الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

# ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

# Y. 1314

(2005/10)

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

خصائص بروتوكول الإنترنت – النقل

# تفكيك وظائف الشبكة الخاصة التقديرية

التوصيـــة ITU-T Y.1314

ITU-T

## البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

| | |
|---|---|
| **البنية التحتية العالمية للمعلومات** | |
| اعتبارات عامة | Y.199 – Y.100 |
| الخدمات والتطبيقات، والبرمجيات الوسيطة | Y.299 – Y.200 |
| الجوانب الخاصة بالشبكات | Y.399 – Y.300 |
| السطوح البينية والبروتوكولات | Y.499 – Y.400 |
| الترقيم والعنونة والتسمية | Y.599 – Y.500 |
| الإدارة والتشغيل والصيانة | Y.699 – Y.600 |
| الأمن | Y.799 – Y.700 |
| مستويات الأداء | Y.899 – Y.800 |
| **جوانب متعلقة ببروتوكول الإنترنت** | |
| اعتبارات عامة | Y.1099 – Y.1000 |
| الخدمات والتطبيقات | Y.1199 – Y.1100 |
| المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد | Y.1299 – Y.1200 |
| **النقل** | **Y.1399 – Y.1300** |
| التشغيل البيني | Y.1499 – Y.1400 |
| 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 |
| **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 والشبكات | Y.2299 – Y.2250 |
| الترقيم والتسمية والعنونة | Y.2399 – Y.2300 |
| إدارة الشبكة | Y.2499 – Y.2400 |
| معمارية الشبكة وبروتوكولات التحكم في الشبكة | Y.2599 – Y.2500 |
| الأمن | Y.2799 – Y.2700 |
| التنقلية المعممة | Y.2899 – Y.2800 |

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

**التوصيـــة ITU-T Y.1314**

# البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل الثاني


## ملخص

تصف هذه التوصية مجموعة الوظائف اللازمة لإنشاء وتشغيل وصيانة شبكات العميل/المخدم الخاصة التقديرية والشبكات الخاصة التقديرية لمستوى القرين (VPN). ويوصَف العنصر الوظيفي للشبكة انطلاقاً من وجهة نظر مستوى الشبكة، مع مراعاة كل من بنية الشبكة (VPN) المكونة من طبقات والمعلومات المميزة للعميل وحالات تصاحب العميل/المخدم وطوبولوجيا الترابط الشبكي والعنصر الوظيفي لشبكة الطبقة.

وتُوصف النماذج الوظيفية بتطبيق منهجية النمذجة التي يرد وصف لها في التوصيتين G.805 وG.809 الصادرتين عن قطاع تقييس الاتصالات في الاتحاد (ITU-T). ومنهجية النمذجة المُستعملة مستقلة عن تكنولوجيا الشبكة المُشغلة، ولذلك تنطبق النماذج الوظيفية والوظائف المصاحبة الموصوفة على جميع تكنولوجيات شبكة الطبقة VPN.



## المصدر

وافقت لجنة الدراسات 13 (2005-2008) التابعة لقطاع تقييس الاتصالات في الاتحاد (ITU-T) بتاريخ 14 أكتوبر 2005 على التوصية ITU-T Y.1314 بموجب الإجراء المحدد في التوصية ITU-T A.8.

## تمهيد

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).

## ملاحظة

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

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

## حقوق الملكية الفكرية

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

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

© ITU 2006

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

## المحتويات

**الصفحة**


1 مجال التطبيق ..... 1

2 المراجع ..... 1

3 التعاريف ..... 1

4 الصيغ المقتضبة والمختصرات..... 3

5 الشبكات الخاصة التقديرية (VPN) العميل/المخدم ..... 7

1.5 التوليفات الممكنة بين العميل والمخدم ..... 8

2.5 شفافية طبقة العميل VPN ..... 9

6 شبكات VPN لمستوى القرين..... 10

1.6 ترشيح الرزم/الطرق ..... 11

2.6 التجفير ..... 11

3.6 شبكات المنطقة المحلية التقديرية (VLAN) إثرنت ..... 12

7 المعمارية الوظيفية لشبكات VPN ..... 13

1.7 شبكات طبقة VPN الموجهة التوصيل..... 14

2.7 شبكات طبقة VPN عديمة التوصيل..... 14

3.7 العلاقات القائمة بين طبقات العميل/المخدم VPN..... 15

4.7 طبقات العميل VPN المتعددة..... 20

5.7 طبقات المخدم VPN المتعددة..... 22

6.7 نمذجة الشبكة VPN باستعمال التجزئة..... 24

7.7 طبقة القرين VPN..... 25

8 دعم طوبولوجيا الشبكة VPN ..... 27

1.8 طوبولوجيات VPN المتشابكة كلياً ..... 28

2.8 طوبولوجيات VPN المتشابكة جزئياً ..... 28

3.8 طوبولوجيات VPN المركز والفروع (شكل النجمة) ..... 29

9 اعتبارات بشأن نوعية خدمة (QoS) الشبكة VPN ..... 29

1.9 شبكات طبقة تبديل الدارات ..... 30

2.9 شبكات طبقة تبديل الرزم..... 30

**الصفحة**


10 الوظائف المطلوبة لإنشاء شبكات VPN العميل/المخدم ..... 32
1.10 إنشاء طبقة المخدم VPN ..... 32
2.10 التحقق من طبقة العميل VPN وتشكيلها ..... 38
3.10 تسيير طبقة العميل VPN وتشويرها ..... 40
11 الوظائف المطلوبة لإنشاء شبكات VPN لمستوى القرين ..... 43
1.11 اكتشاف عضوية الشبكة VPN ..... 43
2.11 استيقان وتخويل ومحاسبة (AAA) حافة المشترك CE/المستعمل ..... 43
3.11 تسيير طبقة القرين VPN ..... 44
4.11 تشكيل عناصر شبكة طبقة القرين VPN ..... 44
12 وظائف تشغيل وإدارة وصيانة (OAM) شبكات VPN ..... 44
1.12 إدارة الأعطاب ..... 45
2.12 إدارة الأداء ..... 47
3.12 تنشيط/إخماد التشغيل والإدارة والصيانة OAM ..... 47
4.12 العيوب المتصلة بكل أسلوب من أساليب الشبكة ..... 48
13 التقارب الوظيفي وسيناريوهات الخدمة ..... 50
1.13 سيناريوهات خدمات VPN العميل/المخدم ..... 50
2.13 سيناريوهات شبكات VPN لمستوى القرين ..... 50
14 اعتبارات بشأن أمن الشبكة VPN ..... 50
التذييل I تحديد موقع نقطة انتهاء التوصيل TCP/نقطة انتهاء التدفق TFP لطبقة العميل VPN ..... 51
التذييل II شبكات VPN العميل/المخدم الحاوية على عدة طبقات مخدم VPN ..... 54
التذييل III أمثلة على سيناريوهات خدمة VPN العميل/المخدم وخدمة VPN لمستوى القرين ..... 56
ببليوغرافيا ..... 59

# تفكيك وظائف الشبكة الخاصة التقديرية

## 1 مجال التطبيق

تصف هذه التوصية مجموعة الوظائف اللازمة لإنشاء وتشغيل وصيانة شبكات العميل/المخدم الخاصة التقديرية والشبكات الخاصة التقديرية لمستوى القرين (VPN). ويُوصَف العنصر الوظيفي للشبكة انطلاقاً من وجهة نظر مستوى الشبكة، مع مراعاة كل من بنية الشبكة VPN المكونة من طبقات والمعلومات المميزة للعميل وحالات تصاحب العميل/المخدم وطوبولوجيا الترابط الشبكي والعنصر الوظيفي لشبكة الطبقة. وتُوصف النماذج الوظيفية بتطبيق منهجية النمذجة المستقلة عن تكنولوجيا الشبكة التي يرد وصف لها في التوصيتين G.805 وG.809 الصادرتين عن قطاع تقييس الاتصالات في الاتحاد (ITU-T).

## 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، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

- التوصية ITU-T G.805 (2000)، *المعمارية الوظيفية النوعية لشبكات النقل*.
- التوصية ITU-T G.809 (2003)، *المعمارية الوظيفية لشبكات الطبقة عديمة التوصيل*.
- التوصية ITU-T Y.1306/G.8010 (2004)، *معمارية شبكات طبقة إثرنت*.
- التوصية ITU-T Y.1311 (2002)، *الشبكات الخاصة التقديرية (VPN) القائمة على الشبكة- المعمارية النوعية ومتطلبات الخدمة*.

## 3 التعاريف

تستعمل هذه التوصية المصطلحات الواردة أدناه والمعرفة في التوصية ITU-T G.805، وهي:

1.3 نقطة نفاذ *(access point)*

2.3 زمرة نفاذ *(access group)*

3.3 معلومات مكيفة *(adapted information)*

4.3 معلومات مميزة *(characteristic information)*

5.3 علاقة العميل/العميل *(client/server relationship)*

6.3 توصيل *(connection)*

7.3 نقطة توصيل *(connection point)*

8.3 شبكة طبقة *(layer network)*

9.3 وصلة *(link)*

10.3 توصيل وصلة *(link connection)*

11.3 مصفوفة *(matrix)*

12.3 شبكة *(network)*

13.3 توصيل شبكة *(network connection)*

14.3 منفذ *(port)*

15.3 نقطة مرجعية *(reference point)*

16.3 شبكة فرعية *(subnetwork)*

17.3 توصيل شبكة فرعية *(subnetwork connection)*

18.3 نقطة انتهاء التوصيل *(termination connection point)*

19.3 قناة *(trail)*

20.3 انتهاء القناة *(trail termination)*

21.3 نقل *(transport)*

22.3 كيان نقل *(transport entity)*

23.3 وظيفة معالجة النقل *(transport processing function)*

24.3 توصل أحادي الاتجاه *(unidirectional connection)*

25.3 قناة أحادية الاتجاه *(unidirectional trail)*

وتستعمل هذه التوصية المصطلحات الواردة أدناه والمعرفة في التوصية ITU-T G.809 وهي:

26.3 نقطة نفاذ *(access point)*

27.3 زمرة نفاذ *(access group)*

28.3 معلومات مكيفة *(adapted information)*

29.3 معلومات مميزة *(characteristic information)*

30.3 علاقة العميل/المخدم *(client/server relationship)*

31.3 قناة عديمة التوصيل *(connectionless trail)*

32.3 تدفق *(flow)*

33.3 مجال التدفق *(flow domain)*

34.3 تدفق مجال التدفق *(flow domain flow)*

35.3 نقطة تدفق *(flow point)*

36.3 مجموعة نقاط التدفق *(flow point pool)*

37.3 انتهاء التدفق *(flow termination)*

38.3 بئر انتهاء التدفق *(flow termination sink)*

39.3 مصدر انتهاء التدفق *(flow termination source)*

40.3 شبكة طبقة *(layer network)*

41.3 تدفق وصلة *(link flow)*

42.3 شبكة *(network)*

43.3 تدفق شبكة *(network flow)*

44.3 منفذ *(port)*

45.3 نقطة مرجعية *(reference point)*

46.3 وحدة حركة *(traffic unit)*

47.3 نقل *(transport)*

48.3 كيان نقل *(transport entity)*

49.3 وظيفة معالجة النقل *(transport processing function)*

50.3 نقطة انتهاء التدفق *(termination flow point)*

وتستعمل هذه التوصية المصطلح الوارد أدناه والمعرف في التوصية ITU-T Y.1306/G.8010، وهو:

51.3 قطعة مجال التدفق *(flow domain fragment)*

وتستعمل هذه التوصية المصطلحات الواردة أدناه والمعرفة في التوصية ITU-T Y.1311، وهي:

52.3 شبكة VPN الطبقة 1

53.3 شبكة VPN الطبقة 2

54.3 شبكة VPN الطبقة 3

وتعرف هذه التوصية المصطلحات التالية:

**55.3 شبكة طبقة العميل VPN** *(VPN client layer network)*: مكون طوبولوجي في شبكة VPN العميل/المخدم يمثل مجموعة نقاط النفاذ المتشابهة النمط والمتصاحبة لغرض نقل المعلومات المميزة لطبقة العميل VPN.

**56.3 شبكة طبقة المخدم VPN** *(VPN server layer network)*: مكون طوبولوجي في شبكة VPN العميل/المخدم يمثل مجموعة نقاط النفاذ المتشابهة النمط والمتصاحبة لغرض نقل المعلومات المُكيفة لطبقة العميل VPN.

**57.3 شبكة طبقة القرين VPN** *(VPN peer layer network)*: مكون طوبولوجي يمثل مجموعة نقاط النفاذ المتشابهة النمط والمتصاحبة لغرض نقل المعلومات المميزة لطبقة القرين VPN.

## 4 الصيغ المقتضبة والمختصرات

تستعمل هذه التوصية الصيغ المقتضبة والمختصرات التالية:

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

AAL طبقة تكييف بأسلوب نقل غير متزامن (ATM) *(ATM Adaptation Layer)*

AG زمرة نفاذ *(Access Group)*

AI معلومات مكيفة *(Adapted Information)*

AIS إشارة دلالة إنذار *(Alarm Indication Signal)*

AP نقطة نفاذ *(Access Point)*

ASON شبكة بصرية مبدلة أوتوماتياً *(Automatically Switched Optical Network)*

ATM أسلوب نقل غير متزامن *(Asynchronous Transfer Mode)*

BFD كشف أمامي ثنائي الاتجاه *(Bidirectional Forwarding Detection)*

BGP بروتوكول بوابة الحدود *(Border Gateway Protocol)*

CAC تحكم في قبول التوصيلات *(Connection Admission Control)*

CBR معدل بتات ثابت *(Constant Bit Rate)*

CC التحقق من التوصيلية *(Connectivity Check)*

CE حافة المشترك *(Customer Edge)*

CI معلومات مميزة *(Characteristic Information)*

CL-PS تبديل الرزم عديمة التوصيل *(Connectionless Packet-Switched)*

CO-CS تبديل دارة موجهة التوصيل *(Connection-Orientated Circuit-Switched)*

CO-PS تبديل رزمة موجهة التوصيل *(Connection-Orientated Packet-Switched)*

CP نقطة توصيل *(Connection point)*

CV تحقق من التوصيلية *(Connectivity Verification)*

DHCP بروتوكول دينامي لتشكيل المخدم *(Dynamic Host Configuration Protocol)*

DLCI معرف توصيل وصلة البيانات *(Data Link Connection Identifier)*

DSCP نقطة شفرة الخدمات التفاضلية *(Differentiated Services Code Point)*

DWDM تعدد إرسال بتقسيم الموجات الكثيفة *(Dense Wave Division Multiplexing)*

EBGP بروتوكول بوابة الحد الخارجي *(External Border Gateway Protocol)*

E-LMI سطح بيني LMI خارجي *(External LMI)*

ES نظام طرفي *(End System)*

FDF تدفق مجال التدفق *(Flow Domain Flow)*

FDFr قطعة مجال التدفق *(Flow Domain Fragment)*

FDI دلالة عطب في الاتجاه الأمامي *(Forward Defect Indication)*

FP نقطة تدفق *(Flow Point)*

FPP مجموعة نقاط التدفق *(Flow Point Pool)*

FR مرحل أرتال *(Frame Relay)*

FT انتهاء تدفق *(Flow Termination)*

FTP نقطة انتهاء التدفق *(Flow Termination Point)*

GRE تغليف التسيير النوعي *(Generic Routing Encapsulation)*

IGP بروتوكول البوابة الداخلية *(Interior Gateway Protocol)*

IKE تبادل مفاتيح الإنترنت *(Internet Key Exchange)*

IPv4 الصيغة 4 من بروتوكول الإنترنت *(Internet Protocol Version 4)*

IPv6 الصيغة 6 من بروتوكول الإنترنت *(Internet Protocol Version 6)*

ISIS نظام وسيط إلى نظام وسيط *(Intermediate System to Intermediate System)*

L2TP بروتوكول التمرير في نفق الطبقة 2 *(Layer 2 Tunnelling Protocol)*

LDP بروتوكول توزيع الوسم *(Label Distribution Protocol)*

LF تدفق الوصلة *(Link Flow)*

LMI سطح بيني للإدارة المحلية *(Local Management Interface)*

LOC تحكم في النفاذ إلى الوسائط *(Loss Of Continuity)*

LOS من عدة نقاط إلى نقطة *(Loss Of Signal)*

LSP مسير تبديل الوسم *(Label Switched Path)*

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

MP2P من عدة نقاط إلى نقطة *(Multipoint-to-Point)*

MP-BGP بروتوكول BGP المتعدد البروتوكولات *(Multi-Protocol BGP)*

MPLS تبديل متعدد البروتوكولات بالتوسيم *(Multi-Protocol Label Switching)*

MTU وحدة نقل قصوى *(Maximum Transmission Unit)*

NE كيان شبكة *(Network Entity)*

NF تدفق الشبكة *(Network Flow)*

NMS نظام إدارة الشبكة *(Network Management System)*

NSAP نقطة نفاذ إلى خدمة الإنترنت *(Network Service Access Point)*

OAM التشغيل والإدارة والصيانة *(Operations, Administration and Maintenance)*

OOB خارج النطاق *(Out Of Band)*

OSI التوصيل البيني للأنظمة المفتوحة *(Open Systems Interconnection)*

OSPF أول أقصر مسير مفتوح *(Open Shortest Path First)*

OSS نظام الدعم التشغيلي *(Operational Support System)*

P مورد (عقدة) *((Provider (Node))*

P2P نقطة إلى نقطة *(Point-to-Point)*

P2MP نقطة إلى عدة نقاط *(Point-to-Multipoint)*

PCR معدل خلايا الذروة *(Peak Cell Rate)*

PE حافة المورد *(Provider Edge)*

PM مراقبة الأداء *(Performance Monitoring)*

PNNI سطح بيني من شبكة خاصة إلى أخرى *(Private Network-to-Network Interface)*

PHP كبت القفزة قبل الأخيرة *(Penultimate Hop Popping)*

PM مراقبة الأداء *(Performance Monitoring)*

PW سلك زائف *(Pseudo Wire)*

QoS نوعية الخدمة *(Quality of Service)*

RADIUS خدمة الاستيقان عن بعد لمستعمل المراقمة الداخلية *(Remote Authentication Dial In User Service)*

RIP بروتوكول معلومات التسيير *(Routing Information Protocol)*

RPR حلقة رزمة مرنة *(Resilient Packet Ring)*

RMON مراقبة عن بعد *(Remote MONitoring)*

RSVP-TE بروتوكول حجز الموارد بهندسة الحركة (تمديدات)
*(Resource ReserVation Protocol (with) Traffic) Engineering (extensions)*

SCR معدل خلايا مُستدام *(Sustained Cell Rate)*

SDH تراتب رقمي متزامن *(Synchronous Digital Hierarchy)*

SES ثانية شديدة الخطأ *(Severely Errored Second)*

SLA اتفاق مستوى الخدمة *(Service Level Agreement)*

SNC توصيل شبكة فرعية *(SubNetwork Connection)*

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

SONET شبكة بصرية متزامنة *(Synchronous Optical NETwork)*

SPVC دارة تقديرية دائمة التبديل *(Switched Permanent Virtual Circuit)*

SSL طبقة مقبس آمن *(Secure Socket Layer)*

STP بروتوكول شجرة ممتدة *(Spanning Tree Protocol)*

SVC دارة تقديرية دائمة التبديل *(Switched Virtual Circuit)*

TCP نقطة انتهاء التوصيل *(Termination Connection Point)*

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

TFP نقطة انتهاء التدفق *(Termination Flow Point)*

TTL زمن الحياة *(Time-To-Live)*

TTSI معرف مصدر انتهاء القناة *(Trail Termination Source Identifier)*

UNI سطح بيني من المستعمل إلى الشبكة *(User-to-Network Interface)*

VC دارة/قناة تقديرية *(Virtual Circuit/Channel)*

VCCV تحقق من توصيلية الدارة التقديرية *(Virtual Circuit Connectivity Verification)*

VCI معرف القناة التقديرية *(Virtual Channel Identifier)*

VLAN شبكة المنقطة المحلية التقديرية *(Virtual Local Area Network)*

VPI معرف هوية المسير التقديري *(Virtual Path Identifier)*

VPN شبكة خاصة تقديرية *(Virtual Private Network)*

WDM تعدد إرسال بتقاسم طول الموجات *(Wavelength Division Multiplexing)*

## 5 الشبكات الخاصة التقديرية (VPN) العميل/المخدم

هذه الشبكات ذات تراتب مكون من طبقتين تُستعمل فيه شبكة طبقة المخدم VPN لتدعيم شبكة واحدة أو أكثر من شبكات طبقة العميل VPN.

وتصف التوصية ITU-T Y.1311 شبكات VPN العميل/المخدم على أساس أنماط خدمة VPN وأنماط نقل VPN، حيث يشير فيها تعبير نمط خدمة VPN إلى طبقة العميل VPN بينما يشير فيها التعبير نمط النقل VPN إلى طبقة المخدم VPN. وتصنف التوصية المذكورة مختلف أنماط خدمة ونقل VPN (العميل والمخدم) على غرار الوصف الوارد في الجدول 5-1 أدناه.

**الجدول Y.1314/1-5 – أنماط الخدمة المُحددة في التوصية Y.1311**

| نمط الخدمة | الوصف |
|---|---|
| الطبقة 1 | تقدم خدمة طبقة مادية بين مواقع المشترك التابعة لنفس شبكة VPN. ويمكن استعمال التوصيلات بالاستناد إلى منافذ مادية معينة، أو أطوال موجات بصرية، أو إلى دارات/قنوات تقديرية (VC) بتراتب رقمي متزامن (SDH)/ بشبكة بصرية متزامنة (SONET)، أو قنوات تردد، أو إلى حصص زمنية. |
| الطبقة 2 | تقدم خدمة طبقة وصلة بيانات بين عُقد المشترك التابعة لنفس شبكة VPN. ويستند إرسال رزم بيانات المستعمل إلى المعلومات الواردة في رأسيات طبقة وصلة بيانات الرزم (كعناوين معرف توصيل وصلة البيانات (DLCI)، أو عناوين معرف هوية القناة التقديرية (VCI)/معرف المسير التقديري (VPI) بأسلوب نقل غير متزامن (ATM)، أو عناوين التحكم في النفاذ إلى الوسائط (MAC)). |
| الطبقة 3 | تقدم خدمة طبقة شبكة معينة بين عُقد المشترك التابعة لنفس شبكة VPN. ويستند إرسال رزم بيانات المستعمل إلى المعلومات الواردة في رأسية الطبقة 3 (مثل عنوان مقصد الصيغة 4 من بروتوكول الإنترنت (IPv4) أو الصيغة 6 من بروتوكول الإنترنت (IPv6). |

وتنطوي طريقة التصنيف المُستعملة في التوصية ITU-T Y.1311 على عيب يتمثل في عدم صلاحية التبديل المتعدد البروتوكولات بالتوسيم (MPLS) لأي واحدة من هذه الفئات المُصنفة، ولذلك يجب معالجتها بوصفها تكنولوجيا شبكة طبقة وحيدة. وثمة عيب آخر هو إمكانية اختلاف خصائص ومتطلبات تكنولوجيات الشبكة التي تندرج ضمن نطاق نفس الطبقة اختلافاً كبيراً من وجهة النظر الوظيفية، فإثرنت وأسلوب النقل غير المتزامن (ATM) مثلاً تكنولوجيتان من تكنولوجيات الطبقة 2 على حد سواء؛ غير أن إثرنت تكنولوجيا عديمة التوصيل قائمة على الإذاعة، في حين أن الأسلوب ATM هو تكنولوجيا توصيل غير إذاعية.

وهناك طريقة بديلة لتصنيف تكنولوجيات الشبكة، وهي تصنيفها بحسب أسلوب الشبكة الذي تنتمي إليه التكنولوجيات. ويمكن مقابلة جميع هذه التكنولوجيات بواحد من الأساليب الثلاثة التالية: رزمة مبدلة عديمة التوصيل (CL-PS)، ورزمة مبدلة

بأسلوب التوصيل (CO-PS)، ودارة مبدلة بأسلوب التوصيل (CO-CS). وتختلف المتطلبات الوظيفية لكل أسلوب من هذه الأساليب لأن لكل أسلوب خصائص مختلفة. ويبين الجدول 5-2 أدناه أمثلة على تكنولوجيات طبقة الشبكة VPN والأسلوب الذي تنتمي إليه.

**الجدول Y.1314/2-5 – أساليب تشغيل الشبكات وأمثلة عليها**

| أسلوب التشغيل | أمثلة |
|---|---|
| تبديل الرزم عديمة التوصيل | بروتوكول الإنترنت (IP)، إثرنت، تبديل متعدد البروتوكولات بالتوسيم من عدة نقاط إلى نقطة (MPLS MP2P) (الملاحظة 1) |
| تبديل رزمة موجهة التوصيل | مرحل أرتال، تبديل متعدد البروتوكولات بالتوسيم من نقطة إلى نقطة/من نقطة إلى عدة نقاط (MPLS P2P/ P2MP) (الملاحظة 2)، أسلوب نقل غير متزامن (ATM) |
| تبديل دارة موجهة التوصيل | تراتب رقمي متزامن (SDH)/شبكة بصرية متزامنة (SONET)، تعدد إرسال بتقسيم الزمن (TDM) |
| **الملاحظة 1** – يتم إنشاء المسيرات المُبدلة بالتوسيم (LSP) بتبديل متعدد البروتوكولات بالتوسيم من عدة نقاط إلى نقطة (MPLS MP2P)، باستعمال بروتوكول توزيع بالتوسيم (LDP) بتطبيق أسلوب تحكم هابط غير مطلوب، يتجاوز مباشرةً أقران البروتوكول LDP المتجاور. | |
| **الملاحظة 2** – يتم إنشاء المسيرات المُبدلة بالتوسيم (LSP) بتبديل متعدد البروتوكولات بالتوسيم من نقطة إلى نقطة (MPLS P2P) أو من نقطة إلى عدة نقاط (P2MP)، باستعمال بروتوكول حجز الموارد بهندسة الحركة (RSVP-TE) الذي يجتاز أقران البروتوكول RSVP-TE، أو يتم إنشاء المسيرات LSP من نقطة إلى نقطة باستعمال البروتوكول LDP المُستهدف/المُوجه بين أقران البروتوكول LDP غير المتجاور. | |

## 1.5 التوليفات الممكنة بين العميل والمخدم

يوجد تسع توليفات ممكنة بين العميل والمخدم تستند إلى أساليب الشبكة الثلاثة المذكورة، ومع ذلك، فإن بعض هذه التوليفات أكثر تواؤماً من غيرها. ويصف الجدول 5-3 التوليفات الممكنة ويقدم بعض المعلومات عن تواؤمها.

وينبغي أن يكون بمقدور شبكة طبقة المخدم VPN أن تحقق تعدد الإرسال/إزالة تعدد الإرسال لتؤمن فصل مستوي البيانات بين العديد من طبقات العميل VPN، كما ينبغي أن يكون بمقدور الطبقات المذكورة أن تطبق حالات تكييف حركة العميل، والتي تخص العميل/المخدم حصراً وتعتمد على أساليب تشغيل شبكة طبقة العميل والمخدم وعلى التكنولوجيات المُستعملة فيها تحديداً. وثمة شرط مهم للتكييف يتعلق بعملاء شبكة VPN المبدلة الدارات تنفذه طبقة مخدم شبكة VPN المبدلة الدارات، يتمثل في ضرورة أن تؤمن وظيفة التكييف فك اقتران المعدلات (أي، الملء في حالة الراحة) وتعيين حدود رزم طبقة العميل VPN. وهناك شرط أساسي يتعلق بالحالات التي يكون فيها العميل/المخدم على حد سواء برزم مبدلة (بأسلوب التوصيل أو عديمة التوصيل)، والمتمثل في ضرورة أن تؤمن وظيفة التكييف التقطيع والتتابع إذا كانت وحدة حركة طبقة المخدم VPN (أي، رزم وحدات النقل القصوى (MTU)) أصغر من وحدة حركة طبقة العميل VPN. وتشتمل وظائف التكييف الأخرى التي قد تكون ضرورية اعتماداً على تكنولوجيات العميل/المخدم VPN المُستعملة تحديداً، على ما يلي: التشفير، وتكييف المعدل، والتراصف.

**الجدول Y.1314/3-5 – توليفات العميل/المخدم القائمة على أسلوب تشغيل الشبكة**

| | طبقة العميل CL-PS VPN | طبقة العميل CO-PS VPN | طبقة العميل CO-CS VPN |
|---|---|---|---|
| طبقة المخدم CL-PS VPN | – مثالية، رغم أن تقديم ضمانات بشأن كل تسليم تدفق يطرح تحديات تتعلق بالقياس<br>– اللجوء إلى الإفراط في توفير الخدمات والاصطفاف الانتظاري للأولويات على أساس الأصناف (لإدارة الحركة والازدحام اللذين يتسمان بطابع رشقي من أي طرف إلى أي طرف) هو نهج عام لا يقدم ضمانات بشأن كل تسليم تدفق<br>*مثال: طبقة مخدم إثرنت تدعم طبقة عميل ببروتوكول الإنترنت (IP)* | – تقديم ضمانات بشأن كل تسليم تدفق يطرح تحديات تتعلق بالقياس<br>– اللجوء إلى الإفراط في توفير الخدمات والاصطفاف الانتظاري للأولويات على أساس الأصناف هو نهج عام لا يقدم ضمانات بشأن كل تسليم تدفق<br>– يجب أن تكون طبقة العميل VPN قادرة على الاستعادة من وحدات الحركة الخارجة عن التتابع (بسبب احتمال إعادة ترتيب رزم طبقة المخدم)<br>*مثال: طبقة مخدم ببروتوكول الإنترنت (IP) تدعم طبقة عميل بأسلوب ATM* | – تقديم ضمانات لكل تسليم تدفق يطرح تحديات تتعلق بالقياس<br>– اللجوء إلى الإفراط في توفير الخدمات والاصطفاف الانتظاري للأولويات على أساس الأصناف هو نهج عام لا يقدم ضمانات بشأن كل تسليم تدفق<br>– استعادة توقيت الميقاتية أمر ينطوي على تحديات تقنية<br>– يجب أن تكون طبقة العميل VPN قادرة على الاستعادة من وحدات الحركة الخارجة عن التتابع<br>*مثال: طبقة مخدم ببروتوكول الإنترنت (IP) تدعم طبقة عميل بتعدد الإرسال TDM* |
| طبقة المخدم CO-PS VPN | – التكاليف المترتبة على صيانة حالة التوصيل بين شبكات VPN عند الطلب بفترات استبقاء قصيرة، كالدارت التقديرية الدائمة التبديل (SPVC)<br>*مثال: طبقة مخدم بأسلوب ATM تدعم طبقة عميل ببروتوكول الإنترنت (IP)* | – مثالية<br>*مثال: طبقة مخدم بتبديل متعدد البروتوكولات بالتوسيم من نقطة إلى نقطة (P2P MPLS) تدعم طبقة عميل بأسلوب ATM* | – استعادة توقيت الميقاتية أمر ينطوي على تحديات تقنية<br>*مثال: طبقة مخدم بأسلوب ATM تدعم طبقة عميل بتعدد الإرسال TDM* |
| طبقة المخدم CO-CS VPN | – لا يوجد تعدد إرسال إحصائي بين حواصل الجمع<br>– يزداد عرض النطاق المخصص باستمرار أثناء التنفيذ مما يؤدي إلى إساءة استعمال الشبكة<br>– بطء أوقات الاستجابة لإنشاء التوصيل بين شبكات VPN عند الطلب بفترات استبقاء قصيرة<br>*مثال: طبقة مخدم بتراتب SDH تدعم طبقة عميل إثرنت* | – لا يوجد تعدد إرسال إحصائي بين حواصل الجمع<br>– يزداد عرض النطاق المخصص باستمرار أثناء التنفيذ مما يؤدي إلى إساءة استعمال الشبكة<br>– بطء أوقات الاستجابة لإنشاء التوصيل فيما بين شبكات VPN عند الطلب بفترات استبقاء قصيرة<br>*مثال: طبقة مخدم بأسلوب ATM تدعم طبقة عميل بتعدد الإرسال TDM* | – مثالية<br>*مثال: طبقة مخدم بصري (مثل قناة بتعدد الإرسال DWDM) تدعم طبقة عميل بتراتب SDH/شبكة SONET* |

## 2.5 شفافية طبقة العميل VPN

المكونات الوظيفية لأي شبكة VPN من شبكات العميل/المخدم (كالتسيير، والتشوير، والتشغيل والإدارة والصيانة (OAM)، والإدارة، وما إلى ذلك) المنتمية إلى شبكة طبقة العميل VPN، هي مكونات ينبغي أن تكون مستقلة تماماً عن المكونات الوظيفية لشبكة طبقة المخدم VPN.

ورغم إمكانية إيجاد حلول تتعلق بشبكة VPN العميل/المخدم تتمكن بموجبها المكونات الوظيفية لشبكة طبقة المخدم VPN من التفاعل مع المكونات الوظيفية لشبكة طبقة العميل VPN، فإن إتباع هذا النهج يؤدي إلى عدد من التبعات غير المرغوبة من قبيل ما يلي:

1) قد تنقطع خدمة VPN إذا غَير المشترك أي مكون من المكونات الوظيفية لطبقة العميل VPN.

2) من الضروري أن يتابع مورد خدمة VPN التطورات على تكنولوجيا طبقة العميل VPN الخاصة بالمشترك ويدخل تحسينات على شبكته بناء على ذلك.

3) من الصعب إنشاء التوصيل في حالات العطل إذا أصاب العطل شبكة طبقة العميل VPN أو شبكة طبقة المخدم VPN.

واشتراط توفر إمكانية تشغيل شبكة طبقة العميلVPN بشكل منفصل عن شبكة طبقة المخدم VPN هو أمر ينطوي بطبيعة الحال على ضرورة توخي طبقة المخدم VPN الشفافية في نقل طبقة العميل VPN. فإذا كانت مثلاً شبكة طبقة العميل VPN بأسلوب نقل غير متزامن (ATM)، فإن بإمكان هذه الشبكة تنفيذ سمة تسجيل الملكية (مثل الطبقة AAL، والتسيير والتشوير بدون سطح بيني من شبكة خاصة إلى أخرى (PNNI)، والتشغيل والإدارة والصيانة (OAM))، وفي حال عدم تنفيذ السمة بشفافية، فإن ذلك يؤدي إلى انقطاع خدمة VPN.

ولا يعد شرط الشفافية في نقل طبقة العميل شرطاً تقنياً فحسب، بل ينطوي أيضاً على آثار تجارية لأن من المحتمل أن ينظر مورد خدمة VPN في تفاصيل شبكته التي يتعين أن تكون سريعة التأثر بظروف السوق، وعليه يرغب المورد في إخفاء هذه التفاصيل عن جميع شبكات طبقة العميل VPN. فمثلاً، لا يُحبَّذ أن تكون شبكة طبقة المخدم VPN نظيراً لتسيير وتشوير طبقة العميل VPN المذكورة في المثال أعلاه.

## 6 شبكات VPN لمستوى القرين

يستند وصف طوبولوجيات شبكة VPN الوارد في الفقرة 5 إلى علاقة العميل والمخدم القائمة بين طبقة العميل VPN وطبقة المخدم VPN. وتعمل وظيفة تكييف مصدر طبقة المخدم VPN في مثال VPN العميل/المخدم على تكييف المعلومات المميزة (CI) لطبقة العميل VPN لتصبح معلومات مكيفة (AI) في طبقة المخدم VPN، بينما تعمل وظيفة تكييف بئر طبقة المخدم VPN في المثال المذكور على تكييف المعلومات AI لطبقة المخدم VPN لتصبح معلومات CI طبقة العميل VPN. ويشير هذا التكييف أساساً إلى تغليف رتل/إشارة طبقة العميل في رتل/إشارة طبقة المخدم VPN.

ومع ذلك، لا تستند جميع طوبولوجيات الشبكة VPN إلى مثال العميل/المخدم. ويمكن أيضاً توفير شبكات VPN باستعمال تكنولوجيات الشبكة بتبديل الرزم عديمة التوصيل (CL-PS) بالاستناد إلى مثال معين يتم بموجبه تحقيق عزل إمكانية الوصول إلى شبكة VPN داخل مجال مُتقاسم محدد باللجوء إلى وسيلة أخرى خلاف وسيلة تغليف العميل/المخدم. وتشير هذه التوصية إلى هذا النمط من شبكات VPN بوصفها شبكات VPN لمستوى القرين. ويدل تعبير "مستوى القرين" على أن المورد يقوم بنقل رزم VPN المشتركين عبر بنيته التحتية المُتقاسمة عند نفس طبقة الشبكة التي يستقبل بواسطتها الرزم من المشتركين. ولا يشير التعبير المذكور إلى التبادل بين أقران مستوي التحكم في العميل/المورد، فقد يكون العميل والمورد قرينين في مستوي التحكم بصرف النظر عن نمط الشبكة VPN الذي لا يُدعم سوى بأسلوب شبكة تبديل الرزم عديمة التوصيل (CL-PS)، لأن طابع توصيل تكنولوجيا الشبكة في حالتي تبديل الرزم بأسلوب التوصيل (CO-PS) وتبديل دارة موجهة التوصيل (CO-CS) طابع يفرض ضرورة تنفيذ عزل إمكانية الوصول، أي أنه لا يمكن لعناصر الشبكة (NE) أن تتصل سوى بعناصر شبكة تخص نفس التوصيل من نقطة إلى نقطة (P2P) أو من نقطة إلى عدة نقاط (P2MP).

ومن أجل دعم شبكات VPN عبر أحد المجالات المُتقاسمة، يجب أن يكون في تكنولوجيا الشبكة المُستعملة وسيلة ما لتأمين عزل شبكة VPN، أي، لابد أن تكون قدرة عناصر الشبكة مقصورة على الاتصال بعناصر أخرى تخص نفس شبكة VPN أو تكون قادرة على إزالة تجفير الرزم الواردة من عناصر شبكة تخص نفس شبكة VPN.

### 1.6 ترشيح الرزم/الطرق

تتمثل إحدى طرائق تنفيذ عزل الشبكة VPN عبر مجال مُتقاسم معين في استعمال مراشيح رزم إلى جانب حواف مورد (PE) يتقاسمها عدة مشتركين. وتعرف جميع العقد الموجودة في شبكة مورد الخدمة في إطار هذا النهج طرق جميع المشتركين. ويشمل ذلك عُقد حافة المورد (PE) المقابلة لمواقع المشتركين، وعُقد المورد (P) الموجودة في مركز الشبكة. ويتم تقاسم عقد PE في هذه المعمارية من جانب مختلف المشتركين. ويخصص مورد الخدمة جزءاً من مجال عنوانه لمشترك معين ويدير مراشيح الرزم المُرسلة عبر طرق PE ليكفل بذلك إمكانية وصول أي مشترك منفرد وصولاً تاماً فيما بين المواقع، وتحقيق العزل بين المشتركين.

وللتغلب على الحاجة إلى صيانة جداول التسيير المتسقة ومراشيح الرزم على أساس كل مشترك ولكل موقع، ثمة بديل يتمثل في تطبيق حل يستند إلى ترشيح الطرق بدلاً من ترشيح الرزم إلى جانب حواف PE المُخصصة، أي حافة PE واحدة لكل شبكة VPN. وتتضمن عُقد P في هذه المعمارية جميع طرق المشتركين، بيد أن عُقد الحافات PE لا تشتمل سوى طرق تابعة لعميل وحيد. ويتم عزل طرق المشتركين بترشيح الطرق. وتُشكّل عقد PE بمراشيح الطرق التي تسمح للمشتركين بمعرفة الطرق التي تخصهم. وبروتوكول بوابة الحدود (BGP) هو مثال على بروتوكول شائع الاستعمال لتحقيق هذا الغرض داخل شبكة المورّد الرئيسية بسبب تعدد الأدوات التي يستعملها في ترشيح الطرق. والبديل في ترشيح الطرق هو استعمال حالة مختلفة لبروتوكول التسيير في كل شبكة من شبكات VPN. غير أن اتباع هذا النهج من شأنه تمكين الشبكة المُتقاسمة من دعم عدد قليل من شبكات VPN نظراً لاقتصار قدرة عقد P على دعم عدد محدود من حالات بروتوكول التسيير، وتعقيد الجوانب التشغيلية لإدارة العديد من حالات البروتوكول.

وللتغلب على الحاجة إلى استعمال عقدة PE مختلفة لكل شبكة VPN، ثمة نهج بديل يتمثل في استعمال مسيّرات تقديرية (VR). ويستهدف هذا النهج فعالية تقسيم كل واحدة من العقد المادية إلى حجيرات تُدرج في عدد من المسيّرات التقديرية. ويمكن تخصيص مسيّر واحد (أو أكثر) من المسيّرات المذكورة لمشترك معين، وبهذه الطريقة، يمكن لعقدة واحدة أن توفر حالات تسيير مقسمة إلى حجيرات لعدة مشتركين. وتسلك المسيّرات التقديرية الفردية سلوكاً مماثلاً تماماً لسلوك عقد PE المستقلة والمُخصصة لشبكة VPN معينة. وكما هو الشأن في نهج ترشيح الطرق، تحتوي عقد P جميع طرق المشتركين، ولذلك، فإن ترشيح الطرق ضروري عند حواف المورد PE.[1]

### 2.6 التجفير

البديل لترشيح الطرق/الرزم هو توفير إمكانية النفاذ الكامل بين جميع المشتركين الموصولين ببنية تحتية مُتقاسمة مع تجفير الرزم. ويكفل هذا التجفير عدم تمكن المشتركين عند استقبال رزم لا تخصهم من إحدى شبكات VPN، من الحصول على المعلومات الموجودة في الرزم. وبإمكان المشترك تجفير رزم VPN قبل مرور الحركة عبر الشبكة المُتقاسمة، وبالتالي، يكون المشترك مسؤولاً عن إدارة شبكة VPN. وتُسيّر الحركة الموجودة داخل شبكة مورّد الخدمة في إطار هذا النهج بنفس طريقة تسيير أي حركة أخرى لبروتوكول الإنترنت IP، ولا يتسنى لمورّد الخدمة الرؤية داخل النفق. كما أنه ليس من الضروري تشكيل شبكة مورّد الخدمة بطريقة خاصة. ويمكن بدلاً من ذلك تجفير رزم VPN باستعمال تجهيزات يديرها المورّد (أي حواف PE أو حواف CE التي يديرها المورّد) على حافة شبكة المورّد المُتقاسمة. ويكون المورد في هذا النهج مسؤولاً عن إدارة شبكة VPN.

[1] والتطور الطبيعي لهذا النهج هو استعمال تبديل متعدد البروتوكولات بالتوسيم (MPLS) أو نهج أخرى للتمرير لكي لا تكون هناك حاجة لصيانة الطرق الخاصة بالشبكة VPN تحديداً عبر المسيّرات الرئيسية، غير أن هذا الأمر يولد طوبولوجيا شبكة VPN العميل/المخدم، وبالتالي ينطبق هذا النهج على الفقرة 5 بالأحرى لا على هذه الفقرة.

والمعيار RFC 2401 بعنوان معمارية أمن بروتوكول الإنترنت (IPsec)، هو مثال على إحدى المعماريات التي تؤمن التجفير. ويحدد المعيار IPsec خوارزميات تجفيرية وروتينات للاستيقان وإدارة المفاتيح[2] من أجل إنشاء أنفاق آمنة لنقل الحركة ببروتوكول الإنترنت (IP) بين بوابات/عملاء المعيار IPsec الذي يكفل خصوصية البيانات وسلامتها والتحقق من مصدرها في شبكة VPN نظراً لعبور المعلومات بنيه تحتية مُتقاسمة. ومعمارية أمن بروتوكول الإنترنت مفيدة خاصة في توفير شبكات VPN عبر شبكات عمومية من قبيل توفير الإنترنت من موقع إلى آخر والنفاذ عن بعد إلى شبكات VPN. ويمكن توفير وظيفة IPsec بواسطة حافة PE، أو حافة CE، أو بواسطة جهاز مستعمل نهائي (مثل حاسوب شخصي يشغل عميل IPsec).

وشبكات VPN بطبقة مقبس آمن (SSL) هي نمط آخر من أنماط VPN التي تستعمل التجفير لتوفير العزل لكل شبكة VPN. والاستعمال التقليدي لشبكات VPN بطبقة SSL يتمثل في تمكين المستعملين من النفاذ الآمن إلى التطبيقات والملفات عبر الإنترنت. وميزة هذا النهج أنه لا يتطلب إدخال أية تكييفات على تشكيل أنظمة المستعملين النهائيين، ولا حاجة سوى إلى دعم التطبيقات المعيارية (كأجهزة تصفح شبكة الويب، وعملاء البريد الإلكتروني، وما إلى ذلك). وتتسم أيضاً شبكات VPN بطبقة SSL بالشفافية بالنسبة إلى طبقة قرين VPN (لأن التجفير يتم عند طبقة التطبيق) وعليه، لا ضرورة لتشكيل عقد التسيير/التبديل من أجل دعم شبكات VPN بطبقة SSL.

### 3.6 شبكات المنطقة المحلية التقديرية (VLAN) إثرنت

يحدد المعيار IEEE 802.1Q تشغيل جسور الشبكة المحلية LAN التقديرية (VLAN) التي تسمح بتعريف طوبولوجيات الشبكة LAN التقديرية وتشغيلها وإدارتها في إطار البنية التحتية لإحدى شبكات LAN المجسورة. وتسمح شبكات VLAN للمحطات الطرفية الموجودة عبر قطع متعددة لشبكة LAN مادية بالاتصال وكأنها موصولة بنفس قطعة الشبكة LAN. ويمكن تمرير المستعملين النهائيين والمحاور/البدالات إلى شبكات VLAN مختلفة عن طريق تكييف تشكيل هذه الشبكات عبر المنفذ/السطح البيني بواسطة جهاز التبديل المُطابق للمعيار 802.1Q والموصول بالمحطة الطرفية أو المحور/البدالة. وتقيد حدود الشبكة VLAN الأرتال الإذاعية والمتعددة التوزيع، ولذلك لا تستطيع المحطات الطرفية سوى استقبال أرتال إذاعية/متعددة التقسيم تخص الشبكة VLAN. ويعمل هذا الأمر بالاقتران مع كيفية الحصول على عنوان التحكم في النفاذ إلى الوسائط (MAC)، على ضمان تمكين المحطات الطرفية التابعة لنفس شبكة VLAN من الاتصال ببعضها بعضاً، وبالتالي يمكن اعتبارها أعضاء تنتمي إلى نفس شبكة VPN.

ويتم فصل حركة الأرتال التي تخص مختلف شبكات VLAN عبر أي بنية تحتية مُتقاسمة بواسطة إدراج واسم بمعرف VLAN (VID) في كل رتل. ويجب أن يُخصص معرف VID لكل شبكة من شبكات VLAN (من 1 إلى 4096) وينبغي أن يكون هذا المعرف وحيداً على الصعيد العالمي داخل نفس البنية التحتية المادية. ويتمثل أحد عيوب هذا النهج في استعمال المشتركين لشبكات VLAN داخل شبكتهم أيضاً، الأمر الذي يفضي إلى مسائل تتعلق بتخصيص معرفات VID وتقييدها. ولحل هذه المشكلة، يمكن إضافة واسم ثان مطابق للمعيار IEEE 802.1Q إلى رزم المشترك الموسومة والمطابقة للمعيار المذكور والتي تدخل شبكة المورّد (Q-in-Q على النحو المحدد في المعيار IEEE 802.1ad). ويفصل هذا الواسم مجال شبكة VLAN للموردين عن مجال شبكة VLAN المشتركين ويسمح للمشتركين باستعمال أي معرف يريدونه من معرفات VID.[3]

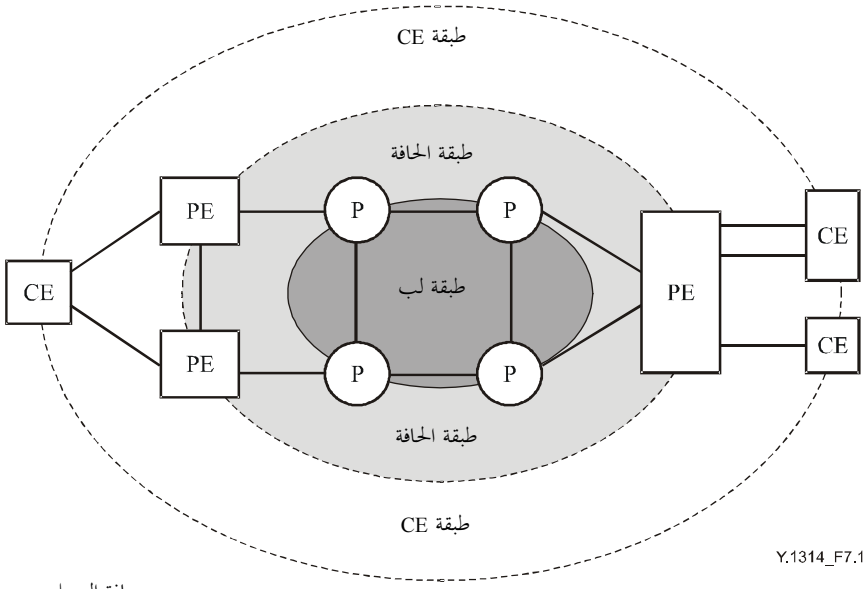
---

[2] المفتاح عبارة عن قطعة معلومات تتحكم في تطبيق خوارزمية التجفير/إزالة التجفير.

[3] ثمة خيار آخر يتمثل في استعمال نهج التحكم MAC في التحكم MAC (MAC–in–MAC) (المُحدد في المعيار IEEE 802.1ah) يضيف بموجبه المورد رأسية إثرنت ثانية إلى رزمة العملاء، غير أن هذا الخيار يكوّن شبكة VPN عميل/مخدم بدلاً من شبكة VPN لسوية النظير، لأن رتل المستعمل مُغلف داخل أحد أرتال المورد.

## 7 المعمارية الوظيفية لشبكات VPN

يوضح الشكل 7-1 المثال المرجعي لشبكة VPN المُستمد من التوصية ITU-T Y.1311.




**الشكل 7-1/Y.1314 – المثال المرجعي لشبكة VPN المُحدد في التوصية ITU-T Y.1311**

وعلى الرغم من أن هذا المثال يوضح الطوبولوجيا المادية ومكونات الشبكة المختلفة، إلا أنه لا يبين الطوبولوجيات المختلفة لطبقة المخدم VPN وطبقة العميل VPN أو موقع وظائف التكييف بين الطبقتين.

والنمذجة الوظيفية طريقة بديلة لتمثيل شبكة VPN العميل/المخدم. ويمكن وصف المعمارية الوظيفية لشبكات طبقات تبديل الرزم موجهة التوصيل (CO-PS)/تبديل دارة موجهة التوصيل (CO-CS) وتبديل رزمة عديمة التوصيل (CL-PS) باستعمال التوصية ITU-T G.805، بعنوان "المعمارية الوظيفية النوعية لشبكات النقل" والتوصية ITU-T G.809 أيضاً بعنوان "المعمارية الوظيفية لشبكات الطبقة عديمة التوصيل" على التوالي.

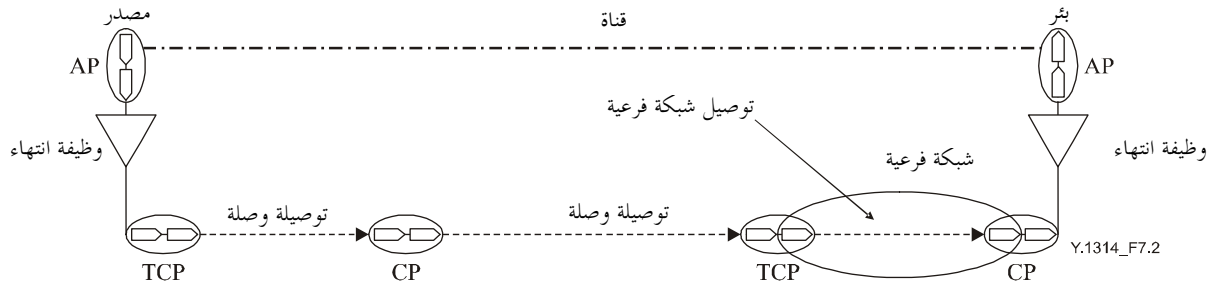
وتوفر التوصيتان المذكورتان طرائق نوعية مفيدة لنمذجة الشبكات من منظور المعمارية الوظيفي والبنيوي. والمصطلحات المُحددة مستقلة عن التكنولوجيا ويمكن استخدامها لوصف المكونات المادية والمنطقية لأي شبكة معينة، وهي مفيدة خاصة في جرد مكونات الشبكة وإدارتها، نظراً لإمكانية الاستناد إليها في نمذجة كامل رؤية الشبكة اعتباراً من الألياف البصرية الموجودة في المجرى وحتى خدمات VPN العاملة على هذه الألياف.

وبالإمكان تقسيم شبكة VPN إلى عدد من شبكات الطبقات المستقلة مع إقامة علاقة العميل/المخدم بين شبكات الطبقات المتجاورة. ومثلما أشِير إلى ذلك في التوصية ITU-T G.805، ينبغي عدم الخلط بين شبكات الطبقات المُحددة باستعمال النمذجة الوظيفية مع طبقات مثال التوصيل البيني للأنظمة المفتوحة (OSI) (المُحدد في التوصية ITU-T X.200. وتقدم كل طبقة موجودة في مثال التوصيل OSI خدمة معينة وتؤدي البروتوكولات المُحددة في كل طبقة منها وظيفة معينة متوافقة مع الطبقة المذكورة، فمثلاً، تقبل طبقة النقل (الطبقة 4) استلام بيانات من طبقة الدورة وتمررها عبر طبقة الشبكة لتقدم بذلك خدمة تسليم من طرف إلى طرف. وعلى العكس تماماً، تقدم كل شبكة طبقة في أي مثال وظيفي يستند إلى التوصية ITU-T G.805 أو التوصية ITU-T G.809 نفس الخدمة، أي نقل البتات/الأرتال بين الدخل والخارج. ويُستعمل عادةً التجريد لإخفاء التفاصيل والتركيز على طبقات/مكونات الشبكة ذات الأهمية، بيد أنه يمكن نمذجة الشبكات انطلاقاً من عناصر الشبكة، كبدالات إثرنت، والأزواج النحاسية، والتراتب الرقمي المتزامن (SDH) عبر التوصيل، وما إلى ذلك.

## 1.7 شبكات طبقة VPN الموجهة التوصيل

لكل واحدة من شبكات طبقة العميل والمخدم VPN مجموعتها الخاصة من حالات دخل وخرج التوصيلية المعروفة بنقاط النفاذ (AP). ونقاط النفاذ يمكن أن تتصاحب مع بعضها بعضاً لنقل المعلومات بشفافية عبر شبكة الطبقة من الدخل إلى الخرج. وتركيبات التصاحب الصحيحة للطوبولوجيا بين نقاط AP التابعة لشبكات طبقة التوصيل (CO) هي عبارة عن تركيبات من نقطة إلى نقطة (P2P) أو من نقطة إلى عدة نقاط (P2MP).

وتعين نقاط AP لطبقة المخدم VPN الحد الوظيفي بين شبكة طبقة المخدم VPN وشبكة طبقة العميل VPN. وانطلاقاً من منظور طبقات المخدم VPN، تمثل نقطة AP لطبقة مخدم VPNمقصد تسيير يمكن أن يدعم إحدى القنوات. أما نقطة AP لطبقة العميل VPN، فهي نقطة تمثل من منظور هذه الطبقة نقطة يمكن فيها الحصول على قدرة الوصلة. ويبين الشكل 7-2 المكونات الوظيفية والنقاط المرجعية في طبقة شبكة التوصيل CO.




**الشكل 7-2/Y.1314 – المكونات الوظيفية والنقاط المرجعية لطبقة الشبكة CO**

والتوصيلات عبارة عن كيانات نقل في شبكات طبقة التوصيل CO، وهي تتكون من زوج متصاحب من التوصيلات الأحادية الاتجاه القادرة على نقل المعلومات في آن معاً باتجاهين متعاكسين بين حالات الدخل والخرج الخاصة بها. وتوصيل الشبكة هو عبارة عن كيان نقل في شبكة طبقة التوصيل CO، ويُكوّن بواسطة سلسلة من توصيلات الوصلة المتجاورة و/أو توصيلات شبكة فرعية بين نقاط انتهاء التوصيل (TCP).

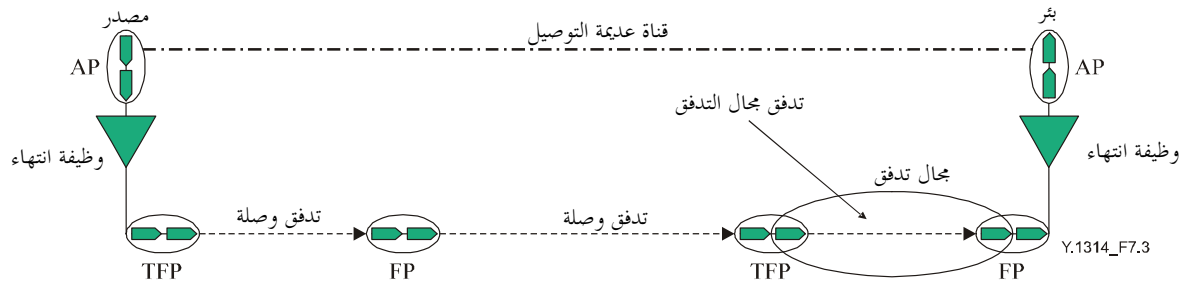
والشبكة الفرعية مكون طوبولوجي في شبكة طبقة التوصيل CO تُستعمل لتنفيذ تسيير معلومات مميزة معينة، وتتضمن مجموعة نقاط مصاحبة لإحدى وظائف الإدارة داخل طبقة وحيدة لشبكة التوصيل CO. ويعمل توصيل الشبكة الفرعية على نقل المعلومات عبر شبكة فرعية معينة، ويُكوّن بتصاحب منافذ (خرج مصدر انتهاء قناة/دخل بئر انتهاء لقناة) عند حد الشبكة الفرعية.

وتقوم توصيلات الوصلة بتوصيل الشبكات الفرعية المتجاورة طوبولوجيا التي لها مجموعة فرعية مشتركة من النقاط توصيلاً بينياً. ونقطة التوصيل (CP) هي النقطة التي يربط فيها دخل توصيل الوصلة بخرج توصيل وصلة آخر. أما النقطة التي يكون فيها خرج مصدر انتهاء القناة في شبكة طبقة التوصيل CO خرجاً مربوطاً بدخل توصيل الشبكة، فهي نقطة TCP للمصدر، بينما تعتبر النقطة التي يربط فيها داخل بئر انتهاء القناة بخرج توصيل الشبكة في نقطة TCP البئر. وهناك موضوع مُدار مُصاحب لنقاط CP ونقاط TCP، ولذلك يمكن تجميع نقاط CP وTCP معاً المنتمية لنفس شبكة VPN لأغراض إدارية.

## 2.7 شبكات طبقة VPN عديمة التوصيل

على نقيض شبكات طبقة التوصيل CO، تدعم شبكات الطبقة عديمة التوصيل (CL) طوبولوجيات الشبكة من عدة نقاط إلى عدة نقاط (MP2MP) أو طوبولوجيات أي نقطة إلى أي نقطة (any-to-any). وتستعمل شبكات الطبقة عديمة التوصيل التدفقات بدلاً من التوصيلات، وهي عبارة عن تجميع لوحدة واحدة أو أكثر من وحدات الحركة بعنصر تسيير مشترك. ويمكن أن تكون التدفقات أحادية أو ثنائية الاتجاه، إذ تكون الثنائية الاتجاه منها مؤلفة من تدفقين متقابلين ثنائي الاتجاه وأحادي الاتجاه. وتدفق الشبكة هو كيان نقل في شبكة الطبقة عديمة التوصيل (CL) يُكوّن بواسطة سلسلة تدفقات متجاورة

بين نقاط انتهاء التدفق (TFP). ويوضح الشكل 7-3 المكونات الوظيفية والنقاط المرجعية في شبكة الطبقة عديمة التوصيل (CL).




**الشكل 7-3/التوصية Y.1314 – المكونات الوظيفية والنقاط المرجعية لطبقة الشبكة CL**

ومجال التدفق عبارة عن مكون طوبولوجي في شبكة الطبقة عديمة التوصيل (CL) يُستعمل لتنفيذ تسيير معلومات مميزة معينة. أما تدفق مجال التدفق، فهو كيان نقل يقوم بنقل المعلومات عبر مجال تدفق ما، ويُكوّن بتصاحب منافذ معينة عند حد مجال التدفق الذي يحوي مجموعة نقاط مصاحبة لإحدى وظائف الإدارة داخل طبقة وحيدة للشبكة عديمة التوصيل (CL).

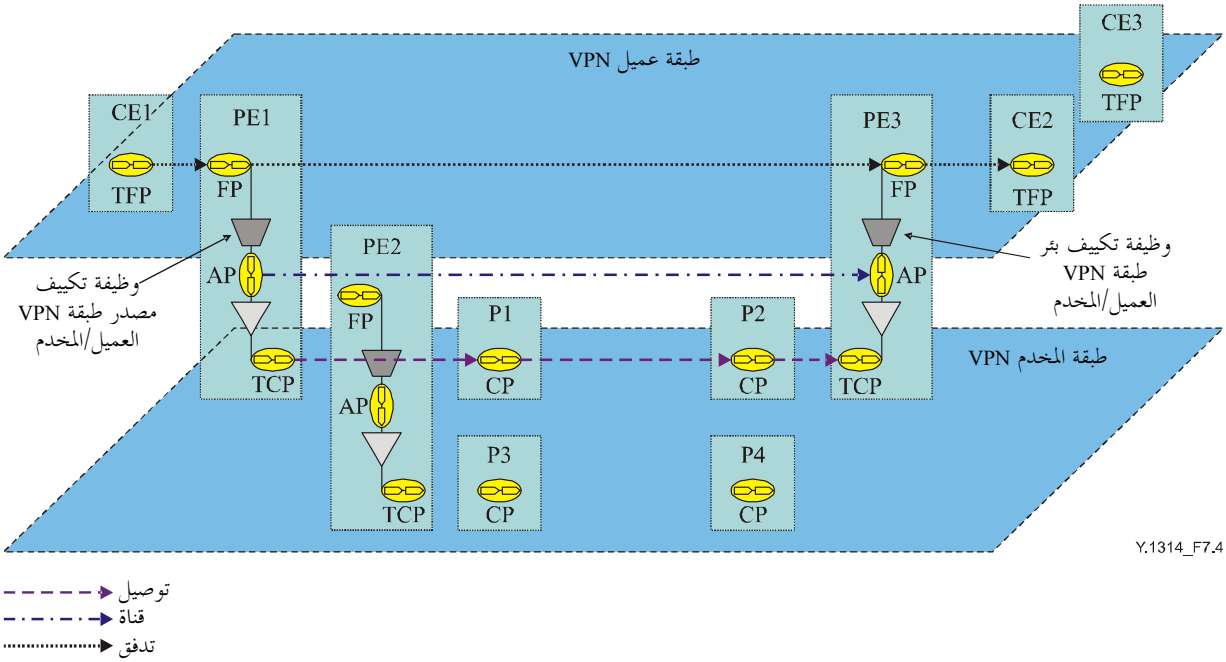
وتقوم تدفقات الوصلة بتوصيل مجالات التدفق المتجاورة طوبولوجياً التي لديها مجموعة فرعية مشتركة من النقاط توصيلاً بينياً. ونقطة التدفق (FP) هي النقطة التي يربط فيها دخل تدفق الوصلة بخرج تدفق وصلة آخر. أما النقطة التي يكون فيها خرج مصدر انتهاء القناة العديمة التوصيل في شبكة الطبقة عديمة التوصيل (CL) خرجاً مربوطاً بدخل تدفق الشبكة، فهي نقطة TFP المصدر، بينما تعتبر النقطة التي يربط فيها دخل بئر انتهاء القناة العديمة التوصيل بخرج تدفق الشبكة فهي نقطة TFP البئر. ومثلما هو حال النقاط CP وTCP في حالة التوصيل CO، يوجد موضوع مُدار مُصاحب لنقاط FP ونقاط TFP في حالة شبكة الطبقة عديمة التوصيل (CL)، ولذلك يمكن تجميع نقاط FP وTFP معاً المنتمية لنفس شبكة VPN لأغراض إدارية.

## 3.7 العلاقات القائمة بين طبقات العميل/المخدم VPN

شبكة طبقة العميل VPN من حيث مضمونها الوظيفي مكون طوبولوجي في شبكة العميل/المخدم VPN تمثل مجموعة نقاط النفاذ المتشابهة النمط والمتصاحبة لغرض نقل المعلومات المميزة لطبقة العميل VPN، والمدعومة بقناة طبقة المخدم VPN أو إحدى القنوات العديمة التوصيل. ونقاط TFP/TCP المصدر/البئر التابعة لتوصيلات/تدفقات طبقة العميل VPN هي نقاط يمكن أن تقع في عقد CE، أو في عقد/أنظمة طرفية توجد في مواقع أخرى في شبكة المشترك. فنقاط TCP مثلاً، الموجودة في طبقة العميل ATM VPN هي نقاط يمكن أن يكون موقعها داخل عقد CE، بينما يُحتمل أن يكون موقع نقاط TFP الموجودة في طبقة العميل VPN إثرنت داخل حواسيب أو مخدمات مستعملين نهائيين. وتحديد موقع نقاط TCP/TFP تدفقات/توصيلات العميل VPN أمر هام من وجهة نظر المشترك، لأن هذا الموقع هو نقطة في شبكة المشترك يجب أن يحدث فيها التكييف بين طبقة العميل VPN والطبقة الأعلى. كما أن هذه النقطة مهمة من منظور وظيفة التشغيل والإدارة والصيانة (OAM)، لأنها تمثل موقع نقاط AP مصدر وبئر القناة/القناة العديمة التوصيل المُصاحبة لتدفق/توصيل تابع لطبقة العميل VPN. ويرد في التذييل I أمثلة على شبكات VPN العميل/المخدم التي توجد فيها مواقع النقاط TCP/TFP في أماكن مختلفة.

أما شبكة طبقة المخدم VPN فهي عبارة عن مكون طوبولوجي في شبكة VPN العميل/المخدم تمثل مجموعة نقاط النفاذ المتشابهة النمط والمتصاحبة لغرض نقل المعلومات المكيفة لطبقة العميل التابعة لتدفق أو توصيل واحد أو أكثر من تدفقات أو توصيلات طبقة العميل VPN. وتحوي طبقة المخدم VPN وظائف تكييف المصدر/البئر التي تتولى تكييف المعلومات المميزة في طبقة العميل VPN إلى/من المعلومات المكيفة في طبقة المخدم VPN. وقد تكون طبقتا العميل والمخدم VPN تابعتين لنفس الأسلوب (أي، عندما تكون طبقتا العميل والمخدم على حد سواء طبقتي CO أو طبقتي CL)، بيد أن التوليف بين الأسلوبين ممكن أيضاً، أي بإمكان طبقات المخدم CO VPN أن تدعم طبقات العميل CL. وبالمثل، يمكن أيضاً أن تدعم طبقات المخدم

CL طبقات العميل CO. ويبين الشكل 7-4 مثالاً لطبقة مخدم CL VPN تدعم طبقة عميل CL VPN من منظور وظيفي يستند إلى الطوبولوجيا المادية لمثال الشبكة المُستمد من التوصية ITU-T Y.1311 والمبين في الشكل 7-1. والطبقة السفلى المبينة في المثال هي طبقة المخدم VPN أما الطبقة العليا فهي طبقة العميل VPN. وبغية التبسيط، لا يوضح الشكل سوى طبقتي العميل/المخدم VPN، أما طبقة العميل المشترك الواقعة فوق طبقة العميل VPN وطبقة المخدم الواقعة تحت طبقة المخدم VPN فغير موضحتين في الشكل. وطبقة المخدم VPN في هذا المثال هي CO (مثل ATM) في حين أن طبقة العميل هي CL (مثل إثرنت)، ومع ذلك يمكن التوليف بين أزواج CO أو أزواج CL.



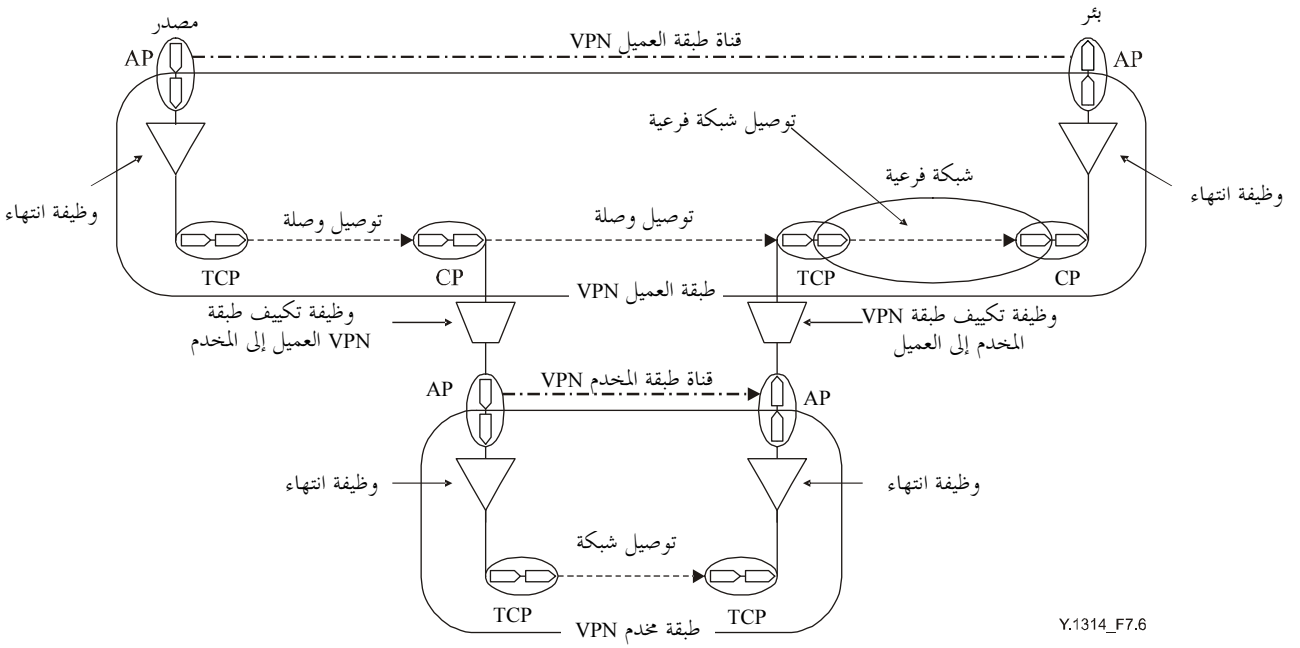

**الشكل Y.1314/4-7 – المثال الوظيفي لشبكة VPN العميل/المخدم**

ويوضح الشكل 7-4 كيفية ارتباط المثال الوظيفي بمخطط الشبكة المبين في الشكل 7-1 عن طريق إبراز ما هو موجود من وظائف ونقاط مرجعية خاصة بالشبكة في عنصر الشبكة (أي عقدة CE أو PE أو عقدة P). والعقدتان CE وP تابعتان لطبقتي العميل والمخدم VPN على التوالي، بينما تخص عقد PE كلتا الطبقتين. وتحدد نقاط TFP الموجودة في طبقة العميل VPN (وهي عقدة CE في هذه الحالة) المكان الذي يبدأ فيه تدفق طبقة العميل P2P VPN (مصدره) انتهائه (بئره) أما نقاط FP فتحدد عقد PE التي يمر من خلالها تدفق P2P. وبالمثل، تحدد نقاط TFP الموجودة في طبقة المخدم VPN مصدر وبئر توصيل طبقة المخدم VPN، بينما تحدد نقاط FP ماهية عقد P التي يمر من خلالها التدفق. وتحدد نقاط النفاذ (AP) الموجودة في طبقة المخدم VPN هوية مصدر/بئر قناة طبقة المخدم VPN.

وتورد الفقرات الفرعية الواردة أدناه كل توليفة من التوليفات الأربع الممكنة لشبكة VPN العميل/المخدم باستخدام النماذج الوظيفية، وتصف دور وظائف تكييف شبكة VPN العميل/المخدم.

### 1.3.7 طبقة العميل CO VPN المدعومة بطبقة المخدم CO VPN

يوضح الشكل 7-5 مثالاً لشبكة طبقة العميل CO VPN المدعومة بشبكة طبقة المخدم CO VPN.

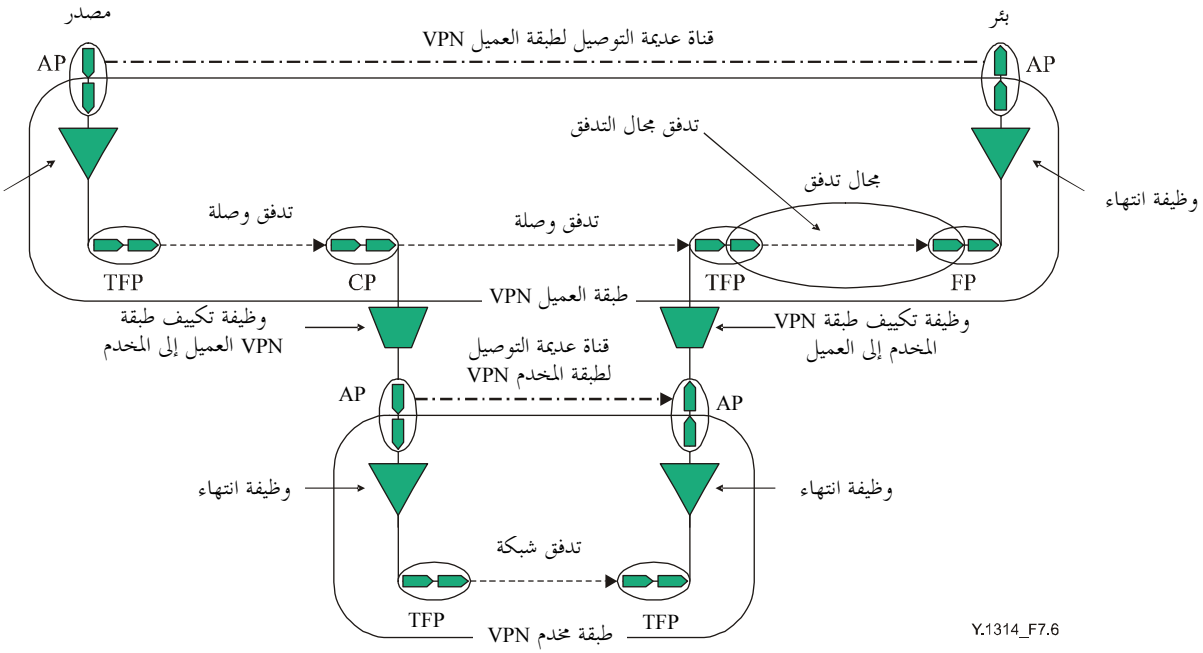



**الشكل Y.1314/5-7 – طبقة مخدم CO VPN مع طبقة عميل CO VPN**

وتدعم قناة طبقة المخدم CO VPN في هذا المثال توصيل طبقة العميل CO VPN. وتتولى وظيفة تكييف مصدر طبقة المخدم CO VPN تكييف المعلومات المميزة (CI) لطبقة العميل CO VPN إلى المعلومات المكيفة (AI) الواردة في طبقة المخدم CO VPN، بينما تقوم وظيفة تكييف بئر طبقة المخدم CO VPN بتكييف معلومات AI طبقة المخدم CO VPN إلى معلومات CI في طبقة العميل CO VPN.

### 2.3.7 طبقة العميل CL VPN المدعومة بطبقة المخدم CL VPN

يوضح الشكل 7-6 مثالاً لشبكة طبقة العميل CL VPN المدعومة بشبكة طبقة المخدم CL VPN.

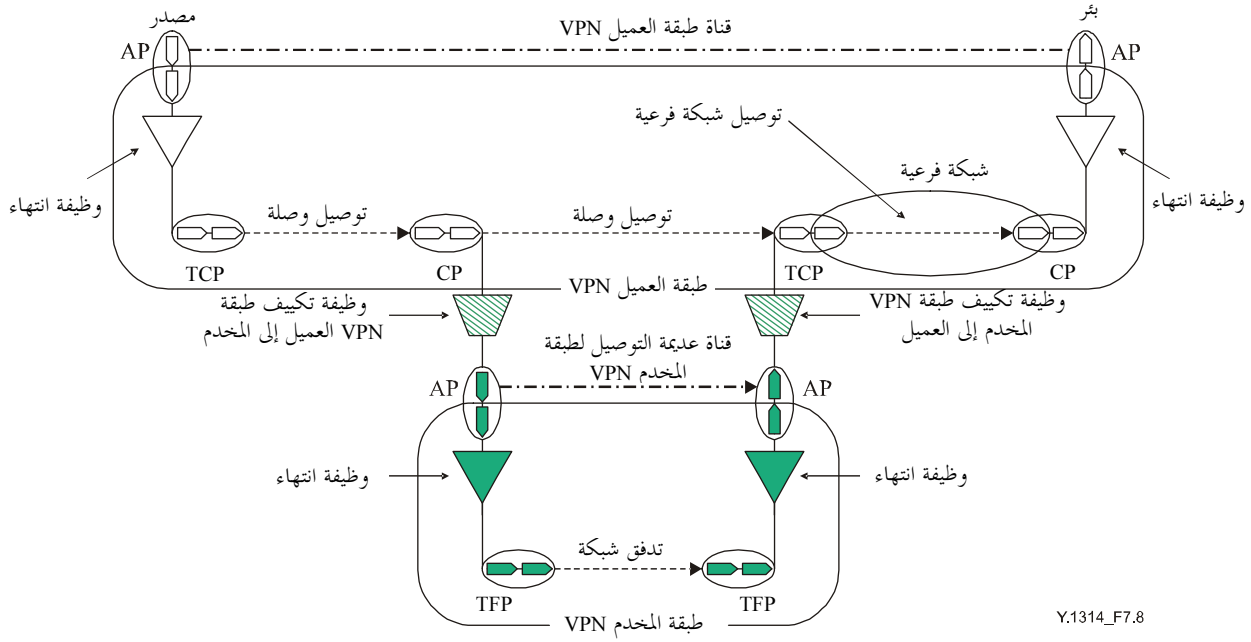



**الشكل Y.1314/6-7 – طبقة مخدم CL VPN مع طبقة عميل CL VPN**

وتدعم قناة طبقة المخدم CL VPN عديمة التوصيل في هذا المثال تدفق طبقة العميل CL VPN. وتتولى وظيفة تكييف مصدر طبقة المخدم CL VPN تكييف المعلومات المميزة (CI) لطبقة العميل CL VPN إلى المعلومات المكيفة (AI) الواردة في طبقة المخدم CL VPN، بينما تقوم وظيفة تكييف بئر طبقة المخدم CL VPN بتكييف معلومات AI طبقة المخدم CL VPN إلى معلومات CI طبقة العميل CL VPN.

### 3.3.7 طبقة العميل CO VPN المدعومة بطبقة المخدم CL VPN

يوضح الشكل 7-7 مثالاً لشبكة طبقة العميل CO VPN المدعومة بشبكة طبقة المخدم CL VPN.

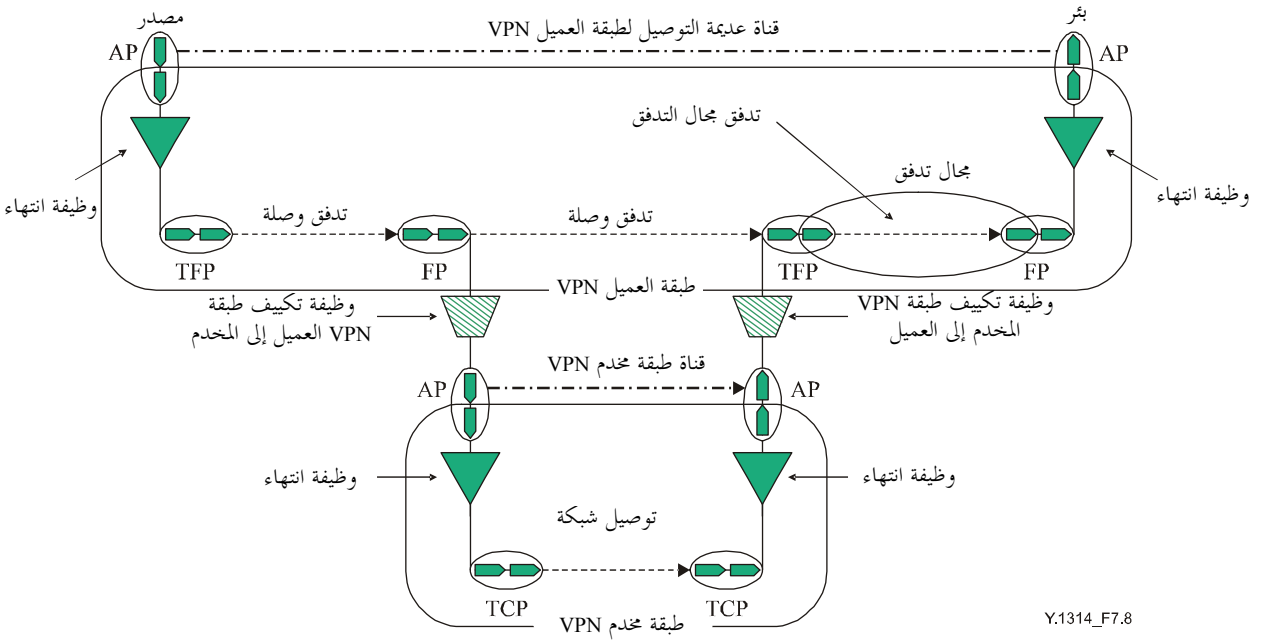



**الشكل Y.1314/7-7 – طبقة مخدم CL VPN بطبقة عميلCO**

وتدعم قناة عديمة التوصيل لطبقة المخدم CL VPN في هذا المثال توصيل طبقة العميل CO VPN. وتتولى وظيفة تكييف مصدر طبقة المخدم CL VPN تكييف المعلومات المميزة (CI) لطبقة العميل CO VPN إلى المعلومات المكيفة (AI) الواردة في طبقة المخدم CL VPN، بينما تقوم وظيفة تكييف بئر طبقة المخدم CL VPN بتكييف معلومات AI طبقة المخدم CL VPN إلى معلومات CI طبقة العميل CO VPN.

### 4.3.7 طبقة العميل CL VPN المدعومة بطبقة المخدم CO VPN

يوضح الشكل 7-8 مثالاً لشبكة طبقة العميل CL VPN المدعومة بشبكة طبقة المخدم CO VPN.




**الشكل Y.1314/8-7 – طبقة مخدم CO VPN مع طبقة عميل CL**

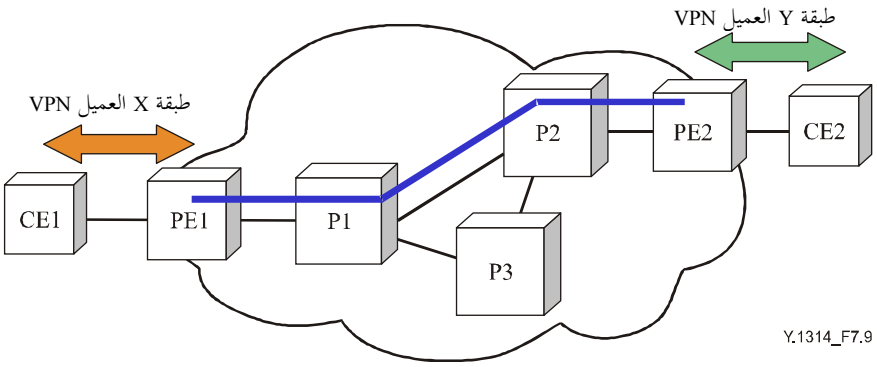
وتدعم قناة طبقة المخدم CO VPN في هذا المثال تدفق طبقة العميل CL VPN. وتتولى وظيفة تكييف مصدر طبقة المخدم CO VPN تكييف المعلومات المميزة (CI) لطبقة العميل CL VPN إلى المعلومات المكيفة (AI) الواردة في طبقة المخدم CO VPN، بينما تقوم وظيفة تكييف بئر طبقة المخدم CO VPN بتكييف المعلومات AI لطبقة المخدم CO VPN إلى معلومات CI طبقة العميل CL VPN.

## 4.7 طبقات العميل VPN المتعددة

يُلاحظ من الأمثلة التي وردت حتى الآن في هذه الفقرة استعمال طبقة وحيدة لعميل VPN من طرف إلى طرف، غير أنه قد لا تكون الحال كذلك على الدوام، فقد يرغب مشترك معين استعمال نمط ما من أنماط طبقة العميل VPN عند أحد طرفي الشبكة VPN، واستعمال نمط آخر للعميل VPN عند طرفها الآخر. ويمكن مثلاً أن تكون طبقة العميل VPN عند أحد الطرفين بروتوكول إنترنت (IP) وقد تكون عند الطرف الآخر تبديل متعدد البروتوكولات بالتوسيم (MPLS)، أو قد يكون أحد الطرفين مرحل أرتال (FR) ويكون الطرف الآخر أسلوب نقل غير متزامن (ATM). ويجب في هذه الحالات تنسيق ربط الشبكتين المختلفتين لطبقة العميل VPN على أساس مستوى القرين.

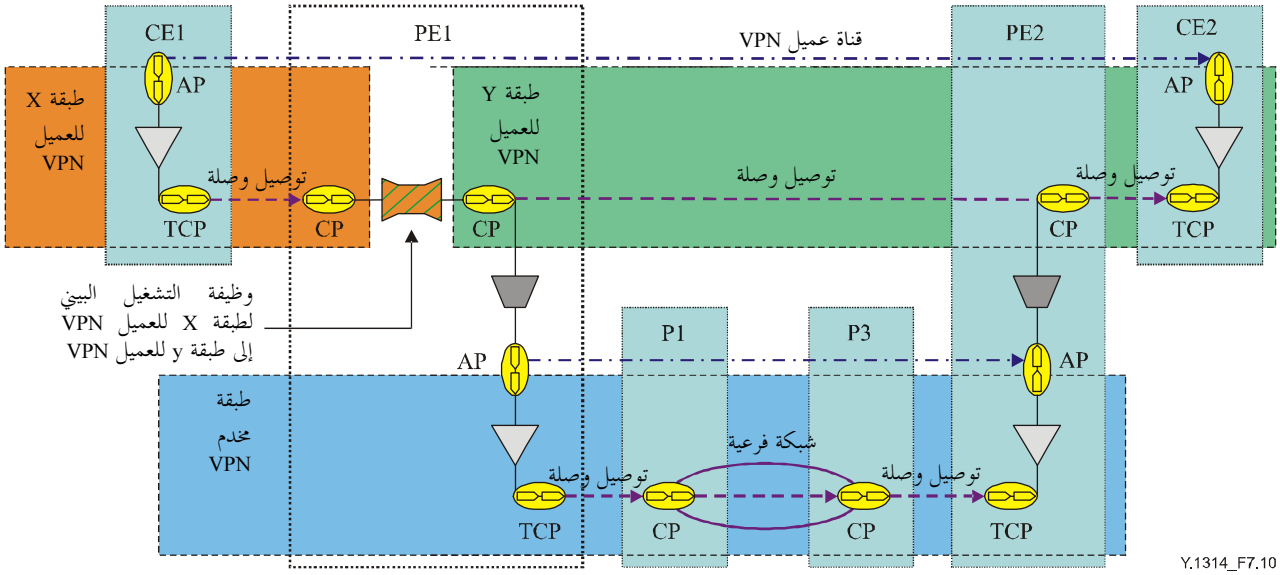
ومن الجدير بالذكر أن تعبير 'شبكة طبقة العميل VPN' المُستعمل هنا يشير إلى مكون طوبولوجي في شبكة VPN العميل/المخدم يمثل مجموعة نقاط النفاذ لذات النمط المُصاحب والمستعملة لغرض نقل معلومات CI طبقة العميل VPN. ولا يشير التعبير إلى تقسيم الشبكة إلى طبقات أي الطبقة 1، والطبقة 2، والطبقة 3، وبعبارة أخرى، يمكن أن تكون تكنولوجيتا الشبكتين المشغلتين بينياً عند طبقة العميل VPN تكنولوجيتا الطبقة 2 على حد سواء (كأن تكون إحداهما أسلوب نقل غير متزامن (ATM) وتكون الأخرى مرحل أرتال (FR))، على أنهما تعتبران شبكتي طبقتين مختلفتين نظراً لاحتوائهما على نقاط نفاذ مختلفة بأنماط مختلفة أيضاً.

وقد تتم وظيفة التشغيل البيني إما قبل وظيفة تكييف مصدر طبقة المخدم VPN أو بعد وظيفة تكييف بئر مخدم VPN. ويوضح الشكل 7-9 الطوبولوجيا المادية لشبكة VPN العميل/المخدم التي تستعمل طبقات مختلفة للعميل VPN عند كل طرف من طرفي الشبكة VPN.




**الشكل Y.1314/9-7 – الطوبولوجيا المادية للتشغيل البيني على مستوى القرين للعميل VPN**

ويبين الشكل 7-10 مثالاً وظيفياً نوعياً للتشغيل البيني للعميل VPN على مستوى القرين بالاستناد إلى الطوبولوجيا المادية المبينة في الشكل 7-9، حيث تتم فيه وظيفة التشغيل البيني قبل وظيفة تكييف مصدر طبقة المخدم VPN.

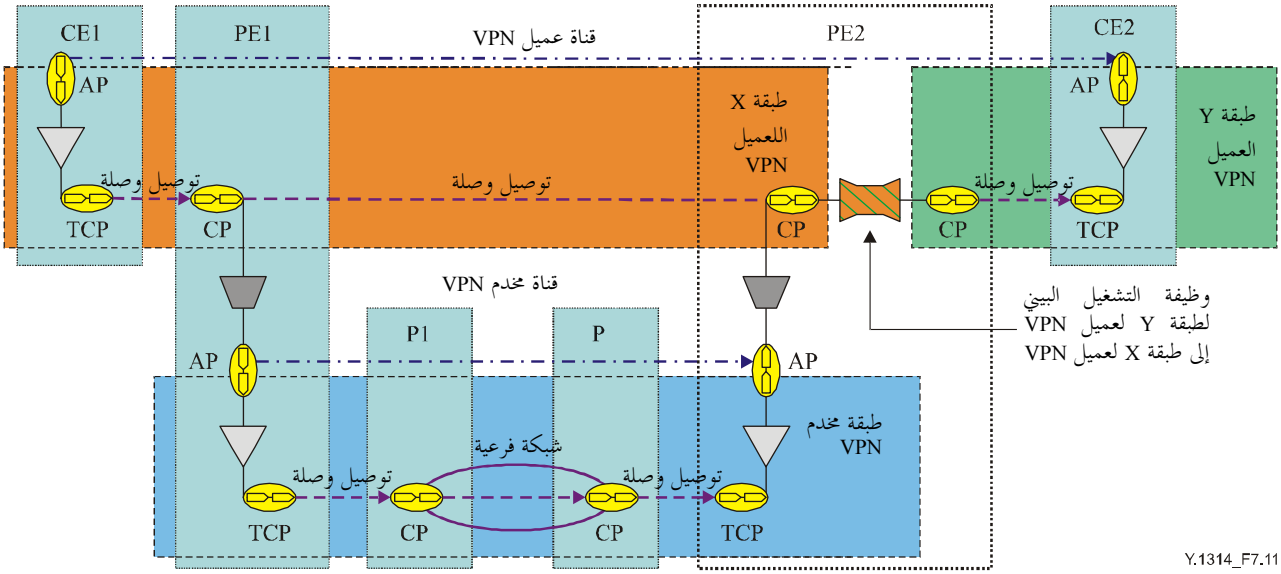



**الشكل Y.1314/10-7 – التشغيل البيني لمستوى القرين للعميل VPN**

**(تكييف سابق لمصدر المخدم VPN)**

والطبقتان المختلفتان للعميل VPN المبينتان في هذا المثال هما الطبقتان X وY للعميل VPN. وتؤدي الحافة PE في هذا المثال وظيفة التشغيل البيني، بيد أن بالإمكان تأديتها أيضاً باستعمال جهاز مستقل. وتحول وظيفة التشغيل البيني معلومات CI الطبقة X للعميل VPN إلى معلومات CI الطبقة Y للعميل VPN. وتتولى وظيفة تكييف مصدر طبقة المخدم VPN تكييف معلومات CI الطبقة Y للعميل VPN إلى معلومات AI الواردة في طبقة المخدم VPN، وتُرسل معلومات AI طبقة المخدم VPN عبر قناة طبقة المخدم VPN. وتقوم وظيفة التكييف عند بئر طبقة المخدم VPN بتكييف معلومات AI طبقة المخدم VPN إلى معلومات CI الطبقة Y للعميل VPN. وكمثال، إذا كانت الطبقة X للعميل VPN مرحل أرتال (FR) وكانت الطبقة Y للعميل VPN أسلوب نقل غير متزامن (ATM)، تقوم عندئذ الحافة PE المصدر بتحويل حركة FR إلى حركة ATM (باستعمال رتل FRF.8 مثلاً) وتُنقل حركة طبقة العميل VPN بوصفها حركة ATM عبر طبقة المخدم VPN.

ويبين الشكل 7-11 مثالاً وظيفياً نوعياً للتشغيل البيني للعميل VPN لمستوى القرين، حيث تتم فيه وظيفة التشغيل البيني بعد وظيفة تكييف بئر طبقة المخدم VPN.




**الشكل Y.1314/11-7 – التشغيل البيني لمستوى القرين للعميل VPN (تكييف لاحق لبئر المخدم VPN)**

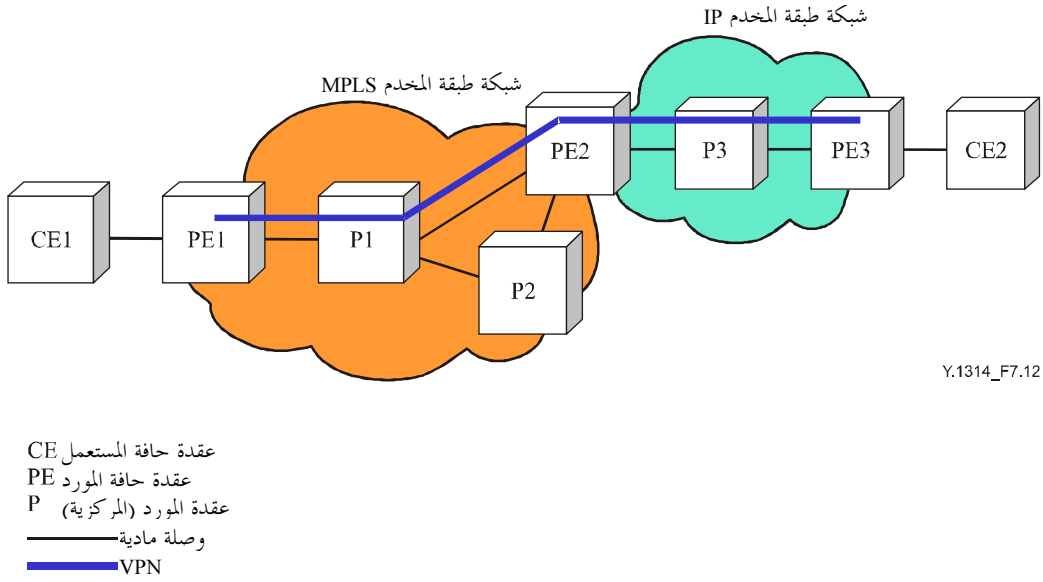
وتتولى وظيفة تكييف مصدر طبقة المخدم VPN تكييف معلومات CI الطبقة X للعميل VPN إلى معلومات AI الواردة في طبقة المخدم VPN، وتُرسل معلومات AI طبقة المخدم VPN عبر قناة طبقة المخدم VPN. وتقوم وظيفة التكييف عند بئر طبقة المخدم VPN بتكييف معلومات AI طبقة المخدم VPN إلى معلومات CI الطبقة X للعميل VPN. وتحول وظيفة التشغيل البيني معلومات CI الطبقة X للعميل VPN إلى معلومات CI الطبقة Y للعميل VPN. وإذا كانت الطبقة X للعميل VPN مرحل أرتال (FR) وكانت الطبقة Y للعميل VPN أسلوب نقل غير متزامن (ATM)، تُنقل عندئذ حركة طبقة العميل VPN بوصفها حركة FR عبر طبقة المخدم VPN وتُحوّل إلى حركة ATM بواسطة حافة PE البئر.

## 5.7 طبقات المخدم VPN المتعددة

استُعمِلت في الأمثلة السابقة طبقة وحيدة لمخدم VPN من طرف إلى طرف عبر شبكة المورّد لدعم طبقة العميل VPN، غير أنه يمكن ألا تكون الحال كذلك على الدوام؛ فقد يتعذر مثلاً على المورّد توفير التوصيلية من طرف إلى طرف باستعمال طبقة وحيدة لمخدم VPN بسبب عدم توفر تغطية الشبكة، أو بسبب حاجة طبقة العميل VPN إلى عبور العديد من شبكات الموردين. ومن الضروري في ظل هذه الظروف توفير العديد من طبقات المخدم VPN. ورهناً بتكنولوجيات الشبكة المُطبقة تحديداً وبقدرات التشغيل البيني لتجهيزات المورد، يمكن تشغيل طبقات مستقلة لمخدم VPN تشغيلاً بينياً على أساس مستوى القرين، أو تشغيلها بينياً مع العميل VPN على أساس العميل/المخدم.

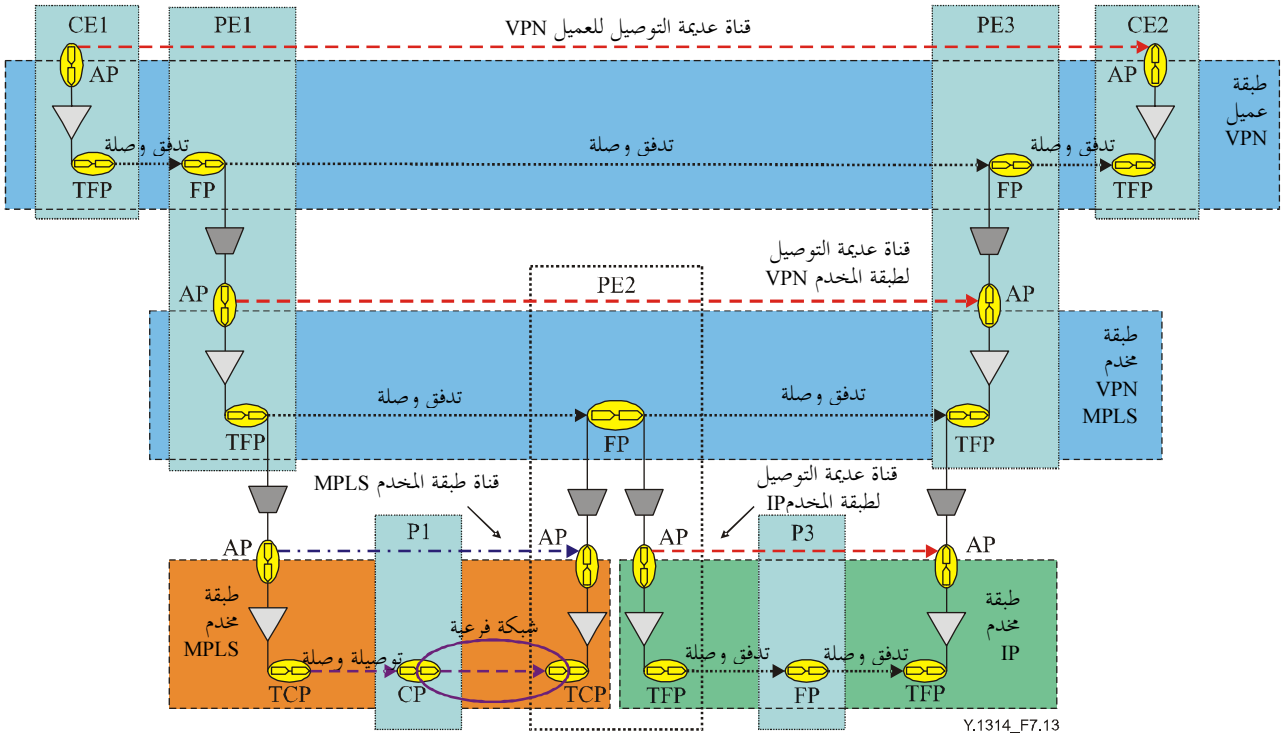
وبرغم توفر إمكانية استعمال العديد من طبقات المخدم VPN، فإن هناك عدة عوامل لابد من مراعاتها عند التفكير في استعمال العديد من طبقات المخدم VPN بتبديل متعدد البروتوكولات بالوسم MPLS. وتعتمد العوامل التي يتوجب مراعاتها على نمط التشغيل البيني المطلوب وتكنولوجيات طبقة المخدم VPN التي يتعين تطبيقها. ويورد التذييل II أمثلة على التشغيل البيني على مستوى القرين وعلى أساس العميل/المخدم وطبقات مخدم متعددة مع بعض التعليقات المتعلقة بكل واحدة منها.

وينبغي ملاحظة ضرورة عدم الخلط بين استعمال العديد من طبقات المخدم أسفل طبقة المخدم VPN واستعمال العديد من طبقات المخدم VPN. ومثلما هو موضح في الشكل 7-12، فإن بإمكان مورد الخدمة أن يستعمل مثلاً طبقة وحيدة للمخدم VPN بتبديل MPLS من طرف إلى طرف، ولكن شريطة استعمال طبقة مخدم بتبديل متعدد البروتوكولات بالوسم MPLS (بالاستفادة من تكديس الوسوم) أسفل طبقة المخدم VPN في أحد أجزاء الشبكة، واستعمال طبقة مخدم ببروتوكول الإنترنت (IP) (باستعمال تغليف التسيير النوعي (GRE) مثلاً) في جزء آخر من الشبكة.




**الشكل 7-12/ Y.1314 – شبكة VPN العميل/المخدم ذات طبقات مخدم بتبديل MPLS وبروتوكول IP**

يجب أن تدعم جميع مسيّرات حافة المورد PE والمورد P التبديل MPLS في طبقة مخدم شبكة MPLS، غير أنه لا تحتاج سوى مسيّرات PE الموجودة في طبقة مخدم IP إلى تقديم الدعم لتبديل MPLS، أما مسيّرات P، فلا تحتاج إلى دعم التبديل MPLS. ويصف الشكل 7-13 المثال الوظيفي المتعلق بالشبكة الموضحة في الشكل 7-12.



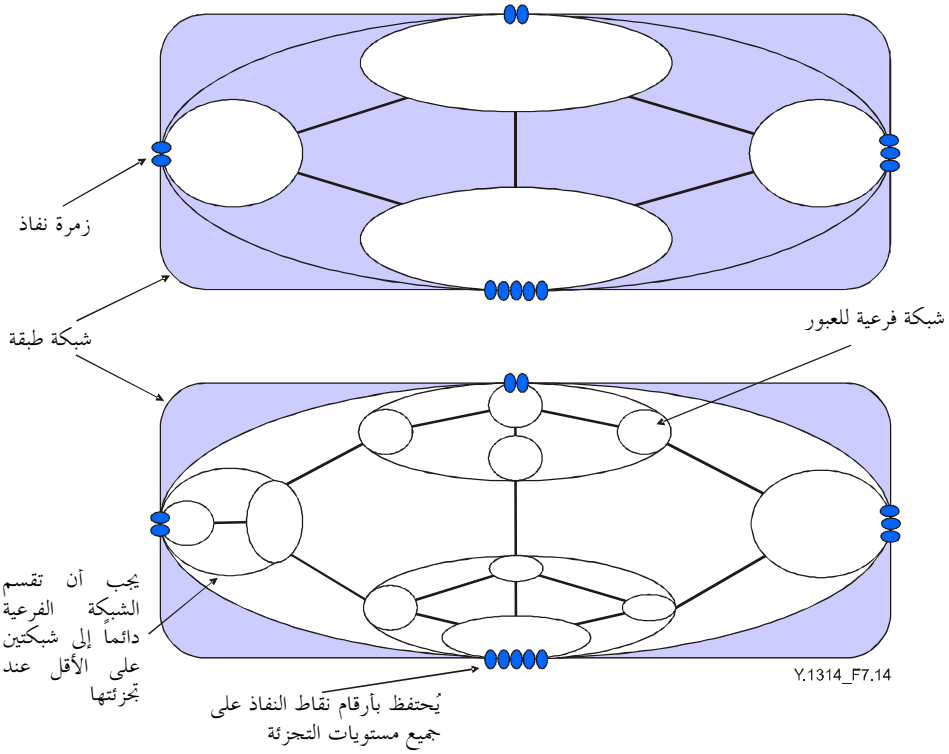

**الشكل 7-13/Y.1314 – طبقة مخدم VPN مدعومة بعدة طبقات مخدم**

وتتولى وظيفة تكييف مصدر طبقة المخدم MPLS في هذا المثال تكييف المعلومات المميزة (CI) لطبقة المخدم MPLS VPN (وهي عميل لطبقة مخدم MPLS) إلى معلومات مكيفة (AI) في طبقة مخدم MPLS، بينما تقوم وظيفة تكييف بئر طبقة المخدم MPLS بتكييف المعلومات AI لطبقة المخدم MPLS إلى معلومات CI في طبقة المخدم MPLS VPN. أما وظيفة تكييف مصدر طبقة المخدم IP، فتقوم بتكييف معلومات CI طبقة مخدم MPLS VPN إلى معلومات AI في طبقة مخدم IP، بينما تكيف وظيفة تكييف بئر طبقة مخدم IP معلومات AI طبقة مخدم IP إلى معلومات CI طبقة مخدم MPLS VPN.

## 6.7 نمذجة الشبكة VPN باستعمال التجزئة

أعِدّت النماذج الوظيفية المبينة في الفقرات السابقة بإتباع نهج مكون من طبقات. ويسمح تفكيك الشبكات إلى عدد من شبكات الطبقات المستقلة بنمذجة علاقة العميل/المخدم القائمة بين شبكات الطبقات المتجاورة وبوصف الوظائف المقابلة للتكييف والانتهاء والتشغيل البيني.

والتجزئة نهج نمذجة بديل يُستعمل لتحديد بنية الشبكة داخل إحدى شبكات الطبقة، وتعيين الحدود الإدارية/التسيير بين مجالات الشبكة، كالشبكات المملوكة مثلاً لمشغلين مختلفين. وتتيح التجزئة بتفكيك أي شبكة فرعية على مستوى معين إلى شبكات فرعية حاوية لها والوصلات الرابطة فيما بينها. ويمكن أن تستمر هذه التجزئة حتى بلوغ حد التكرار، أي بعبارة أخرى، شبكة فرعية وحيدة داخل عنصر شبكة. وتُعرف عملية التجزئة هذه بالمصفوفة التي يرد وصف لها في التوصية ITU-T G.805، ويوضحها الشكل 7-14 أدناه.

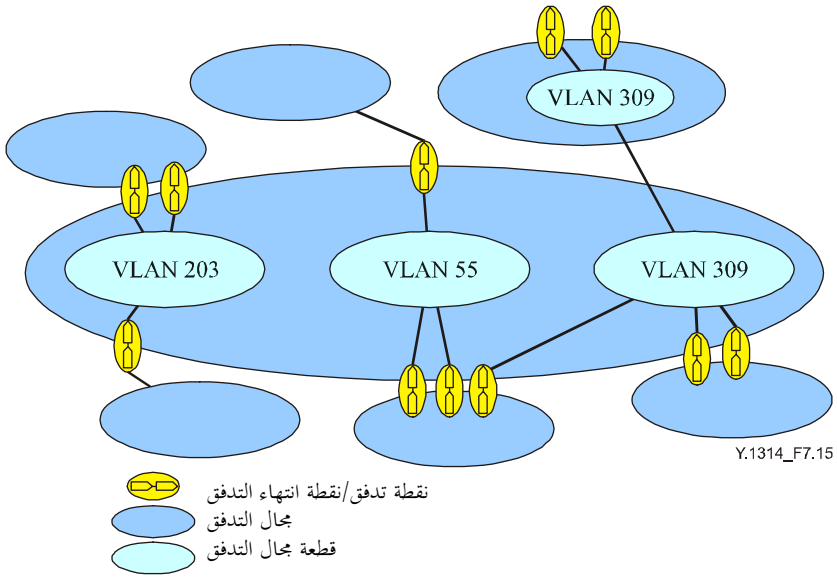



**الشكل Y.1314/14-7 – تجزئة شبكات فرعية داخل شبكة طبقة**

وكجزء من عملية التجزئة، يبقى عدد نقاط التدفق/التوصيل في الشبكة الفرعية الكبرى دون تكييف في إطار التجزئة، بينما يُكشف عن نقاط التوصيل الموجودة داخل الشبكة المذكورة على المستوى التالي للتجزئة. ويمثل (مجال تدفق) الشبكة الفرعية من منظور التوصيلية، نقطة مرونة بين حالات دخل وخرج الشبكة (كنقاط النفاذ إلى المصدر/البئر أو نقاط التدفق/التوصيل). وعموماً، يسمح ذلك بتوصيل أي دخل بأي خرج.

وهذا النموذج مناسب للشبكات العمومية التي يمكن أن يُسلم فيها بتيسر جميع الموارد من أجل استعمالها، غير أنه لا يناسب الشبكات الخاصة التقديرية. والسبب في ذلك اقتصار التوصيلية القائمة بين حالات دخل وخرج مجال الشبكة الفرعية/التدفق على حالات الدخل والخرج الخاصة بنفس الشبكة VPN. وبغية دعم نمذجة إحدى شبكات VPN بإتباع نهج التجزئة، تُستعمل تركيبات قطعة مجال التدفق (FDFr) التي يرد وصف لها في التوصية G.8010 لقطاع تقييس الاتصالات، وتركيبات توصيل الشبكة الفرعية (SNC). وتُجزّأ تركيبات القطعة FDFr/التوصيل SNC إلى قطع بتقسيم حالات دخلها وخرجها إلى زمر مختلفة. وتقتصر التوصيلية على أعضاء نفس الزمرة. وقد تكون هذه الزمرة شبكة VLAN تعمل عبر أحد جسور إثرنت (مجال تدفق إثرنت) أو شبكة VPN تعمل عبر شبكة فرعية أو مجال تدفق. ومن الملاحظ أنه ليس للقطعة نقاط تدفق؛ إذ تصاحب النقاط المذكورة مجال التدفق. ويمكن وسم القطعة FDFr/التوصيل SNC باسم شبكة طبقتها وبعدد القطع، أو

بتجميع نقاط التدفق في قطعة معينة، مثل معرف الشبكة VLAN. ويبين الشكل 7-15 مثالاً لشبكة تستعمل شبكات VLAN لتأمين عزل شبكات VPN.

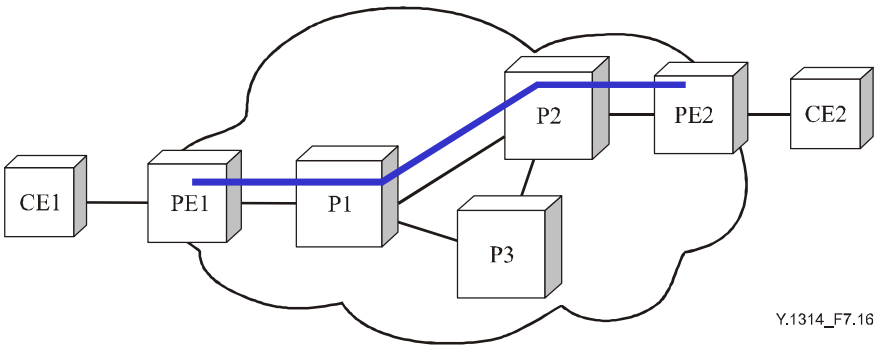



**الشكل 7-Y.1314/15 – مثال للمثال الوظيفي لتجزئة شبكات VPN**

وتتصاحب إحدى قطع FDFr لمجال تدفق واحد مع قطعة FDFr تخص مجال تدفق آخر بواسطة وصلة مكونات التوصيل البيني. وبالمثل، يتصاحب أحد توصيلات SNC لشبكة فرعية واحدة مع توصيل SNC في شبكة فرعية أخرى بواسطة توصيل وصلة التوصيل البيني. ويسمح ذلك بتجزئة التركيب أو تجميعه بما يتفق مع مثال الشبكة الفرعية. هكذا، يتسم المثال بمرونة عالية ويسمح بعرض بنية الشبكة VPN على جميع مستويات تجزئة الشبكة الفرعية.

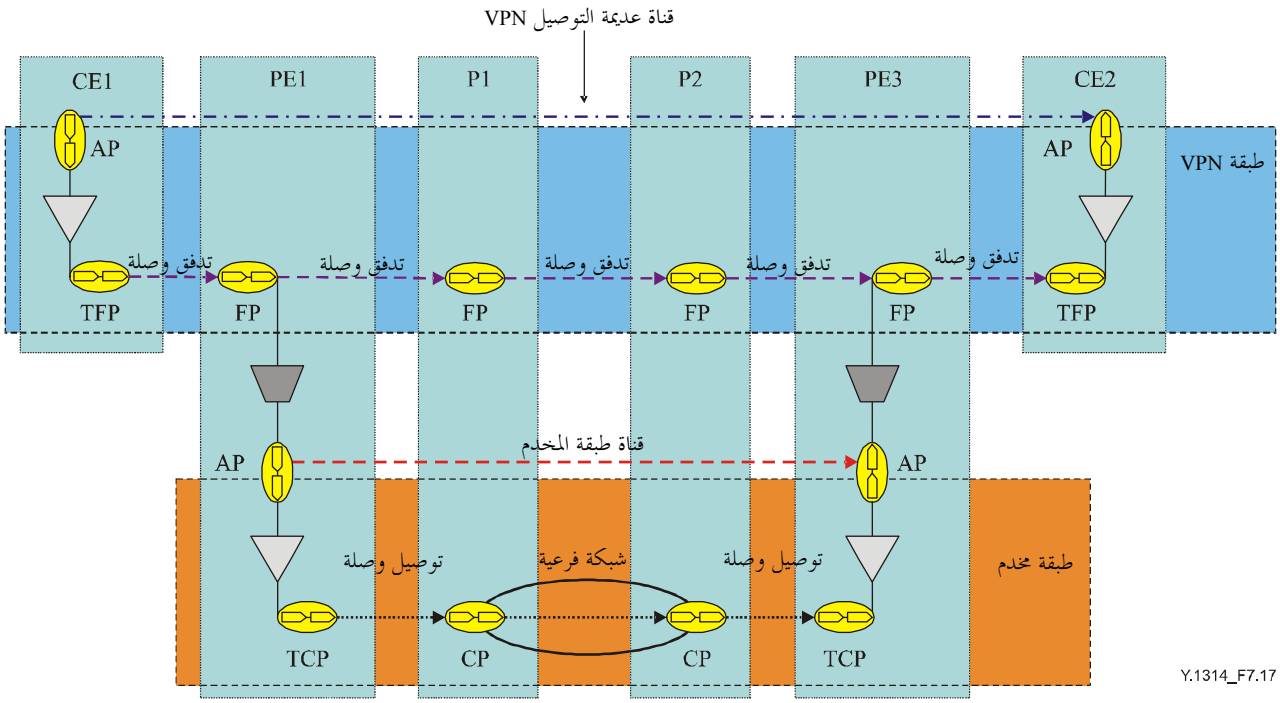
## 7.7 طبقة القرين VPN

يبين الشكل 7-16 الطوبولوجيا المادية لمستوى القرين للشبكة VPN. وتحدد سحابة الشبكة المبينة في المثال مجال الشبكة المُتقاسمة، بينما يحدد الخط الرمادي شبكة VPN من نقطة إلى نقطة (P2P). ويمكن تحقيق فصل الشبكات VPN باتباع أي نهج من النهج المُحددة في الفقرة 6، كنهج شبكة VLAN إثرنت، ونهج نفق معمارية IPsec، وما إلى ذلك.



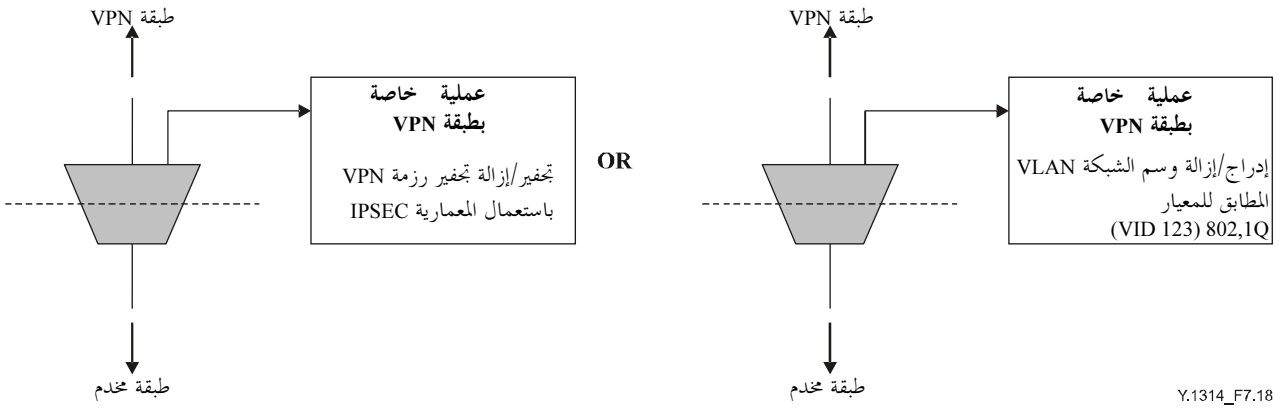

**الشكل 7-Y.1314/16 – مثال الطوبولوجيا المادية لمستوى القرين في الشبكة VPN**

ويصف الشكل 7-17 طوبولوجيا الشبكة VPN الواردة في الشكل 7-1 من منظور وظيفي يبين فيه طبقة VPN وطبقة وحيدة لمخدم أساسي بين حواف PE. وطبقة المخدم في هذا المثال موجهة التوصيل CO، ولكن يمكن أن تكون عديمة التوصيل CL أيضاً.



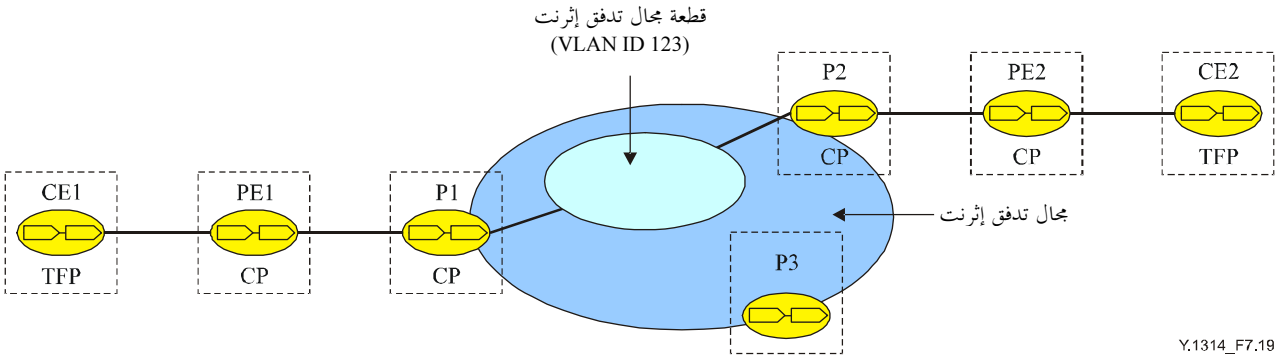

**الشكل 7-17/Y.1314 – نموذج طبقة شبكة VPN بطبقة وحيدة**

وكما يوضح الشكل 7-17، فإن جميع العقد الموجودة في الشبكة (بما فيها عقد P) تخص طبقة VPN، ولذلك يجب أن تكون قادرة على إرسال الرزم إلى المقصد الصحيح باستخدام المعلومات الواردة في رأسيات رزم الطبقة VPN. ونظراً لأن معمارية الشبكة VPN بطبقة وحيدة، فإن مثال تقسيم الشبكة إلى طبقات لا يوفر نفس الكم من المعلومات الذي يوفره عندما يُستعمل في حالة شبكة VPN العميل/المخدم. ولا يقدم نسق العرض المبين في الشكل 7-17 أي معلومات بشأن بداية الشبكة VPN ونهايتها. وثمة طريقة لإدخال هذه المعلومات تتمثل في توسيع نطاق وظائف تكييف طبقة VPN/طبقة المخدم. ويوضح الشكل 7-18 مثالين مختلفين لوظائف تكييف طبقة VPN/طبقة المخدم، أحدهما يستعمل المعمارية IPsec والآخر يستعمل وسوم VLAN إثرنت.




**الشكل 7-18/Y.1314 – زيادة وظائف تكييف طبقة VPN/طبقة المخدم**

وثمة طريقة أخرى لوصف مستوى قرين شبكة VPN تتمثل في استعمال مفهوم التجزئة الوارد في الفقرة 6.7. ويرد في الشكل 19-7 مثال يبين كيف يمكن استعمال التجزئة بهذه الطريقة.




**الشكل Y.1314/19-7 – نمذجة مستوى القرين لشبكة VPN باستعمال التجزئة**

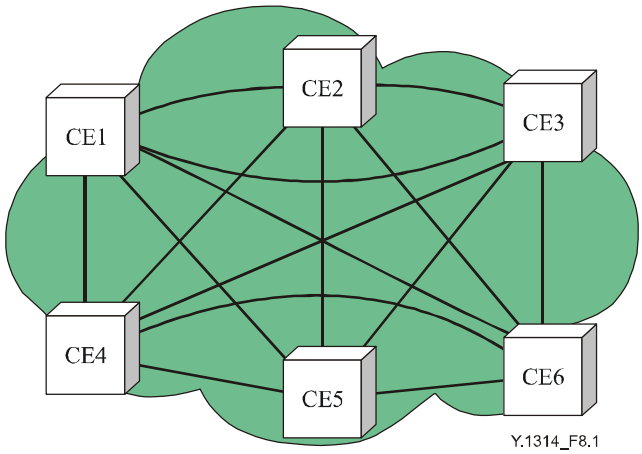
يصف الشكل 19-7 طوبولوجيا مستوى القرين شبكة VPN ويبين أيضاً الشبكة VLAN (123) المقابلة، ولكنه لا يقدم أية معلومات عن مكان بداية الشبكة VPN ونهايتها، أي، مكان إدخال/إزالة وسوم الشبكة VLAN المطابقة للمعيار IEEE 802.1Q. ومن السهل ملاحظة أن العقدتين P1 وP2 المبينتين في الشكل 19-7 تشكلان جزءاً من الشبكة VLAN 123، وعلى الرغم من أن الحافتين PE1 وPE2 هما نقطتا بدء الشبكة VPN ونهايتها، فإن المثال لا يذكر هذه المعلومات، غير أن دمج وظائف تكييف طبقة VPN/طبقة المخدم في مثال التجزئة وتوسيع نطاق المعالجة الخاصة بطبقة VPN تحديداً يمكنهما من تقديم هذه المعلومات (على النحو المبين في الشكل 18-7).

## 8 دعم طوبولوجيا الشبكة VPN

يشير تعبير 'طوبولوجيا VPN' المُستعمل في إطار هذه التوصية إلى طوبولوجيا الشبكة من منظور مستعمل الشبكة VPN، أي الطوبولوجيا الموجودة بين مواقع VPN والتي يمكن أن تكون عقد حافة المستعمل CE أو أنظمة طرفية. ولا يمكن توفير التوصيلية بين مواقع VPN إلا في حال إنشاء قنوات طبقة مخدم VPN أو قنوات طبقة القرين بين المواقع المذكورة. وعموماً، تعتمد طوبولوجيا الطبقة n على الطوبولوجيا التي توفرها قنوات طبقة المخدم عند الطبقة n-1. وبمجرد إنشاء قنوات طبقة مخدم VPN أو قنوات طبقة القرين في الحالات التي تكون فيها تكنولوجيا طبقة العميل VPN أو تكنولوجيا طبقة القرين بتبديل الرزم، فإن من الممكن حينئذ تحسين طوبولوجيا الشبكة VPN عن طريق تقييد التوصيلية بين مواقع معينة داخل الشبكة VPN. وتتمثل إحدى طرائق تقييد التوصيلية بين أعضاء الشبكة VPN في التحكم في توزيع الطرق عند طبقة العميل VPN (يتعذر على مواقع VPN التواصل فيما بينها إذا لم يكن لديها طرقاً للاتصال ببعضها بعضاً). وثمة طريقة أخرى يمكن استعمالها لتقييد التوصيلية باستخدام ترشيح الرزم (بالاستناد مثلاً إلى طبقة العميل VPN أو عناوين مصدر/مقصد طبقة القرين). والطوبولوجيات الأساسية الثلاث لشبكة VPN طوبولوجيات متشابكة كلياً ومتشابكة جزئياً وطوبولوجيات على شكل نجمة (رئيسية وفرعية)، ويرد وصف لها في الفقرات 1.8 و2.8 و3.8 أدناه.

## 1.8 طوبولوجيات VPN المتشابكة كلياً

لكل موقع شبكة VPN في طوبولوجيا VPN المتشابكة كلياً طريق/توصيل يؤدي إلى جميع مواقع VPN الأخرى، مثلما يبين ذلك الشكل 1.8.

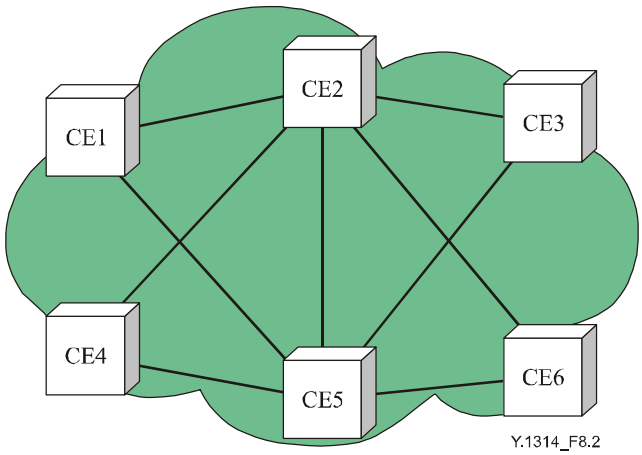



**الشكل Y.1314/1-8 – مثال لطوبولوجيا VPN المتشابكة تماماً**

وتوفر هذه الطوبولوجيا المتشابكة كلياً إطناباً كاملاً، كما يمكنها أن تؤمن فعالية الاستفادة من الشبكة وتحقق كفاءة أدائها لأن بإمكان مواقع VPN أن تستعمل أقصر/أفضل المسيرات/الطرق للاتصال ببعضها بعضاً. وثمة عيب يشوب نهج الطوبولوجيا المتشابكة تماماً وهو احتمال ارتفاع تكلفة تنفيذ التشابك الكامل، مع أن هذا الأمر يتوقف على ما هو مُطبق من أساليب/تكنولوجيات الشبكة VPN (فمن المُحتمل مثلاً أن تكون شبكة VPN المكونة من دارات/قنوات تقديرية (VC) بأسلوب ATM كاملة التشابك أعلى تكلفة من شبكة VPN إثرنت التي تدعم التوصيلية من أي نقطة إلى أي نقطة). وهناك عيب آخر هو أنه بالنظر لزيادة عدد المواقع في التشابك الكامل، فإن عدد التوصيلات/الطرق ومستويات التحكم المتجاورة يزداد أيضاً على نحو يتناسب مع زيادة عدد المواقع (عدد التوصيلات في التشابك الكامل هو $n(n-1)/2$، حيث n عدد مواقع VPN). ويؤدي دعم أعداد كبيرة من التوصيلات/الطرق ومستويات التحكم المجاورة إلى إثارة مشاكل تتعلق بالقياس بسبب زيادة عرض النطاق وموارد وحدة المعالجة المركزية (CPU) اللازمة.

## 2.8 طوبولوجيات VPN المتشابكة جزئياً

لمواقع الشبكة VPN الموجودة في طوبولوجيا VPN المتشابكة جزئياً، طرق/توصيلات ببعض مواقع VPN الأخرى وليس جميعها. ويبين الشكل 2.8 مثالاً لطوبولوجيا متشابكة جزئياً.

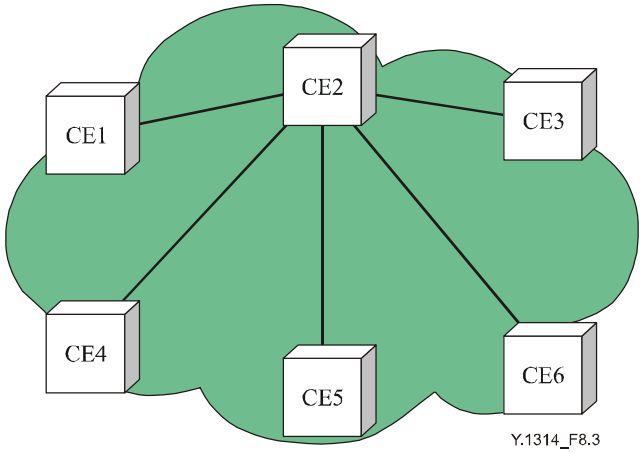



**الشكل Y.1314/2-8 – مثال لطوبولوجيا VPN المتشابكة جزئياً**

ويتسنى لمواقع VPN في بعض الحالات الوصول إلى مواقع VPN أخرى ليس لها طرق/توصيلات مباشرة تؤدي إليها بواسطة مواقع عبور VPN. غير أنه قد يتعذر في الحالات الأخرى الاتصال بين مواقع VPN إذا لم يكن لهذه المواقع طرق/توصيلات مباشرة للوصول إلى بعضها بعضاً. وتتوقف قدرة الاتصال بين العقد التي ليس لها طرق/توصيلات للوصول إلى بعضها بعضاً، على وجود قنوات طبقة المخدم VPN أو قنوات طبقة القرين، وعلى وجود أية قيود على توصيلية الطوبولوجيا (كسياسات التسيير أو مراشيح الرزم). والطوبولوجيات المتشابكة جزئياً قابلة للقياس أكثر من الطوبولوجيات المتشابكة كلياً بسبب تقليل عرض النطاق وموارد وحدة المعالجة المركزية (CPU) اللازمة، وإن كان ذلك يتم على حساب التسيير الأمثل وفعالية استخدام الشبكة (في حال استعمال بعض حواف المشتركين (CE) كعقد للعبور). ويُخفض أيضاً إطناب الشبكة، مع أن الشبكات المتشابكة جزئياً عادة ما تُصمم بطريقة يتسنى فيها استعمال الطرق/التوصيلات البديلة في الحالات التي تمس الحاجة إليها. ففي الشكل 8-2 مثلاً، يمكن أن تكون العقد CE والعقدتين CE2 وCE5 عقد مركزية بينما يمكن أن تكون عقد حافة المستعمل CE الأخرى عقد طرفية. والعقد الطرفية في هذه الحالة المتعلقة بهذه الطوبولوجيا عقد لها توصيلات/طرق اطنابية لتصل إلى المركز. وغالباً ما يُجبر المشتركون على استعمال طوبولوجيات التشابك الجزئي بسبب عوامل من قبيل التكلفة (أي أن شبكات التشابك الكلي أعلى تكلفة) وبسبب القيود الجغرافية.

## 3.8 طوبولوجيات VPN المركز والفروع (شكل النجمة)

يمكن أن يكون موقع VPN في طوبولوجيا VPN ذات المركز والفروع (أو النجمة) إما فرعاً أو مركزاً لشبكة VPN معينة (ومع ذلك، إذا كان موقع VPN يخص العديد من شبكات VPN فإنه يمكن أن يكون مركزاً لشبكات VPN معينة وفرعاً لشبكات أخرى). ولجميع الفروع الموجودة في طوبولوجيا المركز والفرع طرق/توصيلات مباشرة للوصول إلى المركز، ولكن ليس لهذه الفروع طرق/توصيلات مباشرة للوصول إلى بعضها بعضاً. ويبين الشكل 8-3 مثالاً لطوبولوجيا المركز والفروع تمثل فيها عقدة CE2 المركز بينما تمثل جميع عقد CE الأخرى الفروع.




**الشكل Y.1314/3-8 – مثال لطوبولوجيا VPN المركز والفروع**

ويمكن في بعض الحالات تشكيل المركز كعقدة عبور ليتسنى للفروع الاتصال ببعضها بعضاً من خلال المركز، غير أنه قد لا يُسمح في حالات أخرى بتنفيذ التوصيلية بين عقد الفروع. ويتمثل أحد الاستعمالات الشائعة لطوبولوجيا المركز والفروع في توصيل المكاتب (الفروع) بمقر الشركة (المركز). ويسمح استعمال هذه الطوبولوجيا باستخدام موارد الشبكة المركزية (كالنفاذ إلى الإنترنت، والجدار الناري (Firewalls)، ومخدمات البريد الإلكتروني)، مما يمكن أن يؤدي إلى تقليل التكاليف مقارنة بإتباع نهج توزيع موارد الشبكة.

# 9 اعتبارات بشأن نوعية خدمة (QoS) الشبكة VPN

يوجد عدد كبير من مصادر المعلومات المتعلقة بنوعية الخدمة (QoS)، وتحوي تعاريف مختلفة لما تعنيه نوعية الخدمة في الواقع. وتعرِّف التوصية ITU-T E.800 هذه النوعية على أنها التأثير الجماعي لحالات أداء الخدمة التي تحدد مدى ارتياح المستعمل

للخدمة المقدمة. وتوفر التوصية ITU-T G.1000 إطاراً معيناً وتعاريف لنوعية خدمة الاتصالات، أما التوصية ITU-T G.1010، فتحدد مثالاً لفئات نوعية خدمة الوسائط المتعددة من وجهة نظر المستعمل النهائي. وتعتمد الوظائف اللازمة لتلبية متطلبات نوعية الخدمة المُحددة في هذه التوصيات وفي أماكن أخرى على أسلوب تشغيل الشبكة. ولذلك، يمكن أن تؤثر متطلبات نوعية الخدمة على اختيار مورد خدمة VPN لتكنولوجيا طبقة المخدم VPN وتكنولوجيات طبقة العميل VPN التي يمكن دعمها.

## 1.9 شبكات طبقة تبديل الدارات

يُنشأ في شبكات طبقة تبديل الدارات وموجهة التوصيل، مسير يقوم على وصلة مادية، أو على طول موجة بصرية، أو دارة/قناة تقديرية بتراتب رقمي متزامن (SDH)/شبكة بصرية متزامنة (SONET)، أو فاصل زمني بتعدد الإرسال بتقسيم الزمن (TDM) ويُخصص المسير لتوصيل وحيد بين نقاط النفاذ (AP) الموجودة في الشبكة طيلة مدة التوصيل. وعند طلب إنشاء توصيل جديد، يجب أن تقرر الشبكة ما إذا كانت تقبل التوصيل أم لا؛ وفي حال قبوله، ما هو السبيل المُتبع في تسييره عبر الشبكة وما هي الموارد المحجوزة للتوصيل. وتستعمل آليات للتحكم في قبول التوصيلات (CAC) لقبول توصيل ما إذا تيسر عرض النطاق، أو رفضه في الحالات التي يتجاوز فيها عرض نطاق التوصيل المطلوب عرض النطاق المُتيسر.

وترسل البيانات بمعدل بتات ثابت وبنفس الترتيب الذي أرسِلت به تماماً. ويمكن إنشاء التوصيلات يدوياً باستخدام التزويد السكوني، أو دينامياً باستعمال آليات تشوير أو أدوات تزويد أوتوماتية. وتتوقف إمكانية إنشاء توصيلات جديدة على ملكية الشبكة لسعة احتياطية. وفي حال إنشاء التوصيل، يكون تسليم البيانات عبره مضمون.

ومهلة التأخر في شبكات تبديل الدارات موجهة التوصيل (CO-CS) كالشبكة الهاتفية العمومية التبديلية (PSTN)، هي أساساً دالة مسافة الإرسال. وتكون مهلة تأخر التبديل في عقد شبكات CO-CS قصيرة نسبياً إذا قُورِنت بمهلة (انتشار) الإرسال، ولاسيما عندما تجتاز القريناءات دارات طويلة المسافة.

## 2.9 شبكات طبقة تبديل الرزم

تُرسل الرزم عبر شبكات تبديل الرزم بالاستناد إلى المعلومات الواردة في رأسية الرزمة. ويؤمن تبديل الرزم التوصيلية والاستخدام الفعال لموارد الشبكة عن طريق تقاسمها مع الكثير من المستعملين (على أساس الافتراض القاضي بعدم ضرورة استخدام المستعملين لكافة الموارد طوال الوقت). ويمكن وصف سلوك إرسال الرزم إلى التدفقات أو التوصيلات بمجموعة معلمات تُسمى واصفات الحركة. وتشمل أمثلة واصفات الحركة متوسط معدل الرزم/البتات، والحد الأقصى لطول الرشقة/حجم الرزمة، واحتمال وصول الرزمة في غضون فاصل زمني مُحدد. ويُعبر غالباً عن متطلبات نوعية المستعمل بمصطلحات مثل خسارة رزمة مقبولة ومهلة التأخر والارتعاش.

ويمكن استعمال آليات تشكيل الحركة لتنظيم مقدار الحركة المسموح له بدخول الشبكة والذي يُضبط عموماً على أساس كل صف انتظار/تدفق، أو كل توصيل، أو كل سطح بيني. ويمكن أن يحدث الازدحام في الشبكات القائمة على الرزم إذا تجاوز حجم الحركة قدرات إرسال أحد كيانات الشبكة (NE) أو تجاوز سعة الشبكة المتيسرة. وعندما تزدحم الشبكة، يمكن تخزين الرزم في الذاكرة الوسيطة، مما يؤدي إلى تأخر، أو يمكن إهمالها.

وتعتمد مهلة التأخر في شبكات تبديل الرزم على مسافة الإرسال المصاحبة لطبقة المخدم المادية والتحتية، زائداً عدد من العوامل الأخرى على طبقة تبديل الرزم. وتشتمل العوامل التي تسبب مهلة التأخر على طبقة تبديل الرزم على حجم الرزمة، وسرعة الوصلة، ومهلة تأخر الإرسال في كل قفزة (والتي يمكن تقسيمها إلى مهل ترزيم، ومهل انضغاط/إزالة الانضغاط، ومهل تبديل/تسيير، ومهل تخزين في الذاكرة الوسيطة)، وعدد القفزات. و التحكم في الأولويات مطلوب في الشبكات القائمة على الرزم من أجل ضمان الحصول على طائفة متنوعة من مستويات النوعية. ويطبق عموماً التحكم في الأولويات باستعمال صفوف انتظار منفصلة لكل توصيل، أو لكل تدفق، أو لكل صنف من أصناف نوعية الخدمة (QoS) عند كل

سطح بيني، والتحكم في أولوية كل صف انتظار. وتُستعمل آليات جدولة الرزم لتوزيع الرزم على صف انتظار معين وفقاً لسياسات معينة.

### 1.2.9 شبكات طبقة تبديل الرزم وموجهة التوصيل

تُنشأ التوصيلات في شبكات طبقة تبديل الرزم وموجهة التوصيل ويُحتفظ بهذه التوصيلات حتى تنتفي الحاجة إلى هذه التوصيلية (بصرف النظر عما إذا كانت البيانات قد أرسِلت أم لا). وكما هو الحال تماماً مع شبكات طبقة تبديل الدارات وموجهة التوصيل، يمكن في هذه الحالة أيضاً إنشاء التوصيلات بواسطة التزويد اليدوي، أو أحد أنظمة الإدارة، أو أحد بروتوكولات التشوير. وبالإمكان تحديد الحالة الراهنة للشبكة عن طريق مراقبة مدى استخدام موارد الشبكة و/أو من خلال تحديد خصائص سلوك التوصيلات المسموح لها بالفعل بدخول الشبكة. ويمكن استعمال آليات التحكم في قبول التوصيلات (CAC) لحجز عرض نطاق ذروة التوصيل اللازم للحصول على مصادر حركة بمعدل بتات ثابت (CBR). ويمكن بدلاً عن ذلك استعمال مخططات إحصائية لتعدد الإرسال مع آليات التحكم CAC لتخصيص عرض نطاق أقل من عرض نطاق الذروة اللازم لزيادة كفاءة الشبكة. ومع ذلك، يمكن أن يكون تحديد خصائص عرض النطاق اللازم صعباً، لأن عرض النطاق هذا قد يتباين بشكل كبير بمرور الوقت.

وفي حال تقديم الدعم لخدمات النقل بمعدل بتات ثابت (CBR) (دون الإفراط في الاشتراك) عبر شبكات تبديل الرزم موجهة التوصيل (CO-PS) (كشبكات ATM)، يبقى تأخر الإرسال في كل قفزة ثابت، وعليه، يمكن حساب/ضمان المهلة/الارتعاش. غير أنه إذا جرى الإفراط في حجز الخدمات لزيادة استعمال الشبكة (كما هو الحال عادة)، حينئذ تدخل مهل التأخر/الخسارة العقد المزدحمة نتيجة تخزين الحركة غير المُتعاقد عليها داخل الذاكرة الوسيطة أو إهمالها. وبرغم تباين مهل تأخر الإرسال في كل قفزة، تبقى العوامل الأخرى ثابتة من قبيل سرعة الوصلات ومسافات/وعدد القفزات (وحجم الرزمة في حالة أساليب ATM).

### 2.2.9 تبديل الرزم عديمة التوصيل

ما إن تُرسَل البيانات عبر شبكات تبديل الرزم عديمة التوصيل حتى ينقطع التوصيل لحين إرسال أو استقبال المزيد من المعلومات (يمكن النظر إلى أي رزمة على أنها توصيل يُنشأ أثناء المدة الزمنية المُستغرقة في إرسال الرزمة واستقبالها). ولا توجد حالة توصيل مخزونة، وبالتالي، لا داعي أن تتبع الرزم المتعاقبة نفس المسير أو تصل بالترتيب الذي أرسِلت به. وتُرسل الحركة بمعدل بتات متباين وعادة ما تُخصص الموارد حسب الحاجة بالاستناد إلى مبدأ أولوية تقديم الخدمة للقادم أولاً.

وفيما يخص شبكات تبديل الرزم عديمة التوصيل (CL-PS) (كشبكات بروتوكول الإنترنت (IP))، تتباين عوامل تحديد مهل التأخر كحجم الرزمة، وسرع الوصلات، وعدد القفزات، ومهل تأخر الإرسال في كل قفزة، خصوصاً عند استعمال تقنيات معينة لموازنة الحمولة. ويمكن تطبيق تحديد معدل البتات/تشكيل الحركة عند الحافة لتحديد مقدار الحركة الداخلة إلى الشبكة، ولكن بالنظر إلى طبيعة التسيير من أي نقطة إلى أي نقطة الذي تتسم به الحركة في شبكة الرزمة CL-PS (وزيادة التشغيل البيني من قرين إلى قرين)، فإن من الصعب التنبؤ بعرض النطاق المُستعمل في كل وصلة عبر شبكة CL-PS ككل. ويمكن استخدام مراقبة الحركة بالإضافة إلى تقنيات النمذجة لإعداد مصفوفة الحركة، ومن ثم يمكن إدخال تعديلات نهائية على مصفوفات بروتوكول البوابة الداخلية (IGP) لتوفير زيادة استعمال الوصلة، ولكن نظراً لأن حركة CL-PS تتسم بطابع رشقي وغير قابل للتنبؤ، فإن الأسلوب الأبسط/الأكثر أمناً الذي يُكفل بموجبه استيفاء ضمانات الخدمة هو الإفراط في تزويد الشبكة.

ومع ذلك، وحتى عند اللجوء إلى الإفراط في التزويد، فإن العقد/الوصلات الموجودة في شبكة CL-PS يمكن أن تصبح مزدحمة بسبب الطابع غير المحدد للحركة عديمة التوصيل، ولا سيما في حالة تعطل الوصلة/العقدة أو هجمات رفض الخدمة (DoS). كما أن تأثير تعطل الوصلة/العقدة لا يقتصر على الحركة التي تجتاز الوصلة/العقدة المتعطلة، إذ يمكن أن تسبب إعادة التسيير ازدحاماً في أماكن أخرى من الشبكة. ويتمثل النهج الشائع لحماية الحركة الأولية من ازدحام الشبكة في استعمال صفوف الانتظار ذات الأولوية (كتلك المستندة إلى معمارية بروتوكول الإنترنت (IP) للخدمات المتميزة والمتفقة مع

المعيار RFC 2475) بغية التحكم في سلوك الإرسال بالنسبة لكل صنف، أي تتمتع الحركة الأعلى أولوية بمعاملة تفضيلية على الحركة الأدنى أولوية. ويسمح ذلك لمورد الخدمة بتقديم خدمات متعددة المستويات للمشتركين (كالخدمة المتميزة، والخدمة في الوقت الفعلي، وأفضل خدمة) وتسعير الخدمات بناءً على ذلك. ومن عيوب نهج الخدمات المتميزة (Diffserv) هو أنه لا يمكن حجز عرض النطاق إلا على أساس تجميعي، ولذلك، يتعذر ضمان التدفقات الفردية داخل التجميع.

ويوجد نهج بديل (أو تكميلي) يتمثل في استعمال معمارية الخدمات المتكاملة (تستند إلى المعيار RFC 1633) يُستعمل فيها بروتوكول حجز الموارد (RSVP, RFC 2205) لحجز السعة على امتداد مسير ما من طرف إلى طرف عن طريق تشوير متطلبات التدفق قبل إرسال الرزم. ونظراً لأن بالإمكان حجز عرض النطاق على أساس كل تدفق، فإن من الممكن توفير التوريد المضمون للتدفقات الفردية. وتكرر هذه العملية مثال التحكم في قبول التوصيلات (CAC) المُستعمل في شبكات التوصيل (CO) التي لا تُرسل فيها الحركة حتى يتم تنفيذ التحكم CAC من أجل ضمان توفير سعة كافية في الشبكة. ويتمثل العيب الرئيسي لهذا النهج في أنه يلقى عبء معالجة كبير (لبروتوكول حجز الموارد (RSVP)) على المسيّرات المركزية مما يزيد بالتناسب مع عدد تدفقات الرزم التي تتطلب حجز الموارد.

وهناك نهج آخر يدعم حجز الموارد على أساس كل تدفق يتمثل في استعمال مسيّرات قائمة على التدفق. وهي مسيّرات يُحتفظ بها في كل حالة تدفق ولا تقبل سوى التدفقات الجديدة في حال تيسر موارد كافية. وكما هو الحال مع بروتوكول حجز الموارد (RSVP)، فإن التحدي الذي يواجه هذا النهج هو زيادة حمولات المعالجة بزيادة عدد التدفقات. ومع ذلك، تتوفر اليوم مسيّرات تدعم بالفعل التسيير على أساس كل تدفق فيما يخص أعداداً كبيرة من التدفقات.

## 10 الوظائف المطلوبة لإنشاء شبكات VPN العميل/المخدم

عند إنشاء شبكات VPN العميل/المخدم، يجب التقيد بترتيب الأحداث بدقة. ولا يمكن إنشاء تدفقات/توصيلات طبقة العميل VPN حتى تُنشأ تدفقات/توصيلات طبقة المخدم VPN. وبالمثل، يتعذر إنشاء تدفقات/توصيلات طبقة المخدم VPN لحين إنشاء تدفقات/توصيلات طبقة العميل VPN (التي تُعتبر طبقة المخدم VPN عميلها). ويُعزى ترتيب إنشاء التدفقات/التوصيلات إلى واقع إن طوبولوجيا طبقة العميل تُحدد بموجب طوبولوجيا طبقة المخدم التحتية، وهي طبقة متكررة حتى المجرى.

### 1.10 إنشاء طبقة المخدم VPN

بافتراض أن طوبولوجيا طبقة المخدم التحتية قد أنشِأت وأن نقاط TFP/TCP ونقاط FP/CP طبقة المخدم VPN قد شُكِّلت بعناوين، فإن هناك ثلاث خطوات رئيسية يُضطلع بها عند إنشاء توصيلية طبقة المخدم VPN بين أعضاء طبقة العميل VPN، وهي كما يلي:

**الخطوة 1:** اكتشاف أعضاء الشبكة VPN وتخزين معلومات عضوية VPN.

**الخطوة 2:** حساب الطرق بين أعضاء الشبكة VPN وطبقة المخدم VPN.

**الخطوة 3:** إنشاء توصيلات/أنفاق/شبكات VLAN بين أعضاء الشبكة VPN في طبقة المخدم VPN.

ويصف الجدول 10-1 بمزيد من التفصيل كل وظيفة من الوظائف اللازمة لدعم إنشاء طبقة المخدم VPN وصيانتها إلى جانب الكيانات الوظيفية الفردية.

**الجدول Y.1314/1-10 – وظائف طبقة المخدم VPN**

| الوظيفة | الكيانات الوظيفية | عناصر الشبكة | أسلوب طبقة المخدم VPN |
|---|---|---|---|
| اكتشاف عضوية الشبكة VPN | اكتشاف أعضاء الشبكة VPN (نقاط FP/CP طبقة العميل VPN المنتمية لنفس شبكة VPN) | PE | الكل |
| | توزيع/جمع المعلومات المتعلقة بعضوية الشبكة VPN (بما في ذلك المنضمون، المغادرون، التيسر) | PE | الكل |
| | الحفاظ على المعلومات المتعلقة بعضوية الشبكة | PE | الكل |
| | تقابل نقاط FP/CP طبقة العميل VPN مع نقاط AP طبقة المخدم VPN | PE | الكل |
| تسيير طبقة مخدم الشبكة VPN | توزيع/جمع المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/موارد طبقة المخدم VPN | P، PE | الكل |
| | الحفاظ على المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/موارد طبقة المخدم VPN | P ، PE | الكل |
| | حساب أفضل طريق (طرق) بين نقطة نفاذ AP طبقة المخدم VPN | P ، PE | الكل |
| إنشاء أنفاق/توصيلات طبقة مخدم الشبكة VPN | التحكم في قبول التوصيلات (CAC) | P ، PE | الكل |
| | الإشعار بنجاح/فشل طلب إنشاء التوصيل/النفق | P ، PE | الكل |
| | تخصيص وتشكيل مجالات تعدد إرسال طبقة المخدم VPN | P ، PE | الكل |
| | توزيع المعلومات المتعلقة بالتوصيلات/الأنفاق، كنوعية الخدمة (QoS)، مجالات إزالة تعدد الإرسال، عرض النطاق، وما إلى ذلك | P ، PE | الكل |

### 1.1.10 اكتشاف عضوية الشبكة VPN

من أجل إنشاء طوبولوجيا طبقة المخدم VPN بين حافات PE، من الضروري أولاً تحديد الحواف PE الموصولة بحواف المشترك CE التي تعتبر أعضاء في شبكة VPN عميل/مخدم معينة. ويمكن أن يؤدي هذه الوظيفة يدوياً أي مشغل (بشري) بالاستناد إلى طوبولوجيا الشبكة المعروفة. ويمكن بدلاً من ذلك أداء الوظيفة المذكورة دينامياً بواسطة مخدم/نظام مركزي أو بروتوكول مُوزع من أجل أتمتة/تبسيط عملية التزويد. وبغية دعم الاكتشاف الدينامي، يجب تشكيل حواف المورد PE بمعرفات VPN للدلالة على توصيلها بحافة واحدة أو أكثر من حافة CE التابعة لشبكة VPN معينة. وثمة مثال على مخدم/نظام مركزي لاكتشاف العضوية يتمثل في استعمال مخدم استيقان (كخدمة الاستيقان عن بعد لمستعمل المراقمة الداخلية (RADIUS)) لتوزيع المعلومات المتعلقة بأعضاء شبكة VPN كجزء من عملية استيقان العميل. وهناك مثال على البروتوكول المُوزع هو استعمال بروتوكول بوابة الحد (BGP) في شبكات VPN المطابقة للمعيار RFC 2547، والذي يستعمل أهداف طرق كمعرفات الشبكة VPN لضمان ألا تستقبل حافة الموارد PE سوى معلومات تخص شبكات VPN التي تُعد حواف المورد PE أعضاء فيها.

### 2.1.10 تسيير طبقة المخدم VPN

إذا كانت طبقة المخدم التحتية (الواقعة أسفل طبقة المخدم VPN) والواصلة بين نقاط انتهاء طبقة مخدم VPN المصدر/البئر طبقة تمثل توصيلاً/تدفقاً أحادياً بقفزة واحدة من نقطة إلى نقطة (P2P)، فلا داعي حينئذ لتنفيذ أي تسيير نظراً لتيسر طريق/مسير واحد فقط. ومن جهة أخرى، إذا تيسرت مسيرات/طرق بديلة عبر العقد الوسيطة إلى نفس المقصد، أو إذا

كانت طبقة المخدم التحتية توفر طوبولوجيا توصيل من نقطة إلى عدة نقاط (P2MP)[4]، ينبغي عندئذ تطبيق التسيير عند طبقة المخدم VPN من أجل اكتشاف الطوبولوجيا و/أو حساب أفضل طريق (طرق) مؤدي إلى المقصد.

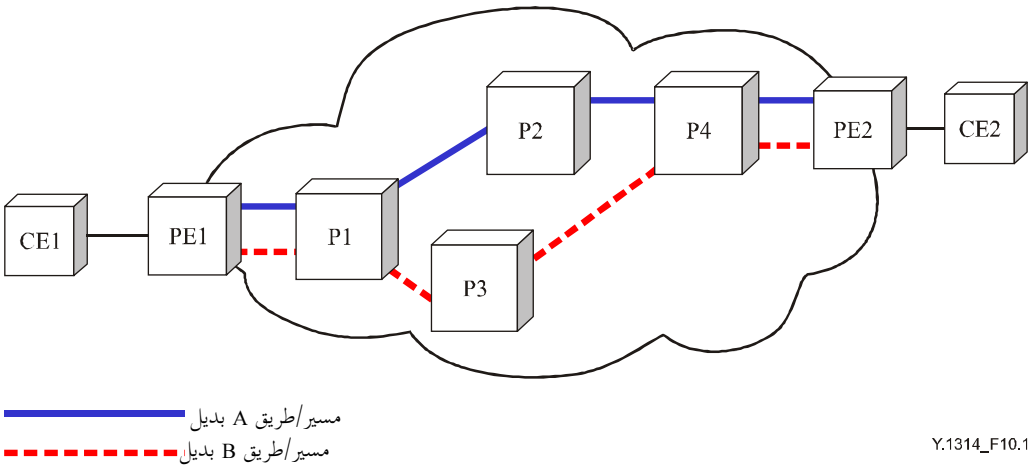
### 1.2.1.10 الحاجة إلى التسيير

لا يمكن إجراء التشوير في حالة شبكات طبقة التوصيل CO إلا بعد حساب الطريق/المسير عند طبقة معينة. ومن المتعذر في حالة شبكة الطبقة عديمة التوصيل CL إرسال الرزم إلا بعد حساب/تشكيل طريق معين يؤدي إلى المقصد. وهذا لا يعني أنه ينبغي أن يكون لكل عقدة في الشبكة طريق واضح يؤدي إلى سائر العقد في الشبكة. ويستعمل عادة تلخيص عناوين الشبكة بالاقتران مع تراتب مجالات التسيير من أجل تحسين قابلية القياس. ويتمثل الشكل النهائي لتلخيص العناوين في استعمال طرق مشكّلة بالتغيب يمكن استخدامها كآلية 'التقاط شامل' لإرسال أي رزمة بصرف النظر عن عنوان مقصدها.

وثمة استثناء على القاعدة القاضية بتعذر إرسال رزمة CL لحين حساب طريق معين (أو تشكيل تسيير بالتغيب)، وهو عندما تكون تكنولوجيا CL قادرة على الإذاعة. والإذاعة تعبير يشير إلى تكرار الرزم وإرسالها بعناوين مقاصد مجهولة عبر جميع قنوات طبقة المخدم داخل الطوبولوجيا (باستثناء القناة التي تستلم الرزمة عبرها). وإثرنت مثال على تكنولوجيا تؤدي هذا العنصر الوظيفي. وهناك استثناء آخر على القاعدة يتمثل في طريقة تشغيل شبكة العلامة الحلقية. وعندما تستلم عقدة في شبكة العلامة الحلقية رزمة ما، فإنها تعيد إرسال الرزمة إلى العقدة التالية في الحلقة حتى تعود إلى عقدة المصدر التي أزيلت منها. وتحتفظ عقدة المقصد بنسخة من الرتل وتشير إلى أنها استلمت الرتل وذلك بضبط بتات الاستجابة في الرتل. وبرغم وجود تكنولوجيات لا تتطلب التسيير، يجدر ملاحظة أن هذه التكنولوجيات لا تتسم بمثالية تكنولوجيات طبقة المخدم VPN. وبغية تمكين شبكات الطبقة من التدرج في تغطية الأعداد الكبيرة من العقد الموزعة على مساحة جغرافية واسعة، فإن التسيير وبنى العناوين التراتبية تعتبر من المتطلبات الأساسية لتحقيق ذلك. واستعمال آليات من قبيل الإذاعة وتمرير العلامة استعمال غير آمن من حيث طبيعته من منظور الشبكة VPN وهي آليات غير فعالة لإرسال حركة البث الأحادي (من نقطة إلى نقطة (P2P)).

### 2.2.1.10 مثال لطوبولوجيات الشبكة التي تتطلب التسيير

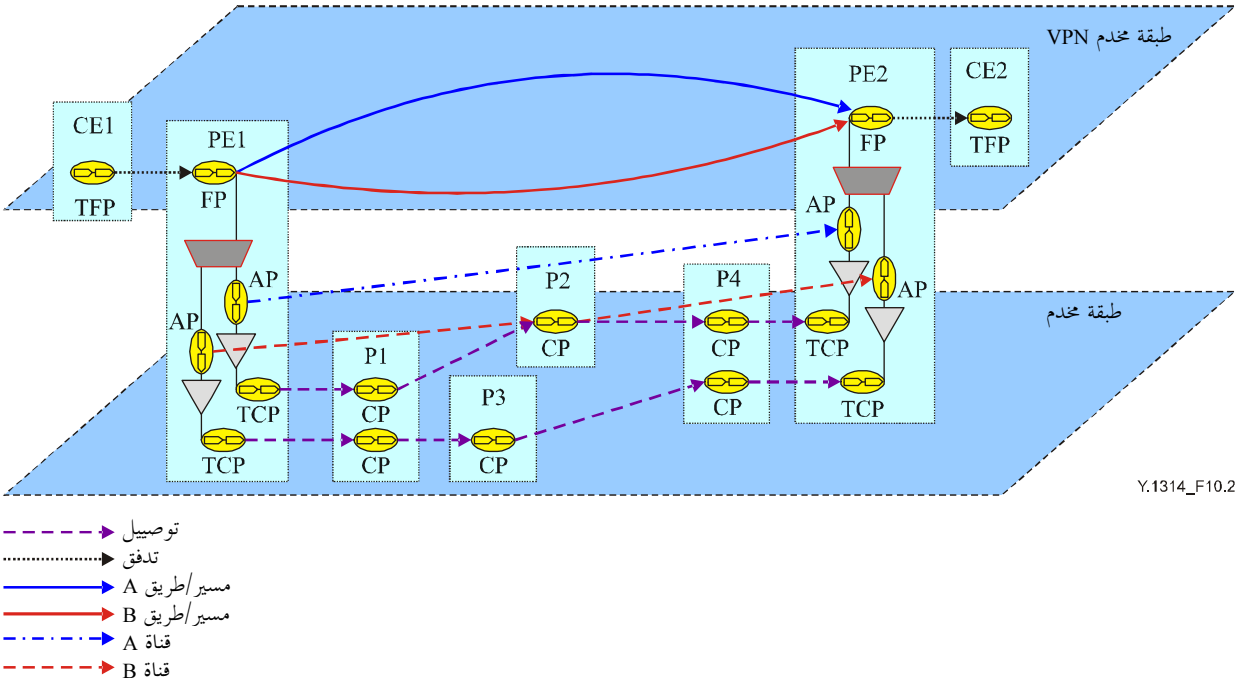
يبين الشكل 10-1 مثالاً لشبكة تحوي طريقين/مسيرين ممكنين هما (A وB) يؤديان إلى ذات المقصد.




**الشكل Y.1314/1-10 – مثال لعدة طرق/مسيرات مؤدية إلى ذات المقصد**

[4] تحيل الإشارة إلى التوصيل P2MP هنا إلى طوبولوجيا طبقة المخدم الخارجة من منظور مصدر وحيد بحافة PE. ويمكن أن تكون طوبولوجيا شبكة طبقة المخدم الشاملة الفعلية طوبولوجيا توصيل من أي نقطة إلى أي نقطة بالاستناد إلى تشابك تام/جزئي للتدفقات/التوصيلات الثنائية الاتجاه بين حافات PE.

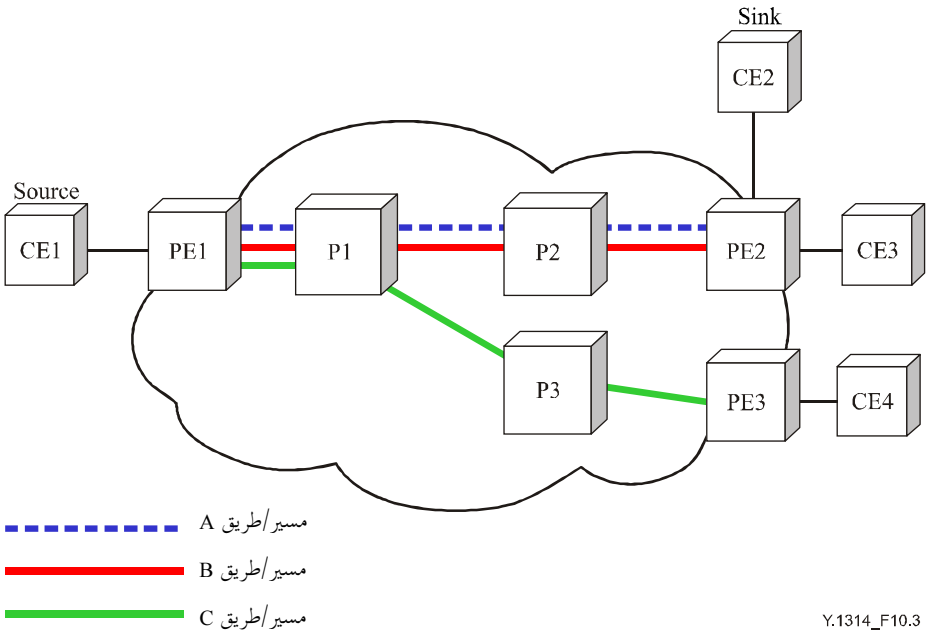
وكما يبين الشكل 10-1 أعلاه، فإن الطريق A بين الحافة CE1 والحافة CE2 يمر عبر الحافة PE1 والنقاط P1 وP2 وP4 والحافة PE2، بينما يمر الطريق B عبر الحافة PE1 والنقاط P1 وP3 وP4 والحافة PE2. ويبين الشكل 10-2 هذه المعلومات في المثال الوظيفي الوارد في الشكل 10-2.




**الشكل Y.1314/2-10 – مثال وظيفي لطرق/مسيرات متعددة**

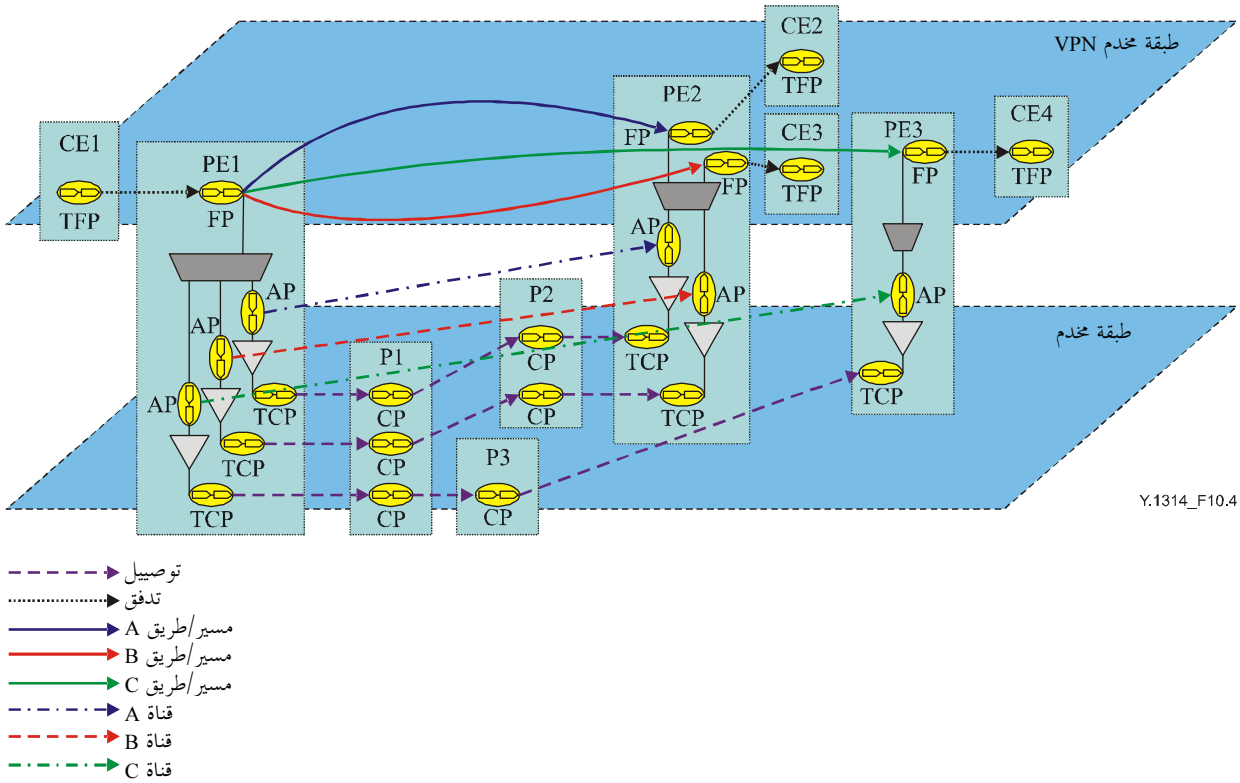
ويوضح الشكل 10-2 قناتين بديلتين لطبقة المخدم، هما (A وB)، يمكن لطبقة المخدم VPN أن تستعملهما. واستناداً إلى الطريق المحسوب بواسطة وظيفة التسيير عند طبقة المخدم VPN، تُنتقى إحدى قناتي طبقة المخدم (أو كلتيهما إذا كانت موازنة الحمولة مطلوبة) من أجل إرسال تدفق (تدفقات) طبقة المخدم VPN بين نقطة TFP مصدر الطبقة المذكورة والواقعة عند الحافة CE1 ونقطة TFP البئر الواقعة عند الحافة CE2.

أما الشكل 10-3 فيبين حالة توفر فيها طبقة المخدم توصيلية من نقطة إلى عدة نقاط (P2MP) من الحافة CE1 (المصدر) إلى الحواف CE2 وCE3 وCE4 (الآبار الفرعية في طوبولوجيا التوصيل P2MP).




**الشكل Y.1314/3-10 – طوبولوجيا طبقة المخدم من نقطة إلى عدة نقاط P2MP**

والشبكة المبينة في الشكل 10-3 موضحة كمثال وظيفي في الشكل 10-4 أدناه.




**الشكل 10-4/Y.1314 – المثال الوظيفي لطوبولوجيا طبقة المخدم P2MP**

وإذا كانت الحافة CE1 المصدر وكانت الحافة CE2 بئر تدفق معين لطبقة المخدم VPN، عندئذ تحتاج الحافة CE1 إلى معرفة الطريق المؤدي للوصول إلى الحافة CE2، غير أن الطرق/المسيرات الموجودة على طبقة المخدم VPN والمبينة في الشكل 10-4 هي طرق/مسيرات توفرها قنوات P2P داخل طبقة المخدم التحتية، أي، لا يوجد سوى طريق واحد من نقطة TFP المصدر إلى كل نقطة من نقاط TFP الآبار الفرعية داخل طوبولوجيا التوصيل P2MP. وهذا يعني أن وظيفة التسيير تحتاج إلى اكتشاف الطوبولوجيا؛ ولا تحتاج إلى القيام بحساب الطريق (نظراً لوجود طريق واحد فحسب إلى كل البئر). وعقب اكتشاف الطوبولوجيا، تسلك التدفقات الوافدة من الحافة CE1 والمتجهة إلى المقصد CE2، الطريق/المسير A الذي توفره قناة طبقة المخدم A.

### 3.2.1.10 نهج تسيير بديلة

عندما يكون التسيير ضرورياً، بإمكان أي مشغل (بشري) أن يؤدي وظيفة التسيير التي يحسب فيها هذا المشغل الطرق المارة بالشبكة على أساس معرفة طوبولوجيا الشبكة ومعرفة المعلومات المتعلقة باستعمال مواردها. ويوجد مثال على الحالة التي يمكن فيها تنفيذ التسيير يدوياً هو تشكيل عقد CE مزدوجة التوصيل عندما تكون طبقة المخدم VPN قائمة على بروتوكول الإنترنت (IP). وقد يكون من المعقول استعمال طرق سكونية في هذا المثال (أي، طريق واحد رئيسي وآخر يجوب الطرق المشكّلة بالتغيب) نظراً لعدم وجود سوى طريقين بديلين.

وفي حال استعمال نظام إدارة الشبكة (NMS) لأداء وظيفة التسيير، عندئذ يجب أن يكتشف نظام الإدارة طوبولوجيا الشبكة عن طريق طلب الحصول على المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/الموارد أو جمعها، ثم يستعمل هذه المعلومات لحساب الطرق وتوزيع معلومات التسيير على عقد الشبكة. وهناك مثال على حالة يؤدي فيها نظام إدارة الشبكة (NMS) وظيفة التسيير، هو إنشاء توصيلات P2P عبر شبكة طبقة قائمة على التراتب الرقمي المتزامن (SDH). ويجب أن يقوم النظام NMS أولاً بحساب أفضل طريق (طرق) يتخلل الشبكة قبل تمكنه من إنشاء التوصيلات.

وعند استعمال بروتوكول تسيير دينامي لأداء وظيفة التسيير، تُوزع حينئذ المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/الموارد عبر الشبكة بواسطة بروتوكول التسيير على كل عقدة، وتُستعمل لحساب أفضل طريق/مسير يؤدي للوصول إلى كل مقصد. وثمة مثال على بروتوكول التسيير الدينامي يتمثل في استعمال مكون تسيير السطح البيني من شبكة خاصة إلى أخرى (PNNI) في شبكات الطبقة بأسلوب نقل غير متزامن (ATM) (مع أنه يمكن استعماله أيضاً مع سائر تكنولوجيات الشبكة) للكشف عن طوبولوجيا الشبكة وحساب الطرق المؤدية إلى التوصيلات الدينامية. ويوجد مثال آخر هو حلقة الترزيم المرنة (RPR) التي تستعمل رسائل الطوبولوجيا للكشف عن طوبولوجيا الحلقة. وعندما تستقبل العقدة رسالة طوبولوجيا، فإنها ترفقها بعنوان التحكم في النفاذ إلى الوسائط (MAC) الخاص بها وتمررها إلى العقدة التالية في الحلقة، وتعود الرزمة في نهاية المطاف إلى مصدرها مع خريطة طوبولوجيا الحلقة (قائمة عناوين).

وهناك حل بديل لاستعمال بروتوكول التسيير الدينامي في مستوي التحكم يتمثل في استخدام معرفة العناوين في مستوي البيانات. وإثرنت مثال على طوبولوجيا الشبكة التي تستعمل أسلوب التشغيل هذا. وتستعمل إثرنت شجرة ممتدة (لتفادي العرى عن طريق تشذيب طوبولوجيا الشبكة) وتجسير شفاف (يستند إلى معرفة عنوان المصدر) في مستوي البيانات لإرسال الرزم إلى المقصد الصحيح دون حاجة إلى إذاعتها على جميع العقد/المحطات الطرفية. غير أنه في حالة استعمال معرفة العناوين في مستوي البيانات، فإنه يجب عندئذ أن تتمكن طوبولوجيا الشبكة أيضاً من دعم الإذاعة من أجل إرسال الرزم بعناوين المقصد التي لم تُعرف بعد. ونظراً لأن الطرق تعتبر غير معروفة طالما لم تستلم الرزم بالعناوين المقابلة فلا يمكن استعمال معرفة العناوين في مستوي البيانات لأداء وظيفة التسيير في شبكات طبقة التوصيل CO، وهو لا يناسب سوى لشبكات الطبقة عديمة التوصيل CL.

### 3.1.10 تشوير طبقة المخدم VPN

لأغراض هذه التوصية، يشير تعبير تشوير إلى تبادل المعلومات اللازمة لإنشاء أنفاق CL (كأنفاق بروتوكول التمرير في النفق للطبقة 2 (L2TP)) وإنشاء توصيلات CO (كمعرفات القنوات التقديرية (VCI)/معرفات هوية المسيرات التقديرية (VPI) بأسلوب نقل غير متزامن (ATM)). وتشمل المعلومات المطلوبة معلمات من قبيل مجالات تعدد الإرسال/إزالة تعدد الإرسال، ونوعية الخدمة (QoS) (كمهلة التأخر، الارتعاش)، وعرض النطاق، ومفاتيح التجفير، والمرونة (مثل الحماية 1+1).

ويتمثل أحد الاختلافات الأساسية بين الأنفاق والتوصيلات في أن التوصيلات تتطلب التشوير دائماً (أو التزويد اليدوي) لإنشاء التوصيلات قبل إرسال بيانات المستعمل. وعلى الرغم من أن بعض تقنيات التمرير في الأنفاق (كأنفاق L2TP، وأنفاق تغليف التسيير النوعي (GRE) المُشكلة بوضوح) تتطلب أيضاً تشوير معلمات النفق قبل إرسال بيانات المستعمل، فإن الأنفاق الأخرى من قبيل أنفاق التغليف GRE البرمجية/الدينامية وأنفاق IP-in-IP لا تشترط أي تشوير. ويقتصر عمل تقنيات التمرير في الأنفاق هذه على تغليف رزمة طبقة العميل VPN داخل رأسية رزمة طبقة المخدم VPN بالاستناد إلى المعلومات المتعلقة بالسياسات المحلية/التسيير. أما العقد الوسيطة (P) التي تُقابل فيما بين نقاط انتهاء مصدر/بئر النفق، فهي عقد تعني فقط برأسية رزمة طبقة المخدم VPN للنظر فيما إذا كان يتعين إرسال الرزمة إلى بئر طبقة المخدم VPN (المقصد PE) وكيفية إرسالها. ولا تُستعمل رأسيات طبقة المخدم VPN إلا عندما تصل الرزمة المقصد PE حيث يقع بئر طبقة المخدم VPN. ومن المُلاحظ أيضاً أن العقد الوسيطة غالباً ما تكون غير مفهومة (كأن تكون قادرة على التسيير) في رأسيات طبقة العميل VPN الداخلية.

ويجري التحكم في قبول التوصيلات (CAC) وقت إنشاء التوصيل لتحديد ما إذا كان هناك عرض نطاق كاف متيسر في طبقة المخدم التحتية للحفاظ على متطلبات نوعية الخدمة (QoS) لطبقة العميل. وتُستعمل واصفات الحركة (من قبيل معدل خلايا الذروة (PCR) ومعدل الخلايا المستدامة (SCR) المستعملان بأسلوب نقل غير متزامن (ATM)) أثناء تشوير طبقة العميل من أجل طلب الحصول على المورد المناسب من طبقة المخدم التحتية. والقدرة على تحديد مقدار عرض النطاق المتيسر عند طبقة المخدم على أساس الطلب المقدم من طبقة العميل، تعني أن وظيفة التحكم CAC يجب أن تنظر في مستوي التحكم بالنسبة لطبقتي المخدم والعميل.

ويستند التحكم CAC في حالة طبقات المخدم CO-CS إلى مقدار عرض النطاق المادي المتيسر في طبقة الشبكة التي يُطلب فيها (كالفواصل الزمنية الاحتياطية لتعدد الإرسال بتقسيم الزمن (TDM) أو أطوال الموجات بتعدد الإرسال بتقاسم طول الموجات (WDM)). أما في حالة طبقات المخدم CO-PS، فيستند التحكم CAC إلى مقدار عرض النطاق الاحتياطي غير المُستعمل من جانب التوصيلات القائمة. وتُتاح هذه المعلومات عن طريق الاحتفاظ بالمعلومات المتعلقة بحالة كل توصيل (مثلاً، صعود/هبوط، مقدار الموارد المُستعملة) عند كل عقدة من عقد شبكة هذه الطبقة تحديداً. وخلافاً لشبكات الطبقة CO-CS التي يُقيّد فيها عرضٍ النطاق المتيسر بعرض النطاق المادي المتيسر، ينبغي تطبيق السياسات المتعلقة بكل توصيل في شبكات CO-PS (وخصوصاً إذا افترض وجود تعدد إرسال إحصائي) عند كل عقدة في الشبكة من أجل ضمان ألا يقوم كل توصيل سوى بإرسال/استقبال مقدار الحركة المُتفق عليه أثناء إنشاء التوصيل.

وفيما يتعلق بحالة طبقات المخدم CL–PS، يمكن إجراء التحكم CAC على أساس عر ض النطاق المتيسر على كل سطح بيني مادي/منطقي، أو صف انتظار/تدفق/صنف من أصناف مستوى الخدمة. وكما هو الشأن مع شبكات الطبقة CO–PS، يجب تطبيق السياسة على كل عقدة في الشبكة بالاستناد إلى عرض النطاق المطلوب. ومع ذلك، وخلافاً لشبكات CO-PS حيث يُحتفظ فيها بحالة كل توصيل، لا يحتفظ عادة بالمعلومات المكافئة (أي المتعلقة بكل تدفق) في شبكات الطبقة عديمة التوصيل CL [5]. وعند اقتران هذا الأمر بحركة CL التي تتسم بطابع غير محدد للتوصيل من أي نقطة إلى أي نقطة، فإن ذلك يعني أن التحكم CAC في شبكات طبقة CL يعتمد على استعمال مراقبة الحركة ونمذجتها بشكل شامل بغية إعداد إحدى مصفوفات الحركة إلى جانب الإفراط في تزويد الشبكة لضمان تيسر عرض النطاق، ولاسيما في حالات التعطل. وإذا تطلب الأمر تطبيق تحكم CAC شديد في شبكة VPN واتفاقات خدمة رفيعة المستوى (SLA)، ينبغي حينئذ استعمال شبكة طبقة المخدم CO بدلاً من شبكة طبقة المخدم CL.

## 2.10 التحقق من طبقة العميل VPN وتشكيلها

يجوز استعمال التزويد السكوني أو استعمال بروتوكولات دينامية لأداء الوظائف اللازمة لإنشاء التوصيلية بين عقدتي التحقق من التوصيلية CE وحافة المورد على PE عند طبقة العميل VPN. وبالإمكان تنفيذ التزويد السكوني بواسطة أنظمة التشكيل اليدوي أو بواسطة الأنظمة الأوتوماتية لإدارة الشبكة. ويبين الجدول 10-2 الكيانات الوظيفية المشاركة في إنشاء توصيلية طبقة العميل VPN.

**الجدول Y.1314/2-10 – وظائف استيقان طبقة العميل VPN وتشكيلها**

| الوظيفة | الكيانات الوظيفية | عناصر الشبكة | أسلوب طبقة العميل VPN |
|---|---|---|---|
| الاستيقان والتخويل والمحاسبة (AAA) لطرف العميل CE/المستعمل | الاستيقان: تحديد حافة CE/المستعمل بالاستناد إلى معلمات الاستيقان، أي اسم مستعمل صحيح وكلمة السر | PE ،CE | الجميع |
| | التخويل: منح أو رفض النفاذ إلى موارد/خدمات شبكة طبقة العميل VPN | PE ،CE | الجميع |
| | المحاسبة: قياس الموارد/الخدمات المستعملة | PE ،CE | الجميع |
| تشكيل عناصر شبكة طبقة العميل VPN | تخصيص وتشكيل معرفات شبكة طبقة العميل VPN عبر نقاط FP/CP ونقاط TFP /TCP طبقة العميل VPN | PE ،CE | الجميع |
| | تخصيص وتشكيل معرفات شبكة VPN عبر نقاط FP/CP طبقة العميل VPN التابعة لنفس شبكة VPN | PE | الجميع |
| | تشكيل ملامح وسياسات كل شبكة VPN | PE ،CE | CO-PS، CL-PS |

[5] تشمل الحالات الاستثنائية استعمال البروتوكول RSVP RFC 2205 (خيار مبني على التشوير من طرف إلى طرف) وتسيير حالة التدفق (خيار كل قفزة على حدة)، حيث يُحتفظ بحالة كل تدفق وتُرفض التدفقات الجديدة إن لم يتيسر عرض نطاق كاف.

### 1.2.10 وظائف AAA CE/المستعمل

تتحكم وظائف AAA CE/المستعمل في النفاذ إلى طبقة العميل VPN، وتعزز تطبيق السياسات، وتدعم مراجعات حساب الاستعمال، وتقدم المعلومات اللازمة لفوترة خدمات VPN. ويمكن أداء وظائف AAA بواسطة جهاز حافة المورد PE الموصول بحافة المشترك CE، أو باستعمال جهاز مستقل، أو توليفة تجمع بين الجهازين.

ومن المحتمل في بعض الحالات أن يستدعي الأمر استعمال مخدم استيقان مركزي من أجل استيقان المستعمل/CE، بينما يُحتمل في حالات أخرى أن تشارك العقدتان CE وPE فقط في عملية الاستيقان. وكمثال على الحالة الأولى، استعمال المعيار IEEE 802.1X لاستيقان أحد أجهزة CE إثرنت، حيث تكون عقدة CE في هذا المثال جهة الاستيقان، ويُستعمل مخدم استيقان مركزي لتنفيذ الاستيقان. أما مثال الحالة الثانية، فهو استيقان رسائل التحكم (كرسائل البروتوكول BGP) الآتية من CE لاستيقان مصدر الرسالة وتوفير الحماية ضد الاحتيال.

### 2.2.10 تشكيل عناصر شبكة طبقة العميل VPN

ينبغي أثناء تزويد طبقة العميل VPN تشكيل عناصر الشبكة عند حافة المستعمل وشبكة المورد بالمعلمات التالية: عناوين شبكة طبقة العميل VPN، ومجالات إزالة تعدد إرسال شبكة طبقة العميل VPN، ومعرفات هوية VPN، وسياسات/وملامح كل شبكة من شبكات VPN. ويمكن أداء التشكيل أثناء عملية الاستيقان/التخويل أو تنفيذه بصورة مستقلة. وكمثال على الحالة الأولى، إمكانية القيام عقب نجاح الاستيقان بتشكيل الحافة CE أوتوماتياً بتخصيص عرض نطاق معين وملمح لتعيين الرزم على أساس ما يُستلم من معلومات من أحد مخدمات الاستيقان. أما مثال الحالة الثانية، فهو استخدام التشكيل اليدوي أو استعمال بروتوكول دينامي لتشكيل المركز (DHCP) لتخصيص أحد عناوين بروتوكول الإنترنت (IP) لحافة CE.

وعناوين طبقة العميل VPN التي يتعين تشكيلها عند نقطة التوصيل CP/نقطة التدفق FP وحافة المورد PE ونقاطTFP/TCP وحافة المستعمل CE أو نقطة CP/نقطة FP هي عناوين تخص شبكة طبقة العميل VPN (كعناوين IP الخاصة بشبكة IP VPN أو عناوين نقطة النفاذ إلى خدمة الإنترنت (NSAP) الخاصة بعميل VPN بأسلوب ATM والمحددة في التوصية ITU-T E.164.

ولا داعي لتشكيل مجالات إزالة تعدد إرسال شبكة طبقة العميل إلا في حال نقل العديد من عملاء VPN عبر نفس وصلة CE إلى PE، أو إذا كانت تكنولوجيا شبكة طبقة العميل VPN المُستعملة تنقل دوماً أحد مجالات إزالة تعدد الإرسال. وكمثال للحالة الأولى، طبقة العميل VPN إثرنت التي لا تحتاج سوى إلى استعمال وسوم الشبكة VLAN إذا اضطرت إلى دعم العديد من شبكات VPN. وكمثال للحالة الثانية، أسلوب ATM الذي يستعمل دوماً قيم VCI/VPI في رأسيات (خلايا) وحدة الحركة. ويعتمد تشكيل مجالات إزالة تعدد الإرسال في بعض الحالات على التشكيل المادي لا على تشكيل قيمة معينة في إحدى رأسيات الرزمة (كإلحاق ليفة بالسطح البيني الصحيح للمدخل عند حافة المورد PE مقابلة لطول الموجة الصحيح لتعدد الإرسال بتقاسم الموجات الكثيفة (DWDM) للمخرج).

وعلى الرغم من أن معرف VPN هو اسم يُستعمل لتحديد هوية شبكة VPN معينة ولا يحتاج سوى إلى تخصيص/تشكيل إذا كان من الضروري دعم الاكتشاف الدينامي لعضوية VPN وتشوير هذه العضوية دينامياً، فإن هذا الاسم يمكن أن يكون مفيداً أيضاً من المنظور التشغيلي (كاستعماله مثلاً للمساعدة في اكتشاف الأعطال وإصلاحها، والفوترة). خاصية مسير الهدف المُستعملة في شبكات VPN المطابقة للمعيار RFC 2547 هي مثال على معرف VPN المُستعمل في الكشف والتشوير الديناميين. ويمكن تشكيل معرف VPN سكونياً عند الحافة PE بواسطة التزويد اليدوي/تزويد نظام الدعم التشغيلي (OSS)، أو تشكيله دينامياً (كتشكيله مثلاً كجزء من عملية الاستيقان باستعمال خدمة الاستيقان عن بعد لمستعمل المراقمة الداخلية (RADIUS)). وإذا تقرر استعمال معرف VPN للاكتشاف/التشوير، ينبغي حينئذ أن يكون هذا المعرف وحيداً ضمن مجال وحيد للتسيير/التشوير على الأقل (وأن الهدف يكون وحيداً إجمالاً إذا كان من الضروري توفير الدعم فيما بين أنظمة التطبيقات (AS)/شبكات VPN المورد).

وقد يكون تشكيل ملامح الشبكة VPN وسياساتها فيما يخص عملاء VPN القائمة على الرزم ضرورياً في جهاز حافة المشترك CE أو في جهاز حافة المورد PE أو في كليهما. وتشتمل أمثلة لملامح الشبكة VPN وسياساتها التي قد تكون بحاجة

إلى تشكيل اعتماداً على خدمة VPN، على ما يلي: تحديد معدل البتات/تشكيل الحركة، وتعيين/تصنيف الرزم، وانتقاء الطريق/التوصيل للمواقع المتعددة التوصيلات (أي، توصيل رئيسي، وآخر احتياطي).

### 3.10 تسيير طبقة العميل VPN وتشويرها

وكما هو الشأن بالنسبة لطبقة المخدم VPN، فإن تسيير طبقة العميل VPN ضروري عند وجود عدة طرق/مسيرات بين مصدر وبئر نقطة انتهاء التوصيل TCP/ونقطة انتهاء التدفق TFP، أو في الحالات التي تنشئ فيها طبقة المخدم VPN طوبولوجيا توصيل من نقطة إلى عدة نقاط (P2MP) عند طبقة العميل VPN. وإذا كانت طبقة العميل VPN طبقة موجهة إلى التوصيل CO وتعين تقديم الدعم للتزويد الدينامي عند طبقة العميل العميل VPN، عندئذ يكون التشوير ضرورياً كذلك.

وتجدر ملاحظة نقطة مهمة هنا وهي ضرورة إنشاء قنوات طبقة المخدم VPN قبل التمكن من تسيير/تشوير طبقة العميل VPN. وتستند طوبولوجيا مستوي بيانات طبقة العميل VPN إلى طوبولوجيا قنوات طبقة مخدم VPN التحتية، وعليه لا يمكن حساب الطريق أو تشوير التوصيلات/الأنفاق طالما لم يتم إنشاء قنوات طبقة المخدم VPN.

ويصف الجدول 10-3 وظائف تسيير وتشوير طبقة العميل VPN إلى جانب الكيانات الوظيفية الفردية للطبقة.

**الجدول 10-3/Y.1314 – وظائف تسيير وتشوير طبقة العميل VPN**

| الوظيفة | الكيانات الوظيفية | عناصر الشبكة | أسلوب طبقة العميل VPN |
|---|---|---|---|
| تسيير طبقة العميل VPN | توزيع/جمع المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/موارد طبقة العميل VPN | PE ،CE | الكل |
| | الحفاظ على المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/موارد طبقة العميل VPN | PE ،CE | الكل |
| | حساب أفضل طريق (طرق) يصل بين نقطة نفاذ AP طبقة عميل VPN | PE ،CE | الكل |
| تشوير أنفاق/توصيلات طبقة العميل VPN | التحكم في قبول التوصيلات (CAC) | P ،PE | CO-CS، PS-CO |
| | الإشعار بنجاح/فشل طلب إنشاء التوصيل/النفق | P ،PE | الكل |
| | تخصيص وتشكيل مجالات إزالة تعدد إرسال طبقة العميل VPN | PE ،CE | PS-CO، PS-CL |
| | توزيع المعلومات المتعلقة بتوصيلات/أنفاق طبقة العميل VPN، كنوعية الخدمة (QoS)، مجالات إزالة تعدد الإرسال، عرض النطاق، وما إلى ذلك. | P ،PE | الكل |

#### 1.3.10 توصيلية طبقة العميل CL-PS VPN من أي نقطة إلى أي نقطة

إذا كانت قنوات طبقة العميل VPN توفر طوبولوجيا متشابكة كلياً/جزئياً من أي نقطة إلى أي نقطة لشبكة طبقة العميل CL-PS VPN بمواقع متعددة، ينبغي عندئذ أن تتخذ العقد الحاوية على نقاط FP/TFP طبقة العميل VPN (أي، عقد PE/ CE وليس عقد P) قرارات إرسال فيما يخص المقصد الذي يتعين أن تُرسل إليه رزمة تستند إلى المعلومات المتعلقة بعناوين طبقة العميل VPN. وهذا يعني أنه يجب أن تتبادل عقد حافة المستعمل CE وحافة المورد PE معلومات تسيير الطبقة المذكورة باستعمال بروتوكولات التسيير الدينامية عبر مستوي التحكم، أو لابد من تشكيل الطرق السكونية باستخدام التزويد اليدوي أو تزويد نظام الدعم التشغيلي (OSS). وثمة بديل لاستعمال بروتوكولات التسيير الدينامي أو التسيير السكوني وهو استخدام معرفة العناوين في مستوي التحكم، كما هو الحال مع إثرنت، إذ تلجأ إلى معرفة عناوين المصدر بغية إرسال الحركة في اتجاه واحد إلى المقصد الصحيح.

ويجب عزل معلومات التسيير المتعلقة بكل شبكة من شبكات VPN عن معلومات التسيير المستمدة من شبكات VPN أخرى. ويؤمن هذا الأمر عزل إرسال VPN (أي، ضمان عدم إرسال الرزم إلى عقد تخص شبكة VPN مختلفة) ويسمح بتراكب مجالات عناوين طبقة العميل VPN المقرر استعمالها. وبالإمكان تحقيق ذلك باستخدام فاصل مادي لكل نقطة من نقاط PE VPN، أو استعمال نقاط PE مشتركة بقواعد بيانات مفصولة منطقياً/تقديرياً تضم معلومات التسيير. والبديل هو استعمال أجهزة حافة مورد PE وجداول تسيير مشتركة، ولكن مع تخصيص مجالات عناوين مستقلة لكل عميل من عملاء VPN[6]. والمعيار RFC 2547 مثال على أحد حلول VPN التي تدعم التسيير عند طبقة العميل VPN. ويستعمل المعيار أعلاه تسييراً دينامياً أو سكونياً من CE إلى PE إلى جانب بروتوكول بوابة الحد المتعدد البروتوكولات (MP-BGP) لتوزيع معلومات تسيير طبقة العميل VPN بين نقاط PE وجداول التسيير التقديرية المنفصلة بغية تأمين عزل تسيير طبقة العميل VPN.

### 2.3.10 إنشاء/قطع التوصيل الدينامي لطبقة العميل VPN عند الطلب

يتم في معظم الحالات تشكيل توصيلات طبقة العميل VPN CS-CO وPS-co تشكيلاً سكونياً بواسطة التزويد اليدوي أو تزويد نظام الدعم التشغيلي (OSS)، غير أنه إذا كان إنشاء التوصيل الدينامي عند الطلب ضرورياً، ينبغي حينئذ أن يتم التبادل فيما بين أقران مستوي التحكم (التسيير والتشوير) عند طبقة العميل VPN، وذلك بين جميع نقاط CP وTCP (أي، بين عقد PE وCE). ولابد أيضاً من تنفيذ التحكم CAC وقت إنشاء التوصيل لتحديد فيما إذا كان هناك عرض نطاق كاف متيسر عند طبقة المخدم VPN لتوصيل طبقة العميل VPN. وهذا يعني أنه يجب أن تكون وظيفة التحكم قريناً لمستويي شبكة طبقة المخدم VPN وشبكة طبقة العميل VPN على حد سواء. وإذا كانت تكنولوجيا طبقة مخدم VPN مختلفة عن تكنولوجيا طبقة عميل VPN، يجب عندئذ أن يتم التشغيل البيني لمستوي التحكم في سوية القرين بين طبقة عميل VPN وطبقة مخدم VPN.

### 3.3.10 التوصيلات المُنشأة عند الطلب بتحكم المشترك

يشير تعبير التوصيلات الدينامية المُنشاة عند الطلب بتحكم المشترك إلى حالة يتحكم فيها المشترك جزئياً (أو كلياً) في عقدة CE مما يسمح بإنشاء توصيلات جديدة لطبقة العميل VPN. وتتمثل ميزة هذه القدرة من منظور المشترك في أنها تمنحه المرونة اللازمة لإنشاء شبكات VPN دينامياً عند الضرورة ومتى دعت الحاجة إلى ذلك، ومن ترسيم استعمالها وفقاً لذلك. وقد يرغب المشترك مثلاً في إنشاء توصيل عند الطلب لفترة قصيرة زمنياً من أجل تحميل/إرسال أحد الملفات الضخمة (من قبيل تطبيق معين أو ملف فيديوي) أو إنشاء توصيل موثوق لأغراض المؤتمرات المرئية. وكمثال لاستعمال الإنشاء الدينامي لتوصيل عند الطلب لطبقة العميل VPN، استعمال السطح البيني من شبكة خاصة إلى أخرى (PNNI) لإنشاء/قطع الدارات التقديرية الدائمة التبديل (SPVC) عبر قنوات طبقة المخدم VPN المتاحة باستعمال مسيرات تقديرية.

وثمة عامل مهم لابد من مراعاته عند النظر في تقديم دعم إضافي للتوصيلات الدينامية عند الطلب لطبقة العميل VPN، هو توزيع المعلومات المتعلقة بالعناوين/الطوبولوجيا. ولأسباب أمنية، لا يُتوقع أن يكون لدى مورد الخدمة رغبة في كشف طوبولوجيا شبكته أو عناوين الشبكة الداخلية للمشتركين. ولذلك، يُستحسن أن تتولى وظيفة التسيير في حافة المورد PE توزيع المعلومات المتعلقة بإمكانية الوصول إلى حافة المشترك CE فحسب. وهناك اعتبار آخر مهم هو البت بشأن الإجراءات الواجب اتخاذها وقت إنشاء التوصيل في حال عدم تيسر عرض النطاق. وتتوقف قدرة إنشاء توصيل جديد لطبقة العميل VPN على مدى تيسر قنوات طبقة المخدم بين نقطتي انتهاء المصدر والبئر. وفي حال عدم وجود قنوات أو عدم تيسر عرض نطاق احتياطي كافٍ، عندئذ يجب أن يُرفض التوصيل، أو يُنشأ توصيل/نفق جديد لطبقة المخدم VPN (أو يُزاد عرض النطاق في التوصيلات/الأنفاق القائمة). ومن أجل إنشاء توصيلات/أنفاق جديدة لطبقة المخدم VPN أو زيادة عرض نطاق التوصيلات/الأنفاق القائمة، يجب أداء وظيفة التحكم CAC لضمان تيسر عرض النطاق في طبقة المخدم التحتية.

---

[6] يشوب هذا النهج عدة عيوب رئيسية تتمثل في ضرورة توخي مورد الخدمة الدقة في إدارة مجالات العناوين، والحصول على موافقة المشترك بشأن استعمال العناوين التي يخصصها مورد الخدمة (قد يرغب المشترك في استعمال عناوين تخصه تحديداً)، وترشيح الرزم لضمان عزل شبكات VPN عن بعضها بعضاً، وهي مهمة مملة وتنطوي على ارتكاب أخطاء.

وإذا كانت طبقة المخدم عديمة التوصيل CL، عندئذ يتعذر أداء وظيفة CAC الشاقة، وعليه ينبغي الإفراط في تزويد الشبكة للسماح بإنشاء أنفاق جديدة لطبقة مخدم VPN. وينطوي هذا النهج على عيب يتمثل في توخي الدقة في تخطيط الشبكة والتحكم فيها وتطبيق سياساتها لضمان عدم تأثر الأنفاق القائمة لطبقة مخدم VPN بأي حال من الأحوال. أما إن كانت طبقة المخدم التحتية طبقة موجهة إلى التوصيل CO، حينئذ يمكن أداء وظيفة التحكم في قبول التوصيلات CAC الشاقة لضمان تيسر عرض النطاق اللازم لإنشاء توصيلات/أنفاق جديدة لطبقة مخدم VPN. ومع ذلك، يؤثر كل طلب من طلبات التوصيل عند الطبقة n على عرض النطاق المتيسر في الطبقة n-1، ويتكرر هذا الأمر نزولاً حتى الوصول إلى المجرى. وباقترابنا أكثر فأكثر من المجرى، تتعاظم تحببية عرض النطاق وتزداد أوقات تزويد/استبقاء التوصيلات. وعموماً، إذا لم تتوفر سعة كافية في إحدى طبقات المخدم التحتية لإنشاء توصيل جديد، ينبغي عندئذ رفض التوصيل. ولابد أن تُوفر سعة طبقة المخدم كنتيجة للاضطلاع بأنشطة التخطيط المتعلقة بالسعة، التي تشمل نمذجة الشبكة وتحليل جوانب استعمالها/التنبؤ بالاستعمال.

### 4.3.10 التوصيلات المُنشأة عند الطلب بتحكم مورد الخدمة

يشير تعبير التوصيلات الدينامية المُنشاة عند الطلب بتحكم مورد الخدمة إلى سيناريو يدير فيه مورد الخدمة عقدة حافة المشترك CE ويستعمل التسيير/التشوير لإنشاء توصيلات جديدة لطبقة العميل VPN إنشاءً دينامياً. وينظر موردو الخدمة إلى هذه القدرة على أنها تتميز بتمكينهم من إنشاء توصيلات من طرف إلى طرف لطبقة العميل VPN بطريقة دينامية بدلاً من إلزامهم باستخدام التشكيل السكوني (أي، التزويد اليدوي أو تزويد نظام الدعم التشغيلي (OSS). وثمة سيناريو مثالي يمكن أن يكون فيه الإنشاء الدينامي لتوصيل طبقة العميل VPN مفيداً، هو عندما تُوصل شبكتان أو أكثر من شبكات النفاذ بأسلوب ATM توصيلاً بينياً بواسطة مركز تبديل متعدد البروتوكولات بالتوسيم (MPLS). ويمكن في هذا المثال استعمال سطح بيني من شبكة خاصة إلى أخرى (PNNI) لإنشاء/قطع الدارات التقديرية الدائمة التبديل (SPVC) عند طبقة العميل VPN عبر جميع قنوات طبقة المخدم VPN بالتبديل MPLS. ونظراً لاختلاف تكنولوجيات طبقتي العميل والمخدم VPN، يجب تطبيق التشغيل البيني لسوية القرين في مستوي التحكم.

وحتى لو قام مورد الخدمة في حالة التوصيلات الدينامية عند الطلب الخاضعة لتحكمه بإدارة عقدة حافة المشترك CE بالنيابة عن المشترك، فإن توزيع المعلومات المتعلقة بالعناوين والطوبولوجيات الداخلية على العقدة المذكورة تنطوي على خطر، إذا كانت هذه العقدة موجودة داخل المباني التابعة للمشترك وليس داخل المباني الخاصة للمورد. وهناك طريقة لتلافي هذه الأخطار الأمنية تتمثل في استعمال التزويد السكوني/اليدوي بين جهاز حافة المشترك CE والعقدة الوسيطة المجاورة في شبكة المورد، واستعمال التسيير/التشوير الدينامي انطلاقاً من العقدة وحتى العودة إلى حافة المورد PE. فمثلاً، إذا كانت طبقة العميل VPN بأسلوب نقل غير متزامن ATM، يمكن حينئذ تزويد الدارة التقديرية (VC) يدوياً بين حافة المستعمل CE وبدالة المورد بأسلوب ATM الموصولة بها، ومن ثم يُستعمل السطح البيني PNNI للتوصيل من طرف إلى طرف بين بدالات ATM. ونظراً لتحكم المورد في التوصيلات عند الطلب فيما يخص التحكم في إنشاء التوصيلات/الأنفاق عند مختلف الطبقات في تراتبية شبكة الطبقات، فإنه يتمتع بتحكم إضافي في ما يحدث داخل الشبكة. ومع ذلك، يتعين توخي الدقة في تخطيط الشبكات وينبغي أيضاً تطبيق مراقبة التوصيلات عند كل طبقة بواسطة نظام إدارة الشبكة (NMS)، وخصوصاً عندما تكون الإدارة التابعة للشركة والمسؤولة عن إدارة طبقة العميل VPN مختلفة عن تلك المسؤولة عن إدارة طبقة المخدم VPN (وطبقات المخدم الواقعة تحتها).

## 11 الوظائف المطلوبة لإنشاء شبكات VPN لمستوى القرين

بافتراض إنشاء طوبولوجيا طبقة المخدم التحتية وأن نقاط TFP ونقاط FP طبقة القرين VPN قد شُكِّلت بعناوين معينة، فإن هناك ثلاث خطوات رئيسية يُضطلع بها في إنشاء توصيلية طبقة القرين VPN بين أعضاء VPN، وهي:

**الخطوة 1:** اكتشاف واستيقان أعضاء VPN وتخزين معلومات عضوية VPN.

**الخطوة 2:** حساب الطرق بين أعضاء الشبكة VPN عند طبقة القرين VPN.

**الخطوة 3:** تشكيل عناصر شبكة طبقة القرين VPN لتأمين عزل VPN.

ويصف الجدول 11-1 مزيد من التفصيل كل وظيفة من الوظائف اللازمة لإنشاء طبقة القرين VPN وصيانتها إلى جانب الكيانات الوظيفية الفردية للطبقة.

**الجدول 11-1/Y.1314 – وظائف طبقة المخدم VPN**

| الوظيفة | الكيانات الوظيفية | عناصر الشبكة |
|---|---|---|
| اكتشاف أعضاء الشبكة VPN | اكتشاف أعضاء الشبكة VPN | PE/CE |
| | توزيع/جمع المعلومات المتعلقة بعضوية الشبكة VPN (بما في ذلك المنضمون، المغادرون، التيسر) | PE/CE |
| | الحفاظ على المعلومات المتعلقة بعضوية الشبكة | PE/CE |
| الاستيقان والتخويل ومحاسبة (AAA) لحافة العميل/المستعمل | الاستيقان: تعرف هوية CE/المستعمل بالاستناد إلى معلمات الاستيقان، من قبيل اسم المستعمل الصحيح وكلمة السر | PE/CE |
| | التخويل: منح أو رفض النفاذ إلى موارد/خدمات شبكة طبقة العميل VPN | PE/CE |
| | الملائمة: قياس مدى استعمال الموارد/الخدمات | PE/CE |
| تسيير طبقة القرين VPN | توزيع/جمع المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/موارد طبقة القرين VPN | P, PE,CE |
| | الحفاظ على المعلومات المتعلقة بإمكانية الوصول/الطوبولوجيا/موارد طبقة القرين VPN | P, PE,CE |
| | حساب أفضل طريق (طرق) بين نقاط AP طبقة القرين VPN | P, PE,CE |
| تشكيل عناصر شبكة طبقة القرين VPN | تشكيل كل مرشاح من مراشيح رزم VPN | PE |
| | تشكيل كل مرشاح من مراشيح طرق VPN | PE |
| | تشكيل وتبادل كل مفتاح من مفاتيح تجفير CE/VPN | PE, CE, ES |
| | تخصيص وتشكيل معرفات (ID) الشبكة VLAN | P, PE, CE |

## 1.11 اكتشاف عضوية الشبكة VPN

في سيناريوهات شبكة VPN لمستوى القرين المُزودة من جانب المشترك، التي تكون فيها شبكة VPN شفافة للمورد (مثل شبكة VPN بمعمارية IPsec عبر الإنترنت)، هي سيناريوهات ينبغي فيها القيام قبل كل شيء، وقبل إنشاء الشبكة VPN، بتحديد حواف المشترك CE التابعة لشبكة VPN. ومن الضروري في سيناريوهات شبكة VPN المُزودة من جانب المورد (كشبكات VPN القائمة على شبكة VLAN إثرنت) أن يكشف المورد عن نقاط PE الموصولة بنقاط CE التي تكون أعضاء في شبكة VPN. وبالإمكان الكشف عنها يدوياً من جانب أي مشغل (بشري) بالاستناد إلى طوبولوجيا الشبكة المعروفة، أو كشفها دينامياً بواسطة مخدم/نظام مركزي أو بروتوكول مُوزع.

## 2.11 استيقان وتخويل ومحاسبة (AAA) حافة المشترك CE/المستعمل

تُستعمل وظيفة AAA CE/المستعمل في سيناريوهات شبكة VPN المُزودة من جانب المورد للتحكم في النفاذ إلى موارد طبقة القرين VPN، كما تُستعمل وظيفة AAA في تعزيز تطبيق السياسات، وتدعيم تدقيق حساب الاستعمال، وتقديم المعلومات اللازمة لفوترة المشترك عن خدمات VPN. ويمكن أداء وظيفة AAA بواسطة جهاز PE، أو باستعمال جهاز مستقل، أو بتوليفة تجمع بين الجهازين. فمثلاً، إذا استُعمِل المعيار IEEE 802.1X لاستيقان أحد أجهزة CE في شبكة VPN قائمة على شبكة VLAN إثرنت، تكون عقدة PE الجهة المستيقنة، ومن الممكن استعمال مخدم استيقان مركزي لتنفيذ الاستيقان.

### 3.11 تسيير طبقة القرين VPN

ينبغي في الحالات التي توجد فيها مسيرات/طرق بديلة بين أعضاء VPN تنفيذ وظيفة التسيير على طبقة القرين VPN من أجل الكشف عن الطوبولوجيا و/أو حساب أفضل طريق (طرق) بين أعضاء VPN. ونظراً لأن عقد CE وPE وP هي جميعاً تابعة لطبقة القرين VPN، فإن الأنماط الثلاثة للعقد المذكورة تشارك في جميع حسابات الطرق/المسيرات. وبالإمكان أداء وظيفة التسيير يدوياً من جانب أي مشغل (بشري)، أو دينامياً بواسطة مخدم/نظام مركزي أو بروتوكول مُوزع. ولأغراض هذه التوصية، يشمل التسيير التجسير الشفاف المبني على معرفة عنوان المصدر في مستوي البيانات.

### 4.11 تشكيل عناصر شبكة طبقة القرين VPN

يوجد عدد من الوظائف البديلة لتوفير عزل VPN. ويتمثل أحد الخيارات في تشكيل كل مرشاح من مراشيح رزم VPN على أساس تقاسم عقد PE لضمان إمكانية الوصول وصولاً تاماً فيما بين المواقع لمشترك وحيد، ولكن بالتلازم مع العزل بين المشتركين. وهناك خيار آخر هو استعمال عقد PE المُخصصة وتشكيل مراشيح الطرق لكي لا يتسنى لعقد PE أن تضم سوى طرقاً مؤدية إلى مشترك واحد، برغم أن عقد P تشمل جميع طرق المشتركين. ولا ينطبق ترشيح الرزم/الطرق سوى على سيناريوهات شبكة VPN المُزودة من جانب المورد، وعليه يجب أن تنفذه عقد PE.

ويمثل اللجوء إلى تجفير الرزم بديلاً لنهج استعمال ترشيح الطرق/الرزم إذا كانت التوصيلية بين المشتركين قائمة (كالتوصيلية عبر الإنترنت). ويكفل استعمال تجفير الرزم عدم تمكن المشتركين الذي يستقبلون رزماً من شبكة VPN لا ينتمون إليها، من الحصول على ما تحتويه الرزم من بيانات. وتنفذ عقد PE تجفير الرزم في حالة شبكات VPN المُزودة من جانب المورد، بينما تنفذها عقد CE أو الأنظمة الطرفية في حالة شبكات VPN المُزودة من جانب المشترك.

وتشتمل الأنماط الشائعة للترميز السري المُستعملة في التجفير/إزالة التجفير على ترميز سري بمفتاح سري ومفتاح عام. والترميز السري بمفتاح سري مناسب تماماً لجماعات المستعملين القريبة من بعضها حيث يمكن في هذه الحالة أن تحتفظ سلطة وحيدة بالمفاتيح السرية وتؤمن توزيعها بين المستعملين، كما هو الحال في بيئة VPN لمنشأة. وميزة الترميز السري بمفتاح عام هي تمكين المستعملين من الاتصال بأمان دون الاضطرار إلى النفاذ مُسبقاً إلى أحد المفاتيح السرية المُتقاسمة. ويستعمل هذا النهج مفتاحين، أحدهما خاص يبقى سرياً وآخر عام يجب توزيعه على جميع أعضاء شبكة VPN. والمفاتيح العامة والخاصة مرتبطة ببعضها بعضاً من حيث الدقة الرياضية، ويتعذر على أي فرد لا يمتلك مفتاحاً خاصاً معيناً أن يزيل تجفير المعلومات الواردة في الرزمة المجفرة. ويتمثل أحد الاستعمالات الشائعة للترميز السري بمفتاح عام في تبادل المفاتيح السرية المعدة لغرض استعمالها في التجفير السري بمفتاح سري.

وفي حال استعمال إثرنت كتكنولوجيا طبقة القرين VPN، من الممكن تحقيق عزل VPN عن طريق تخصيص وتشكيل شبكات VLAN، التي عادةً ما تُخصص وتُشكل يدوياً أو بواسطة نظام الدعم التشغيلي (OSS). ومع ذلك، يمكن أيضاً استعمال بروتوكولات دينامية في تخصيصها وتشكيلها. وبغية توفير التوصيلية من طرف إلى طرف بين عقد حافة المشترك CE، يجب أن تُشكل شبكات VLAN تشكيلاً صحيحاً عبر عقد CE وPE وP.

## 12 وظائف تشغيل وإدارة وصيانة (OAM) شبكات VPN

وسائل ووظائف التشغيل والإدارة والصيانة (OAM) ضرورية لصيانة الكفاءة التشغيلية للشبكات المنتشرة على نطاق واسع. والجودة والسلامة والصلاحية أمثلة على الخصائص المهمة لتوصيلات/تدفقات الشبكة المُعبر عنها بوظائف OAM. وإذا كانت شبكة الطبقة لا تدعم وظائف OAM أو كانت إحدى هذه الوظائف مفتقدة فيها، تكون شبكة الطبقة المعنية عاجزة وظيفياً فيما يخص أداء الوظيفة المفتقدة فيها. ويتعذر استعمال وسائل/وظائف OAM بطبقة أعلى/أدنى كوظائف إحلال/بدائل لأداء نفس العناصر الوظيفية، وخصوصاً عندما يتعلق الأمر بتحديد موقع العطب. وهذا لا يعني أن من المستحيل توفير خدمات VPN باستعمال تكنولوجيات الشبكة التي تفتقر إلى وظائف OAM. ومع ذلك، من المحتمل أن تزيد العناصر الوظيفية OAM المفتقدة تكاليف التشغيل وتعقد جوانب التشغيل بشكل كبير.

ويبين الجدول 12-1 بعض وظائف OAM الأساسية ويحدد عناصر الشبكة التي ينبغي أن تؤدي الوظائف المصاحبة.

**الجدول 12-1/Y.1314 – وظائف OAM العميل/المخدم**

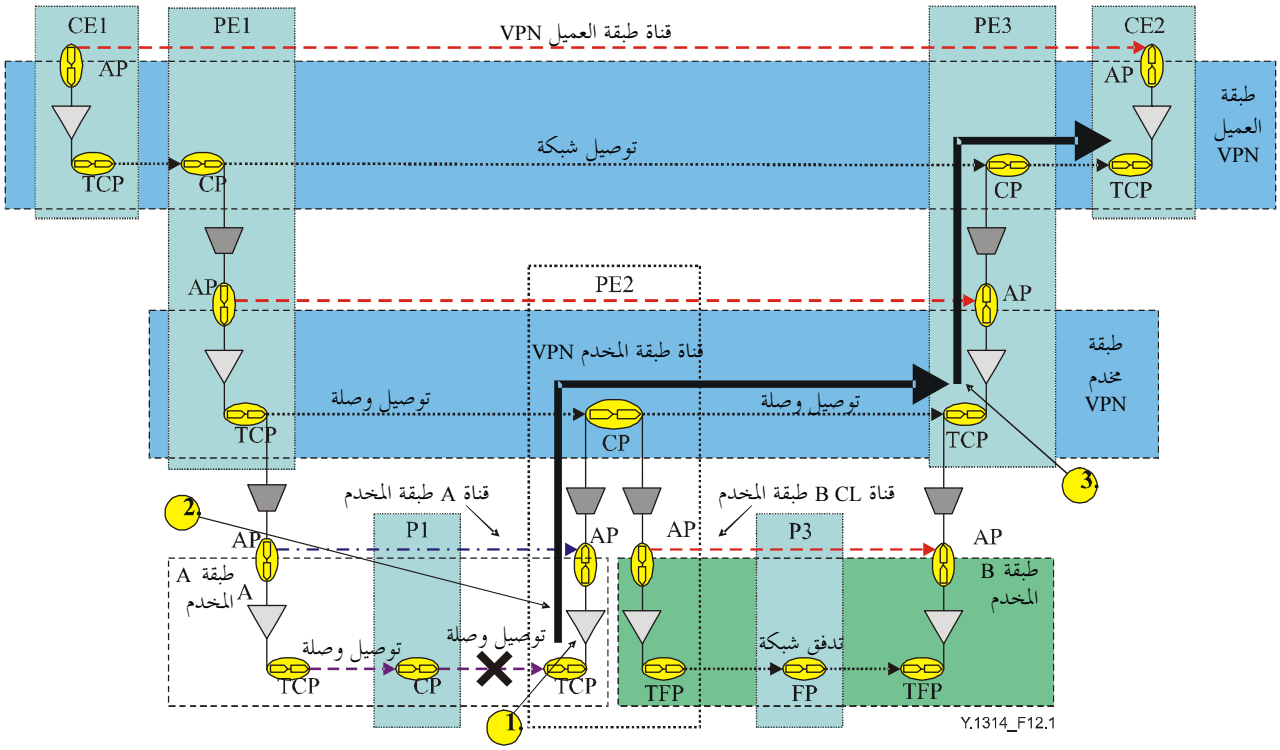
| الوظيفة | الكيانات الوظيفية | عناصر الشبكة |
|---|---|---|
| وظائف OAM لطبقة العميل VPN | كشف/إدارة أعطال طبقة العميل VPN | CE وPE |
| | مراقبة أداء طبقة العميل VPN | CE وPE |
| | تنشيط/إخماد وظائف OAM لطبقة العميل VPN | CE وPE |
| وظائف OAM لطبقة المخدم VPN | كشف/إدارة أعطاب طبقة المخدم VPN | PE وP |
| | مراقبة أداء طبقة المخدم VPN | PE وP |
| | تنشيط/إخماد وظائف OAM طبقة المخدم VPN | PE وP |
| وظائف OAM لطبقة القرين VPN | كشف/إدارة أعطاب طبقة القرين VPN | CE، PE، P (الكل) |
| | مراقبة أداء طبقة القرين VPN | CE، PE، P (الكل) |
| | تنشيط/إخماد وظائف OAM طبقة القرين VPN | CE، PE، P (الكل) |

## 1.12 إدارة الأعطاب

تشمل إدارة الأعطاب الكشف عن الأعطاب وتحديد موقعها وتصحيحها واختبار تشخيصها عند الطلب. ويجب اكتشاف الأعطال ومعالجتها عند نقطة انتهاء بئر توصيل/تدفق شبكة الطبقة التي تحدث فيها هذه الأعطال. ويؤدي عدم القيام بذلك إلى ظهور دلالات عطب غامضة تزيد بشكل كبير من تعقيدات جوانب التشغيل والوقت المُستغرق في إصلاح عطب معين. ولدى الكشف عن عطب ما، وبالإضافة إلى إصدار الإنذارات وإرسالها بشأنه إلى نظام إدارة الشبكة (NMS)، وللحيلولة دون اكتساح شبكات طبقة العميل بوابل من الإنذارات، ينبغي تمرير إشارة دلالة العطل في الاتجاه الأمامي (FDI) أو إشارة دلالة الإنذار (AIS) إلى شبكة (شبكات) طبقة العميل باستعمال قواعد التركيب المناسبة لوظيفة OAM التي تستعملها التكنولوجيا المتأثرة (إن وجدت) لطبقة العميل المعنية.

وتتمثل أهم آليات اكتشاف الأعطاب في التحقق من التوصيلية (CV)، وهي شرط مشترك بين جميع الأساليب الثلاثة للتوصيل بواسطة الشبكات، وهي ببساطة تلزم مصدر تدفق الحركة بحتمية التعريف بنفسه (بطريقة ما) للبئر. وتتوقف سبل تحقيق ذلك على أسلوب التوصيل بواسطة الشبكات، ويرد شرحها في الفقرات التالية. وتحديد موقع العطل شرط آخر من الشروط الأساسية بين جميع الأساليب الثلاثة للتوصيل بواسطة الشبكات من أجل الوقوف على الأسباب الجذرية للعطب. ويمكن استعمال أدوات لاختبار تشخيص العطل عند الطلب بغية تحديد موقع العطل بالإضافة إلى المعلومات الأولية المقدمة عن العطل.

ويصف الشكل 12-1 مثالاً لسيناريو عطل في طبقة مخدم VPN من منظور وظيفي.




1. *تكشف طبقة A المخدم عن خسارة الاستمرارية (LOC) على أساس عدم استقبال رزم CV*
2. *ترسل طبقة A المخدم الدلالة إلى طبقة المخدم VPN*
3. *تستقبل طبقة المخدم VPN الدلالة FDI وتنشرها على طبقة العميل VPN العليا*

**الشكل Y.1314/1-12 – انتشار دلالة عطل في الاتجاه الأمامي (FDI) للعميل/المخدم**

ويؤدي كشف وظيفة انتهاء البئر عن عطب الوصلة في طبقة المخدم A المبينة في هذا المثال إلى تكوين دلالة عطل في الاتجاه الأمامي (FDI)/إشارة دلالة الإنذار (AIS) وتمريرها عبر طبقة المخدم VPN. وتنتشر دلالة FDI في وظيفة انتهاء بئر طبقة المخدم VPN، التي ترسل بدورها دلالة FDI إلى طبقة العميل. ويتكرر هذا السلوك حتى يبلغ شبكة طبقة لا تدعم دلالة العطل في الاتجاه الأمامي (FDI). وعليه، وبرغم عدم بيان ذلك هنا، فإن بإمكان طبقة العميل VPN عندما تستقبل دلالة FDI أن ترسل الدلالة FDI إلى الطبقة التي تقع فوقها، ويتوقف ذلك على تكنولوجيا الطبقة التي فوقها (مثل أسلوب ATM، إثرنت، بروتوكول IP، وما إلى ذلك).

والمكان الوحيد الذي ينبغي أن يُطلق فيه الإنذار هو نقطة انتهاء القناة في شبكة الطبقة حيث يكتشف العطل الأصلي. وينبغي تحديداً ألا تُطلق أية إنذارات في أي طبقة من طبقات العميل المتأثرة (وهو الغرض الرئيسي من إرسال الدلالة FDI إلى هذه الطبقات). وعلاوة على ذلك، إذا اقتضت الضرورة تنفيذ مراقبة أحادية الطرف في كلا الاتجاهين، يمكن عندئذ إرسال مبين عطل في الاتجاه الخلفي (BDI) بالاتجاه المعاكس. وبالإمكان الاطلاع على المزيد من التفاصيل المتعلقة بكيفية إرسال المبينات/الإنذارات الخاصة بالأعطال (بما فيها تفاصيل العطل وعدم إمكانية تيسر معايير الدخول والخروج والإجراءات اللاحقة) بالرجوع إلى التوصيات المعنية بوظائف OAM المستعملة لأغراض تكنولوجيات شبكة الطبقة، كالتوصية ITU-T Y.1711 والمتعلقة بتشغيل وإدارة وصيانة (OAM) التبديل المتعدد البروتوكولات بالتوسيم (MPLS).

ووظيفة تصحيح الأعطال مسؤولة عن إصلاح العطل والتحكم في الإجراءات التي تستعمل موارد إطنابية لاستبدال التجهيزات أو المرافق المتعطلة. ويمكن مثلاً استعمال تبديل الحماية أو إعادة تسيير التوصيل لاستعادة الخدمة/صيانتها في حال انقطاع الليفة أو عطب العقدة.

وتُستعمل عموماً أدوات اختبار تشخيص العطل عند الطلب لتحديد موقع العطل، ولكن يمكن أيضاً استعمال هذه الأدوات في التحقق من صحة توصيلية/تشكيل التوصيل/النفق قبل إدخاله الخدمة. وعروة الرجعة مثال على اختبار تشخيص العطل

الذي تقوم خلاله عروة تمتد عبر توصيل الشبكة من المصدر بالرجوع في اتجاه المصدر عبر نقطة توصيل أو نقطة انتهاء توصيل معينة لتعزل بذلك هذا القسم من التوصيل.

## 2.12 إدارة الأداء

مراقبة الأداء (PM) هي عملية تجميع بيانات الأداء وتحليلها وتبليغها. وتستعمل البيانات المذكورة لتقييم أداء الشبكة وصيانتها فضلاً عن توثيق نوعية الخدمة التي تقدمها للمشتركين. وفي حال دعم العديد من مستويات أصناف الخدمة (كدعمها مثلاً بالاستناد إلى معمارية الخدمات المتميزة (Diffserv)، ينبغي حينئذ مراقبة الأداء على أساس مراقبة كل صنف من أصناف الخدمة على حدة. وتشمل مراقبة الأداء، ضمن جملة أمور، الكشف عن انحطاط الإشارة، ومراقبة الكمون/الارتعاش، وحساب خسارة الرزم. ويوجد عدد من الأهداف المختلفة التي تتطلع مراقبة الأداء إلى تحقيقها وتشمل صيانة اتفاق مستوى الخدمة (SLA)، وتقديم الدعم لهندسة الحركة، ومحاسبة كل مشترك، واستعادة الخدمة/تبديل الحماية (الناتجة مثلاً عن انحطاط الإشارة).

ومن الضروري إقامة علاقة بين الأعطال ومدى التيسر ومراقبة الأداء (PM). وثمة ترتيب معين يمكن تلخيصه فيما يلي:

1) يحدد أسلوب الشبكة الأعطال ذات الصلة (التي تختلف من أسلوب إلى آخر) وطابع التشغيل OAM اللازم.

2) ينبغي تحديد جميع الأعطال بالاستناد إلى معايير دخول/خروج قياسية واتخاذ إجراءات بشأنها.

3) يتم الدخول في حالة عدم التيسر عند وقوع عطل أو انحطاط غير مقبول في الأداء يستمر لعدة ثواني متعاقبة. ويتم الدخول في حالة عدم التيسر بالنسبة للتراتب الرقمي المتزامن (SDH) عقب فترة تستغرق 10 ثواني متعاقبة شديدة الخطأ[7] (SES)، ويتم الخروج من هذه الحالة بعد فترة تستغرق 10 ثواني متعاقبة ليست شديدة الخطأ. ولضمان تحقيق المواءمة، ينبغي أن تكون فترة عدم التيسر متساوية في جميع شبكات الطبقة، أي، 10 ثواني.

4) لا تصح مراقبة الأداء (PM) المُطبقة لأغراض صيانة اتفاق مستوى الخدمة (SLA) سوى في حالة التيسر، وعليه يجب تعليقها عند الدخول في حالة عدم التيسر.

ومراقبة الأداء PM المُطبقة لأغراض اتفاق مستوى الخدمة SLA قياس أحادي الاتجاه في حالة التيسر، غير أنه نظراً لأن معظم التطبيقات تتطلب العمل في الاتجاهين على حد سواء (الصاعد والهابط)، فإن كلاهما يُعتبر مخفقاً من منظور التطبيق في حال إخفاق أحدهما. وهذا يعني أن حالة عدم التيسر هي إحدى وظائف "OR" لكلا الاتجاهين، وهكذا، إذا دخل أي اتجاه منهما حالة عدم التيسر، عندئذ ينبغي تعليق مراقبة الأداء PM المُطبقة لأغراض اتفاق مستوى الخدمة SLA في كليهما.

## 3.12 تنشيط/إخماد التشغيل والإدارة والصيانة OAM

من الضروري في الأسلوبين CO-CS وCO-PS تنشيط/إخماد آليات التشغيل والإدارة والصيانة الأساسية OAM المعنية بالكشف عن الأعطال/معالجتها وذلك بالتزامن مع إنشاء القنوات وقطعها الذي يمكن إتمامه بواسطة تزويد نظام إدارة الشبكة (NMS)/تزويد نظام الدعم التشغيلي (OSS) أو بواسطة التشوير. وينبغي مثلاً تنشيط التحقق من التوصيلية (CV) عند المصدر قبل تنشيط الكشف عن التحقق CV عند البئر للحيلولة دون إصدار إنذارات غير مفهومة. كما ينبغي أن تكون طريقة التزويد أو التشوير المُستعملة لإنشاء القنوات قادرة على إبلاغ نقطة بئر القناة بمعرف المصدر (كالسطح البيني لنقل النص إلى كلام (TTSI) المُحدد في التوصية ITU-T Y.1711) الذي يُتوقع وجوده في مستوي البيانات اللازم لقناة معينة من أجل تحديد الجهة التي تنتمي إليها القناة التي تستقبل رزم OAM.

[7] الثانية الشديدة الخطأ (SES) هي فترة ثانية واحدة بمعدل خطأ في البتات يبلغ 3–1E أو أكثر، أو هي فترة يُكشف خلالها عن خسارة الإشارة (LOS) أو عن إشارة دلالة الإنذار (AIS).

## 4.12 العيوب المتصلة بكل أسلوب من أساليب الشبكة

تتوقف عيوب النقل التي يُحتمل حدوثها في شبكة طبقة العميل أو المخدم VPN على أسلوب الشبكة الذي تنتمي إليه تكنولوجيا شبكة الطبقة. وفيما يلي ملخص بالعيوب المحتملة والمعتمدة على أسلوب الشبكة:

- **طبقة CL-PS**: انقطاعات فقط؛
- **طبقة CO-PS**: انقطاعات، ومبادلات، وحالات دمج؛
- **طبقة CO-PS**: انقطاعات، مبادلات (ولكن بين الكيانات المتماثلة فحسب).

ويرد في الفقرات المبينة أدناه وصف أكثر تفصيلاً لكل أسلوب من أساليب الشبكة لوصف المتطلبات والاعتبارات الأساسية المتعلقة بالتشغيل والإدارة والصيانة OAM واللازمة للأسلوب المعني تحديداً. ومن الجدير بالذكر أن هذا الوصف لا يُقصد به تقديم قائمة شاملة بمتطلبات OAM اللازمة لكل أسلوب. ولا يُسلط الضوء هنا سوى على الاختلافات الوظيفية الجوهرية من أجل بيان الكيفية التي يؤثر بها أسلوب الشبكة الذي تنتمي إليه طبقات العميل والمخدم VPN على وظائف/أدوات OAM اللازمة.

### 1.4.12 شبكات طبقة CL-PS

يتعذر حدوث عيوب ناجمة عن سوء التوصيلية (كالمبادلات أو حالات الدمج) في شبكات طبقة CL-PS في إطار افتراض الحصول على معلومات تسيير متسقة وصحيحة (تنطبق في واقع الأمر على جميع الأساليب). وتحتوي كل رزمة على كل من عنوان المصدر (وظيفة التحقق CV) وعنوان المقصد الذي يضم جميع المعلومات اللازمة لتسيير الرزمة بطريقة صحيحة في كل عقدة من عقد الشبكة. وعليه، فإن العيب الوحيد الذي يمكن أن يحدث في شبكات طبقة CL-PS هو في حالة حدوث انقطاع (ينجم مثلاً عن خطأ في التسيير، أو عطل الوصلة، أو عطل العقدة). وتعتبر وظيفة التحقق CV في الشبكات المذكورة جزءاً لا يتجزأ من رأسيات الرزم لأن كل رزمة تتضمن عنوان مصدر/مقصد وحيد للشبكة. وعادةً ما تتقاسم بيانات التحكم والمستعمل نفس مسير البيانات في شبكات طبقة CL-PS، وبالتالي، إذا حدث عطل في مستوي التحكم (كهبوط تجاور التسيير)، عندئذ يمكن التسليم ضمناً بخسارة التوصيلية وتعذر إرسال بيانات المستعمل كذلك. وبهذه الطريقة يُكشف عموماً عن أعطال شبكات طبقة CL-PS ويتم تصحيحها على هذا الأساس، إذ يشير مثلاً عدم استقبال نداءات التسيير في مستوي التحكم إلى حدوث عطل في مستوي البيانات، ولذلك يجب اتخاذ إجراء علاجي (من قبيل انتقاء طريق بديل). غير أن هناك حالة لا يمكن فيها اتخاذ هذا الإجراء، وهي عند اللجوء إلى موازنة الحمولة في شبكات طبقة البروتوكول الإنترنت IP. وتوجد في هذه الحالة عدة طرق تؤدي إلى نفس المقصد، وهكذا، إذا أصبح أحد الطرق غير متيسر، فقد يتعذر على مستوي التحكم أن يكشف عنه، لأن حركة التحكم يمكن أن تستعمل ببساطة طريقاً آخر من الطرق المتيسرة. وبغية الكشف عن الأعطال في حالة استعمال موازنة الحمولة، ينبغي استعمال آلية OAM التي تتولى اختبار التوصيلية عبر جميع الطرق المتيسرة.

### 2.4.12 شبكات طبقة CO-PS

نقاط النفاذ إلى شبكة الطبقة في حالة شبكات طبقة CO-PS هي النقاط الوحيدة الملمّة بالعناوين الوحيدة للشبكة التي تستعملها وظيفة التسيير لحساب أفضل طريق/مسير يؤدي إلى التوصيل عبر الشبكة. وحالما يتم حساب الطريق/المسير، يُستعمل التشوير (أو التزويد اليدوي) لتخصيص وتشكيل المجالات التي تكتسي دلالة على الصعيد المحلي لتعدد إرسال/إزالة تعدد إرسال المداخل/المخارج (أو معرفات توصيلات الوصلة)، المُستعملة في مستوي البيانات لتبديل الرزمة وإرسالها إلى المقصد الصحيح. وبالنظر إلى أن مجالات تعدد الإرسال/إزالة تعدد الإرسال هي مجالات ذات دلالة على الصعيد المحلي فحسب، فإن بإمكان العقد الصاعدة/الهابطة إعادة استعمال نفس القيم في ذات التوصيل، أو في توصيلات مختلفة. وإعادة استعمال مجالات تعدد الإرسال/إزالة تعدد الإرسال بالاقتران مع الافتقار إلى العناوين الوحيدة للشبكة في مستوي البيانات، أمر يدل على أننا يمكن أن نشهد وقوع أعطال مبادلة ودمج في شبكات طبقة CO-PS بالإضافة إلى الانقطاعات. ونظراً لإرسال رزم CO-PS بالتزامن، وعدم احتوائها على عناوين وحيدة لشبكة المصدر/المقصد، فإن من الضروري إتباع طريقة

محددة في إضافة وظيفة التحقق CV، التي تتم عادةً عن طريق إرسال رزم CV بمعدل بتات معين. وثمة حاجة إلى توخي الدقة في مراعاة معدل إرسال رزم CV لضمان عدم اتخاذ إجراءات غير ضرورية في حالة حصول رشقات خاطئة انتقالية.

### 3.4.12 شبكات طبقة CO-CS

لا تتعرض شبكات طبقة CO-CS للدمج لأن مجالات تعدد الإرسال/إزالة تعدد الإرسال تستند إلى معرفات مادية لتوصيلات وصلة الزمن/المجال/التردد بمعدل بتات ثابت. وتشمل الأعطال الممكنة في شبكة طبقة CO-CS الانقطاعات والتوصيلات المتبادلة، غير أن أعطال التوصيلات المدمجة لا يمكن أن تحدث إلا بين القنوات المتشابهة تماماً، إذ يتعذر حدوث دمج مثلاً بين القناتين التقديريتين VC12 وVC4 في التراتب الرقمي المتزامن (SDH). وكما هو حال شبكات طبقة CO-PS، ينبغي إتباع طريقة محددة معينة في إضافة وظيفة التحقق CV في حالة شبكات طبقة CO-CS. وعندما يُنقل رتل CO-CS بمعدل بتات ثابت (سواء كانت هناك بيانات يتعين إرسالها أم لا)، فإن بالإمكان نقل معلومات CV في كل رتل باستعمال معدل إرسال الأرتال بوصفه معدل إرسال معلومات التحقق من التوصيلة CV، فمثلاً، في رسالة تتابع J0 الواردة في الرتل VC4 بالتراتب SDH بمعدل أساسي للإدراج قدرة 125 µs. وتُنقل حركة التحكم في حالة شبكات CO-CS خارج النطاق (OOB) دائماً، ولذلك ينبغي تأمين وظائف OAM على أساس كل توصيل على حدة في مستويي بيانات المستعمل وبيانات التحكم.

### 4.4.12 الفصل بين مستويي بيانات التحكم وبيانات المستعمل

يمكن نقل بيانات التحكم وبيانات المستعمل في حالة شبكات طبقة CO-PS باستعمال مستويات بيانات مختلفة (يُشار إليها عادةً بالتحكم خارج النطاق (OOB))؛ وكما اتضح من الفقرة السابقة، يُعتبر هذا السلوك في أسلوب CO-CS سلوكاً إلزامياً في جميع الحالات. والفصل بين مستويي بيانات التحكم وبيانات المستعمل مفيد لعدة أسباب، ولاسيما من منظور أمن الشبكة واستقرارها، حيث يحمي مستوي التحكم من هجمات مستوي المستعمل ومن مشاكل زيادة الحمولة/مشاكل الازدحام الناجمة عن حركة مستوي المستعمل. وعند فصل مستوي بيانات المستعمل عن مستوي بيانات التحكم، يتضح أن من المتعذر التسليم بأن وقوع عطل في مستوي التحكم يدل على وقوع عطل في مستوي بيانات المستعمل (أو العكس بالعكس في واقع الأمر). وبناء على ذلك، يجب استعمال آليات OAM في شبكات طبقة CO-PS حيث يستخدم التحكم خارج النطاق OOB، على أساس مستوى البيانات (أي، لكل توصيل). ويصح ذلك أيضاً في الحالات التي قد تستعمل فيها حركة التحكم نفس مستوي البيانات كجزء من حركة المستعمل، ولكن ليس جميعها (قد يستعمل مثلاً التبديل MPLS هندسة الحركة (TE) لتوفير تسيير صريح لبعض أنماط الحركة. ولذلك، فإن حركة بيانات المستعمل ليست في حاجة إلى اتباع نفس المسير المستعمل من جانب رزم التحكم لإنشاء أنفاق هندسة الحركة TE).

ويمكن أن يؤدي عدم استعمال آليات OAM القائمة على مستوي بيانات المستعمل إلى سيناريو يمكن أن يتعرض فيه توصيل يحمل رزم بيانات لعطل ما، ولكن نظراً لنقل حركة التحكم باستعمال توصيل مستقل، فإن معلومات التحكم تواصل تدفقها، وهكذا لا يكتشف مستوي التحكم العطل. وعندما لا يطبق مصدر التوصيل آلية الكشف OAM على مستوي البيانات، فإن هذا المصدر يستمر في إرسال بيانات المستعمل محدثاً ثقباً أسوداً في الحركة، أو مسبباً ما هو أسوأ من ذلك، ليتعرض بالتالي أمن بيانات المشترك للخطر من خلال إرسال الحركة إلى الموقع الخطأ.

وينبغي لوظائف التشغيل والإدارة والصيانة OAM أن تعمل باتجاه واحد فقط لتحدد بطريقة لا لبس فيها اتجاه حصول العطل، وتحرياً للصواب في معالجة الأعطال في توصيلات P2P وP2MP على حد سواء. كما ينبغي دعم مراقبة الأعطال في كلا الاتجاهين مراقبة أحادية الطرف إن أمكن. ولهذا الأمر أهمية خاصة في الحالات التي يتمكن فيها مشترك أو مورد معين من التحكم في طرف واحد من التوصيل/النفق، ولكنه لا يتمكن من ذلك في الطرف الآخر، مثل سيناريو VPN المشترك بين الموردين حيث يقع فيه أحد طرفي توصيل طبقة العميل P2P VPN في شبكة مورد خدمة مختلف.

## 13 التقارب الوظيفي وسيناريوهات الخدمة

يسمح تقابل متطلبات الخدمة VPN اللازمة لأداء الوظائف التي يرد وصف لها في هذه التوصية لمشغلي الشبكات بانتقاء أفضل ما يناسبهم من تكنولوجيات الشبكة وآلياتها اللازمة لتوفير خدمات VPN التي يرغبون في تقديمها. ويسمح انتقاء أفضل توليفة تجمع بين الآليات/البروتوكولات اللازمة لأداء كل وظيفة بتطور فرادي المكونات الوظيفية على بطريقة مستقلة. كما يدعم هذا النهج إعادة استعمال الآليات/البروتوكولات المشتركة عبر مختلف تكنولوجيات شبكة VPN (عند اللزوم) بغية تخفيض التكاليف وتقليل أوجه التعقيد.

### 1.13 سيناريوهات خدمات VPN العميل/المخدم

يتوقف أداء الوظائف (وبالتالي الآليات/البروتوكولات) اللازمة لدعم شبكات VPN العميل/المخدم على أساليب شبكة العميل/المخدم فضلاً عن خدمة VPN المقدمة فعلاً. فقد يرغب مثلاً بعض المشتركين في تمكينهم من إنشاء دارات تقديرية مبدلة (SVC) عند الطلب بين عدة مواقع عند اللزوم ومتى دعت الحاجة إلى ذلك. في حين قد لا يرغب البعض الآخر سوى في إنشاء توصيلات دائمة تستند إلى طوبولوجيا سكونية معروفة. وثمة مثال آخر هو أن بعض المشتركين قد يرغب في استعمال الاستيقان بالنسبة لكل مستعمل/عقدة CE لرفع مستوى الأمن. بينما قد يرى مشتركون آخرون أن تقييد النفاذ المادي إلى البنية التحتية للشبكة يُعتبر كافياً. ويبين الجدولان 1.III و2.III بعض الأمثلة على سيناريوهات خدمة مختلفة ويحددان هوية آليات/بروتوكولات مثالية معينة يمكن استعمالها لأداء الوظائف المطلوبة.

### 2.13 سيناريوهات شبكات VPN لمستوى القرين

يعتمد أداء الوظائف اللازمة لدعم شبكات VPN لمستوى القرين على تكنولوجيا شبكة طبقة القرين ونمط خدمة VPN المُقدمة. ويتسم مثلاً الاستيقان في حالة شبكات VPN القائمة على التجفير بطابع إلزامي من أجل استعمال المفاتيح الصحيحة، بينما يعمل الاستيقان في حالة شبكات VPN المستندة إلى شبكات VLAN إثرنت (كاستعمال المعيار IEEE 802.1X مثلاً) على توفير المزيد من الأمن ولكنه ليس ضرورياً. ويورد الجدول 3.III بعض الأمثلة على سيناريوهات خدمة مختلفة ويحدد هوية بعض الآليات/البروتوكولات النموذجية التي يمكن استعمالها لأداء الوظائف المطلوبة.

## 14 اعتبارات بشأن أمن الشبكة VPN

لا تطرح هذه التوصية أية مسائل جديدة بخصوص أمن الشبكة، غير أن الأمن جانب مهم يستحق المراعاة عند تصميم/استحداث شبكات VPN من أجل انتقاء تكنولوجيات الشبكة والمكونات الوظيفية التي تستوفي متطلبات أمن المشترك. وهناك مخاطر أمنية ملازمة تصاحب جميع تكنولوجيات VPN يسببها استعمال بنية تحتية مُتقاسمة لنقل الحركة إلى عدة مشتركين.

وأمن الشبكة مجال واسع بحد ذاته، ولذلك لا تتناوله هذه التوصية بالتفصيل. وعند النظر إلى جوانب الأمن من منظور بعيد، يجب توفير الحماية للبنية التحتية المادية لشبكة VPN من النفاذ غير المرخص أو الهجمات الضارة (عن طريق حظر النفاذ إلى المباني الحاوية على تجهيزات الشبكة على سبيل المثال). بالإضافة إلى ذلك، يجب منع النفاذ غير المرخص عن بعد من خارج البنية التحتية المادية لشبكة VPN (من خلال مثلاً استعمال الجدار الناري من مصادر الهجمات الوافدة من الإنترنت).

وكما تصف ذلك الفقرة 1.5، يجب أن تكون شبكة طبقة المخدم VPN في حالة شبكات VPN العميل/المخدم، قادرة على تطبيق تعدد الإرسال/إزالة تعدد الإرسال لتأمين فصل مستوي البيانات فيما بين العديد من طبقات العميل VPN. ويجب أن يقترن فصل الحركة هذا بفعالية التحكم في النفاذ إلى شبكة VPN عند حافة الشبكة بالاستناد إلى كل سياسة من سياسات VPN المُطبقة على المشترك.

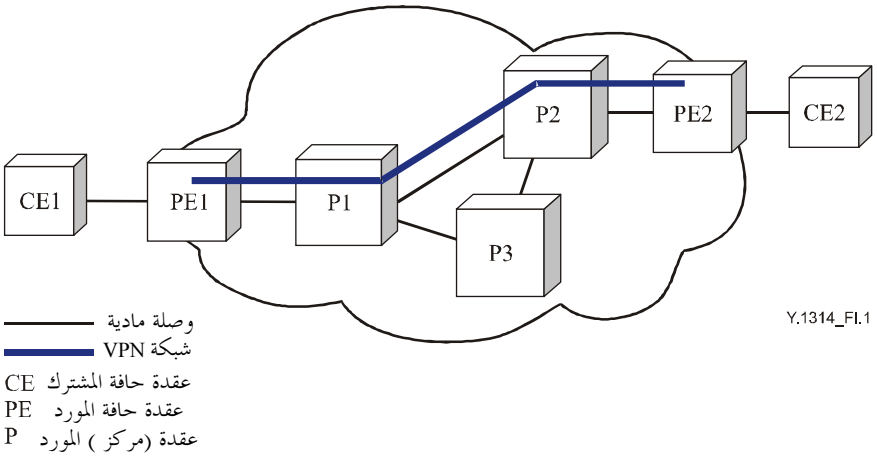
أما في حالة شبكات VPN لمستوى القرين، وكما تصف ذلك الفقرة 6، يجب أن يكون لتكنولوجيا الشبكة المُطبقة وسيلة ما لتأمين عزل VPN من أجل دعم شبكات VPN عبر أحد المجالات المُتقاسمة. ويجب أن تقتصر قدرة العقد CE على الاتصال مع غيرها من عقد CE التابعة لنفس شبكة VPN، أو تكون قادرة فحسب على إزالة تجفير الرزم الوافدة من عقد CE التابعة لنفس شبكة VPN.

ويمكن رفع مستوى الأمن في شبكات VPN العميل/المخدم وشبكات VPN لمستوى القرين على حد سواء، عن طريق استعمال الترميز لتجفير وحدات حركة المستعمل/التحكم، كما يمكن تطبيق الاستيقان على المستعملين وعقد الشبكة للتحقق منها. ويرد في الفقرتين 1.2.10 و2.11 على التوالي وصف أكثر تفصيلاً لاستيقان شبكات VPN العميل/المخدم وشبكات VPN لمستوى القرين. أما الترميز فيرد وصفه بمزيد من التفصيل في الفقرتين 2.6 و4.11.

# التذييل I

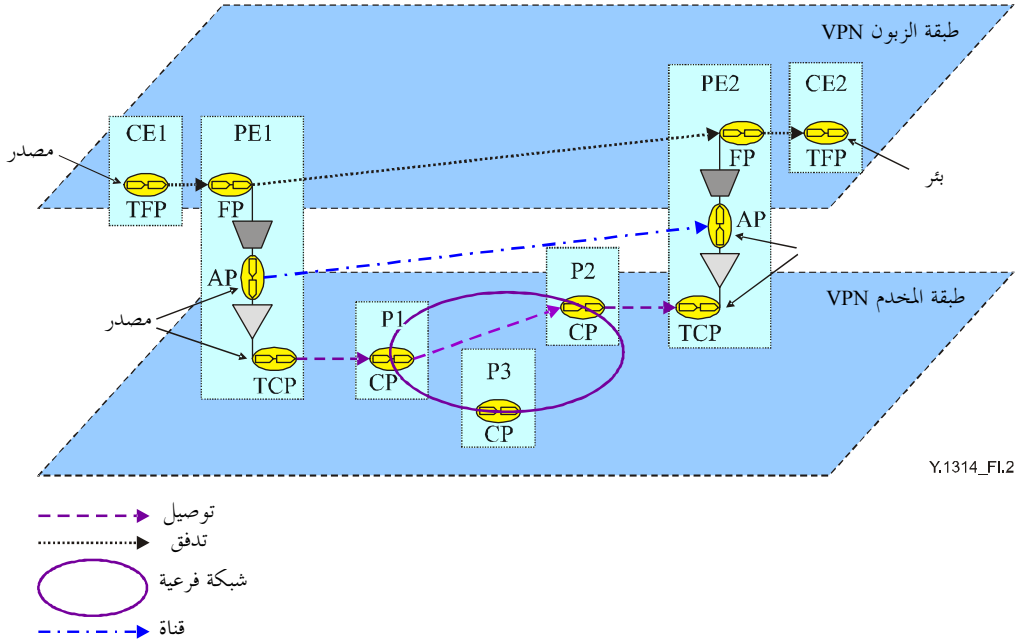
## تحديد موقع نقطة انتهاء التوصيل TCP/نقطة انتهاء التدفق TFP لطبقة العميل VPN

يورد الشكل 1.I مثالاً لشبكة VPN العميل/المخدم، ويوضح الطوبولوجيا المادية للشبكة، ويمثل فيه الخط الأسود طبقة المخدم VPN، بينما تمثل الخطوط الرمادية الوصلات المادية بين العقد.




**الشكل I.1/ Y.1314 – الطوبولوجيا المادية لشبكة VPN العميل/المخدم – المثال 1**

ومع أن الشكل 1.I يوضح الطوبولوجيا المادية وطبقة المخدم VPN، إلا أنه لا يبين الطوبولوجيتين المستقلتين لطبقة العميل VPN وطبقة المخدم VPN، أو أين تقع نقاط TCP/ TFP فيها. ويوضح الشكل 2.I مثالاً وظيفياً يستند إلى الطوبولوجيا المادية المبينة في الشكل 1.I الذي يبين أن موقع نقاط TFP هو داخل عقد CE. وطبقة المخدم VPN في هذا المثال هي طبقة CO (مثل أسلوب ATM) بينما طبقة العميل VPN هي CL (مثل إثرنت)، غير أنه يمكن استعمال أي توليفة تجمع بين أزواج CO أو CL.

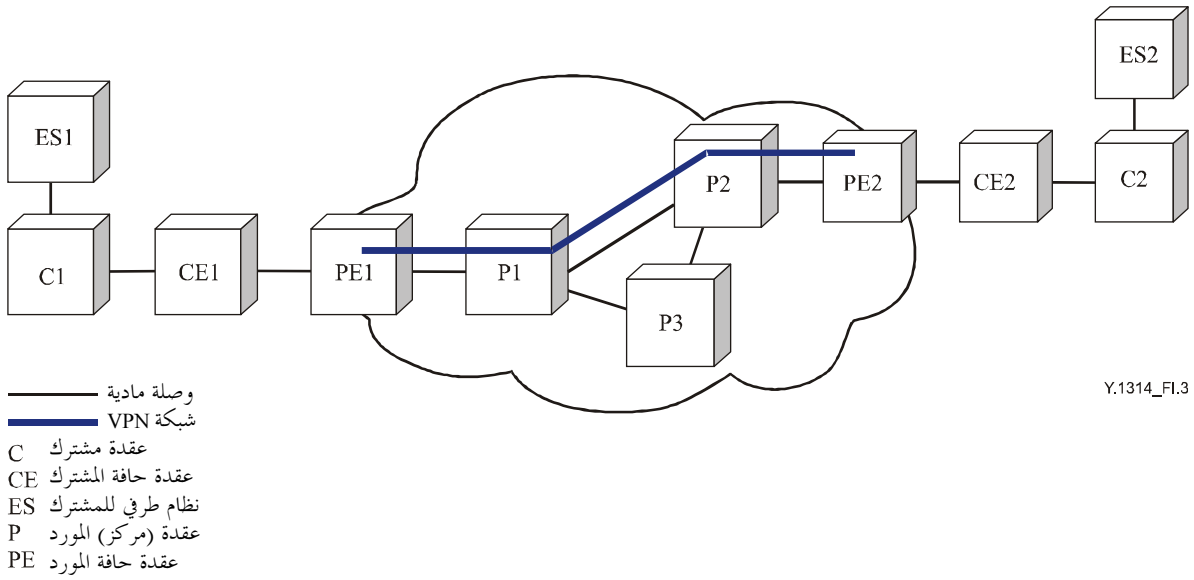



**الشكل Y.1314/2.I – موقع نقاط TFP طبقة العميل VPN الواقعة في عُقد CE**

وتخص عقد CE وP طبقتي العميل والمخدم VPN على التوالي، في حين تخص عقد PE كلتا الطبقتين. وتحدد نقطتا TFP الموجودتين في طبقة العميل VPN مكان بدء (مصدر) تدفق طبقة العميل P2P VPN (وهو عقدة CE في هذه الحالة) مكان انتهائه (بئره)، بينما تحدد نقطتا FP عقد PE التي يمر بها تدفق P2P. وبالمثل، تحدد نقطتا TFP الموجودتين في طبقة المخدم VPN مصدر وبئر توصيل الطبقة المذكورة، بينما تحدد نقطتا FP عقد P التي يمر بها التدفق. أما نقطتا AP المبينتان في طبقة المخدم VPN، فتحددان مصدر/بئر قناة طبقة المخدم VPN.

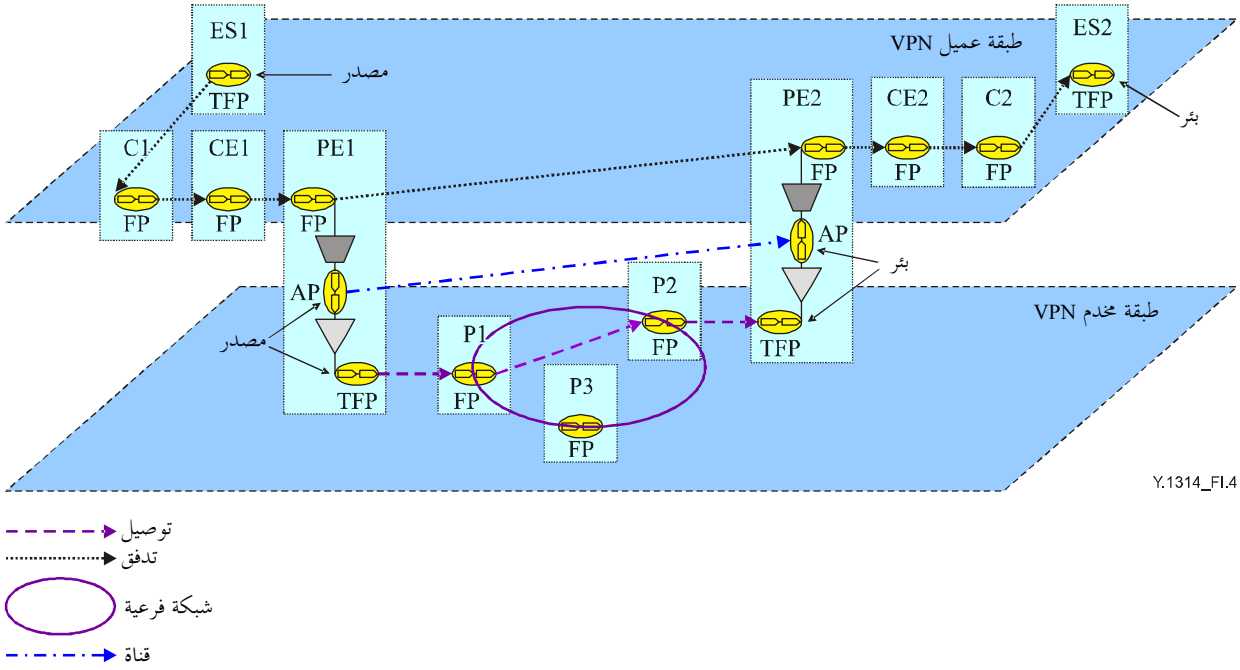
وتقع نقطتا TFP طبقة العميل VPN المبينتان في المثال السابق داخل عقد CE (CE1 وCE2)، غير أن الأمر ليس كذلك في جميع علاقات العميل/المخدم VPN، فقد تكون مثلاً طبقة العميل VPN إثرنت أو شبكة طبقة IP حيث تقع فيها نقطتا TFPفي المراكز/الأنظمة الطرفية.

ويوضح الشكل 3.I الطوبولوجيا المادية لشبكة VPN العميل/االمخدم. وإذا كانت طبقة العميل VPN هي إثرنت، عندئذ تكون عقد C بدالات إثرنت، وتكون الأنظمة الطرفية/المراكز، حواسيب/مخدمات بسطوح بينية لإثرنت.




**الشكل Y.1314/3.I – الطوبولوجيا المادية لشبكة VPN العميل/المخدم – المثال 2**

ويرد في الشكل 4.I مثال وظيفي يستند إلى الشبكة المادية المبينة في الشكل 3.I، حيث تقع نقاط TCP/TFP طبقة العميل VPN داخل الأنظمة الطرفية/المراكز وليس في نقاط CE.




**الشكل Y.1314/4.I – نقطة انتهاء تدفق TFP طبقة العميل VPN في الأنظمة الطرفية/المراكز**

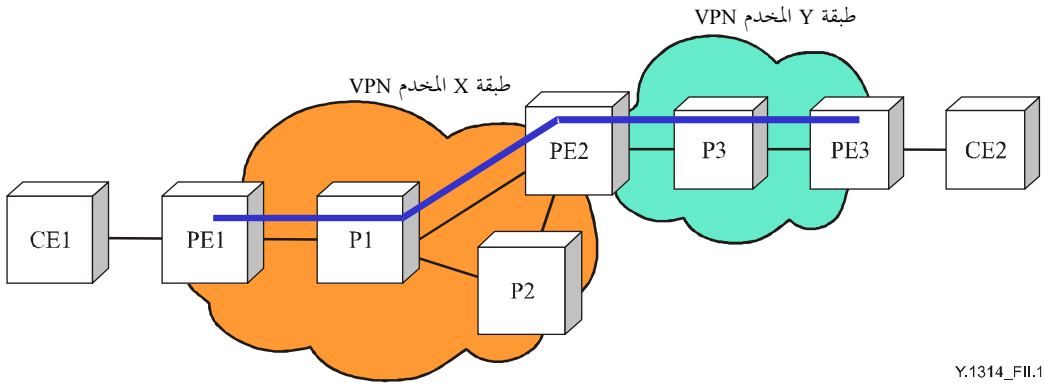
تنتمي عقد العميل C وحافة المشترك CE إلى جانب الأنظمة الطرفية ES إلى طبقة العميل VPN. وتخص عقد PE كل من طبقة المخدم VPN وطبقة العميل VPN، في حين تخص عقد P طبقة المخدم VPN فحسب. وتحدد نقطتا TFP الموجودتان في طبقة العميل VPN مصدر وبئر تدفق طبقة العميل VPN (وهما ES1 وES2 على التوالي)، بينما تحدد نقطتا FP عقد C، وCE، وPE التي يمر بها التدفق.

ورغم عدم توضيحها في الأمثلة السابقة، فإن من الممكن أيضاً أن يقع أحد طرفي TCP/TFP مصدر أو بئر الشبكة VPN على حافة المشترك CE، في حين يمكن ألا يكون موقع النقطة TFP في الطرف الآخر على حافة العميل، أي تقع نقطة التوصيل CP/نقطة التدفق FP على حافة المشترك CE بينما تقع نقطة TCP/TFP داخل إحدى عقد المشترك أو في نظام طرفي ES.

# التذييل II

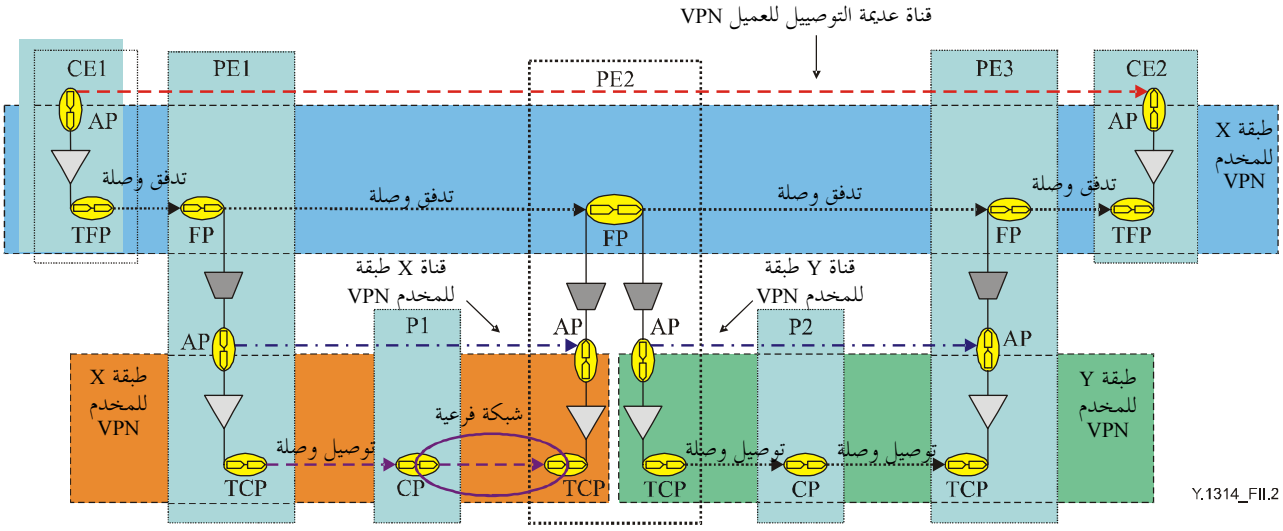
## شبكات VPN العميل/المخدم الحاوية على عدة طبقات مخدم VPN

يورد الشكل 1.II الطوبولوجيا المادية لشبكة VPN عميل/مخدم تستعمل طبقتين مختلفتين من طبقات المخدم VPN، هما X وY. وتخص عقد PE1 وP1 وP2 طبقة X للمخدم VPN، بينما تخص عقدتا P3 وPE3 الطبقة Y للمخدم VPN. أما العقدة PE2 فتخص كلتا طبقتي المخدم وهي بمثابة بوابة بينهما.




**الشكل Y.1314/1.II – الطوبولوجيا المادية للتشغيل البيني لطبقتي المخدم VPN**

وثمة طريقة للتشغيل البيني لطبقتي X وY المخدم VPN تتمثل في استخدام التشغيل البيني للعميل/المخدم على النحو الموضح في الشكل 2.II. وتخص عقدة PE2 الواردة في هذا المثال طبقتي X وY المخدم VPN، بينما تخص عقد PE الثلاث جميعها طبقة العميل VPN.



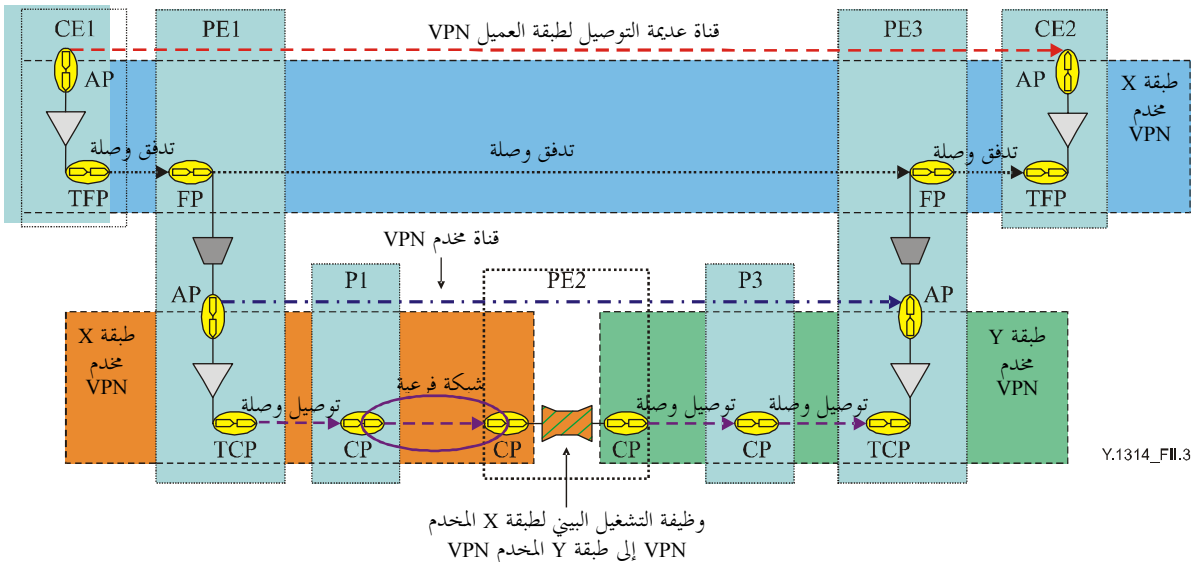

**الشكل Y.1314/2.II – التشغيل البيني لعميل/مخدم طبقة المخدم VPN**

وتعمل وظيفة تكييف مصدر طبقة X لمخدم VPN على تكييف المعلومات المميزة (CI) لطبقة العميل VPN لتصبح معلومات مكيفة (AI) في طبقة X لمخدم VPN، بينما تعمل وظيفة تكييف بئر طبقة X لمخدم VPN على تكييف معلومات AI طبقة X لمخدم VPN لتصبح معلومات CI طبقة العميل VPN. وبالمثل، تعمل وظيفة تكييف مصدر طبقة Y لمخدم VPN على تكييف معلومات CI طبقة العميل VPN لتصبح معلومات AI في طبقة Y لمخدم VPN، بينما تعمل وظيفة تكييف بئر طبقة Y لمخدم VPN على تكييف معلومات AI طبقة Y لمخدم VPN لتصبح معلومات CI طبقة العميل VPN.

وتشتمل عناصر الشبكة التي يُطبّق فيها تكييف العميل/المخدم على نقاط FP أو نقاط CP التابعة لطبقة العميل VPN، والتي يجب تحديد هويتها باستعمال عناوين طبقة العميل VPN. وهكذا، إذا كانت مثلاً طبقة عميل VPN بروتوكول IP، فإن نقاط PE1 وPE2 وPE3 تحتاج إلى عناوين بروتوكول IP التابعة لهذه الطبقة.

واستعمال عدة طبقات من طبقات المخدم VPN بتكييف العميل/المخدم في طبقات العميل CO VPN يعني أنه يجب حساب الطريق/المسير بطريقة دينامية/يدوية عبر نقاط التوصيل CP وإنشاء توصيلين على الأقل من توصيلات الوصلة من طرف إلى طرف في طبقة العميل VPN داخل شبكة المورد. أما في حال استعمال عدة طبقات من طبقات المخدم VPN بتكييف العميل/المخدم في طبقات العميل CL VPN، فإن ذلك يعني أنه يجب حساب الطريق/المسير بطريقة دينامية/يدوية عبر نقاط التدفق FP، وأنه يجب إرسال وحدات الحركة CL (أي الرزم) بالاستناد إلى معلومات العنوان الموجودة في طبقة العميل VPN. ويتعارض ذلك مع حالة إنشاء طبقة مخدم VPN واحدة من طرف إلى طرف عبر شبكة المورد بين نقاط FP/CP في طبقة العميل VPN. ولا تقتضي هذه الحالة سوى إنشاء توصيل/تدفق وصلة وحيد داخل شبكة المورد بين مصدر وبئر قناة طبقة المخدم VPN، وعليه، لا توجد ضرورة لحساب الطريق/المسير عبر شبكة المورد في طبقة العميل VPN.

وتوجد طريقة بديلة للتشغيل البيني لطبقتي X وY المخدم VPN المبينتين في الشكل 2.II تتمثل في استخدام التشغيل البيني لمستوى القرين المُوضح في الشكل 3.II. وتخص عقدة PE2 المبينة في هذا المثال طبقتي X وY المخدم VPN، ولكنها لا تخص طبقة العميل VPN. بينما تخص عقدتا PE1 وPE3 طبقتي X وY المخدم VPN على التوالي، كما تخصان طبقة العميل VPN.




**الشكل Y.1314/3.II – التشغيل البيني لمستوى القرين لطبقة المخدم VPN**

وتعمل وظيفة تكييف مصدر طبقة X للمخدم VPN على تكييف معلومات CI طبقة العميل VPN لتصبح معلومات AI في طبقة X للمخدم VPN، بينما تعمل وظيفة تكييف التشغيل البيني لطبقتي X وY المخدم VPN على تكييف معلومات AI طبقة X للمخدم VPN لتصبح معلومات AI طبقة Y للمخدم VPN. وتعمل وظيفة تكييف بئر طبقة Y للمخدم VPN على تكييف معلومات AI الطبقة Y للمخدم VPN لتصبح معلومات CI طبقة العميل VPN.

وثمة عامل رئيسي ينبغي مراعاته عند بحث التشغيل البيني لمستوى القرين، هو أن إمكانية التشغيل البيني بالاستناد إلى مستوى القرين تقتصر على تكنولوجيا معينة من تكنولوجيات الشبكة، فمثلاً، يمكن تشغيل شبكات ATM وشبكات ترحيل الأرتال تشغيلاً بينياً على أساس مستوى القرين (باستعمال رتل FRF.8)، بيد أنه يتعذر تشغيل شبكات IP وشبكات TDM على هذا الأساس. ولا يتطلب التشغيل البيني لمستوى القرين تشغيل الشبكات بينياً في مستوى البيانات فحسب، بل يتطلب أيضاً تشغيلها في مستوى التحكم من أجل أداء وظائف من قبيل التسيير، والتشوير، والتشغيل والإدارة والصيانة (OAM).

# التذييل III

## أمثلة على سيناريوهات خدمة VPN العميل/المخدم وخدمة VPN لمستوى القرين

تبين الجداول الواردة أدناه بعض الأمثلة على سيناريوهات مختلفة لخدمة VPN وتحدد هوية بعض الآليات/البروتوكولات النموذجية التي يمكن استعمالها لأداء الوظائف المطلوبة.

**ملاحظة** – يرد في ثبت المراجع المزيد من المراجع المتعلقة بالجداول الواردة في هذا التذييل.

**الجدول Y.1314/1.III – السيناريو 1 من سيناريوهات خدمة VPN العميل/المخدم**

| | **خدمة ترحيل أرتال الطبقة 2 عبر التبديل MPLS** | **خدمة VPWS إثرنت الطبقة 2 عبر بروتوكول IP/الصيغة L2TPv3** | **خدمة VPN المطابقة للمعيار RFC 2547/البروتوكول IP للطبقة 3** |
|---|---|---|---|
| **طبقة العميل VPN** | مرحل أرتال | إثرنت | IP |
| **طبقة المخدم VPN** | MPLS PW | L2TPv3/IP | MPLS |
| **الكشف عن عضوية VPN** | RADIUS، BGP، يدوي، NMS | RADIUS، BGP، LDP، RSVP-TE، يدوي، NMS | BGP |
| **تسيير طبقة المخدم VPN** | IGP، BGP، يدوي، NMS | IGP، BGP، يدوي، NMS | BGP |
| **إنشاء أنفاق/توصيلات طبقة المخدم VPN** | LDP، BGP، يدوي، NMS | تشوير L2TPv3 | BGP |
| **استيقان وتخويل ومحاسبة (AAA)/CE المستعمل** | RADIUS، المعيار IEEE 802.1X، RMON، NMS، SNMP | RADIUS، المعيار IEEE 802.1X، RMON، NMS، SNMP | بروتوكول التسيير CE-PE (مثل EBGP مع MD5)، RMON، SNMP، NMS |
| **تشكيل عناصر شبكة طبقة العميل VPN** | NMS، يدوي | NMS، يدوي، E-LMI | DHCP، NMS، يدوي |
| **تسيير طبقة العميل VPN** | NMS، يدوي | تعلم عناوين MAC | EBGP، OSPF، يدوي/سكوني |
| **تشوير أنفاق/توصيلات طبقة العميل VPN** | NMS، يدوي | غير مطلوبة لأن العميل هو CL-PS | غير مطلوبة لأن العميل هو CL-PS |
| **تشغيل وإدارة وصيانة (OAM) طبقة العميل VPN** | مرحل أرتال LMI | المعيار IEEE 802.1ag، E-LMI، المعيار IEEE 802.3ah، التوصية ITU-T Y.1731 | ضوضاء/طريق تتبع IP |
| **تشغيل وإدارة وصيانة (OAM) طبقة المخدم VPN** | التوصية ITU-T Y.1711، التوصية ITU-T Y.1713، MPLS، VCCV، ضوضاء LSP/BFD | ضوضاء/طريق تتبع IP | التوصية ITU-T Y.1711، التوصية ITU-T Y.1713، ضوضاء/طريق تتبع LSP |

**الجدول Y.1314/2.III – السيناريو 2 من سيناريوهات خدمة VPN العميل/المخدم**

| | خدمة SDH VPN الطبقة 1 عبر OTN | خدمة TDM VPN الطبقة 1 عبر التبديل MPLS | خدمة ATM VPN الطبقة 2 عبر التراتب SDH |
|---|---|---|---|
| **طبقة العميل VPN** | SDH (مثل STM-16) | TDM (E1 مثلاً) | ATM |
| **طبقة المخدم VPN** | قناة مسير ضوئية/بصرية (OCh) | MPLS PW | SDH (VC4 مثلاً) |
| **الكشف عن عضوية VPN** | التوصية ITU-T Y.1705.1/G.7714.1، يدوي، NMS | RADIUS، BGP، LDP، يدوي، NMS | يدوي، NMS |
| **تسيير طبقة المخدم VPN** | بروتوكولات التسيير ASON/GMPLS، يدوي، NMS | IGP، BGP، يدوي، NMS | بروتوكولات التسيير ASON/GMPLS، يدوي، NMS |
| **إنشاء أنفاق/توصيلات طبقة المخدم VPN** | بروتوكولات التشوير ASON/GMPLS، يدوي، NMS | LDP، BGP، يدوي، NMS | بروتوكولات التشوير ASON/GMPLS، يدوي، NMS |
| **استيقان وتخويل ومحاسبة (AAA) CE/المستعمل** | بروتوكولات ASON/GMPLS، SNMP، NMS | RMON، SNMP، NMS | ATM، أمن UNI/PNNI، RMON، SNMP، NMS |
| **تشكيل عناصر شبكة طبقة العميل VPN** | NMS، يدوي | NMS، يدوي | UNI ATM، يدوي، NMS |
| **تسيير طبقة العميل VPN** | بروتوكولات التسيير ASON/GMPLS، يدوي، NMS | يدوي، NMS | يدوي/سكوني، NMS، PNNI |
| **تشوير أنفاق/توصيلات طبقة العميل VPN** | بروتوكولات التشوير ASON/GMPLS، يدوي، NMS | يدوي، NMS | يدوي، NMS، PNNI |
| **تشغيل وإدارة وصيانة (OAM) طبقة العميل VPN** | رأسية SDH (مثل بايتات التتبع J0/J1/J2، بايتة حالة المسير G1) | التوصية ITU-T G.755، AIS/LOS | إدارة الخطأين F4 وF5، وعروة الرجعة، والتحقق من الاستمرارية (CC) |
| **تشغيل وإدارة وصيانة (OAM) طبقة المخدم VPN** | رأسية OCh (مثل معرف هوية تتبع القناة (TTI) المُستعمل في مراقبة المسير/القسم (PM/SM)) | التوصية ITU-T Y.1711، التوصية ITU-T Y.1713، MPLS VCCV، ضوضاء LSP/BFD | رأسية SDH (بايتات التتبع J0/J1/J2، بايتة حالة المسير G1 مثلاً) |

**الجدول Y.1314/3.III – سيناريوهات الخدمة VPN لمستوى القرين**

| | الخدمة IPsec VPN عبر الإنترنت | الخدمة VLAN VPN إثرنت |
|---|---|---|
| **طبقة القرين VPN** | IP | إثرنت |
| **الكشف عن عضوية VPN** | يدوي، NMS | يدوي، NMS، RADIUS |
| **استيقان وتخويل ومحاسبة (AAA) CE/المستعمل** | الاستيقان الأولي IKE (على أساس المفاتيح المُتقاسمة مسبقاً أو التوقيعات الرقمية)، RMON، SNMP، NMS | المعيار IEEE 802.1x، RADIUS، RMON، SNMP، NMS |
| **تسيير طبقة القرين VPN** | بروتوكولات التسيير IGP (ISIS، OSPF، RIP مثلاً)، BGP، يدوي، NMS | تحسين طوبولوجية STP وتعلم عناوين مستوي المعطيات (تجسير شفاف) |
| **تشكيل عناصر شبكة طبقة القرين VPN** | تشكيل المفتاح المُتقاسم أو طلب شهادة من هيئة إصدار الشهادات | تشكيل شبكات VLAN باستعمال التشكيل اليدوي، أو NMS، أو برتوكولات دينامية |
| **تشغيل وإدارة وصيانة (OAM) طبقة القرين VPN** | ضوضاء IP، طريق تتبع | المعيار IEEE 802.1ag، E-LMI، المعيار IEEE 802.3ah، التوصية ITU-T Y.1731 |

## ببليوغرافيا

تخضع المراجع المبينة هنا للتنقيح، ويُشجع مستعملو هذه التوصية على البحث عن آخر طبعة/مشروع من هذه المراجع.


ATM UNI: ATM Forum UNI 4.1 (2002), "*ATM User Network Interface (UNI) Signalling Specification version 4.1*", af-sig-0061.001.

ATM Forum PNNI 1.1 (2002), *Private Network-Network Interface Specification v.1.1*, af-pnni-0055.001.

IEEE 802.1ad (2005, Draft 6.0), *Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges*.

IEEE 802.1ag (2005, Draft 4.1), *Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management*, status: PAR approved, Task Group ballot in progress.

IEEE 802.1ah (Aug 2005, Draft 1.2), *Virtual Bridged Local Area Networks – Amendment 6: Provider Backbone Bridges*, status: PAR approved, Task Group ballot.

IEEE 802.1Q (2005), *Virtual Bridged Local Area Networks*, status: published.

IEEE 802.1X (2004), *Port-Based Network Access Control*, status: published.

IEEE 802.17 (2004), *Specific requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specifications*, status: published.

IEEE 802.3ah (2004), *Specific requirements – Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications* Amendment: *Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*, Ethernet in the First Mile amendment to IEEE Std 802.3.

IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview*.

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

IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

IETF RFC 3036 (2001), *LDP Specification*.

IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

IETF draft-ietf-bfd-base-03.txt (2005), *Bidirectional Forwarding Detection,* work in progress.

IETF draft-ietf-bfd-mpls-02.txt (2005), *BFD For MPLS LSPs*, work in progress.

IETF draft-ietf-l2tpext-l2vpn-05.txt (2005), *L2VPN Extensions for L2TP*, work in progress.

IETF draft-ietf-l2vpn-radius-pe-discovery-01.txt (2005), *Using RADIUS for PE-Based VPN Discovery,* work in progress.

IETF draft-ietf-l3vpn-bgpvpn-auto-06.txt (2005), *Using BGP as an Auto-Discovery Mechanism for Network-based VPNs*, work in progress.

IETF draft-ietf-l3vpn-rfc2547bis-03.txt (2004), *BGP/MPLS VPNs*, work in progress.

IETF draft-ietf-mpls-lsp-ping-09.txt (2005), *Detecting MPLS Data Plane Failures*, work in progress.

IETF draft-ietf-pwe3-control-protocol-17.txt (2005), *Pseudowire Setup and Maintenance using the Label Distribution Protocol*, work in progress.

IETF draft-ietf-pwe3-frame-relay-05.txt (2005), *Encapsulation Methods for Transport of Frame Relay Over MPLS Networks*, work in progress.

IETF draft-ietf-pwe3-vccv-06.txt (2005), *Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)*, work in progress.

ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan*.

ITU-T Recommendation E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*.

ITU-T Recommendation G.775 (1998), *Loss of Signal (LOS), Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) defect detection and clearance criteria for PDH signals*.

ITU-T Recommendation G.826 (2002), *End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections*.

ITU-T Recommendation G.827 (2003), *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*.

ITU-T Recommendation G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

ITU-T Recommendation G.1010 (2001), *End-user multimedia QoS categories*.

ITU-T Recommendation G.7714.1/Y.1705.1 (2003), *Protocol for automatic discovery in SDH and OTN networks*.

ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

ITU-T Recommendation Q.933 (2003), *ISDN Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*.

ITU-T Recommendation Q.2931 (1995), *Digital Subscriber Signalling System No. 2 – User-Network Interface (UNI) layer 3 specification for basic call/connection control*.

ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

ITU-T Recommendation Y.1413 (2004), *TDM-MPLS network interworking – User plane interworking*.

ITU-T Recommendation Y.1415 (2005), *Ethernet-MPLS network interworking – User plane interworking*.

ITU-T Recommendation Y.1711 (2004), *Operation & Maintenance mechanism for MPLS networks*.

ITU-T Recommendation Y.1713 (2004), *Misbranching detection for MPLS networks*.

ITU-T Recommendation Y.1731 (2006), *OAM functions and mechanisms for Ethernet based networks*.

MEF ETH OAM (2003), *Ethernet Services OAM*, Draft.

Frame Relay Forum FRF.8 (1995), *Frame Relay/ATM PVC Service Interworking Implementation Agreement*.

## 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 البرامج الإذاعية الصوتية والتلفزيونية 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 والأمن |
| **السلسلة Y** | **البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي** |
| السلسلة Z | لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات |

طبعت في سويسرا
جنيف، 2006