الخطة الوطنية للانتقال

إلى الإصدار السادس من بروتوكول الإنترنت

فريق عمل الخاص بالانتقال إلى الإصدار السادس من بروتوكول الإنترنت

(IPv6 Task Force)

نسخة رقم: 1.0

تاريخ الإصدار : 11/ 08 / 2024م

جدول المحتويات

1. مقدمة

في إطار تنفيذ الاستراتيجية الوطنية للاتصالات والمعلوماتية 2023 – 2027 م، شكلت الهيئة العامة للاتصالات والمعلوماتية فريقًا يضم مجموعة من المتخصصين والخبراء من شركات الاتصالات العامة والخاصة للبدء في وضع خطة للانتقال إلى الإصدار السادس لبروتوكول الإنترنت (IPv6)، حيث يعد هذا الانتقال من أهم الركائز التي تساهم في المضي قدمًا لتنفيذ هذه الاستراتيجية، مما يحتم علينا تعزيز وتسريع هذا الانتقال.

والجدير بالذكر أن عناوين الإصدار الرابع لبروتوكول الإنترنت (IPv4) قد استنفذت على مستوى سلطات تخصيص عناوين الإنترنت وبعض الموزعين الإقليميين، وقد أثبت الإصدار الرابع محدوديته فيما يخص قدرته على تلبية متطلبات النمو الاجتماعي والاقتصادي، ونتيجة لذلك أصبح الانتقال إلى الإصدار السادس ضرورة ملحة.

ومع التطور السريع للتكنولوجيا والانتشار المتنامي للخدمات الجديدة المعتمدة على شبكة الإنترنت، فإننا لا نحتاج فقط إلى عناوين لأجهزة الكمبيوتر الشخصية والخوادم، ولكن أيضًا لجميع أنواع أجهزة إنترنت الأشياء، ولمواكبة هذا التطور السريع لا يسعنا إلا أن نسارع في تطبيق الإصدار السادس (IPv6). بالإضافة إلى أن الإصدار السادس سيساهم في العديد من التحسينات من حيث الأمان وسرعة الوصول إلى وجهة الاتصال وجودة الخدمة (QoS)، وبالتالي يتيح للمستخدمين خدمة أفضل وأمانًا أكبر.

ولتطبيق وتسريع الانتقال إلى بروتوكول الإصدار السادس، تولى الفريق إعداد هذه الخطة ومتابعة تنفيذها، من خلال دعم الجهات المعنية في عملية الانتقال من الإصدار الرابع (IPv4) إلى الإصدار السادس (IPv6) لبروتوكول الإنترنت.

2. أهداف الخطة

تتلخص أهداف الخطة الوطنية للانتقال إلى الإصدار السادس لبروتوكول الإنترنت في الآتي:

- ✓ الاستعداد لما بعد نفاذ عناوين الاصدار الرابع من خلال دعم الإصدار السادس وضمان الاستقرار واستمرارية الأعمال والتطور المستمر في شبكة الانترنت داخل ليبيا.
- ✓ حث الجهات العامة والخاصة، ورفع مستوى الوعي بأهمية نشر الإصدار السادس والعمل به.
- ✓ ضمان سلاسة عملية الانتقال إلى الإصدار السادس من قبل الجهات المعنية والحد من المخاطر.

- ✓ تقديم المعلومات اللازمة من خلال فريق عمل الإصدار السادس لبروتوكول الإنترنت لمساعدة الجهات المعنية على تطوير خطة الانتقال داخل الجهة.

3. حول فريق العمل

بمبادرة من الهيئة العامة للاتصالات تم إنشاء فريق عمل وطني للانتقال إلى الإصدار السادس لبروتوكول الإنترنت يضم معظم أصحاب المصلحة الرئيسيين المعنيين من القطاعين الحكومي والخاص لوضع خطة الانتقال ورفع مستوى الوعي بأهمية الإصدار السادس ونشره والمشاركة في المشاريع والأنشطة ذات الصلة.

يعمل أعضاء الفريق على وضع خطة محكمة للانتقال إلى IPv6 وتحديد الموارد ووضع الجدول الزمني المناسب. كما يقوم أعضاء فريق العمل بالتحليل والتخطيط من خلال البنية التحتية الحالية وتحليل التوافق مع IPv6. قد يختلف حجم وتكوين فريق العمل وفقًا لحجم المشروع ونطاق الانتقال إلى IPv6، قد يكون هناك فريق متخصص داخل المؤسسة، وقد يتم التعاون مع شركاء من خارج المؤسسة.

1.3 أهداف فريق العمل

تتلخص أهداف فريق العمل كالتالي:

1. زيادة الوعي حول استنفاذ عناوين الإصدار الرابع وبأهداف خطة الانتقال لدعم تبني ونشر الإصدار السادس لضمان استقرار الشبكة واستمرارية الأعمال ودعم نموها وتطورها المستقبلي.
2. تنظيم المؤتمرات والأنشطة الخاصة بدعم نشر الإصدار السادس في الدولة.
3. إيجاد الحوافز لمقدمي خدمات الإنترنت وغيرهم من المعنيين، بغرض تشجيعهم على الانتقال إلى استخدام الإصدار السادس.
4. العمل كجهة اتصال أساسية بشأن كل الأنشطة ذات الصلة بالإصدار السادس في الدولة، لتجنب ازدواجية الجهود أو غياب الاتصال بين الأطراف المعنية.

2.3 مسؤوليات فريق العمل

يتحمل فريق العمل مسؤوليات متنوعة ومهمة لضمان نجاح تنفيذ IPv6 وانتقال الشبكة إلى هذا الإصدار الجديد، حيث تتضمن المسؤوليات الرئيسية التي يتحملها فريق العمل كالتالي:

1. وضع خطة الانتقال إلى الإصدار السادس من بروتوكول الإنترنت (IPv6).

2. متابعة سير عمل الخطة ومعالجة المشاكل المتعلقة بهذا الانتقال كتخصيص العناوين، تغيير المعدات، بناء القدرات، وكل ما له علاقة بهذا الانتقال
3. إصدار وثيقة أو دليل إرشادي للانتقال للإصدار السادس من بروتوكول الإنترنت (IPv6).
4. بناء القدرات من خلال اقتراح تأسيس وتجهيز معمل خاص بالتجارب والدورات التدريبية حول الإصدار السادس لبروتوكول الانترنت (IPv6) لتشجيع أصحاب المصلحة.
5. دراسة وفهم آليات الانتقال، ودراسة تجارب الدول المجاورة والمتقدمة لتفادي الوقوع في نفس الأخطاء وبالتالي تسريع عملية الانتقال وتوفير الوقت والجهد والمال.
6. تجميع بيانات حول البنى التحتية لشبكات الاتصالات ودراسة إمكانية التحول في كل مؤسسة.
7. زيادة الوعي حول مشكلة انتهاء عناوين الإصدار الحالي لبروتوكول الإنترنت IPv4 ، لتوضيح أهمية البدء في تبني الإصدار السادس IPv6.
8. توحيد الجهود لتفادي تكرار العمل، وزيادة التعاون بين الجهات ذات العلاقة.
9. تنظيم المؤتمرات والأنشطة الخاصة بدعم نشر الإصدار السادس.

3.3 أعضاء فريق العمل

كما يتضمن فريق عمل الانتقال إلى الإصدار السادس لبروتوكول الإنترنت IPv6 :

1. مدير الإدارة العامة لشؤون التنظيم	مشرف عام
2. مدير الإدارة العامة لتطوير قطاع الاتصالات	نائباً للمشرف العام
3. مدير إدارة تنظيم خدمات المعلوماتية	منسقاً عاماً
4. نائب رئيس مجلس ليبيا للإصدار السادس لبروتوكول الإنترنت IPv6	مستشار
5. مدير مكتب الشبكات والبنية التحتية	عضواً
6. رئيس قسم النطاقات وحماية البيانات	عضواً
7. رئيس وحدة الخدمات الجديدة والناشئة	عضواً
8. مندوباً عن الهيئة الوطنية لأمن وسلامة المعلومات	عضواً
9. مندوباً عن شركة الاتصالات الدولية	عضواً
10. مندوباً عن شركة ليبيا للاتصالات والتقنية	عضواً
11. مندوباً عن شركة هاتف ليبيا	عضواً
12. مندوباً عن شركة الجيل الجديد	عضواً
13. مندوباً عن شركة المدار الجديد	عضواً
14. مندوباً عن أكاديمية الاتصالات تقنية المعلومات	عضواً
15. مندوبون عن الشركات الخاصة من مزودي خدمة الإنترنت (ISPs)	عضواً
16. مندوباً عن الشركة العامة للكهرباء	عضواً
17. مندوباً عن شركة العنكبوت الليبي	عضواً

18. مندوبـــــــاً عن الأكاديمية الليبية للدراسات العلـــيـــــــــــا عضـــــــــــواً

4. أدوار ومسؤوليات أصحاب المصلحة

1.4 القطاع العام والخاص

المهام الرئيسية للمؤسسات العامة والخاصة

1.1.4. تخصيص وإعداد عناوين IPv6 للأجهزة والشبكات المختلفة.

2.1.4. عقد ورش عمل عملية لتدريب الموظفين على إعداد ومراقبة وصيانة الشبكات التي تعتمد على IPv6.

3.1.4. تحديث البرمجيات الثابتة (firmware) وبرامج الشبكة لضمان التوافق مع IPv6.

4.1.4. إجراء اختبارات على الشبكات الجديدة لضمان التوافق والأداء الأمثل.

5.1.4. تنفيذ التحويل تدريجيًا لتقليل المخاطر والاضطرابات.

6.1.4. مراقبة الشبكات بانتظام وصيانتها لضمان الأداء المستدام.

7.1.4. إعداد تقارير دورية لتقييم الأداء واكتشاف أي مشاكل محتملة.

2.4 مزودي خدمة الإنترنت

تتمثل أهم أدوار مزودي خدمة الإنترنت إلى عدة عوامل خاصة بالمعدات سواء بالشبكة الحالية أو المعدات التي ستورد لاحقا كذلك دور عمل المؤسسات وعمليات النقل الى الاصدار السادس مع ضمان الخدمات:

أولا: يجب أن يكون لدى مزودي الخدمات فريق عمل قادر على ضمان وتنفيذ الاختبارات على المعدات وتجهيز البنية التحتية لذلك وفيما يلي أهم الاختبارات :

أ. ترقية الأجهزة:

i. أجهزة التوجيه والمحولات: تحديث أو استبدال أجهزة التوجيه والمحولات لدعم IPv6.

ii. خوادم **DHCP** و**DNS:** تهيئة خوادم DHCPv6 لدعم توزيع عناوين IPv6 وتحديث خوادم DNS لدعم سجلاتAAAA.

ب. تهيئة **Dual-Stack:**

i. تفعيل **Dual-Stack:** إعداد الشبكة لدعم كل من IPv4 وIPv6 في الوقت نفسه لضمان استمرارية الخدمة خلال فترة الانتقال.

ج. بيئات الاختبار:

i. اختبار الشبكة: إنشاء بيئات اختبار تحتوي على كل من IPv4 وIPv6 لضمان التوافق والاختبار الشامل قبل التنفيذ الكامل.

د. الانتقال التدريجي:

i. تنفيذ عملية الانتقال على مراحل، بدءً من الأقسام غير الحيوية للشبكة، ثم الانتقال إلى الأجزاء الأكثر أهمية.

ه. التعامل مع التوافق:

i. استخدام تقنيات الانتقال: استخدام تقنيات مثل NAT64 وDNS64 لضمان التوافق بين IPv4 وIPv6 خلال فترة الانتقال.

أولا: المستفيدين من المؤسسات والشركات:

1. جميع الاتصالات السلكية واللاسلكية الجديدة المقدمة للمستفيدين يجب أن تكون قادرة على حمل حركة مرور IPv6.
2. أما بخصوص المستفيدين الحاليين الذين ليسوا جاهزين فإنه يجب على مزود خدمة الانترنت أن يقوم بتثقيف وتشجيع المستفيدين على التحول إلى IPv6.

ثانيا: المستفيدين من التجزئة السلكية:

1. جميع اتصالات مستفيدين التجزئة السلكية الجديدة التي يقدمها مزودو خدمة الإنترنت يجب أن تكون قادرة على حمل حركة مرور IPv6 مع الربع الأول سنة 2025
2. يجب أن يسعى مزود خدمة الإنترنت إلى استبدال أو ترقية معدات المستفيدين المملوكة له بشكل تدريجي.
3. المعدات (CPE) التي ليست جاهزة لـ IPv6 وفقًا للجداول الزمنية التالية:
   أ. استبدال / ترقية 50% من CPE بحلول النصف الأول لسنة 2025
   ب. استبدال / ترقية 100 % من CPE مع نهاية سنة 2025

4. فيما يتعلق بالمستفيدين الذين يملكون CPE خاص بهم، والذين ليسوا جاهزين لـ IPv6، يجب على مزود خدمة الإنترنت تثقيفهم وتشجعهم على استبدال / ترقية CPE.

ثالثا. المستفيدين من التجزئة اللاسلكية:

- بدءً من العام القادم، جميع مستفيدين التطور طويل الأمد (LTE) الجدد يجب أن تكون الاتصالات التي يقدمها مزودو خدمات الإنترنت قادرة على حمل حركة مرور IPv6.

3.4 مطوري التطبيقات

تتمثل أهم أدوار ومسؤوليات مطوري التطبيقات في التالي:

1.3.4. العمل على تبنّي دعم التطبيقات لكل من الإصدارين الرابع والسادس في بداية مراحل الانتقال إلى تمكين الإصدار السادس لبروتوكول الإنترنت.

2.3.4. تحديد التطبيقات التي من المحتمل أن تتأثر بعملية الانتقال إلى الإصدار السادس وذلك يشمل (أنظمة التشغيل – التطبيقات المؤسسية – نظام إدارة الشبكة – وقواعد البيانات).

3.3.4. العمل على توفير إمكانية تحديث أو استبدال التطبيقات الغير متوافقة مع الإصدار السادس لبروتوكول الإنترنت واتخاذ التدابير اللازمة للحد من أخطاء البرمجة والتعريفات لهذه التطبيقات.

4.3.4. البيئة المستخدمة لديهم تدعم IPv6

5.3.4. المكتبات المستخدمة في التطبيقات تدعم IPv6

6.3.4. فهم التغييرات التي قد تحدث بسبب اختلاف آلية نقل البيانات بين ال IPv6 وIPv4، وضع في الاعتبار الآثار المترتبة على larger header sizes عند تصميم بروتوكولات الشبكة وخوارزميات نقل البيانات.

7.3.4. تجربة التطبيقات التي تم تطويرها.

4.4 مستوردي المعدات

يجب على مستوردي المعدات الالتزام والتقيد بالآتي:

1.4.4. عدم استيراد المعدات الغير متوافقة مع الإصدار السادس لبروتوكول الإنترنت.

2.4.4. إجراء اختبارات معملية على المعدات قبل استيرادها والتأكد من أنها تدعم كلا الإصدارين الرابع والسادس لبروتوكول الإنترنت في آن واحد.

3.4.4. أن يكون التوافق مع الإصدار السادس لبروتوكول الإنترنت شرطا إلزاميا في جميع عقود شراء معدات تكنولوجيا الاتصالات والمعلومات.

4.4.4. أن تتوافق جميع أجهزة ومعدات تكنولوجيا الاتصالات والمعلومات مع المتطلبات المذكورة في لائحة الاعتماد النوعي المنشورة في موقع الهيئة www.cim.gov.ly.

5. آليات الانتقال إلى الإصدار السادس لبروتوكول الإنترنت

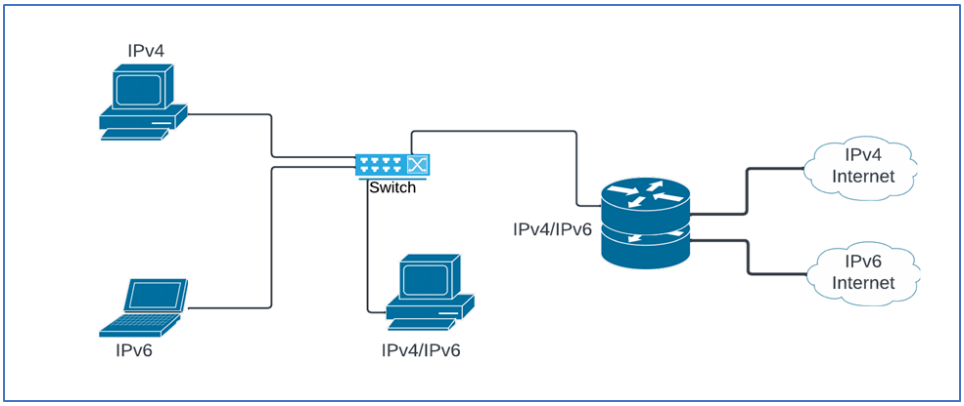
توجد ثلاث آليات للانتقال من IPv4 إلى IPv6 وهي كالتالي:

- الاستخدام المزدوج للإصدارين الرابع والسادس (Dual-Stack).
- استخدام القنوات والتمرير (Tunneling).
- استخدام طريقة الاقتران (Protocol Translation).

فيما يلي شرح تفصيلي للآليات الثلاثة:

1.5. الاستخدام المزدوج للإصدارين الرابع والسادس (Dual-Stack)

يقوم كل جهاز على الإنترنت بتنفيذ IPv6 وIPv4 وتمكينه، وتسمح هذه الألية للمستفيدين الذين يدعمون IPv6 بالتواصل مع الخوادم التي تستخدم اتصال IPv6 / IPv4، يوضح الشكل 1 بنية Dual-Stack.



الشكل 1 - بنية **Dual Stack**

1.1.5 الآثار الأمنية للاستخدام المزدوج للإصدارين الرابع والسادس (Dual-Stack)

بما آن كل جهاز سيتم تنفيذه وتشغيله باستخدام مجموعتين مختلفتين من البروتوكولات(IPv6 و IPv4), من الواضح أن تنفيذ ونشر وتشغيل Stack إضافي يزيد من سطح الهجوم المحتمل, على وجه الخصوص، نظراً لأن مستوى نضج تطبيقات IPv6 لا يتطابق عموماً مع مستوى تطبيقات IPv4 الحالية، فمن المحتمل جداً أن يتم اكتشاف أخطاء جديدة ربما لها آثار أمنية في كود IPv6، وبالتالي يجب توخي الحذر بشكل خاص للحفاظ على نظام التشغيل والتطبيقات محدثة

2.1.5 توصيات الاستخدام المزدوج للإصدارين الرابع والسادس (Dual-Stack)

يعد Dual-Stack عموماً الآلية المثالية للانتقال إلى IPv6، نظراً لأنها تستخدم اتصال IPv6 الأصلي و IPv4 الأصلي. العيب الوحيد لهذه التقنية الانتقالية هو أنها تتطلب تشغيل وإدارة شبكتين منفصلتين شبكة IPv6 وشبكة IPv4.

2.5. استخدام القنوات والتمرير (Tunneling)

تسمح هذه الآلية لحزم بيانات الإصدار السادس بأن يتم إرسالها عبر شبكات عناوين الإصدار الرابع الحالية، عن طريق تغليفها ضمن حزم الإصدار الرابع. وعادة ما يستخدم هذا الأمر كبداية للانتقال إلى الإصدار السادس أو عند عدم توفر الدعم لبروتوكول الإصدار السادس على بعض الأجهزة، فعلى سبيل المثال تستخدم للربط مع مزودي الخدمة الذين لا يدعمون بروتوكول الإصدار السادس في شبكاتهم.

1.2.5 الآثار الأمنية لاستخدام القنوات والتمرير (Tunneling)

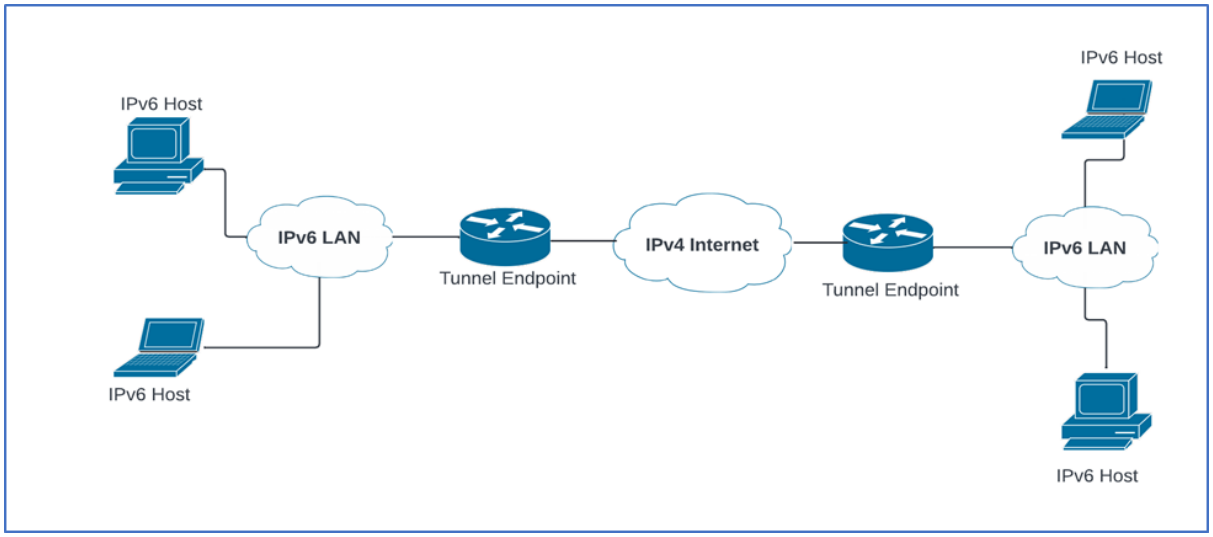
يشير نموذج النفق إلى ضرورة تغليف حزم IPv6 في IPv4 لاجتياز شبكات IPv4 فقط. من الواضح أن استخدام أي شكل من أشكال آلية الأنفاق يؤدي إلى تعقيد إضافي في حركة المرور الناتجة. على سبيل المثال، قد لا يتمكن جدار الحماية أو جهاز IDS/IPS من فحص حزمة IPv6 المغلفة عند استخدام الاتصال النفقي. قد يعني هذا أنه يمكن التحايل على بعض الضوابط الأمنية نتيجة لحركة المرور عبر الأنفاق.

بالإضافة إلى ذلك، قد تتفاعل بعض آليات تجهيز الأنفاق التلقائية بطرق غير متوقعة: على سبيل المثال، ما لم يتم اتخاذ إجراءات التخفيف المناسبة، فقد تتعرض لهجمات حلقة التوجيه التي قد تؤدي إلى سيناريوهات رفض الخدمة DoS.

وأخيراً، قد يؤدي الاستخدام غير المقصود لآلية تجهيز الأنفاق التلقائية إلى زيادة سطح الهجوم للشبكات التي يُفترض أنها "IPv4 فقط".

2.2.5 الأنفاق المكونة (6 في 4) Configured tunnels - 6in4

تتطلب الأنفاق التي يتم تكوينها يدوياً بأن يقوم مسؤول الشبكة بتكوين نقاط نهاية الأنفاق يدوياً. في حين أن هذا ينطوي على بعض العبء على مسؤول الشبكة، فإن هذا يعني أيضاً أن مشكلات اتصال IPv6 (ستكون سهلة في استكشاف الأخطاء وإصلاحها، نظراً لأن نقطتي نهاية النفق محددة)، يوضح الشكل 2 سيناريو نموذجي لنفق 6 في 4.

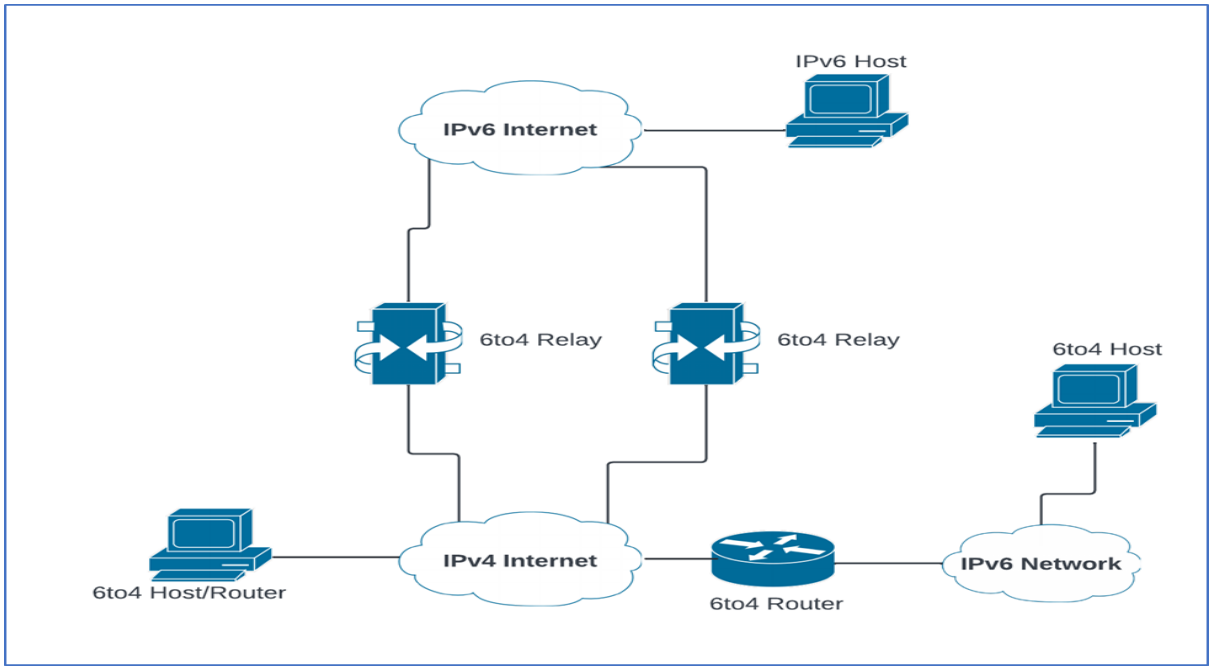


الشكل 2 - سيناريو النفق النموذجي 6 في 4

3.2.5 اتصال مجالات IPv6 عبر سحابات IPv4

Connection of IPv6 Domains via IPv4 Clouds (6to4)

(6to4) عبارة عن آلية تحويل تلقائي يمكن أن توفر اتصال IPv6 بشبكة IPv4 التي تستخدم عناوين IPv4 عالمية، أو حيث يمكن لجهاز التوجيه الأخير استخدام عنوان عالمي للعمل كموجه 4to6, يوضح الشكل 3 بنية 4to6.

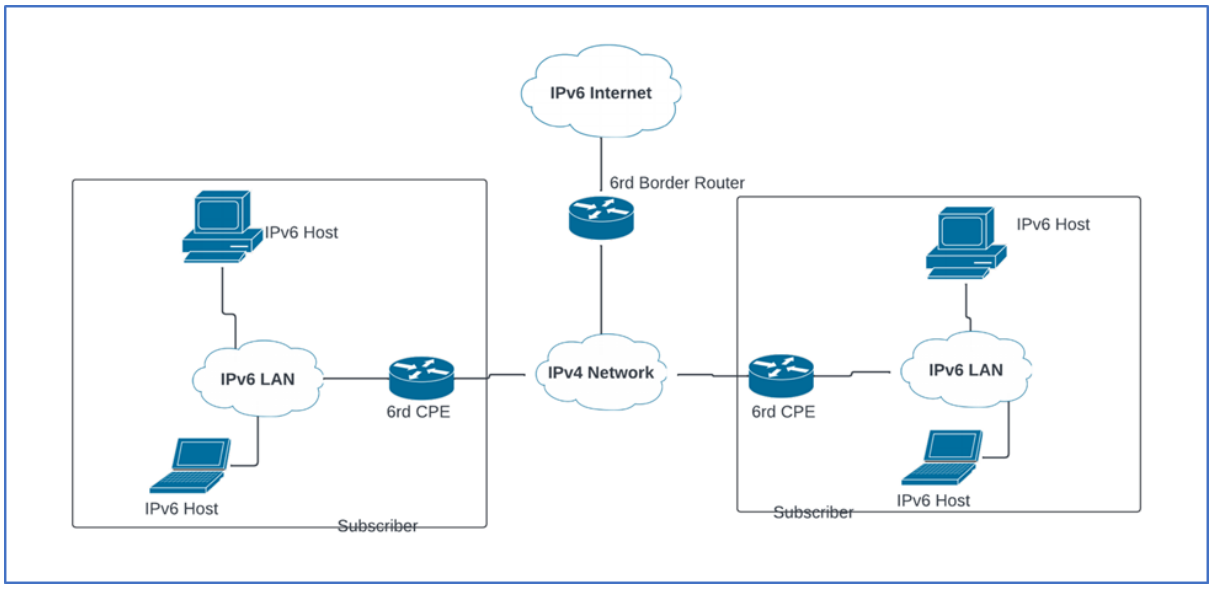


الشكل 3 - بنية 6to4

4.2.5 آلية النشر السريع لـ IPv6 -IPv6 Rapid Deployment (6rd)

تعتمد بنية بروتوكول 6rd على بروتوكول 4to6، وله نفس الحد الأدنى من ال overheads مثل جميع البروتوكولات التي تستخدم تغليف البروتوكول 41. تتمثل الاختلافات الرئيسية بين 6rd و4to6 في أن 6rd مخصص للاستخدام داخل شبكة مزود الخدمة ولا يستخدم بادئة IPv6 خاصة ولكن بادئة واحدة أو أكثر يتم توجيهها إلى مزود الخدمة. على هذا النحو، لا يمكن التعرف على مستخدمي 6rd على الفور من خلال عنوان IPv6 الخاص بهم كما هو الحال مع مستخدمي 4to6, بينما يستخدم 4to6 مرحلات تعتمد على التوجيه، يستخدم 6rd مرحلات مقدمة ومدارة من قبل مزود الخدمة. وبسبب هذه البنية، لا يجتاز النفق شبكات غير معروفة؛ وهذا يجعل أي تصحيح للأخطاء أسهل بكثير.

يوضح الشكل 4 نموذج نشر 6rd.



الشكل 4 - نموذج نشر **6rd**

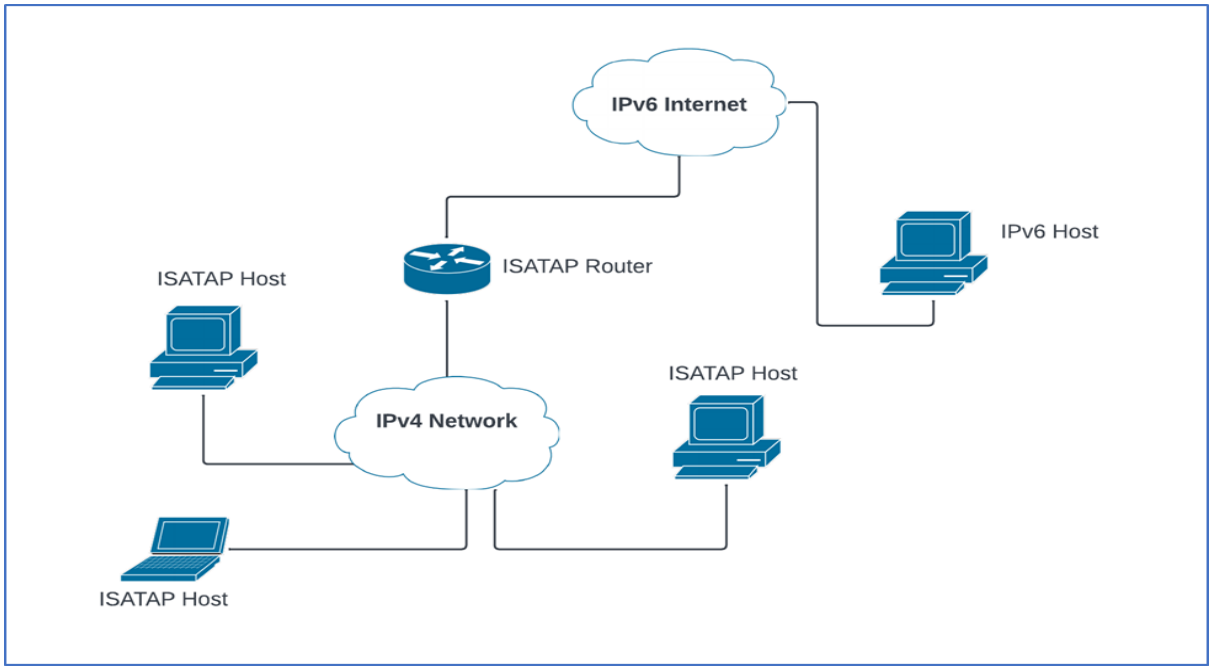
5.2.5 بروتوكول IPv6 الأصلي خلف NAT44 CPEs - Native IPv6 behind NAT44 CPEs (6a44)

الغرض من 6a44 هو تمكين مزودي خدمة الإنترنت من إنشاء اتصال IPv6 لكافة المستفيدين، على الرغم من استخدام جهاز CPE أو بوابة منزلية غير مهيأة للإصدار IPv6. البنية التحتية المطلوبة لذلك هي مرحل 44a6 في شبكة مزود خدمة الإنترنت وعميل 44a6 في الشبكة الداخلية للعميل. 44a6 بالنسبة إلى Teredo ما هو إلا 6rd بالنسبة إلى 4to6. وهذا يعني أنه مصمم لتجنب قيود Teredo مع 44a6، يتمتع مزودي خدمات الإنترنت بالتحكم الكامل في المرحلات (Relays) المعنية، بحيث يتم تجنب أوجه القصور المعروفة في Teredo. في حين تم تصميم Teredo كحل عالمي دون الاعتماد على تعاون مزودي خدمة الإنترنت، فإن نفق 44a6 يفترض صراحةً تعاون مزودي خدمة الإنترنت. بدلاً من استخدام بادئة Teredo المعروفة، يتم استخدام بادئة /48 من مساحة عنوان موفر خدمة الإنترنت. تم تعيين عنوان IPv4 معروف (anycast) للمرحل 44a6 ليتم تشغيله داخل شبكة موفر خدمة الإنترنت دون أي تكوين للعميل. يتم تخصيص هذا العنوان المعروف جيداً من نفس 24 / IPv6 مثل 4to6.كجزء من عملية التمهيد الخاصة به، يطلب عميل 44a6 عنواناً من مرحل 44a6، ويحافظ على حالة التعيين في شبكات NAT وجدران الحماية على المسار. يتم تغليف حركة المرور التي يتم تمريرها من إنترنت IPv6 الأصلي إلى a446 في UDP و IPv4 بواسطة المرحل ويتم فك تغليفها بواسطة عميل 44a6؛ ويتم العكس في الاتجاه الآخر.

6.2.5 بروتوكول العنونة النفقية التلقائية داخل الموقع - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

ISATAP هي آلية تحويل تلقائي تسمح بالنشر التدريجي لـ IPv6 داخل شبكة تنظيمية ل IPv4 فقط. وهي مشابهة لـ 4over6، ولكن دون اشتراط أن تدعم شبكة IPv4 البث المتعدد (Multi Cast)؛ وعلى عكس 4over6، تستخدم ISATAP نموذج اتصال غير متعدد البث والوصول وبالتالي لا تدعم البث المتعدد.

يوضح الشكل 5 نموذجاً لنشر ISATAP.

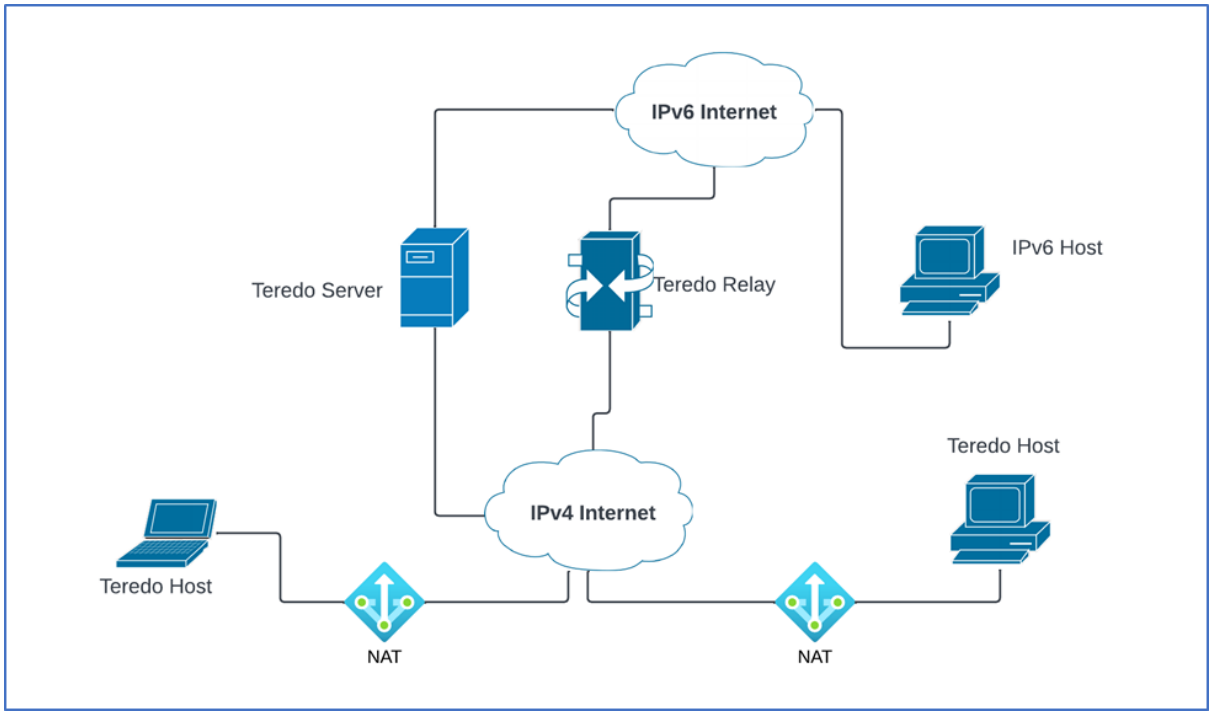


الشكل 5 - نموذج لنشر ISATAP

7.2.5 تمرير IPv6 عبر UDP من خلال شبكات NAT -

Tunnelling IPv6 over UDP through NATs (Teredo)

Teredo - هي آلية تحويل تلقائي مصممة خصيصاً لتوفير اتصال IPv6 إلى عقد IPv4 خلف محولات عناوين الشبكة (NATs). في حين يمكن اعتبار Teredo تصميمًا ذكيًا للتغلب على التحدي الذي تمثله شبكات NAT، إلا أنه يعاني من العديد من عيوب آليات التحويل التلقائي الأخرى. إلى جانب ذلك، عادة ما يؤدي ذلك إلى ضعف اتصال IPv6 (على سبيل المثال من حيث التأخير)، وبالتالي لا يشجع نشر تريدو, يوضح الشكل 6 بنية Teredo.



الشكل 6 - بنية Teredo

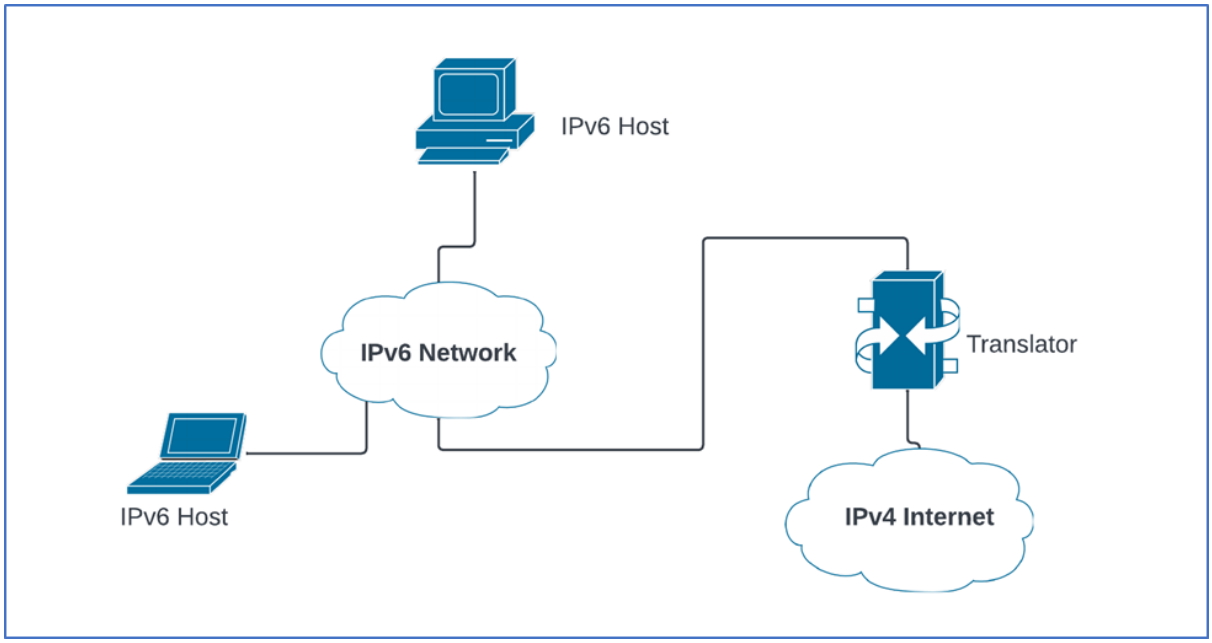
3.5. استخدام طريقة الاقتران (الترجمة) (Protocol Translation)

تتضمن الترجمة بشكل أساسي ترجمة حزم بروتوكول طبقة الإنترنت. من منظور الانتقال إلى IPv6، هناك سيناريوهان مختلفان لتطبيق الترجمة:

شبكتين تستخدمان بروتوكولات طبقة-3 مختلفة (على سبيل المثال IPv6 و IPv4) تحتاجان إلى الربط البيني.

أجهزة متعددة تحتاج إلى دمج الإرسال في عنوان طبقة-3 واحد.

في السيناريو الأول، تتم ترجمة حزم IPv6 إلى حزم IPv4، والعكس صحيح. يسمح ذلك لشبكات IPv6 فقط التواصل مع شبكات IPv4، وإن كان ذلك مع بعض القيود. يوضح الشكل 7 إعداداً نموذجياً.



الشكل 7- إعداد ترجمة نموذجي

الحالة الثانية هي تلك التي تحتاج فيها أجهزة متعددة إلى دمج الإرسال في عنوان IP واحد.

6PE: إستخدم IPv6 عبر MPLS

6PE) IPv6 Provider Edge) هو تقنية تُستخدم لنقل حركة IPv6 عبر شبكة MPLS (Multiprotocol Label Switching)) التي تعتمد على IPv4. تُعد هذه التقنية مهمة لمقدمي خدمات الإنترنت (ISPs) الذين يرغبون في تقديم خدمات IPv6 دون الحاجة إلى تحويل كامل الشبكة الأساسية إلى IPv6.

كيفية عمل PE6

1. العقد الطرفية لمقدمي الخدمة (Provider Edge Routers):

1.1 تعمل العقد الطرفية لمقدمي الخدمة (PE) كجسور بين شبكات IPv6 المحلية (LAN) وشبكة MPLS الأساسية التي تعمل بـ IPv4.

2.1 تقوم هذه العقد بإضافة تسميات MPLS إلى حزم IPv6، مما يتيح نقلها عبر شبكة MPLS.

2. نقل الحزم عبر MPLS:

1.2 عندما تصل حزمة IPv6 إلى عقدة PE، تُغلف الحزمة بإطار MPLS يحمل تسميات MPLS.

2.2 تُنقل الحزم عبر شبكة MPLS باستخدام توجيه التسميات بدلاً من التوجيه القائم على IP.

3. تفريغ الحزم في العقد الطرفية:

1.3 عند وصول الحزمة إلى عقدة PE النهائية، تُزال التسميات، ويُعاد الحزمة إلى شكلها الأصلي (IPv6) لتسليمها إلى الوجهة النهائية.

الفوائد الرئيسية لاستخدام PE:6

1. استفادة من البنية التحتية الحالية:

1.1 يسمح PE6 باستخدام البنية التحتية القائمة على IPv4, مما يقلل الحاجة إلى تحديث الشبكة الأساسية بالكامل.

2.1 يوفر ذلك حلاً عملياً وفعالاً من حيث التكلفة لمقدمي الخدمات الذين يرغبون في تقديم خدمات IPv6.

2. تبسيط الإنتقال إلى **IPv6**:

1.2 يوفر PE6 طريقة سلسة لتقديم IPv6 دون الحاجة إلى إعادة تصميم الشبكة بالكامل.

2.2 يساعد في تسهيل التحول التدريجي نحو تبني IPv6.

3. التوافق مع MPLS:

1.3 يعمل PE6 بشكل فعال مع الشبكات التي تستخدم MPLS, مما يوفر أداء عالياً وكفاءة في التوجيه.

المتطلبات الفنية لاستخدام PE6

عقد طرفية داعمة لـ IPv6 وMPLS:

يجب أن تكون العقد الطرفية قادرة على التعامل مع عناوين IPv6 وإضافة تسميات MPLS.

.2بنية MPLS داعمة لـ :IPv4

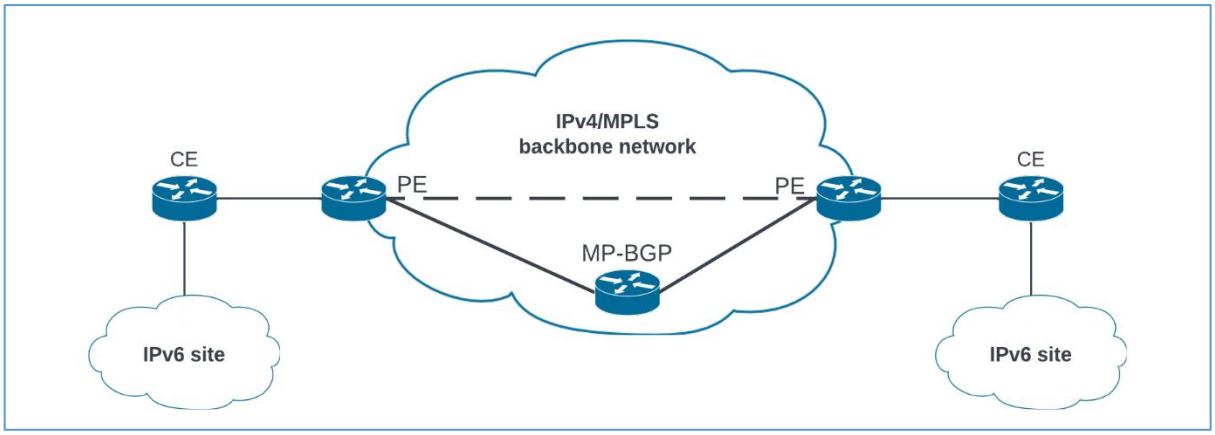
1.2 يجب أن تكون الشبكة الأساسية القائمة على MPLS قادرة على التعامل مع حزم MPLS المسمية.

3. بروتوكول :BGP

1.3 يُستخدم بروتوكول BGP (Border Gateway Protocol) لنقل معلومات التوجيه الخاصة بـ IPv6.

3.5 الآثار الأمنية المترتبة على الترجمة

قد تقدم تقنيات الترجمة، في العديد من الحالات، "نقطة فشل وحيدة": قد يؤدي فشل أو نجاح الهجوم على جهاز الترجمة إلى الحرمان من الخدمة للعديد من الاجهزة / والانظمة. ولأسباب واضحة، فإن الترجمة تجعل التخفيف من هجمات الحرمان من الخدمة أكثر صعوبة.



Intra-AS 6PE

6. مراحل الانتقال

خطوات ومراحل الانتقال إلى الإصدار السادس من بروتوكول الإنترنت (IPv6) تشمل ما يلي:

تحقيق الانتقال السلس والتام إلى الإصدار السادس للإنترنت يستلزم خطة تمر عبر عدة مراحل على فترة زمنية تعتمد على مستوى تعقيد واستعداد شبكات المشغلين، سواء كانت مؤسسات عامة أو خاصة. خطة الانتقال النموذجية قد تمر ببعض أو كل المراحل التالية:

أ. تعيين فريق الانتقال.
ب. التدريب.
ج. التقييم.
د. اختبار الخدمات والتطبيقات.
ه. وضع خطة واستراتيجية.
و. حجز أرقام الانترنت (ASN and IPv6 addresses).
ز. الاختبار التجريبي.
ح. التنفيذ.
ط. التدقيق والمراقبة.
ي. إدارة الشبكة.

1.6 تعيين فريق انتقال

فريق الانتقال يخول بالإشراف والدفع بالانتقال إلى الإصدار السادس لبروتوكول الإنترنت داخل المؤسسة أثناء فترة المشروع. حيث تشمل مسؤوليات فريق الانتقال:

- تحديد الجهات ذات العلاقة داخل المؤسسة (مثل أقسام المشتريات، الشبكات والتطبيقات).
- تحديد الجهات الخارجية ذات العلاقة.
- تحديد نطاق الأصول التي يشملها الانتقال (مثل معدات الشبكة، المنظومات والخدمات والتطبيقات التي تستعمل بروتوكول الإنترنت).
- تحليل الثغرات الحالية في مهارات الموارد البشرية والتكنولوجيا المستعملة والخدمات.
- تحديد متطلبات الانتقال.
- تشكيل فريق لوضع وتنفيذ خطة الانتقال.
- تقييم التكاليف المتعلقة بالانتقال شاملة لكل الجوانب بما فيها الزمن المطلوب، الموارد البشرية، المعدات والأدوات، هندسة واختبارات الشبكة.

2.6 التدريب

لضمان سير سلس لعملية الانتقال بدون مشاكل نتيجة الأخطاء البشرية فإنه من المهم تطوير مهارات الموارد البشرية المنخرطة في العملية. هذا يتطلب تحديد الأشخاص ذوي العلاقة الميدانية بالانتقال وإعداد وتنفيذ خطة لتدريبهم على الإصدار السادس لبروتوكول الإنترنت. هذه العملية قد تسير بالتوازي مع خطوات تنفيذ الانتقال.

3.6 التقييم

خطة الانتقال من الأفضل مناقشتها مع كل الأطراف ذوي العلاقة للقيام بتقييم تفصيلي على عدة مستويات بما فيها:

- تقييم الشبكة.
- تقييم التطبيقات.
- تقييم الخدمات.
- تقييم أمن الشبكة.

كل مشروع يجب أن يبدأ بتدقيق وتسجيل للوضع الحالي والتغييرات المخطط لها في البنية التحتية للشبكة. هذا يشمل معدات المستخدمين، أنظمة التشغيل، التطبيقات، الخوادم، خدمات الشبكة، منظومات أمن الشبكة،

وكل معدات الشبكة. كما أنه من الضروري اختبار الشبكة من عدة مناطق على الانترنت للتأكد من أنه يتم الوصول إلى الشبكة من أي مكان على الانترنت.

4.6 اختبار الخدمات والتطبيقات

من الضروري اختبار الخدمات لتحديد التحديات والمشاكل التي يمكن أن تعيق عملية التحول. هذا يشمل اختبار التطبيقات التي تستعمل العناوين النصية والبرمجيات القديمة التي لا تدعم الإصدار السادس لبروتوكول الانترنت، والتطبيقات التي مازالت تستعمل عناوين 32 بت في قواعد البيانات. قي هذه المرحلة من المهم التواصل مع مزودي المنظومات والتطبيقات وذلك أنه بإمكانهم التأكيد ما إذا كانت تطبيقاتهم متوافقة مع الإصدار السادس لبروتوكول الإنترنت أو لا.

5.6 وضع خطة إستراتيجية

في هذه المرحلة يتم وضع خطة تفصيلية ووضع استراتيجية انتقال بناءاً على المعلومات والاستنتاجات التي تم تحصيلها من مرحلتي التقييم واختبار الخدمات. الخطة يجب أن تأخذ في الاعتبار التطبيقات والخدمات المستقبلية لضمان دعم الشبكة وخدماتها للتطورات المستقبلية. هذه المرحلة يمكن أن تأخذ الجوانب الفنية التالية في الاعتبار:

- تطوير خطة لتخصيص عناوين IPv6: وفي هذا السياق من المفضل البداية من الصفر وعدم الاعتماد على عناوين IPv4 حيث أن الكثير من عناوين الإصدار الرابع لبروتوكول الإنترنت هي عناوين خاصة ومن المحتمل أنها مستعملة في أماكن أخرى من الانترنت.
- استعمال بروتوكول البوابة الحدودية (BGP): بما أنه ليس هناك حاجة لترجمة عنوان الشبكة باستعمال الـ NAT في شبكة تدعم الإصدار السادس فإنه من الممارسات الجيدة استعمال بروتوكول البوابة الحدودية. هذا سيساعد أيضاً في تجنب إعادة الترقيم عند تغيير مزود خدمة الانترنت.
- استعمال نظام اسم المجال (DNS): التحول للإصدار السادس يتطلب استعمال أكثر كثافة لنظام الـ DNS حيث أنه سيكون بمقدور أنظمة التشغيل والتطبيقات الاختيار واتخاذ القرار ما إذا كان يلزم استعمال الإصدار الرابع أو السادس في الاتصال.
- تخصيص عناوين IPv6: يمكن تخصيص عناوين الإصدار السادس لبروتوكول الإنترنت عبر عدة طرق مثل طريقة SLAAC أو DHCPv6 أو عن طريق الاثنين في آن واحد. من المهم معرفة أي المعدات وأنظمة التشغيل تستعمل أي طرق في تخصيص العناوين.

6.6 حجز أرقام الانترنت

أرقام الأنظمة المستقلة (ASN) يمكن أن تحصل عليها المؤسسات الخاصة والعامة من سجل الانترنت الأفريقي (AFRINIC). هذا الرقم مطلوب لتجنب الحاجة لإعادة الترقيم والتمكن من الحصول على عناوين خاصة عن طريق الـ BGP.

7.6 الاختبار التجريبي

قبل تنفيذ عملية الانتقال من الضروري إجراء اختبار تجريبي للشبكة. الاختبار يجب أن يشمل الجاهزية لتشغيل IPv6 على كل المعدات والتطبيقات والخدمات وقابلية التعامل مع الإصدار الرابع لبروتوكول الإنترنت. في هذه المرحلة يجب أيضاً التدقيق في الجوانب الأمنية للشبكة.

8.6 التنفيذ

بعد إجراء عملية الاختبار بنجاح يتم تنفيذ خطة الانتقال التي تم وضعها في البداية والذي سيشمل تنصيب المعدات في الشبكة والانتقال بالتطبيقات والخدمات الى الإصدار السادس.

9.6 التدقيق

أثناء التنفيذ من الضروري التدقيق في أداء الشبكة والخدمات والتطبيقات للتأكد من أن الشبكة بمكوناتها جاهزة للعمل الإصدار السادس لبروتوكول الإنترنت. بعد إنهاء عملية التدقيق بنجاح يمكن للشبكة وتطبيقاتها أن تحصل على شهادة الجاهزية لتشغيل الإصدار السادس لبروتوكول الإنترنت.

10.6 إدارة الشبكة

في هذه المرحلة يتم إدارة الشبكة ومراقبتها للتأكد من عدم حدوث أي مشاكل بعد تنفيذ عملية الانتقال إلى الإصدار السادس لبروتوكول الإنترنت.

7. الأمن السيبراني

- يوفر IPv6 ميزات تشفير مدمجة تضمن سرية البيانات وسلامتها ويوفر تشفيراً شاملاً لحزم البيانات، وهذا يعني أن حزم البيانات يتم تشفيرها في المصدر وفك تشفيرها في الوجهة، مما يضمن أمان البيانات أثناء الاتصال ويوفر IPSec أيضاً ميزات المصادقة وتكامل البيانات التي تحمي من التلاعب بالبيانات.

- يحتوي IPv6 على مساحة عنوان أكبر من IPv4، مما يعني أنه يوفر المزيد من العناوين التي يمكن تخصيصها للأجهزة. تجعل هذه الميزة من الصعب على المخترقين تخمين العنوان الرئيسي على الشبكة أو البحث عنه.
- يوفر IPv6 جدار حماية مدمجاً يسمح لمسؤولي الشبكة والتحكم في الوصول إلى شبكتها ويمكن تكوين جدار الحماية للسماح بحركة المرور أو حظرها بناءً على عناوين IP والمنافذ والبروتوكولات، تساعد هذه الميزة على منع الوصول غير المصرح به إلى الشبكة والحماية من الهجمات السيبرانية.
- يصعب عمل مسح ومراقبة تدفق البيانات للشبكة الداخلية للمؤسسات وذلك لوجود عدد كبير من العناوين.
- صعوبة توافق نظام سجل البيانات ونظام مراقبة العمليات الأمنية مثل SIEM System.
- من الجذير بالذكر أن منهجيات الانتقال الثلاث تحمل نفس مخاطر الأمن السيبراني. حيث أن العيب الرئيسي لأساليب الانتقال هذه أنها تعتمد أساسًا تشغيل الشبكتين معاً (شبكة تستخدم بروتوكول الانترنت الاصدار الرابع والأخرى تستخدم الإصدار السادس). وبالتالي يجب تأمين كلا البروتوكولين ومراقبتها وإدارتها. كما أن الحفاظ على مستويات الأداء المتوقعة لنوعين من الشبكات لا يتأتّى إلا بتوفير أدوات أمان إضافية للشبكة واستشاريين وفنيين مدربين، وكل هذا سيؤدي إلى زيادة التكلفة التشغيلية.
- كما أن الآثار المترتبة على أمن المعلومات عند تشغيل نظام هجين ثنائي البروتوكول ليست مفهومة تمامًا، ويجب أن يؤخذ في الاعتبار ما إذا كانت البنى التحتية القائمة على IPv4 ستتكيّف أم أنها ستدخل مشكلات أمنية في بيئة IPv6 والعكس صحيح. بالإضافة إلى ثغرات IPv4 الشائعة، هناك بعض ميزات الأمان المتأصلة في IPv6 (على سبيل المثال، تشفير محتوى الحزمة Encryption of packet content) والتي إذا تم تنفيذها بالكامل ستجعل جانب مراقبة IPv4 من بنية النقل غير قابل للتشغيل.
- يجب أن يتم في مرحلة الانتقال تصميم الشبكة بحيث يأخذ بعين الاعتبار كل خدمات العنونة والتسمية لبروتوكول الإنترنت الإصدار السادس، ومتطلبات أمن وسلامة المعلومات، وتطبيقات البرامج، بحيث لا يكون هذا الانتقال معطّلاً للأعمال والخدمات الأساسية التي تقدمها أي مؤسسة.