واحد بعد بدء إجراءات الحماية.

3.1.13 الأنماط المعمارية

تحدَّد في التوصية [ITU-T G.808.1] الأنماط المعمارية التالية، ويرد ملخص عنها أدناه.

1.3.1.13 معمارية الحماية 1+1

في نمط معمارية الحماية 1+1، يكرَّس كيان نقل الحماية كمنشأة رديفة لكيان النقل العامل.

2.3.1.13 معمارية الحماية 1:n

في نمط معمارية الحماية 1:n، يكون كيان نقل الحماية المكرس منشأة رديفة مشتركة لكيانات النقل العاملة.

3.3.1.13 معمارية الحماية m:n

في نمط معمارية الحماية m:n، تشترك كيانات نقل حماية عددها m في منشآت رديفة لكيانات نقل عاملة عددها n، حيث $m \leq n$ عادةً.

4.1.13 أنماط التبديل

يمكن لأنماط تبديل الحماية أن تكون نمط تبديل أحادي الاتجاه أو نمط تبديل ثنائي الاتجاه.

وتجدر الإشارة إلى أن جميع أنماط التبديل، عدا تبديل 1+1 أحادي الاتجاه، تتطلب قناة اتصال بين طرفي ميدان محمي. وتدعى تلك القناة قناة تبديل الحماية التلقائي (APS).

وترد في التوصية [ITU–T G.808.1] قائمة بمزايا وعيوب تطبيق أنماط التبديل على جميع الحالات أعلاه.

وفي سياق الاتصالات في حالات الطوارئ القائمة على بروتوكول الإنترنت، قد يُكتفى بالتبديل أحادي الاتجاه نظراً لعدم الارتباط المباشر عموماً للمسيرات في كل اتجاه جراء الطبيعة أحادية الاتجاه للمسيرات/التسيير عبر الشبكات القائمة على بروتوكول الإنترنت.

5.1.13 أنماط التشغيل

يمكن أن تكون أنماط تشغيل الحماية من نمط التشغيل غير العائد أو من نمط التشغيل العائد.

ففي التشغيل العائد، تعود إشارة (خدمة) الحركة دوماً (أو تظل مشغَّلة) إلى كيان النقل العامل عندما تتعافى من العطل.

أما في التشغيل غير العائد، فلا تعود إشارة (خدمة) الحركة إلى كيان النقل العامل الأصلي.

ويُذكر في التوصية [ITU–T G.873.1] أن الحماية 1+1 غالباً ما تزوَّد كحماية غير عائدة، لأن الحماية مكرسة بالكامل في أي حال، ومن شأن ذلك أن يحول دون ظهور "عثرة" ثانية أمام الحركة. ومع ذلك، فقد تكون هناك أسباب لتزويد هذه الحماية كحماية عائدة (بحيث تلتف الحركة مثلاً في الاتجاه "القصير" حول حلقة إلا في ظروف التعطل. كما تملي بعض سياسات المشغل تشغيلاً عائداً حتى في نمط 1+1).

2.13 معماريات حماية التراتب الرقمي المتزامن (SDH)

توفر التوصية [ITU-T G.841] المواصفات اللازمة على مستوى المعدات لتنفيذ الخيارات المختلفة من الحماية لمعماريات شبكات التراتب الرقمي المتزامن (SDH).

ويمكن أن تتراوح الكيانات المحمية بين قسم واحد لتعدد إرسال التراتب الرقمي المتزامن (كحماية قسم تعدد الإرسال الخطي) وجزء من مسير التراتب الرقمي المتزامن من طرف إلى طرف (كحماية توصيل الشبكة الفرعية) أو مسير التراتب الرقمي المتزامن من طرف إلى طرف برمته. وقد يشمل التنفيذ المادي لمعماريات الحماية هذه حلقات أو سلاسل خطية من العقد. ويتضمن كل تصنيف حماية مبادئ توجيهية بشأن أهداف الشبكة والمعمارية والخصائص الوظيفية للتطبيق ومعايير التبديل وبروتوكولات وخوارزميات.

وبالإضافة إلى ذلك، توفر التوصية [ITU-T G.842] مواصفات العمل البيني لمعماريات حماية الشبكة. وهي تغطي على وجه التحديد التوصيل البيني بعقدة أحادية ومزدوجة ما بين حلقات الحماية المشتركة في قسم تعدد الإرسال (MS) وحلقات حماية توصيلة الشبكة الفرعية (SNCP) ذات الأنماط المتماثلة أو المختلفة.

3.13 شبكة النقل البصرية (OTN)

تعرّف التوصية [ITU-T G.873.1] بروتوكول تبديل الحماية التلقائي (APS) وتشغيل تبديل الحماية في خطط الحماية الخطية لشبكة النقل البصرية على مستوى وحدة بيانات القناة البصرية (ODUk).

أما خطط الحماية التي يُنظر فيها في التوصية [ITU-T G.873.1] فهي كما يلي:

- حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية (ODUk) مع المراقبة الكامنة (1+1, 1:n)؛
- حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية (ODUk) مع المراقبة غير التدخلية (1+1)؛
- حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية (ODUk) مع مراقبة الطبقة الفرعية (1+1, 1:n).

وفي اتجاه إرسال معين، يستطيع "طرف الرأس" للإشارة المحمية أن يقوم بوظيفة الجسر التي ستودع نسخة عن إشارة الحركة الطبيعية لدى كيان حماية عند اللزوم. وسيقوم "طرف الذيل" بوظيفة المنتقي القادر على انتقاء إشارة الحركة الطبيعية إما من كيانه العامل المعتاد أو من كيان الحماية. وفي حالة الإرسال ثنائي الاتجاه، حيث يُحمى كلا اتجاهي الإرسال، يوفر كلا طرفي الإشارة المحمية عادةً وظيفتي الجسر والمتلقي معاً.

4.13 تبديل الحماية الخطية للإثرنت

تصف التوصية [ITU-T G.8031] تفاصيل تبديل الحماية لإشارات الشبكة المحلية الافتراضية (VLAN) في الإثرنت. وترد التفاصيل المتعلقة بخصائص حماية الشبكة في طبقة الإثرنت (ETH) ومعمارياتها وبروتوكول تبديل الحماية التلقائي (APS).

وفي التوصية [ITU-T G.8031] ، تعرَّف معماريتا تبديل الحماية الخطية 1+1 و1:1 بتبديل أحادي الاتجاه وثنائي الاتجاه.

وفي معمارية تبديل الحماية الخطية 1+1، يكرَّس كيان نقل حماية لكل كيان نقل عامل. وتُنسخ الحركة الطبيعية وتلقَّم إلى كياني النقل العامل ونقل الحماية على السواء بواسطة جسر دائم في مصدر الميدان المحمي. وتُرسَل الحركة في كياني النقل

العامل ونقل الحماية في الوقت نفسه إلى مخرج الميدان المحمي حيث يجري الانتقاء ما بين كياني النقل العامل ونقل الحماية استناداً إلى معايير ما محددة سلفاً، مثل بيان عطل في المخدم.

ورغم أن الانتقاء ينحصر في مخرج الميدان المحمي في معمارية تبديل الحماية الخطية 1+1، فإن تبديل الحماية ثنائية الاتجاه 1+1 تحتاج لبروتوكول تنسيق بروتوكول تبديل الحماية التلقائي (APS) بحيث ينتقي المنتقيان في كلا الاتجاهين الكيان نفسه.

وفي معمارية تبديل الحماية الخطية 1:1، يكرَّس كيان نقل الحماية لكيان النقل العامل. بيد أن الحركة الطبيعية تُنقل إما على كيان النقل العامل أو على كيان نقل الحماية بواسطة الجسر المنتقي في مصدر الميدان المحمي. ويقوم المنتقي في مخرج الميدان المحمي بانتقاء الكيان الذي يحمل الحركة الطبيعية. ونظراً للحاجة لتنسيق المصدر والمخرج لضمان انتقاء الجسر المنتقي في المصدر والجسر المنتقي في المخرج الكيان نفسه، لا بد من بروتوكول تنسيق بروتوكول تبديل الحماية التلقائي (APS).

5.13 تبديل الحماية الحلقية للإثرنت

تعرّف التوصية [ITU-T G.8032] بروتوكول تبديل الحماية التلقائي (APS) وآليات تبديل الحماية للطبولوجيات الحلقية للشبكة في طبقة الإثرنت (ETH). وترد التفاصيل المتعلقة بخصائص الحماية الحلقية للإثرنت ومعمارياتها وبروتوكول تبديل الحماية التلقائي (APS) الحلقي.

ويمكّن بروتوكول الحماية المحدد في التوصية [ITU-T G.8032] من تحقيق التوصيلية المحمية من نقطة إلى نقطة ومن نقطة إلى عدة نقاط ومن عدة نقاط إلى عدة نقاط داخل حلقة أو حلقات موصولة بينياً تدعى طبولوجيا "الشبكة متعددة الحلقات/السلَّم".

6.13 تبديل الحماية الخطية لشبكات نقل تبديل الوسم بعدة بروتوكولات (T-MPLS)

توفر التوصية [ITU-T G.8131] متطلبات وآليات المسار من طرف إلى طرف وتبديل حماية توصيلة شبكة فرعية (SNC) لشبكات نقل تبديل الوسم بعدة بروتوكولات (T-MPLS). وهي تصف حماية المسار وأنماط معماريات حماية توصيلة شبكة فرعية ونمطي التبديل أحادي وثنائي الاتجاه ونمطي التشغيل العائد وغير العائد. وتعرّف بروتوكول تبديل الحماية التلقائي (APS) المستخدم لمواءمة كلا طرفي الميدان المحمي.

وتوصّف هذه التوصية معمارية 1+1 ومعمارية 1:1. إذ تعمل معمارية 1+1 بالتبديل أحادي الاتجاه، بينما تعمل معمارية 1:1 بالتبديل ثنائي الاتجاه.

7.13 تبديل حماية أسلوب النقل غير المتزامن (ATM)

توفر التوصية [ITU-T I.630] معماريات وآليات تبديل الحماية في طبقة أسلوب النقل غير المتزامن (ATM). وتتضمن المعمارية مدى الميدان المحمي وترتيبه. ويكون مورد كيانات الحماية موزعاً مسبقاً. وتشمل الآليات آليات إطلاق تبديل الحماية والتمهل، وبروتوكول التحكم في تبديل الحماية.

وتصف التوصية [ITU-T I.630] الحماية الفردية والحماية الجماعية للمسير الافتراضي (VP)/القناة الافتراضية (VC). أما الحماية الفردية للمسير الافتراضي (VP)/القناة الافتراضية (VC) فهي تقنية يُستخدم فيها توصيل شبكة و/أو شبكة فرعية واحد للكيان العامل وكيان الحماية. وأما الحماية الجماعية فهي تقنية تُستخدم فيها حزمة منطقية لواحد أو أكثر من توصيلات شبكة و/أو شبكة فرعية للكيان العامل وكيان الحماية.

وحالياً، تصف التوصية [ITU–T I.630] تبديل الحماية ثنائي الاتجاه 1+1 و1:1 فضلاً تبديل الحماية أحادي الاتجاه 1+1.

8.13 تبديل الحماية لشبكات تبديل الوسم بعدة بروتوكولات (MPLS)

توفر التوصية [ITU–T Y.1720] متطلبات وآليات التشابك المشترك 1+1 و1:1 والخصائص الوظيفية لتبديل حماية الرزم 1+1 لمستوي المستخدم في شبكات طبقة MPLS. وقد صُممت الآلية المحددة في تلك التوصية لدعم مسيرات تبديل الوسم (LSP) من نقطة إلى نقطة ومن طرف إلى طرف.

وقد وُضعت التوصية [ITU–T Y.1720] لتوصّف تقنيات تبديل الحماية. وتشرح التوصية [ITU–T Y.1720] الفرق بين تبديل الحماية وإعادة التسيير على النحو التالي:

تبديل الحماية: يعني ضمناً الحساب المسبق للتسيير والموارد معاً وتوزيعها في مسير تبديل وسم (LSP) ذي حماية مكرسة قبل وقوع العطل. ومن ثم، فإن تبديل الحماية يقدم ضماناً قوياً للقدرة على استعادة موارد الشبكة اللازمة بعد وقوع العطل.

إعادة التسيير: يعني ضمناً عدم تحديد مسير تبديل وسم (LSP) ذي حماية مكرسة. إذن لا يوجد حساب أو توزيع مسبق لا للتسيير ولا للموارد قبل وقوع العطل. ويشيع استخدام إعادة التسيير في الحالات التي تكون فيها وظائف التسيير والتشوير قيد التشغيل، ويُتقدم "بطلب إعادة توصيل" بعد وقوع عطل (من جانب إما الشبكة أو العميل) ويواجه هذا الطلب أنماط حركة مماثلة للحصول على المورد المطلوب. لذلك، فإن إعادة التسيير لا تقدم ضماناً للقدرة على استعادة موارد الشبكة اللازمة بعد وقوع العطل، وهي أبطأ عموماً من تبديل الحماية.

وتبديل الحماية ضروري لتدارك الأعطال بسرعة مما يعزز أداء الموثوقية والتيسر في شبكات تبديل الوسم بعدة بروتوكولات (MPLS).

وتلزم الميزات التالية من أجل تبديل الحماية:

1) ينبغي تطبيق تبديل الحماية على مسير تبديل وسم (LSP) كله.

2) حماية ذات أولوية بين انقطاع الإشارة وطلبات تبديل المشغل.

3) ينبغي توفير إمكانية تحقيق الحماية على طبقة تبديل الوسم بعدة بروتوكولات في أسرع وقت ممكن (رهناً بالاستبانة الزمنية لآلية الكشف).

4) حماية بنسبة 100%، أي حماية 100% من الحركة العاملة المعاقة من التعطل في مسير تبديل وسم واحد عامل.

5) ينبغي دعم قدرة حركة زائدة عندما يكون ذلك ممكناً.

التذييل I

فئات اتصالات الطوارئ

(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I اتصالات الطوارئ من فرد إلى سلطة

اتصال الطوارئ من فرد إلى سلطة هو اتصال يقيمه شخص ما باستعمال مقدرات اتصالات طوارئ وطنية من أجل طلب مساعدة مستعجلة أثناء حالة طارئة فردية (شخصية) أو حتى أثناء حالة طارئة محصورة. وعلى سبيل المثال، قد ينطوي نداء من فرد إلى سلطة على رقم قصير (مثل 112، 911 وغيرها) يوفر للمستعمل الفرد اتصالاً مع مركز تلقي نداءات الطوارئ. ويرسل المركز عندئذٍ الخدمات الملائمة (الشرطة أو رجال الإطفاء أو سيارة إسعاف مثلاً) نيابة عن الطالب. وقد يكون هناك معلومات إضافية ترسل تلقائياً إلى مركز النداءات مثل موقع الطالب. وتساعد هذه المعلومات على التحرك بسرعة لأن الطالب قد لا يكون قادراً أو ليس لديه الوقت أو إمكانية إعطاء هذه المعلومات بنفسه. وهذا النوع من الاتصال عموماً هو اتصال من نقطة إلى نقطة يتفاعل فيه الطالب مع الجهة المطلوبة بشكل أساسي. وتتعلق الغالبية العظمى من هذه الاتصالات بحالة طوارئ محدودة (مثل حريق منزلي) غالباً ما تنتج عن أحداث غير مترابطة ومع ذلك فإن الأحداث واسعة النطاق (هزة أرضية مثلاً) تؤدي إلى اتصالات كثيرة مترابطة ومتآونة. (ويستعمل مصطلح "فرد" هنا بمعناه الواسع ويعني كل شخص يحتاج إلى مساعدة مستعجلة (تغطي أشخاصاً مثل المواطنين أو الزائرين أو سكان آخرين في مكان ما.)). ويستطيع المشاركون في اتصالات الطوارئ أن يتواصلوا فيما بينهم باستعمال أنواع متعددة من الوسائط منها الصوتية والفيديوية والكتابة في الوقت الفعلي والرسائل الآنية.

2.I اتصالات الطوارئ من فرد إلى فرد

اتصال الطوارئ من فرد إلى فرد هو اتصال ينشأ عن شخص أو جهاز من عامة الجمهور إلى منظمة ما. ففي أثناء حالات الطوارئ أو بعدها مباشرة يحتاج الناس بشدة إلى الاتصال فيما بينهم. ونتيجة لذلك، يزداد الطلب على الاتصالات من فرد إلى فرد ازدياداً كبيراً في الوقت الذي تتناقص فيه موارد الاتصالات بسبب الأضرار الناجمة عن حالة الطوارئ. وتتسبب هذه العوامل مجتمعة في ازدحام شبكات الاتصالات.

3.I اتصالات الطوارئ من سلطة إلى سلطة

يكون اتصال الطوارئ من سلطة إلى سلطة عادةً اتصال يقوم به مستعمل مخوّل لاتصالات الطوارئ (أو المؤسسة التي يعمل فيها) مع مستعمل مخوّل آخر بهدف:

1) تسهيل عمليات الخروج من حالة الطوارئ (مثال ذلك إنشاء مراكز إدارة عمليات الطوارئ وعمليات إدارية مرتبطة بها من أجل تمكين الحكومة أو منظمات أخرى من تقديم المساعدة)؛

2) ترميم بنية تحتية أساسية لدى المجتمع (مثل استعادة خدمات الماء والكهرباء وغيرها)؛

3) اتخاذ تدابير من أجل إعادة الأمور إلى نصابها على المدى الطويل (مثال ذلك إعادة بناء الطرق والجسور والمباني وغيرها).

وتحدث عادة اتصالات الطوارئ من سلطة إلى سلطة (وتسمى أحياناً اتصالات السلامة العامة) التي تستخدم الشبكات العمومية في نفس الوقت الذي تكون فيه موارد الاتصالات مزدحمة بسبب الاتصالات المتزايدة بين الأفراد.

ونظراً إلى القدرة الكبيرة لاتصالات الطوارئ من سلطة إلى سلطة على تسهيل عمليات استعادة الحالة الطبيعية وعلى تجنيب الأرواح والممتلكات أخطار إضافية، فإن هذه الفئة من اتصالات الطوارئ تتمتع بالأولوية نسبة إلى الفئات الأخرى خلال أوقات إعلان حالة الطوارئ أو عند تفاقمها.

4.I اتصالات الطوارئ من سلطة إلى فرد

أخيراً، هنالك الاتصالات من سلطة إلى فرد (وتصنف أحياناً كأنظمة الإنذار المبكر) التي تحتوي عادة على معلومات موجهة إلى الجمهور وصادرة عن مصدر مرخص له بذلك. وقد تكون معلومات موجهة إلى جماعة حلّت بها كارثة وتضم تعليمات وإرشادات ونصائح تتعلق بالسلامة. وعادةً يقيم مستعمل مرخص له هذا الاتصال ويوجهه إلى أشخاص كثر.

اتصال من أي نقطة–إلى–أي نقطة: وهو مثال لخدمة ETS من موقع/جهاز يتصل بأي مستعمل آخر (ETS أو عامة الجمهور) من خلال وسيط ذي أفضلية في البنية التحتية للاتصالات. والخدمة GETS في الشبكة PSTN هي مثال واضح لذلك، حيث الخدمة التفضيلية غير معممة وغير مقيدة بمجموعة انتقائية من الأجهزة المطرافية أو المقاصد.

اتصال من نقطة–إلى–نقطة: يعتبر هذا الاتصال في سياق اتصالات الطوارئ نوعاً متفرعاً من حالة الاتصالات من أي نقطة–إلى–أي نقطة. وتقتصر المشاركة في هذه الحالة على اثنين من مستعملي الخدمة ETS.

اتصال من عدة نقاط–إلى–نقطة: يظهر هذا النموذج في شكل معمارية الزبون–المخدم وفي شبكة الويب حيث ينفذ أي مستعمل إلى موقع محدد معروف جيداً للحصول على المعلومات. وتستعمل الشبكة PSTN هذا النموذج في أنظمة الأرقام 911 و112 وغيرها، حيث ترسل الجلسات ضمن منطقة واحدة إلى نقطة استجابة واحدة بشأن السلامة العامة (PSAP).

اتصال من نقطة–إلى–عدة نقاط: ترسل المعلومات في هذا النموذج من مصدر واحد إلى مجموعة من المستقبلات (المستعملون النهائيون) التي اختارت المشاركة في تعميم البيانات. ويقدم التلفزيون والراديو، في حالة الوسائط الإذاعية، أوضح مثالين على هذا النموذج إذ إن المستقبلات لا تحصل على المعلومات إلا من القنوات التي اختارتها. وفي نموذج إرسال البيانات، يمكن التمييز بين علاقة نموذج من نقطة–إلى–عدة نقاط ونموذج الإذاعة فهذا الأخير يفترض أن تتلقى العقد جميعها الرسالة، سواء اختارت ذلك أم لا، بينما يفترض النموذج الأول الانتماء المباشر إلى مجموعة ما.

التذييل II

أمثلة لاستعمال أنظمة الإنذار المبكر

(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II نموذج الدفع

يقدم كل من القطاعين الخاص والعام أو الحكومي أنظمة إنذار تستند إلى نموذج الدفع. لكن هذه التوصية تقدم مثالاً من القطاع العام على نموذج الدفع في القطاع العام أو الحكومي هو مركز المعلومات عن حالات الطوارئ في الموقع الإلكتروني للإدارة المحلية من مدينة واشنطن العاصمة (http://alert.dc.gov/eic/site/default.asp). يسجل المستعملون معلومات الاتصال بهم على شكل عنوان بريد إلكتروني أو جهاز استدعاء أو رقم هاتف متنقل (إما للمراسلة الكتابية أو للمراسلة الصوتية التلقائية). وتقابل المراسلة الصوتية التلقائية نظام الخدمة 911 معكوساً، وجميع مواطني مقاطعة كولومبيا مسجلون تلقائياً في هذه الخدمة عن طريق بدالة الخطوط البرية المعنية. وفيما يتعلق بالبريد الإلكتروني وأجهزة الاستدعاء، فإن خدمة الإنذار لا تقتصر على المقيمين في واشنطن العاصمة.

2.II نموذج الجذب

أفضل مثال على نموذج الجذب العامل في الإنترنت هو المشروع I-AM-Alive القائم في اليابان (http://www.isoc.org/inet2000/cdproceedings/8l/8l_3.htm، http://www.iaa-alliance.net/en/). ورأى هذا المشروع النور إثر الزلزال الذي ضرب مدينة كوبي عام 1995، وهدفه مساعدة الناس على معرفة حال أقاربهم الذين تعرضوا للزلزال وتحديد مكان وجودهم إن أمكن. وهو يعمل كمركز جمع معلومات يتلقى ما يقدمه أوائل المنقذين من معلومات حصلوا عليها. وبالمقابل يعمل أيضاً كمركز توزيع معلومات يستخدمه الأصدقاء والأقارب ممن يريدون معرفة أحوال الناس الذين تعرضوا للكارثة.

ويقوم النظام I-AM-Alive بتخزين المعلومات التي يرسلها الأفراد أو المنقذون عبر الفاكس والهاتف والويب. ثم توزع هذه المعلومات في شكل صفحات ويب بصورة أساسية، ويمكن أيضاً الحصول على بعض المعلومات من أرقام هواتف معروفة متصلة بالنظام.

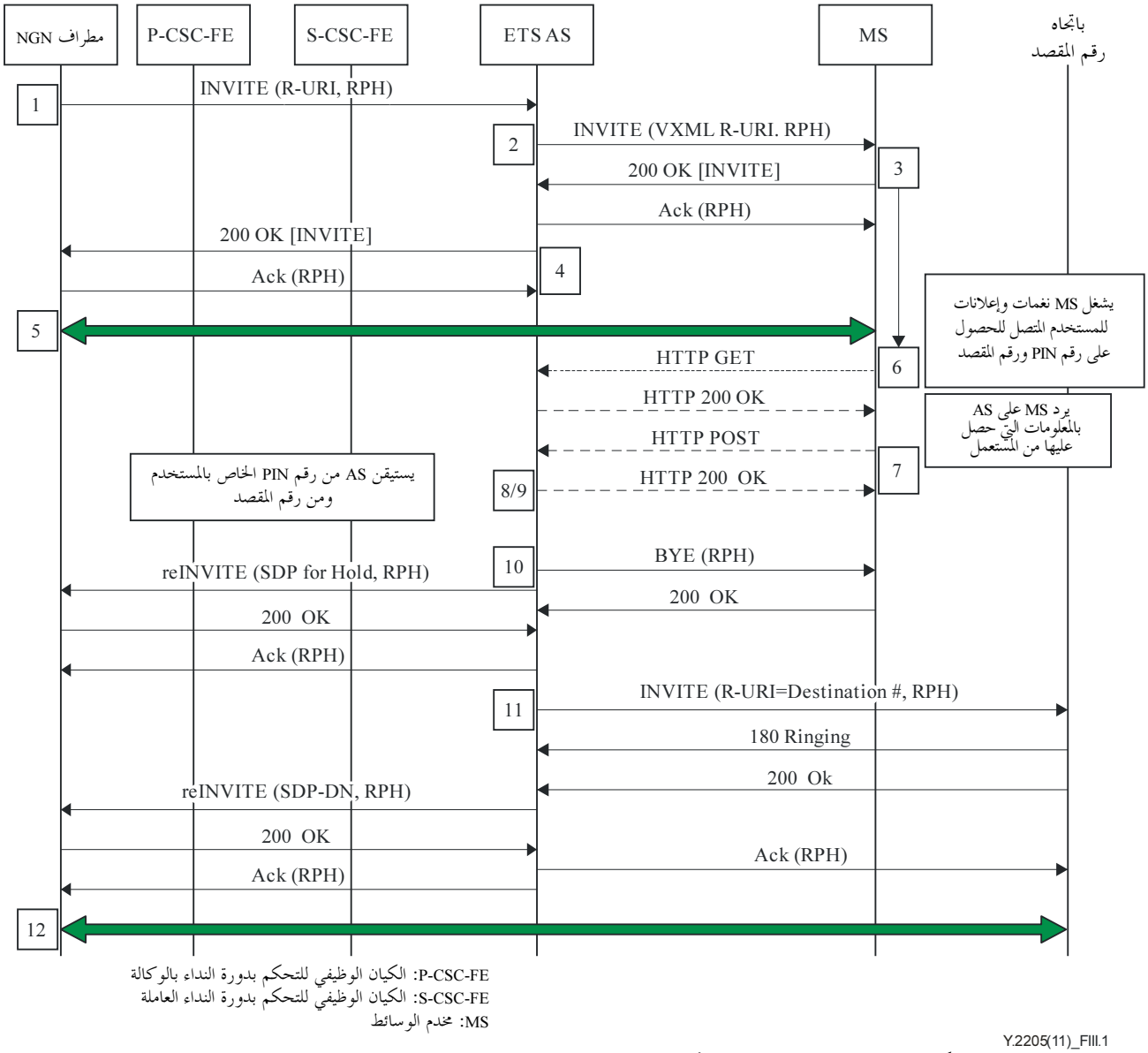
التذييل III

مثال عن تدفقات النداء/الدورة لخدمة اتصالات الطوارئ (ETS) في شبكات الجيل التالي (NGN)

(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

يوفر هذا التذييل مثالاً مأخوذاً من الإضافة 57 إلى سلسلة التوصيات ITU-T Q عن تدفق النداء أو الدورة في خدمة اتصالات الطوارئ (ETS) ويمكن تطبيقه على شبكات الجيل التالي. ويوضح تدفق النداء هذا إعداداً ناجحاً للنداء أو الدورة في خدمة اتصالات الطوارئ (ETS) حيث يستعمل الاستيقان من المستخدم والتخويل له رقم تعريف الهوية الشخصي (PIN).

ويوضح الشكل 1.III طريقة استيقان من مستخدم خدمة اتصالات الطوارئ (ETS) تستعمل رقم تعريف الهوية الشخصي (PIN) الذي يدخله المستخدم في شبكة بروتوكول إنترنت (IP). ويجمع مخدم الوسائط (MS) بين الكيان الوظيفي للتحكم في موارد الوسائط والكيان الوظيفي لمعالجة موارد الوسائط (MRC-FE/MRP-FE). وتتضمن طلبات بروتوكول استهلال الدورة (SIP) جميعها رأسية أولوية المورد (RPH) [IETF RFC 4412] لبيان معالجة الأولوية اللازمة.



Y.2205(11)_FIII.1

الشكل 1.III – إعداد النداء أو الدورة في خدمة اتصالات الطوارئ (ETS) باستيقان يستعمل رقم تعريف الهوية الشخصي (PIN)

1) يُسيَّر النداء/الدورة إلى مخدم تطبيق (AS) خدمة اتصالات الطوارئ (ETS) حيث تُستهل معالجة الاستيقان من المستخدم.

2) يرسل مخدم تطبيق خدمة اتصالات الطوارئ (ETS AS) رسالة دعوة (INVITE) إلى مخدم الوسائط (MS) المختار مشفوعة بعرض بروتوكول وصف الدورة (SDP) يرتبط بالمتصل. وتتضمن رسالة الدعوة عنوان موقع الموارد الموحد (URL) لنص XML الصوتي (VoiceXML) المخزن في مخدم تطبيق خدمة اتصالات الطوارئ. ويصف النص كيف ينبغي لمخدم الوسائط (MS) أن يتفاعل مع المتصل (ماهية الإعلان الواجب تشغيله، وكيفية جمع الأرقام، وعدد الأرقام الواجب جمعها، والمؤقتات بين الأرقام، وغير ذلك).

3) عند استلام رسالة الدعوة (INVITE)، على مخدم الوسائط (MS) بما يلي:

- يمكنه أو يرسل "100 يحاول" (100 Trying) إلى ETS AS؛
- يستخرج نص VoiceXML من ETS AS مباشرةً مستخدماً HTTP وURL في رسالة الدعوة (INVITE) (يرسل مخدم الوسائط (MS) رسالة جلب HTTP (HTTP GET) إلى ETS AS الذي يرد بنص VoiceXML مفاده HTTP 200 OK)؛
- ويتحقق من صحة النص؛
- ويصيغ رسالة 200 OK تحتوي على SDP الخاص به ويرسلها إلى ETS AS.

4) يرسل ETS AS رسالة 200 OK باتجاه الطرف المتصل (مطراف NGN) ويضمِّنها معلومات الدورة التي وردته من MS.

5) وفي هذه المرحلة، يتاح توصيل الوسائط ما بين MS والطرف المتصل.

6) عند استلام ACK ونص VXML في رسالة HTTP 200 OK، ينفذ MS نص VoiceXML. ويشغل نغمة ويجمع أرقام (PIN) التي يدخلها الطرف المتصل.

7) ثم يرسل MS الأرقام التي جمعها إلى ETS AS مباشرةً مستخدماً رسالة HTTP POST.

8) عند استلام الأرقام التي تم جمعها، يتحقق من صحة أرقام (PIN) الواردة.

- إذا كانت الأرقام التي وردت غير صالحة (من حيث عدد الأرقام الواردة أو الرقم الخطأ)، يقرر ETS AS لزوم إجراء المزيد من التفاعل مع المتصل. ويرد ETS AS على MS برسالة HTTP 200 OK مشفوعة بنص VoiceXML جديد. ويعطي ETS AS تعليمات بشأن معالجة التعامل النهائي.
- أما إذا كانت الأرقام التي وردت صالحة، يكلف ETS AS مخدم الوسائط (MS) بتشغيل إعلان لجمع الأرقام (رقم المقصد).

9) يقرر ETS AS أن أرقام المقصد التي أدخلها الطرف المتصل صالحة.

10) يحرر ETS AS مخدم الوسائط (MS) من النداء أو الدورة بتعليمة SIP BYE، ويرسل رسالة تكرار الدعوة (reINVITE) إلى الطرف المتصل مشفوعة ببروتوكول SDP لوضع الوسائط في حالة انتظار.

11) يرسل ETS AS رسالة دعوة (INVITE) إلى الطرف في المقصد. وعند استلام رسالة 200 OK (جواب)، يرسل ETS AS رسالة تكرار الدعوة (reINVITE) إلى الطرف المتصل مشفوعة ببروتوكول SDP المرتبط بالمقصد.

12) يُنشأ مسير الوسائط بين الطرف المتصل ورقم المقصد مع وجود مخدم تطبيق خدمة اتصالات الطوارئ (ETS AS) القائم بالاستيقان في مسير التحكم في النداء.

بيبليوغرافيا

[b-ITU-T Q-Sup.62] ITU-T Q-series Recommendations – Supplement 62 (2011), *Overview of the work of standards development organizations and other organizations on emergency telecommunications service*.

[b-UN Global Survey] United Nations/International Strategy for Disaster Reduction (2006), *Final Report on a "Global Survey of Early Warning Systems"*. <http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf>

[b-ATIS 1000010] ATIS-1000010.2006, *Support of Emergency Telecommunications Service (ETS) in IP Networks*.

[b-IEEE 802.11] IEEE Std 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.16] IEEE Std 802.16-2009, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems*.

[b-IEEE 802.16m] IEEE Std 802.16m-2011, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 3: Advanced Air Interface*.

[b-IEEE 802.1p] IEEE Std 802.1D-2004, *IEEE Standard for Local and metropolitan area networks; Media Access Control (MAC) Bridges*.

[b-3GPP TR 23.854] 3GPP TR 23.854 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancements for Multimedia Priority Service (Release 10)*.

[b-3GPP TS 22.153] 3GPP TS 22.153 (06/2008), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia priority service (Release 8)*.

[b-3GPP TS 23.203] 3GPP TS 23.203 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 10)*.

[b-3GPP TS 23.272] 3GPP TS 23.272 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2 (Release 10)*.

[b-3GPP TS 23.328] 3GPP TS 23.228 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 10)*.

[b-3GPP TS 23.401] 3GPP TS 23.401 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 10)*.

[b-3GPP TS 29.212] 3GPP TS 29.212, version 9 6.1 (2011-04), *Universal Mobile Telecommunications System (UMTS);* LTE; *Policy and Charging Control over Gx reference point (Release 9)*.

[b-3GPP TS 29.214] 3GPP TS 29.214 (in force), *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 10)*.

[b-3GPP TS 29.229] 3GPP TS 29.229, version 9.3.0 (2010-10), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS);*

LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 9).

[b-3GPP TS 29.329] 3GPP TS 29.329 v9.4.0 (2011-01), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (Release 9)*.

[b-3GPP2 S.R0117-0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements*.

[b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.

[b-IETF RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP) – Specific Event Notification*.

[b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*.

[b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP)*.

[b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony*.

[b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*.

[b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow*.

[b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol (SIP)*.

[b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams*.

[b-TM Forum GB917] TM Forum GB917 (in force), *SLA Management Handbook, Release 3.0*.

[b-WFM Stage 1-r1] WiMAX Forum – WFM-T31-122-R016v01 (2009), *Service Provider Working Group (SPWG) ETS Phase 1 Requirements for Release 1.6*.

[b-WFM Stage 1-r2] WiMAX Forum – WFM-T31-122-R020v01 (2009), *SPWG ETS Requirements, Release 2.0*.

[b-WFM Stage 2-a1] WiMAX Forum – WFM-T32-001-R016v01 (2010), *Network Architecture – Architecture Tenets, Reference Model and Reference Points, Base Specification, Release 1.6,) ETS Stage 2 Specification (Section 7.14)*.

[b-WFM Stage 3-a1] WiMAX Forum – WFM-T33-001-R016v01 (2010), *Network Architecture – Detailed Protocols and Procedures, Base Specification, Release 1.6, ETS Stage 3 Specification (Section 4.19)*.

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	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
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، 2012