

الجمهورية العربية السورية

وزارة التعليم العالي

الجامعة السورية الخاصة

الجامعة السورية الخاصة
SYRIAN PRIVATE UNIVERSITY

Design and implementation of a secure network from one site to another

تصميم وتنفيذ شبكة آمنة من موقع إلى آخر

مشروع الفصل - تخصص هندسة أمن النظم والشبكات الحاسوبية

الاعداد :

يزن ماجد شيخوني

ابراهيم تحسين رمضان

الاشراف

م.فراص خير بك

الفهرس :

6	المقدمة :
7	هدف المشروع :
8	1.1 فصل الاول : الدراسة النظرية
9	1.1.1 قسم الاول : المقدمة العامة ل MPLS
10	1.1.2 1. المبدأ الأساسي لعمل MPLS وتفاصيله التقنية :
11	1.1.3 المكونات الأساسية لشبكة MPLS وأدوارها الوظيفية :
12	1.1.4 عمليات التسمية الأساسية في MPLS وآليات التنفيذ:
13	1.1.5 بروتوكولات توزيع التسميات وآلية التنسيق :
14	1.1.6 خدمات MPLS VPN وأنواعها المختلفة :
15	1.1.7 هندسة المرور Traffic Engineering في MPLS
16	1.1.8 جودة الخدمة QoS في شبكات MPLS
17	1.1.9 مقارنة شاملة بين MPLS والشبكات التقليدية :
18	1.1.10 1. مستقبل MPLS والتطورات التقنية الحديثة :
19	2.1 فصل الثاني : بيئة العمل
20	2.1.1 مقدمة الفصل :
20	2.1.2 2. البيئة المادية(Hardware Environment)
20	2.1.2.1 2.1.2.1 الموجات(Routers)
21	2.1.2.2 2.1.2.2 أجهزة الحاسوب(End Hosts)
21	2.1.2.3 2.1.2.3 واجهات الاتصال :
21	2.2 2. وجهاة WAN/MPLS: لربط الموجهين معًا عبر شبكة Host-Only تحاكي وصلة.
22	2.2.1 2.2.1 نظام MikroTik RouterOS
22	2.2.2 2.2.2 أنظمة تشغيل الحواسيب
22	2.2.3 2.2.3 أدوات الاختبار
22	2.3 2.3 بنية الشبكة(Network Topology)
22	2.3.1 2.3.1 الموقع الأول(Site A)

23	الموقع الثاني (Site B) 2.3.2
23	إعدادات العنونة (IP Addressing) 2.3.3
23	إعداد خادم DHCP 2.4
24	DHCP في الموقع الثاني 2.4.1
24	إعدادات NAT والجدار النارى 2.5
25	بروتوكول التوجيه OSPF 2.6
26	تقنية MPLS و LDP 2.7
26	MPLS تفعيل 2.7.1
26	LDP بروتوكول 2.7.2
26	MPLS جدول التحويل 2.7.3
26	الاختبارات والتحقق 2.8
26	ملخص الفصل الثاني 2.9
27	فصل الثالث : الحل المقترن 3.1
28	الاعدادات لل Site A : 3.1.1
41	الاعدادات ل Site B 3.2.1
61	الفصل الرابع : المقارنات والتحليل 4.1
62	4.1.1 التحليل النتائج المحققة
64	4.1.2 التوجيهات المستقبلية والمقررات
64	4.1.3 التطوير الأول: مسارات هجينه ذكية (Hybrid Intelligent Paths)
64	4.1.4 التطوير الثاني: نظام اتصال صوتي متكامل (VOIP)
64	4.2 الخلاصة

فهرس الاشكال :

- 28.....الشكل 3.1 Interfaces
- 29.....الشكل 3.2 IP address configuration
- 30.....الشكل 3.3 NAT configuration on WAN
- 31.....الشكل 3.4 اعدادات Routing OSPF
- 32.....الشكل 3.5 OSPF Conf
- 33.....الشكل 3.6 MPLS LDP enabling
- 34.....الشكل 3.7 اعدادات بروتوكول MPLS
- 35.....الشكل 3.8 ip add conf (voip+data)
- 36.....الشكل 3.9 firewall ip address-list
- 37.....الشكل 3.10 ip firewall mangle
- 38.....الشكل 3.11 firewall nat for voip and data
- 39.....الشكل 3.12 queue tree for priority and service
- 40.....الشكل 3.13 mpls interfaces (voip+data+lan)
- 41.....الشكل 3.2.1 interfaces Site B
- 42.....الشكل 3.2.2 اعدادات عناوين IP
- 43.....الشكل 3.2.3 NAT configuration on WAN
- 44.....الشكل 3.2.4 Routing ospf interfaces
- 45.....الشكل 3.2.5 Routing Ospf Network

- 46.....MPLS LDP enabling 3.2.6
- 47.....MPLS 3.2.7
- 48..... ip add conf (voip+data) 3.2.8
- 49.....firewall ip address-list 3.2.9
- 50.....ip firewall mangle 3.2.10
- 51.....firewall nat for voip and data 3.2.11
- 52.....queue tree for priority and service 3.2.12
- 53..... mpls interfaces (voip+data+lan) 3.2.13
- 55..... الشكل 3.1.14 تحليل حركة الشبكة باستخدام Wireshark
- 62.....MLPS 4.1 مخطط التدفق
- 63..... الشكل 4.2 تطبيق Traffic Engineer + QOS

المقدمة :

تُعد تقنية **MPLS – Multiprotocol Label Switching** من أهم تكنولوجيات الربط المستخدمة في شبكات المؤسسات، حيث تعتمد على توجيه البيانات باستخدام ملصقات بدلاً من العناوين التقليدية، مما يوفر سرعة أعلى وتحكمًا أكبر في حركة المرور داخل الشبكة، وفي هذا المشروع قمنا بتطبيق هذه التقنية بشكل عملي داخل بيئة افتراضية للتعرف على كيفية عملها واختبار إمكانياتها في ربط موقعين بطريقة آمنة وفعالة.

جاءت فكرة المشروع من الحاجة إلى فهم طريقة عمل MPLS بشكل عملي، وتجربة خطوات إعدادها وتطبيقها على أجهزة الشبكات الافتراضية للوصول إلى نموذج حقيقي يشبه ما يستخدم في المؤسسات والشركات، في هذا المشروع قمنا بإنشاء بيئة عمل كاملة على منصة VMware ، والتي تسمح بمحاكاة أجهزة الشبكة وتشغيل عدة أنظمة في وقت واحد دون الحاجة إلى تجهيزات فعلية، وقد تم استخدام أجهزة MikroTik CHR باعتبارها مناسبة لتطبيق تكنولوجيا التوجيه المتقدمة ودعمها الكامل لبروتوكولات MPLS و LDP ، مما جعلها الخيار الأفضل لتنفيذ السيناريو المطلوب.

اعتمدنا في عملنا على تجهيز كل موقع افتراضي على شكل شبكة مستقلة، ثم العمل على ربطهما باستخدام MPLS لضمان مرور حركة البيانات بينهما بشكل آمن وسلس، ساعدتنا هذه التجربة في التعرف على خطوات إعداد الشبكات من الصفر، بدءاً من إنشاء الروتارات الافتراضية، مروراً بضبط بروتوكولات التوجيه، ووصولاً إلى تفعيل MPLS ومراقبة أداء الشبكة بعد الربط.

يمثل هذا المشروع تجربة عملية متكاملة توضح كيفية بناء شبكة MPLS في بيئة افتراضية، وتحسن فهماً أعمق لكيفية تعامل الروتارات مع الملصقات وكيفية انتقال البيانات عبر المسارات المختلفة، كما يسمح المشروع باختبار عدة سيناريوهات واقعية مثل تتبع الحزم، فحص المسارات، ومحاكاة حركة المرور، وهو ما ساعدنا في تطوير فهم عملي لتقنيات الشبكات الحديثة وأساليب تطبيقها.

هدف المشروع :

يهدف هذا المشروع إلى تصميم وتنفيذ شبكة MPLS مسطحة (Flat) تربط موقعين منفصلين باستخدام أجهزة MikroTik CHR في بيئة محاكاة واقعية، يركز المشروع على بناء بنية شبكة متكاملة تعمل بتقنية MPLS من البداية إلى النهاية، مع دعم كامل لاتصال الآمن والموثوق بين الشبكات المحلية في كلا الموقعين يتضمن الهدف العملي تكوين الواجهات الأساسية.

وتعيين عناوين IP الثابتة والمنطقية لكل موقع، وإنشاء خوادم DHCP لتوزيع العناوين الديناميكية على الأجهزة المتصلة في الشبكات المحلية، كما يهدف المشروع إلى تكوين جدار الحماية (Firewall) وقواعد NAT لضمان أمن الشبكة مع السماح بمرور حركة المرور بين الموقعين عبر روابط MPLS دون تعقيد. يهدف الفريق إلى تفعيل بروتوكول OSPF للتوجيه الديناميكي بين الرافوترات، لضمان اكتشاف المسارات المثلثي تلقائياً والحفاظ على استقرار الشبكة واستمراريتها.

بالإضافة إلى ذلك، يهدف المشروع إلى تمكين تقنية MPLS وبروتوكول LDP على الواجهات المخصصة لضمان تبديل التسميات ونقل البيانات بكفاءة عالية عبر الشبكة الواسعة، يهدف المشروع إلى التحقق من صحة الاتصال الشامل من خلال إجراء اختبارات ping بين المضيفين في الموقعين، وتحليل حركة المرور عبر أداة Wireshark للتأكد من وجود تسميات MPLS في الحزم المنقول، أخيراً، يهدف المشروع إلى تقديم وثيقة تقنية شاملة توضح جميع خطوات التكوين والإعداد، لتكون مرجعاً عملياً للمهندسين والمتدربين لفهم وتطبيق شبكات MPLS المسطحة في بيئات حقيقة أو افتراضية، مع التركيز على الجانب التطبيقي والعملي للเทคโนโลยيا.

1.1 فصل الاول : الدراسة النظرية

1.1.1 قسم الاول : المقدمة العامة ل MPLS

تعتبر تقنية MPLS المعروفة اختصاراً بـ Multiprotocol Label Switching واحدة من أهم الابتكارات التقنية التي غيرت وجه شبكات البيانات العالمية خلال العقود الماضيين. ظهرت هذه التقنية المتقدمة في أواخر التسعينيات كحل عملي يجمع بين مزايا تبديل الطبقة الثانية وسرعة توجيه الطبقة الثالثة في نموذج OSI السباعي.

تم تطوير MPLS أساساً لمعالجة التحديات المتزايدة المتعلقة بسرعة نقل البيانات وكفاءة استخدام الموارد في الشبكات الواسعة WAN، خاصة مع التوسع الكبير في استخدام الإنترنت والتطبيقات الشبكية. تعمل هذه التقنية الفريدة على مبدأ استخدام التسميات Labels الرقمية بدلاً من العناوين IP الطويلة والمعقدة لتوجيه حزم البيانات عبر الشبكة، مما يقلل بشكل كبير من وقت المعالجة في أجهزة التوجيه ويزيد من كفاءة الشبكة بشكل عام.

تندرج MPLS بشكل فريد بين الطبقتين الثانية والثالثة في نموذج OSI، مما يجعلها مستقلة عن البروتوكولات الأساسية وقادرة على العمل مع مختلف أنواع الشبكات والتقنيات دون مشاكل توافق، أصبحت MPLS العمود الفقري للعديد من شبكات مزودي الخدمة حول العالم نظراً لكافتها العالمية في إدارة حركة البيانات وتوفير جودة خدمة متميزة للتطبيقات المختلفة، توفر هذه التقنية أيضاً إمكانيات متقدمة لهندسة المرور Traffic Engineering وضمان جودة الخدمة QoS، مما يجعلها الخيار الأمثل للتطبيقات الحساسة مثل الصوت والفيديو والخدمات المهمة.

تطورت MPLS من مجرد تقنية نقل بسيطة إلى منصة شاملة لخدمات المتقدمة تشمل VPN والخدمات السحابية والتطبيقات المؤسسية المعقدة، تعتمد العديد من المؤسسات المالية والحكومية والشركات الكبرى على MPLS لربط فروعها بشكل آمن وموثوق عبر مختلف المناطق الجغرافية، تشير الدراسات إلى أن MPLS تستخدم في أكثر من 70% من شبكات الناقلين العالمية الكبرى، مما يؤكد مكانتها الريادية في عالم الشبكات، تواصل التقنية التطور لمواكبة المتطلبات الحديثة مثل دعم السحابة الإلكترونية وإنترنت الأشياء والتطبيقات الذكية المختلفة.

1.1.2 المبدأ الأساسي لعمل MPLS وتفاصيله التقنية :

يعتمد المبدأ الأساسي لتشغيل MPLS على فكرة التبديل السريع للتسميات الرقمية بدلاً من البحث المعقّد في جداول التوجيه التقليدية القائمة على عناوين IP الطويلة، عندما تدخل حزمة البيانات إلى شبكة MPLS من خلال جهاز حافة، يتم وضع تسمية رقمية عليها تشبه الطابع البريدي الذكي الذي يوجهها عبر مسار محدد مسبقاً بناءً على سياسات معينة، تكون هذه التسمية من 32 بتاً مقسمة بدقة إلى عدة أجزاء رئيسية: 20 بت للمعرف الفريد Label الذي يمثل القيمة الأساسية للتوجيه، و3 برات لتحديد فئة المرور Traffic Class المستخدمة في جودة الخدمة، و3 برات لمؤشر المكدس Stack، و8 برات لوقت الحياة TTL الذي يمنع الحزم من الدوران بشكل لانهائي في الشبكة.

توضع التسمية تقنياً بين رأس الطبقة الثانية (Data Link Layer) ورأس الطبقة الثالثة (Network Layer) في حزمة البيانات، مما يحافظ على الهيكل الأصلي لحزمة IP مع إضافة معلومات التوجيه الإضافية اللازمة للعملية، تكمن القوة التقنية لـ MPLS في أن كل جهاز توجيه على المسار ينظر فقط إلى التسمية ويستبدلها بأخرى جديدة توجه الحزمة للجهاز التالي، دون الحاجة لتحليل رأس IP الكامل في كل عقدة مما يوفر وقتاً ثميناً. هذه الآلية الذكية تقلل زمن الانتقال Latency وتحسن أداء الشبكة بشكل ملحوظ يمكن قياسه عملياً.

يعمل نظام MPLS مع مختلف بروتوكولات الطبقة الثانية مثل الإيثرنت و ATM و Frame Relay، مما يجعله متعدد البروتوكولات حقاً. تدعم MPLS أيضاً تكديس التسميات Label Stacking الذي يسمح باستخدام عدة تسميات في وقت واحد لتطبيقات متقدمة، تسمح هذه المرونة الفنية بإنشاء شبكات معقدة تدعم خدمات متعددة على نفس البنية التحتية، بعد فهم آلية عمل التسميات أساسياً لفهم كيفية توفير MPLS للسرعة والكفاءة في نقل البيانات عبر المسافات الطويلة.

1.1.3 المكونات الأساسية لشبكة MPLS وأدوارها الوظيفية :

ت تكون شبكة MPLS من عدة أنواع من الأجهزة المتخصصة التي تؤدي أدواراً وظيفية متكاملة ومحددة لضمان التشغيل الفعال والموثوق للشبكة، توجد أجهزة حافة التسمية Label Edge Routers التي تعمل كنقط دخول وخروج استراتيجية لشبكة MPLS، حيث تضيف التسميات على الحزم الداخلية وتزيلها عن الحزم الخارجية وفق قواعد محددة.

داخل الشبكة الأساسية توجد أجهزة تبديل التسميات Label Switch Routers التي تنقل البيانات باستخدام التسميات فقط دون التعامل المباشر مع عناوين IP، مما يبسط عملية التوجيه هناك أيضاً مسارات مبدلة بالتسميات Label Switched Paths وهي المسارات المحددة مسبقاً ديناميكياً أو يدوياً التي تسلكها الحزم عبر الشبكة من نقطة الدخول إلى نقطة الخروج.

بالإضافة إلى ذلك، توجد فئات التوجيه المكافئ Forwarding Equivalence Classes التي تجمع الحزم المشابهة في خصائصها وتوجهها بنفس الطريقة عبر نفس المسار لضمان الاتساق تعمل هذه المكونات الأساسية معاً بشكل متاغم ومتزامن لإنشاء شبكة فعالة وموثوقة تدعم خدمات متعددة ومتطلبات متنوعة. كما توجد أنواع فرعية متخصصة من الأجهزة مثل Provider Edge Routers التي تربط بين شبكات العملاء وشبكة المزود.

و Provider Routers التي تشكل النواة الداخلية لشبكة المزود، تتفاعل جميع هذه المكونات عبر بروتوكولات توزيع خاصة مثل RSVP-TE و LDP لتبادل معلومات التسميات وإنشاء المسارات. تحتوي كل جهاز على جداول خاصة مثل Label Forwarding و Label Information Base لتخزين ومعالجة معلومات التسميات، يضمن هذا التقسيم الوظيفي الدقيق توزيع المهام بشكل مثالى يحقق أقصى استفادة من موارد الشبكة.

1.1.4 عمليات التسمية الأساسية في MPLS وآليات التنفيذ:

تمر حزم البيانات في شبكة MPLS بثلاث عمليات رئيسية للتسمية تحدد بدقة كيفية انتقالها من المصدر إلى الوجهة عبر الشبكة المعقدة، العملية الأولى هي Push أو الإضافة، حيث يتم وضع تسمية جديدة على الحزمة عند دخولها إلى شبكة MPLS من خلال جهاز الحافة الدخلة Ingress LER، وتحدد هذه التسمية المسار الذي ستسلكه الحزمة عبر الشبكة. العملية الثانية هي Swap أو الاستبدال، حيث يتم تبديل التسمية القديمة بأخرى جديدة في كل نقطة عبور داخل الشبكة بواسطة أجهزة LSR، مما يوجه الحزمة للخطوة التالية في مسارها المحدد بناءً على جداول التوجيه.

العملية الثالثة هي Pop أو الإزالة، حيث يتم نزع التسمية من الحزمة عند خروجها من شبكة MPLS عبر جهاز الحافة الخارجة Egress LER، لتعود إلى شكلها الأصلي قبل تسليمها للشبكة الهدف النهائية، بالإضافة إلى هذه العمليات الأساسية، تدعم Swap with Push عملية متقدمة تسمى MPLS للتعامل مع التسميات المتعددة في المكبس لسيناريوهات معقدة، تتم هذه العمليات بسرعة عالية جداً باستخدام دوائر متخصصة في الأجهزة، مما يقلل زمن المعالجة إلى حدود الدنيا.

يعتمد تنفيذ هذه العمليات على خوارزميات فعالة تحدد العلاقة بين التسميات الواردة والصادرة في كل جهاز. تسمح هذه الآليات بإنشاء مسارات افتراضية مستقلة عن الطبقة المادية الأساسية للشبكة، يمكن برمجة هذه العمليات لدعم سياسات متقدمة مثل جودة الخدمة وهندسة المرور، يضمن التسلسل المنظم لهذه العمليات نقل البيانات بكفاءة وموثوقية عالية عبر مسافات طويلة.

1.1.5 بروتوكولات توزيع التسميات وآلية التنسيق :

تعتمد شبكات MPLS بشكل أساسي على عدة بروتوكولات متخصصة ومتكاملة لتوزيع وإدارة التسميات بين الأجهزة المختلفة والتنسيق بينها، أشهر هذه البروتوكولات هو Label Distribution Protocol أو LDP، وهو البروتوكول الأساسي الذي تستخدمه الأجهزة لتبادل معلومات التسميات وإنشاء مسارات تبديل التسميات تلقائياً باستخدام جداول التوجيه الموجودة.

هناك أيضاً RSVP-TE أو Resource Reservation Protocol – Traffic Engineering الذي يستخدم لإنشاء مسارات مهندسة تحجز موارد محددة وتضمن جودة الخدمة للتطبيقات الحساسة مثل الصوت والفيديو، بالإضافة إلى ذلك، يستخدم MP-BGP أو Multiprotocol BGP في شبكات MPLS VPN لنقل معلومات التوجيه بين موقع العملاء المختلفة عبر شبكة المزود المشتركة.

تعمل هذه البروتوكولات معاً بشكل متكامل لضمان أن كل جهاز في الشبكة يعرف التسميات المناسبة وكيفية التعامل معها في مختلف السيناريوهات، يستخدم LDP آليات الجلسات المجاورة لنقل معلومات التسميات بين الأجهزة مباشرة وإنشاء علاقات اتصال موثوقة يدعم RSVP-TE إنشاء مسارات أحادية وثنائية الاتجاه مع حجز موارد مضمونة للنطاق الترددية والجودة.

يقوم MP-BGP بنشر معلومات VPN بين أجهزة PE مع الحفاظ على عزل الشبكات الافتراضية المختلفة. تتضمن آلية التنسيق أيضاً بروتوكولات مساعدة لتحسين الأداء والموثوقية مثل BFD للكشف السريع عن الأعطال، يضمن هذا النظام المتكامل من البروتوكولات تشغيلًا سلساً لشبكات MPLS المعقدة والمتعلقة بالخدمات.

1.1.6 خدمات MPLS VPN وأنواعها المختلفة :

تعد خدمات الشبكات الخاصة الافتراضية VPN واحدة من أهم التطبيقات العملية والأكثر شيوعاً لـ

MPLS في العالم الحقيقي، تقسم هذه الخدمات المتقدمة إلى نوعين رئисيين: MPLS L3 VPN التي

تعمل على طبقة الشبكة Layer 3، حيث يتم تبادل معلومات التوجيه بين موقع العميل عبر شبكة المزود

باستخدام بروتوكولات مثل BGP، والنوع الثاني هو MPLS L2 VPN التي تعمل على طبقة وصلة

البيانات 2 Layer 2 ، مما يجعل الموقع المختلفة تبدو وكأنها متصلة بشبكة محلية واحدة موحدة.

توفر خدمات MPLS VPN عزل كامل وأمن متقدم بين عملاء مختلفين يستخدمون نفس البنية التحتية

المادية، مع الحفاظ على خصوصية وسرية بيانات كل عميل بشكل منفصل، تعتبر MPLS VPN أكثر

كفاءة وأماناً من تقنيات VPN التقليدية بسبب استخدام التسميات بدلاً من الأنفاق المعقدة.

تدعم MPLS L3 VPN نموذجين رئисيين: نموذج 4364 (المعروف سابقاً بـ RFC 2547)

الذي يستخدم MP-BGP، ونموذج Virtual Router الذي يوفر عزل تام بين العملاء. أما MPLS L2

فتقضي تقنيات مثل VPLS للشبكات الواسعة الظاهري و VPWS للدوائر الافتراضية.

توفر هذه الخدمات مرونة عالية في ربط الفروع والمكاتب البعيدة بجودة عالية وتكلفة فعالة. تمكن

MPLS VPN المؤسسات من توسيع شبكاتها المحلية عبر مناطق جغرافية واسعة دون التضحية بالأداء

أو الأمان.

1.1.7 هندسة المرور Traffic Engineering في MPLS :

تمثل هندسة المرور Traffic Engineering واحدة من أقوى الميزات وأكثرها قيمة في تقنية MPLS، حيث تسمح بالتحكم الدقيق والمتقدم في كيفية تدفق البيانات عبر الشبكة المعقّدة، تمكن MPLS Traffic Engineering المشغلين والمهندسين من تحديد مسارات محددة ومخصصة لأنواع معينة من البيانات وحتى للتطبيقات الفردية، بدلاً من الاعتماد على مسارات التوجيه القصيرة التقليدية فقط.

هذا التحكم المتقدم يتيح تجنب مناطق الازدحام الشبكية، وتوزيع الحمل بشكل متوازن على الروابط المختلفة، وضمان جودة الخدمة المثلث للتطبيقات الحساسة مثل الصوت والفيديو والبيانات المهمة، كما تسمح تقنية TE بإنشاء مسارات احتياطية مسبقة التجهيز تعمل تلقائياً وفوراً عند حدوث أي عطل في المسارات الرئيسية، مما يضمن استمرارية الخدمة وموثوقية عالية لا تتزعزع.

تستخدم بروتوكول RSVP-TE لإرسال رسائل التحكم وإنشاء الأنفاق المهندسة مع حجز الموارد المطلوبة، تدعم أيضاً Constraint-based Routing الذي يأخذ في الاعتبار قيود متعددة مثل النطاق الترددية والتأخير والمتطلبات الأخرى. تسمح هذه التقنيات بتحسين استخدام موارد الشبكة بشكل عام وتقليل الهدر في السعة المتاحة، يمكن تطبيق سياسات متقدمة لإعطاء أولوية لأنواع محددة من البيانات في أوقات الذروة، تجعل هذه الإمكانيات MPLS الخيار الأمثل للشبكات الكبيرة التي تحتاج إلى إدارة ذكية لحركة المرور المعقّدة.

1.1.8 جودة الخدمة QoS في شبكات MPLS :

توفر MPLS إمكانيات متقدمة ومرنة لضمان جودة الخدمة QoS من خلال دمج آليات متعددة للتصنيف والتمييز والجدولة والتحكم في حركة المرور، يمكن تصنيف حركة المرور الشبكية بدقة إلى فئات مختلفة بناءً على متطلباتها ومستوياتها أهميتها، مثل البيانات العادية والصوت والفيديو والبيانات الحرجية للتطبيقات المؤسسية، لكل فئة من هذه الفئات يمكن تحديد أولوية وسلوك مختلف في حالة الازدحام الشبكي، مما يضمن حصول التطبيقات الحساسة على النطاق التردد المطلوب والأداء المناسب حتى في الظروف الصعبة.

تسمح MPLS أيضاً بإنشاء أنفاق مهندسة مع حجز موارد مضمونة ومحددة سلفاً، مما يحسن أداء التطبيقات في الوقت الحقيقي بشكل ملحوظ تستخدم حقل Experimental Bits المكون من 3 بتات في رأس التسمية لحمل معلومات جودة الخدمة بين الأجهزة المختلفة تدعى تقنيات مثل DiffServ-
MPLS تكامل أنظمة QoS المعتمدة على DiffServ مع بنية MPLS الأساسية.
يمكن تطبيق سياسات متعددة المستويات لمعالجة حركة المرور على مستوى التطبيق أو المستخدم أو الموقع تتيح هذه الإمكانيات للمؤسسات ضمان أداء متسق للتطبيقات المهمة عبر الشبكة الواسعة، تجعل هذه القدرات المتقدمة MPLS الخيار الأمثل للشركات التي تعتمد على تطبيقات متقدمة وحساسة للأداء تتطلب ضمانات أداء مضمونة ومستقرة.

1.1.9 مقارنة شاملة بين MPLS والشبكات التقليدية :

تفوق MPLS على الشبكات التقليدية القائمة على IP بشكل واضح في عدة جوانب مهمة وحاسمة تؤثر على أداء وموثوقية الشبكة من حيث السرعة والأداء، تقلل MPLS وقت معالجة الحزم بشكل كبير جداً لأن الأجهزة تتعامل مع التسميات البسيطة بدلاً من عناوين IP المعقدة والطويلة التي تتطلب بحثاً في جداول كبيرة.

في مجال المرونة والتكييف، تسمح MPLS بإنشاء مسارات مخصصة ومهندسة لأنواع مختلفة من البيانات، بينما تعتمد الشبكات التقليدية فقط على مسارات التوجيه القصيرة التي قد لا تكون مثالية، بالنسبة للموثوقية واستمرارية الخدمة، توفر MPLS آليات استعادة أسرع وأكثر كفاءة عند حدوث الأعطال مقارنة بالشبكات التقليدية.

كما أن MPLS توفر مستوى أعلى من الخصوصية والأمان من خلال عزل حركة مرور العملاء المختلفين بشكل تام على نفس البنية المادية، رغم أن التكلفة الأولية لتنفيذ MPLS أعلى من الشبكات التقليدية، إلا أن فوائدها العديدة على المدى الطويل تجعلها استثماراً مجدياً للعديد من المؤسسات الكبيرة والمتوسطة.

تدعم MPLS أيضاً خدمات متقدمة مثل VPN و QoS و TE بشكل أفضل من التقنيات التقليدية، تقدم قابلية توسيع أكبر للمؤسسات التي تتوقع النمو والتوسيع في المستقبل. توفر MPLS أيضاً إدارة مبسطة للشبكات المعقدة مقارنة بالحلول التقليدية المتدايرة.

1.1.10 مستقبل MPLS والتطورات التقنية الحديثة :

يتجه مستقبل تقنية MPLS بشكل واضح نحو التكامل العميق مع التقنيات الحديثة المتطرفة مثل الشبكات المعرفة بالبرمجيات SDN والحوسبة السحابية المتقدمة وإنترنت الأشياء IoT، يشهد تطور MPLS-TP المصمم خصيصاً لطبقة النقل توسيعاً كبيراً في نطاق تطبيقات MPLS ليشمل شبكات النقل التقليدية ومراكم البيانات المتقدمة.

كما تتحسن آليات الأمان في MPLS بشكل مستمر من خلال دمج بروتوكولات التشفير القوية مثل MACsec و IPsec لضمان حماية متكاملة للبيانات المنقولة، تواصل الأبحاث والتطويرات تحسين قابلية توسيع MPLS وجعلها أكثر ملائمة للشبكات الضخمة والعملقة التي تتطلب أداءً عالياً، مع تزايد اعتماد المؤسسات على التطبيقات السحابية والخدمات الرقمية المتقدمة التي تتطلب أداءً عالياً وموثوقية لا تنزعزع، ستستمر MPLS في لعب دور محوري في البنية التحتية للشبكات العالمية.

يتوقع الخبراء أن MPLS ستتطور لتشمل دعم خدمات جديدة مثل الشبكات الخاصة G5 والحوسبة الطرفية Edge Computing جنباً إلى جنب مع التقنيات الناشئة لتوفير حلول شاملة للاتصال الحديث ستحافظ MPLS على مكانتها كتقنية أساسية مع التكيف المستمر مع المتطلبات الجديدة والتحديات الناشئة في عالم الشبكات المتتطور بسرعة.

2.1 فصل الثاني : بيئة العمل

2.1.1 مقدمة الفصل :

يعرض هذا الفصل بيئة العمل التي تم الاعتماد عليها في تنفيذ مشروع Flat MPLS Site-to-Site، ويستند بشكل كامل إلى الملف التطبيقي الخاص بالمشروع، يهدف الفصل إلى توضيح جميع مكونات البيئة المستخدمة سواء من الناحية المادية أو البرمجية، مع شرح بنية الشبكة، عناوين IP ، تقنيات الربط، وبروتوكولات التوجيه والتبديل، وذلك لتهيئة القارئ لفهم خطوات التنفيذ العملية في الفصول اللاحقة.

تم تصميم بيئة العمل بحيث تحاكي شبكة حقيقة تربط موقعين مختلفين باستخدام تقنية MPLS ، مع الاعتماد على موجهات MikroTik من نوع CHR وأجهزة حاسوب تعمل بنظام Windows ، وتطبيق بروتوكولات توجيه ديناميكية لضمان الاتصال الكامل بين الشبكتين.

2.1.2 البيئة المادية (Hardware Environment) :

تعتمد البيئة المادية للمشروع على عدد محدود من المكونات، إلا أنها كافية لتنفيذ شبكة MPLS متكاملة من موقع إلى موقع.

2.1.2.1 الموجهات (Routers) :

تم استخدام عدد (2) موجه من نوع **MikroTik CHR (Cloud Hosted Router)**, حيث يمثل كل موجه موقعاً مستقلاً **Site A** و **Site B** وتكون أهمية هذه الموجهات في دعمها الكامل لتقنيات **MPLS** و **OSPF** و **LDP**, إضافة إلى خصائص الجدار الناري (Firewall) و **NAT**.

مهام الموجهات في المشروع:

- ربط الشبكات المحلية بالمواقعين.
- تشغيل بروتوكول **OSPF** للتوجيه динамический.
- تفعيل **MPLS** و **LDP** لتمرير البيانات باستخدام التسميات **(Labels)**.
- تطبيق سياسات الأمان والجدار الناري.

2.1.2.2 : أجهزة الحاسوب (End Hosts)

تم استخدام جهاز حاسوب واحد في كل موقع يعمل بنظام تشغيل **Windows 7**, ويمثل المستخدم النهائي داخل الشبكة المحلية **(LAN)** ، تستخدم هذه الأجهزة لاختبار الاتصال، واستلام عناوين IP تلقائياً من خادم **DHCP**

2.1.2.3 : واجهات الاتصال :

واجهة **LAN**: لربط الموجه مع الشبكة المحلية.

- واجهة **WAN/MPLS**: لربط الموجهين معاً عبر شبكة **Host-Only** تحاكي وصلة **MPLS**.

2.2 البيئة البرمجية (Software Environment)

2.2.1 نظام MikroTik RouterOS

تم الاعتماد على نظام MikroTik RouterOS الخاص بشركة MikroTik، والذي يوفر إمكانيات متقدمة في التوجيه، الأمان، وMPLS. تم من خلاله تنفيذ جميع إعدادات الشبكة مثل العناوين، OSPF، DHCP، العناوين، وLDP.

2.2.2 أنظمة تشغيل الحواسيب

تم استخدام نظام Windows 7 على الأجهزة الطرفية، حيث تم ضبط إعدادات الشبكة لاستقبال عناوين IP تلقائياً من خادم DHCP واستخدامه في اختبارات الاتصال.

2.2.3 أدوات الاختبار

- أوامر Ping للتحقق من الاتصال.
- Wireshark لمراقبة حزم MPLS والتأكد من وجود Label Stack Entry.

2.3 بنية الشبكة (Network Topology)

ت تكون بنية الشبكة من موقعين منفصلين جغرافياً، يتم الربط بينهما باستخدام تقنية MPLS.

2.3.1 الموقع الأول (Site A)

- شبكة LAN: 172.168.10.0/24

- بوابة الشبكة: 172.168.10.1

- واجهة WAN/MPLS: 10.0.0.1/30

2.3.2 الموقع الثاني (Site B)

- شبكة LAN: 172.168.20.0/24

- بوابة الشبكة: 172.168.20.1

- واجهة WAN/MPLS: 10.0.0.2/30

2.3.3 إعدادات العنونة (IP Addressing)

تم اعتماد عنونة ثابتة على الموجهات، وعنونة ديناميكية للأجهزة الطرفية.

- Site A LAN: 172.168.10.0/24

- Site B LAN: 172.168.20.0/24

- WAN/MPLS Link: 10.0.0.0/30

2.4 إعداد خادم DHCP

2.4.1 الموقع الأول في DHCP

- نطاق العناوين: 172.168.10.100 – 172.168.10.200

- البوابة الافتراضية: 172.168.10.1

2.4.1 DHCP في الموقع الثاني

- نطاق العناوين: 172.168.20.100 – 172.168.20.200

- البوابة الافتراضية: 172.168.20.1

يساهم DHCP في تسهيل إدارة العناوين وتقليل الأخطاء اليدوية.

2.5 إعدادات NAT والجدار النارى

: NAT

تم تفعيل (Masquerade) NAT للاتصال بالإنترنت (اختياري).

تم تعطيل NAT لحركة MPLS بين الشبكتين لضمان تمرير الحزم بشكل صحيح.

الجدار النارى (Firewall) :

تم تطبيق مجموعة من القواعد الأمنية، تشمل:

• السماح بالاتصالات Related و Established.

• السماح ببروتوكول OSPF (Protocol 89).

• السماح ببروتوكول TCP 646 عبر المنفذ LDP.

منع أي حركة مرور غير مصرح بها .

2.6 بروتوكول التوجيه OSPF

تم استخدام بروتوكول OSPF كخيار توجيه ديناميكي:

Site A: 172.168.10.1 في Router ID •

Site B: 172.168.20.1 في Router ID •

تم الإعلان عن:

شبكات LAN.

شبكة WAN/MPLS.

ويجب أن تكون حالة الجوار (Adjacency) في وضع FULL.

2.7 تقنية MPLS و LDP

2.7.1 تفعيل MPLS

تم تفعيل MPLS على واجهة wan2_mpls في كلا الموقعين.

2.7.2 بروتوكول LDP

تم تفعيل LDP لتبادل التسميات بين الموجهين، والتأكد من ظهور الجيران بشكل فعال.

2.7.3 جدول التحويل MPLS

يحتوي كل موجه على تسميات (Labels) خاصة بشبكة الموقع الآخر، مما يسمح بتمرير الحزم بكفاءة عالية.

2.8 الاختبارات والتحقق

تم إجراء مجموعة من الاختبارات للتأكد من سلامة بيئه العمل:

- اختبار Ping بين أجهزة LAN في الموقعين.
- التحقق من استلام عناوين IP عبر DHCP.
- مراقبة حزم MPLS باستخدام Wireshark.

2.9 ملخص الفصل الثاني

في هذا الفصل تم استعراض بيئه العمل الكاملة لمشروع Flat MPLS Site-to-Site ، مع شرح مفصل للأجهزة، البرمجيات، بنية الشبكة، إعدادات العنونة، بروتوكولات التوجيه، وتقنية MPLS يشكل هذا الفصل الأساس النظري والعملي الذي سيتم الاعتماد عليه في فصل التنفيذ والتطبيق العملي.

3.1 فصل الثالث : الحل المقترن

3.1.1 : Site A الاعدادات

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME          TYPE      ACTUAL-MTU L2MTU
0  LAN           ether     1500
1  MPLS          ether     1500
```

الشكل 3.1 Interfaces

في هذا الشكل، يتم عرض الواجهات الشبكية المعرفة على جهاز MikroTik في موقع Site A. تم تنفيذ الأمر `interface print` داخل واجهة الطرفية الخاصة بجهاز MikroTik CHR، ويُظهر الناتج الواجهات المتوفرة على الجهاز، مع توضيح حالتها ومواصفاتها نلاحظ وجود واجهتين من نوع "ether" وهما:

LAN: وهي الواجهة المحلية التي تربط الجهاز بالشبكة الداخلية للموقع.
MPLS: وهي الواجهة المخصصة للربط بين المواقعين باستخدام بروتوكول MPLS لتأمين الاتصال.

هذه الخطوة أساسية في التحقق من جاهزية الجهاز قبل البدء بتكوين الاتصال الآمن بين المواقعين، وتُظهر أن الواجهات مفعّلة وجاهزة لاستقبال الإعدادات التالية

- وللقيام بتنفيذ الامر `interface print` نستخدم الاوامر التالية :
`system identity set name=SiteA/`

`/interface print`

`/interface ethernet set [find default-name=ether1] name=LAN`

`/interface ethernet set [find default-name=ether2] name=wan2_mpls`

الشكل 3.2 : IP address configuration

```
      MMM      MMM      KKK      TTTTTTTTTT      KKK
      MMMMM     MMMMM     KKK      TTTTTTTTTT      KKK
      MMM  MMMMM  MMM  IIII  KKK  KKK  RRRRRR  000000  TTT  IIII  KKK  KKK
      MMM  MM  MMM  IIII  KKKKKK  RRR  RRR  000  000  TTT  IIII  KKKKKK
      MMM      MMM  IIII  KKK  KKK  RRRRRR  000  000  TTT  IIII  KKK  KKK
      MMM      MMM  IIII  KKK  KKK  RRR  RRR  000000  TTT  IIII  KKK  KKK

MikroTik RouterOS 6.49.13 (c) 1999-2024      http://www.mikrotik.com/

[?]      Gives the list of available commands
command [?]      Gives help on the command and list of arguments
[Tab]      Completes the command/word. If the input is ambiguous,
           a second [Tab] gives possible options
/
..      Move up one level
/command      Use command at the base level

[admin@MikroTik] > ip add pr
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK          INTERFACE
0   172.168.10.1/24    172.168.10.0    LAN
1   10.0.0.1/28        10.0.0.0        MPLS
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات عناوين IP على جهاز MikroTik في موقع Site A.

تم تنفيذ الأمر `ip address print` داخل واجهة الطرفية الخاصة بجهاز MikroTik CHR، ويُظهر الناتج العناوين المعينة لكل واجهة، بالإضافة إلى الشبكة المرتبطة بها. نلاحظ ما يلي:

- تم تعيين العنوان 172.168.10.1/24 على واجهة LAN، وهي الشبكة الداخلية للموقع.
- تم تعيين العنوان 10.0.0.1/28 على واجهة MPLS، وهي الواجهة المخصصة لربط بين المواقع عبر قناة آمنة.

• ولি�تم تنفيذ الواجهات نستخدم الاوامر التالية :

```
/ip address add address=172.168.10.1/24 interface=LAN
```

```
/ip address add address=10.0.0.1/28 interface=wan2_mpls
```

NAT configuration on WAN 3.3 الشكل

```
[admin@MikroTik] > ip firewall nat print
flags: X - disabled, I - invalid, D - dynamic
0    chain=srcnat action=masquerade out-interface=MPLS log=no log-prefix=""
[admin@MikroTik] > _
```

في هذا الشكل، يتم عرض إعدادات ترجمة عناوين الشبكة (NAT) على جهاز MikroTik في موقع .Site A

تم تنفيذ الأمر ip firewall nat print داخل واجهة الطرفية، ويُظهر الناتج قاعدة NAT واحدة تم إنشاؤها لتأمين الاتصال الخارجي عبر واجهة MPLS. تفاصيل القاعدة كالتالي:

:chain=srcnat – تشير إلى أن القاعدة تطبق على حركة البيانات الخارجة من الجهاز.

:action=masquerade – تُستخدم لإخفاء عنوان IP الداخلي واستبداله بعنوان الجهاز الخارجي، مما يوفر طبقة حماية إضافية.

:out-interface=MPLS – تحدد أن هذه القاعدة تطبق فقط على البيانات الخارجة عبر واجهة MPLS.

عدم وجود أعلام مثل X أو I يدل على أن القاعدة مفعّلة وصحيحة، وتعمل كما هو متوقع.

هذه الخطوة ضرورية لضمان أن الأجهزة داخل الشبكة المحلية يمكنها الوصول إلى الشبكة المقابلة أو الإنترن特 بشكل آمن، دون الكشف عن تفاصيل العناوين الداخلية، مما يعزز من مستوى الأمان في التصميم العام للشبكة

- وللقيام بتنفيذ الواجهات نستخدم الأوامر التالية :

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

الشكل 3.4 اعدادات Routing OSPF

[admin@MikroTik] > routing ospf interface pr						
Flags: X - disabled, I - inactive, D - dynamic, P - passive	#	INTERFACE	COST	PRI	NETWORK-TYPE	AUT...
	0 D	MPLS	10	1	broadcast	none
	1 D	LAN	10	1	broadcast	none

في هذا الشكل، يتم عرض إعدادات واجهات بروتوكول التوجيه динамический OSPF على جهاز

.Site A في موقع MikroTik

تم تنفيذ الأمر `routing ospf interface print` داخل واجهة الطرفية، ويُظهر الناتج الواجهات التي

تم تفعيل OSPF عليها، مع تفاصيل التكوين لكل واجهة. نلاحظ ما يلي:

- تم تفعيل OSPF على واجهتي LAN و MPLS، وكلاهما يظهر بعلم D مما يدل على أنهما

معرفتان ديناميكياً من خلال إعدادات OSPF.

- $\text{Cost} = 10$: وهي قيمة تُستخدم لحساب أفضل مسار في الشبكة، وكلما كانت أقل زادت أولوية

المسار.

هذه الخطوة تعد أساسية في بناء شبكة ديناميكية بين المواقعين، حيث يمكن OSPF من تبادل

معلومات التوجيه تلقائياً، مما يسهل إدارة الشبكة ويحسن من كفاءتها واستجابتها للتغيرات

الشكل 3.5 OSPF Conf

```
[admin@MikroTik] > routing ospf network print
Flags: X - disabled, I - invalid
#   NETWORK           AREA
0   10.0.0.0/28      backbone
1   172.168.10.0/24  backbone
```

في هذا الشكل، يتم عرض الشبكات المعرفة ضمن بروتوكول OSPF على جهاز MikroTik في موقع Site A.

تم تنفيذ الأمر `routing ospf network print` داخل واجهة الطرفية، ويُظهر الناتج الشبكات التي تم إدراجهما ضمن عملية التوجيه الديناميكي باستخدام OSPF. نلاحظ ما يلي:

- تم تعريف الشبكة `10.0.0.0/28`، وهي الشبكة المرتبطة بواجهة MPLS.
- تم تعريف الشبكة `172.168.10.0/24`، وهي الشبكة الداخلية المرتبطة بواجهة LAN.
- كلا الشبكتين تم إدراجهما ضمن منطقة التوجيه الأساسية `backbone`، وهي المنطقة الافتراضية في OSPF والتي تُستخدم لربط جميع المناطق الأخرى.

هذه الخطوة تُعد من أساسيات بناء شبكة OSPF فعالة، حيث تُمكن الأجهزة من تبادل معلومات التوجيه بشكل تلقائي، مما يُحسن من كفاءة الشبكة ويسهل إدارتها، خاصة في بيئة متعددة المواقع

- وللقيام بذلك، نستخدم الاوامر التالية :

```
/routing ospf instance set [ find default=yes ] router-id=172.168.10.1
```

```
/routing ospf network add network=172.168.10.0/24 area=backbone
```

```
/routing ospf network add network=10.0.0.0/30 area=backbone
```

MPLS LDP enabling 3.6

```
[admin@MikroTik] > mpls ldp pr  
enabled: yes
```

في هذا الشكل، يتم عرض حالة تفعيل بروتوكول توزيع العلامات (LDP) ضمن إعدادات MPLS على جهاز MikroTik في موقع Site A.

تم تنفيذ الأمر `mpls ldp print` داخل واجهة الطرفية، ويُظهر الناتج أن الخيار `enabled` مضبوط على `yes`، مما يدل على أن بروتوكول LDP مفعل.

يُعد تفعيل LDP خطوة ضرورية في بيئة MPLS، حيث يستخدم هذا البروتوكول لتبادل معلومات العلامات بين أجهزة التوجيه، مما يمكن من بناء مسارات فعالة لنقل البيانات عبر الشبكة.

هذا التكوين يعزز من أداء الشبكة ويسهل من تطبيق السياسات الأمنية والتوجيهية، خاصة في المشاريع التي تعتمد على الربط بين مواقع متعددة باستخدام MPLS.

```
/mpls ldp add lsr-id=172.168.10.1
```

```
/mpls ldp interface add interface=wan2_mpls
```

الشكل 3.7 اعدادات بروتوكول MPLS :

```
[admin@MikroTik] > mpls print
    dynamic-label-range: 16-1048575
        propagate-ttl: yes
        allow-fast-path: yes
```

في هذا الشكل، يتم عرض إعدادات بروتوكول MPLS على جهاز MikroTik في موقع Site A.

تم تنفيذ الأمر `mpls print` داخل واجهة الطرفية، ويُظهر الناتج مجموعة من الإعدادات الأساسية التي تحكم سلوك MPLS داخل الجهاز:

- `dynamic-label-range: 16-1048575`: يُحدد نطاق العلامات الديناميكية التي يمكن استخدامها لتوجيه الحزم عبر الشبكة، مما يوفر مرونة كبيرة في إدارة المسارات.

- `propagate-ttl: yes`: يشير إلى أن قيمة TTL (Time To Live) تُنقل مع الحزمة، مما يساعد في تتبع المسارات ومنع الحلقات التوجيهية.

- `allow-fast-path: yes`: يمكن من استخدام المسار السريع (Fast Path) لتحسين أداء التوجيه وقليل زمن الاستجابة.

هذه الإعدادات تعد ضرورية لضمان أن بروتوكول MPLS يعمل بكفاءة، ويساهم في بناء شبكة عالية الأداء وأمنة بين المواقعين، خاصة عند استخدام تقنيات مثل OSPF و LDP في التوجيه الديناميكي.

الشكل 3.8 ip add conf (voip+data)

Flags: X - disabled, I - invalid, D - dynamic	ADDRESS	NETWORK	INTERFACE
	0 172.168.10.1/24	172.168.10.0	LAN
	1 10.0.0.1/28	10.0.0.0	MPLS_VOIP
	2 11.0.0.1/28	11.0.0.0	MPLS_DATA
[admin@MikroTik] > _			

في هذا الشكل، يتم عرض إعدادات عناوين IP على جهاز MikroTik في موقع Site A بعد إضافة واجهات جديدة مخصصة لخدمات متعددة.

تم تنفيذ الأمر `ip address print` داخل واجهة الطرفية، ويُظهر الناتج توزيع العناوين على ثلاثة واجهات مختلفة، كل منها تخدم غرضاً معيناً داخل الشبكة:

- LAN: تم تعيين العنوان 172.168.10.1/24، وهو يمثل الشبكة الداخلية للموقع.

- MPLS_VOIP: تم تعيين العنوان 10.0.0.1/28، وهي واجهة مخصصة لنقل بيانات الصوت عبر بروتوكول MPLS.

- MPLS_DATA: تم تعيين العنوان 11.0.0.1/28، وهي واجهة مخصصة لنقل البيانات العامة عبر MPLS.

كل واجهة مرتبطة بشبكة فرعية مستقلة، مما يسهم في فصل حركة البيانات حسب نوع الخدمة، ويعزز من كفاءة التوجيه والتحكم في السياسات الأمنية.

الشكل 3.9 firewall ip address-list

```
[admin@MikroTik] > ip firewall address-list print detail  
Flags: X - disabled, D - dynamic  
0 list=site2 address=172.168.20.0/24 creation-time=dec/25/2025 21:47:58  
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إدخال جديد ضمن قائمة العناوين في الجدار الناري (Firewall

.Site A) على جهاز MikroTik في موقع

تم تنفيذ الأمر ip firewall address-list print detail داخل واجهة الطرفية، ويُظهر الناتج إدخالاً واحداً في القائمة تحت اسم site2، ويشمل ما يلي:

- address=172.168.20.0/24: يُمثل شبكة فرعية كاملة تم إدراجها ضمن القائمة.

- list=site2: يستخدم لتجميع العناوين تحت اسم محدد يمكن الرجوع إليه لاحقاً في قواعد الجدار الناري.

- creation-time=dec/25/2025 21:47:58: يوضح وقت إنشاء هذا الإدخال، مما يُساعد في التوثيق والمراجعة.

هذه الخطوة تُعد من الأساليب الفعالة في إدارة الجدار الناري، حيث تتيح تصنيف العناوين ضمن قوائم يمكن استخدامها لاحقاً في قواعد الحظر أو السماح، مما يُبسط من عملية التحكم في حركة البيانات ويعزز من أمان الشبكة.

الشكل 3.10 ip firewall mangle

```
# list=site2 address=172.168.20.0/24 creation-time=dec/23/2025 21:47:58
[admin@MikroTik] > ip firewall mangle pr detail
Flags: X - disabled, I - invalid, D - dynamic
  0  chain=prerouting action=mark-connection new-connection-mark=con_voip
    passthrough=yes protocol=udp dst-address-list=site2
    dst-port=5060,10000-20000 log=no log-prefix=""
  1  chain=prerouting action=mark-packet new-packet-mark=pkt_voip
    passthrough=no connection-mark=con_voip log=no log-prefix=""
  2  chain=prerouting action=mark-routing new-routing-mark=VOIP_PATH
    passthrough=no packet-mark=pkt_voip log=no log-prefix=""
  3  chain=prerouting action=mark-routing new-routing-mark=DATA_PATH
    passthrough=no dst-address-list=site2 connection-mark=!con_voip log=no
    log-prefix=""
  4  chain=prerouting action=mark-packet new-packet-mark=pkt_icmp
    passthrough=no protocol=icmp connection-mark="" log=no log-prefix=""
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات قواعد Mangle ضمن الجدار النارى على جهاز MikroTik في موقع Site A، وذلك بهدف تصنيف حركة البيانات وتوجيهها حسب نوع الخدمة.

تم تنفيذ الأمر `ip firewall mangle print detail` داخل واجهة الطرفية، ويُظهر الناتج مجموعة من القواعد التي تُستخدم لتحديد نوع الاتصال، ووضع علامات على الحزم، وتوجيهها عبر المسارات المناسبة. نلاحظ ما يلي:

- القاعدة 0: تُستخدم لتحديد الاتصالات الخاصة بـ VoIP عبر بروتوكول UDP، وتُعطيها علامة اتصال باسم `con_voip`، بناءً على قائمة العناوين site2 والمنافذ 5060 و 10000-20000.
- القاعدة 1: تُستخدم لوضع علامة على الحزم المرتبطة بالاتصالات التي تحمل العلامة `con_voip`، وتُعطيها علامة حزمة باسم `.pkt_voip`.
- القاعدة 2: تُستخدم لتوجيه الحزم التي تحمل العلامة `pkt_voip` عبر المسار المخصص لخدمة الصوت `.VOIP_PATH`.
- القاعدة 3: تُستخدم لتوجيه باقى الحزم المرتبطة بـ site2 والتي لا تحمل علامة `con_voip` عبر المسار المخصص للبيانات `.DATA_PATH`.

- القاعدة 4: تُستخدم لوضع علامة على الحزم من نوع ICMP، وتُعطيها علامة باسم .pkt_icmp.

هذه القواعد تُعد من الأدوات المتقدمة في MikroTik، وتُستخدم لتحقيق فصل منطقي بين أنواع الحركة داخل الشبكة، مما يُسهم في تحسين الأداء، وتطبيق سياسات QoS، وضمان توجيه الحزم عبر المسارات المناسبة حسب نوع الخدمة

الشكل 3.11 firewall nat for voip and data

```
[admin@MikroTik] > ip firewall nat pr det
Flags: X - disabled, I - invalid, D - dynamic
0  chain=srcnat action=masquerade routing-mark=VOIP_PATH
  out-interface=MPLS_VOIP log=no log-prefix=""
1  chain=srcnat action=masquerade routing-mark=DATA_PATH connection-mark=""
  out-interface=MPLS_DATA log=no log-prefix=""
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات ترجمة العناوين (NAT) على جهاز MikroTik في موقع Site A، وذلك باستخدام علامات التوجيه لتحديد المسارات المناسبة لكل نوع من أنواع الحركة.

تم تنفيذ الأمر ip firewall nat print detail داخل واجهة الطرفية، ويُظهر الناتج وجود قاعدتين مفعّلتين ضمن سلسلة srcnat، وتفاصيلهما كالتالي:

- القاعدة الأولى: تُطبق على الحزم التي تحمل علامة التوجيه VOIP_PATH، وتُستخدم واجهة MPLS_VOIP كمسار للخروج، مع تنفيذ إجراء masquerade لإخفاء عنوان المصدر الداخلي.

- القاعدة الثانية: تُطبق على الحزم التي تحمل علامة التوجيه DATA_PATH، وتخرج عبر واجهة MPLS_DATA، مع تنفيذ نفس الإجراء لإخفاء العنوان الداخلي.

هذه الخطوة تُعد من الأساليب المتقدمة في إدارة حركة البيانات، حيث يتم توجيه الحزم حسب نوعها (صوت أو بيانات) عبر المسارات المناسبة، مما يُسهم في تحسين الأداء، وتطبيق سياسات أمنية دقيقة، وضمان استقرار الاتصال بين الموقعين

الشكل 3.12 queue tree for priority and service

```
[admin@MikroTik] > queue tree print detail
Flags: X - disabled, I - invalid
0  name="VOIP_TOTAL" parent=MPLS_VOIP packet-mark="" limit-at=0
queue=default-small priority=8 max-limit=5M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

1  name="VOIP" parent=VOIP_TOTAL packet-mark=pkt	voip limit-at=0
queue=default-small priority=1 max-limit=2M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

2  name="DATA_TOTAL" parent=MPLS_DATA packet-mark="" limit-at=0
queue=default-small priority=8 max-limit=10M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

3  name="DATA" parent=DATA_TOTAL packet-mark="" limit-at=0
queue=default-small priority=8 max-limit=8M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

4  name="ICMP" parent=DATA_TOTAL packet-mark=pkt_icmp limit-at=0
queue=default-small priority=1 max-limit=1M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1
[admin@MikroTik] > _
```

في هذا الشكل، يتم عرض إعدادات شجرة الانتظار (Queue Tree) على جهاز MikroTik في موقع Site A، وذلك بهدف تنظيم حركة البيانات وتحديد أولويات الخدمة حسب نوع الحزم.

تم تفزيذ الأمر queue tree print detail داخل واجهة الطرفية، ويُظهر الناتج مجموعة من القواعد التي تُستخدم لتوزيع عرض النطاق الترددية وتحديد الأولوية لكل نوع من أنواع الحركة. نلاحظ ما يلي:

- VOIP_TOTAL: تم ربطها بواجهة MPLS_VOIP، وتُستخدم كمجموعة رئيسية لحركة الصوت، بحد أقصى M5 وأولوية 8.

- VOIP: تدرج تحت VOIP_TOTAL، وتُطبق على الحزم التي تحمل العلامة pkt.voip، بحد أقصى M2 وأولوية 8.

- DATA_TOTAL: تم ربطها بواجهة MPLS_DATA، وتُستخدم كمجموعة رئيسية لحركة البيانات، بحد أقصى M10 وأولوية 8.

- DATA: تدرج تحت DATA_TOTAL، وتُطبق على الحزم العامة، بحد أقصى M8 وأولوية 8.

ICMP - أيضاً تحت DATA_TOTAL، وتُطبق على الحزم التي تحمل العلامة pkt_icmp، بحد أقصى M1 وأولوية 1، مما يدل على أنها تُعطى أولوية عالية في المعالجة.

عدم وجود إعدادات للـ burst يدل على أن التوزيع ثابت، مما يسهم في استقرار الأداء.

هذه الخطوة تعد من أهم مراحل تحسين جودة الخدمة داخل الشبكة، حيث يتم التحكم في توزيع الموارد حسب نوع الحركة، مما يقلل من التأخير ويحسن تجربة المستخدم، خاصة في الخدمات الحساسة مثل VoIP

الشكل 3.13 mpls interfaces (voip+data+lan)

```
[admin@MikroTik] > mpls interface pr detail
Flags: X - disabled, * - default
  0  * interface=MPLS_VOIP mpls-mtu=1508
    1      interface=LAN mpls-mtu=1508
    2      interface=MPLS_DATA mpls-mtu=1508
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات واجهات MPLS على جهاز MikroTik في موقع Site A، مع تحديد قيمة MTU الخاصة بكل واجهة.

تم تنفيذ الأمر mpls interface print detail داخل واجهة الطرفية، ويُظهر الناتج ثلاث واجهات تم تفعيل MPLS عليها، وهي:

MPLS_VOIP - وهي الواجهة الافتراضية، وتُستخدم لنقل حركة الصوت عبر بروتوكول .MPLS

LAN - الواجهة المحلية التي تربط الجهاز بالشبكة الداخلية.

MPLS_DATA - واجهة مخصصة لنقل البيانات العامة عبر .MPLS

كل واجهة تم ضبطها على قيمة $mpls-mtu = 1508$ ، وهي قيمة مناسبة لضمان أن الحزم الموجهة عبر MPLS لا تتعرض للتجزئة، مما يحسن من كفاءة التوجيه ويقلل من التأخير.

هذه الخطوة تُعد من الأساسيات في إعداد MPLS، حيث أن ضبط قيمة MTU بشكل صحيح يسهم في استقرار الشبكة ويحسن من أداء نقل البيانات بين المواقع

3.2.1 الاعدادات ل Site B

interfaces Site B 3.2.1

#	NAME	TYPE	ACTUAL-MTU	L2MTU
0	R LAN	ether	1500	
1	R MPLS	ether	1500	

في هذا الشكل، يتم عرض الواجهات المعرفة على جهاز MikroTik في موقع .Site B

تم تنفيذ الأمر `interface print` داخل واجهة الطرفية الخاصة بجهاز MikroTik CHR، ويُظهر الناتج الواجهات المتوفرة على الجهاز، مع توضيح حالتها ومواصفاتها. نلاحظ وجود واجهتين من نوع "ether" ، وهما:

- LAN: الواجهة المحلية التي تربط الجهاز بالشبكة الداخلية للموقع.

- MPLS: الواجهة المخصصة للربط بين الموقع باستخدام بروتوكول MPLS لتأمين الاتصال.

هذه الخطوة تُعد أساسية في التحقق من جاهزية الجهاز قبل البدء في إعدادات التوجيه، وتُساهم في ضمان أن الاتصال بين الأجهزة داخل الموقع يتم بشكل صحيح ومستقر

الشكل 3.2.2 اعدادات عناوين IP

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - d
#      ADDRESS          NETWORK
0      10.0.0.2/28      10.0.0.0
1      172.168.20.1/24  172.168.20.0
2      11.0.0.2/28      11.0.0.0
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات عناوين IP على جهاز MikroTik في موقع Site B.

تم تنفيذ الأمر ip address print داخل واجهة الطرفية، ويُظهر الناتج توزيع العناوين على ثلاثة شبكات فرعية مختلفة، كل منها مرتبطة بواجهة معينة داخل الموقع:

.28/10.0.0.2 - يُمثل عنوان الجهاز ضمن شبكة MPLS الخاصة بخدمة VoIP.

.24/172.168.20.1 - يُمثل عنوان الجهاز ضمن الشبكة الداخلية المحلية للموقع.

.28/11.0.0.2 - يُمثل عنوان الجهاز ضمن شبكة MPLS الخاصة بنقل البيانات العامة.

كل عنوان مرتبط بشبكة فرعية مستقلة، مما يُسهم في فصل حركة البيانات حسب نوع الخدمة، ويعزز من كفاءة التوجيه والتحكم في السياسات الأمنية داخل موقع Site B.

هذه الخطوة تعد ضرورية لضمان أن كل واجهة في الجهاز تحمل عنواناً مناسباً ضمن نطاقها، مما يمكن من تطبيق التوجيه الدинامي والسياسات الأمنية بشكل دقيق وفعال.

الشكل 3.2.3 NAT configuration on WAN

```
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0    chain=srcnat action=masquerade out-interface=MPLS_VOIP log=no
      log-prefix=""
1    chain=srcnat action=masquerade out-interface=mpls_data log=no
      log-prefix=""
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات ترجمة العناوين (NAT) على جهاز MikroTik في موقع Site B.

تم تنفيذ الأمر `ip firewall nat print` داخل واجهة الطرفية، ويُظهر الناتج وجود قاعدتين مفعّلتين ضمن سلسلة srcnat، وتفاصيلهما كالتالي:

- القاعدة الأولى: تُطبق على الحزم الخارجة عبر واجهة MPLS_VOIP، ويتم تنفيذ إجراء masquerade لإخفاء عنوان المصدر الداخلي.

- القاعدة الثانية: تُطبق على الحزم الخارجة عبر واجهة mpls_data، بنفس الإجراء لإخفاء العنوان الداخلي.

عدم وجود أعلام مثل X أو I يدل على أن القواعد مفعّلة وصحيحة، وتعمل كما هو متوقع.

هذه الخطوة تعد ضرورية لضمان أن الأجهزة داخل الشبكة المحلية في موقع Site B يمكنها الوصول إلى الشبكة المقابلة أو الإنترن特 بشكل آمن، دون الكشف عن تفاصيل العناوين الداخلية، مما يعزز من مستوى الأمان في التصميم العام للشبكة.

الشكل 3.2.4 Routing ospf interfaces

```
[admin@MikroTik] > routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
#  INTERFACE          COST PRI NETWORK-TYPE  AUT... AUTHENTICATIO...
0 D  MPLS_VOIP        10   1 broadcast    none
1 D  mpls_data         10   1 broadcast    none
2 D  LAN               10   1 broadcast    none
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات واجهات بروتوكول التوجيه динамический OSPF على جهاز MikroTik في موقع Site B.

تم تنفيذ الأمر `routing ospf interface print` داخل واجهة الطرفية، ويُظهر الناتج الواجهات التي تم تفعيل OSPF عليها، مع تفاصيل التكوين لكل واجهة. نلاحظ ما يلي:

- تم تفعيل OSPF على ثلاثة واجهات: LAN، mpls_data، و MPLS_VOIP، و جميعها تظاهر بعلم D مما يدل على أنها معرفات ديناميكياً من خلال إعدادات OSPF.

- $\text{Cost} = 10$ وهي القيمة المستخدمة لحساب أفضل مسار في الشبكة، وكلما كانت أقل زادت أولوية المسار.

- $\text{Priority} = 1$ تُستخدم لتحديد أولوية اختيار جهاز التوجيه الرئيسي (DR) في الشبكات من نوع broadcast.

- $\text{Network-Type} = \text{broadcast}$ يدل على أن الواجهات تعمل في بيئة شبكية تسمح بإرسال البيانات إلى جميع الأجهزة.

- $\text{Authentication} = \text{none}$ لم يتم تفعيل المصادقة، مما يعني أن التوجيه يتم بدون تحقق من الهوية، وهو أمر يمكن تحسينه لاحقاً لتعزيز الأمان.

هذه الخطوة تعد أساسية في بناء شبكة ديناميكية داخل موقع Site B، حيث يمكن OSPF من تبادل معلومات التوجيه تلقائياً، مما يسهل إدارة الشبكة ويحسن من كفاءتها واستجابتها للتغيرات.

الشكل 3.2.5 Routing Ospf Network

```
[admin@MikroTik] > routing ospf network print
Flags: X - disabled, I - invalid
#   NETWORK          AREA
0   172.168.20.0/24 backbone
1   10.0.0.0/28    backbone
2   11.0.0.0/28    backbone
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض الشبكات المعرفة ضمن بروتوكول OSPF على جهاز MikroTik في موقع Site B.

تم تنفيذ الأمر `routing ospf network print` داخل واجهة الطرفية، ويُظهر الناتج الشبكات التي تم إدراجها ضمن عملية التوجيه الديناميكي باستخدام OSPF. نلاحظ ما يلي:

.Site B: تمثل الشبكة الداخلية المحلية لموقع 24/172.168.20.0 –

.VoIP: تمثل شبكة MPLS الخاصة بخدمة 28/10.0.0.0 –

.: تمثل شبكة MPLS الخاصة بنقل البيانات العامة 28/11.0.0.0 –

جميع الشبكات تم إدراجها ضمن منطقة التوجيه الأساسية `backbone`، وهي المنطقة الافتراضية في OSPF والتي تُستخدم لربط جميع المناطق الأخرى.

هذه الخطوة تعد من أساسيات بناء شبكة OSPF فعالة داخل موقع Site B، حيث تُمكن الأجهزة من تبادل معلومات التوجيه بشكل تلقائي، مما يحسن من كفاءة الشبكة ويسهل إدارتها، خاصة في بيئة متعددة الخدمات.

الشكل 3.2.6 MPLS LDP enabling

```
[admin@MikroTik] > mpls ldp print  
enabled: yes
```

في هذا الشكل، يتم عرض حالة تفعيل بروتوكول توزيع العلامات (LDP) ضمن إعدادات MPLS على جهاز MikroTik في موقع Site B.

تم تنفيذ الأمر `mpls ldp print` داخل واجهة الطرفية، ويُظهر الناتج أن الخيار `enabled` مضبوط على `yes`، مما يدل على أن بروتوكول LDP مفعل.

يُعد تفعيل LDP خطوة أساسية في بيئة MPLS، حيث يستخدم هذا البروتوكول لتبادل معلومات العلامات بين أجهزة التوجيه، مما يمكن من بناء مسارات فعالة لنقل البيانات عبر الشبكة.

هذه الخطوة تُعزز من أداء الشبكة داخل موقع Site B، وتُسهل من تطبيق السياسات التوجيهية، خاصة عند استخدام تقنيات مثل OSPF و Mangle لتصنيف الحزم وتوجيهها حسب نوع الخدمة.

MPLS 3.2.7 الشكل

```
[admin@MikroTik] > mpls pr
    dynamic-label-range: 16-1048575
        propagate-ttl: yes
        allow-fast-path: yes
```

في هذا الشكل، يتم عرض إعدادات بروتوكول MPLS على جهاز MikroTik في موقع .Site B

تم تنفيذ الأمر mpls print داخل واجهة الطرفية، ويُظهر الناتج مجموعة من الإعدادات الأساسية التي تحكم سلوك MPLS داخل الجهاز:

- dynamic-label-range: 16-1048575: يُحدد نطاق العلامات الديناميكية التي يمكن استخدامها لتوجيه الحزم عبر الشبكة، مما يوفر مرونة كبيرة في إدارة المسارات.

- propagate-ttl: yes: يشير إلى أن قيمة TTL (Time To Live) تُنقل مع الحزمة، مما يساعد في تتبع المسارات ومنع الحلقات التوجيهية.

- allow-fast-path: yes: يُمكن من استخدام المسار السريع (Fast Path) لتحسين أداء التوجيه وتقليل زمن الاستجابة.

هذه الإعدادات تُعد ضرورية لضمان أن بروتوكول MPLS يعمل بكفاءة داخل موقع Site B، وتساهم في بناء شبكة عالية الأداء وآمنة، خاصة عند دمجها مع تقنيات مثل OSPF و LDP لتوسيع نطاق الحزم بشكل ديناميكي وفعال.

الشكل 3.2.8 ip add conf (voip+data)

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS           NETWORK           INTERFACE
0 10.0.0.2/28      10.0.0.0        MPLS_VOIP
1 172.168.20.1/24  172.168.20.0    LAN
2 11.0.0.2/28      11.0.0.0        mpls_data
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض توزيع عناوين IP على الواجهات المختلفة لجهاز MikroTik في موقع .Site B

تم تنفيذ الأمر ip address print داخل واجهة الطرفية، ويُظهر الناتج ثلاثة واجهات تم تعيين عناوين IP لها، وهي:

- MPLS_VOIP: تم تعيين العنوان 28/10.0.0.2، وهو مخصص لنقل حركة الصوت عبر بروتوكول .MPLS

- LAN: تم تعيين العنوان 24/172.168.20.1، وهو يمثل الشبكة الداخلية المحلية للموقع.

- mpls_data: تم تعيين العنوان 28/11.0.0.2، ويُستخدم لنقل البيانات العامة عبر .MPLS

كل واجهة مرتبطة بشبكة فرعية مستقلة، مما يُسهم في فصل حركة البيانات حسب نوع الخدمة، ويعزز من كفاءة التوجيه والتحكم في السياسات الأمنية داخل موقع .Site B

هذه الخطوة تعد ضرورية لضمان أن كل واجهة في الجهاز تحمل عنواناً مناسباً ضمن نطاقها، مما يُمكن من تطبيق التوجيه الديناميكي والسياسات الأمنية بشكل دقيق وفعال

الشكل 3.2.9 firewall ip address-list

```
[admin@MikroTik] > ip firewall address-list print detail
Flags: X - disabled, D - dynamic
0  list=SITE1 address=172.168.10.0/24 creation-time=jan/07/2026 15:06:55
[admin@MikroTik] > _
```

في هذا الشكل، يتم عرض إدخال جديد ضمن قائمة العناوين في الجدار الناري (Firewall .Site B) على جهاز MikroTik في موقع (Address List

تم تنفيذ الأمر ip firewall address-list print detail داخل واجهة الطرفية، ويُظهر الناتج إدخالاً واحداً في القائمة تحت اسم SITE1، ويشمل ما يلي:

- address=172.168.10.0/24 : يمثل شبكة فرعية كاملة تم إدراجها ضمن القائمة، وهي خاصة .Site A بموقع

- list=SITE1 : يستخدم لتجميع العناوين تحت اسم محدد يمكن الرجوع إليه لاحقاً في قواعد الجدار النارى.

- creation-time=jan/07/2026 15:06:55 : يوضح وقت إنشاء هذا الإدخال، مما يساعد في التوثيق والرجوع.

هذه الخطوة تعد من الأساليب الفعالة في إدارة الجدار النارى داخل موقع Site B، حيث تتيح تصنيف العناوين ضمن قوائم يمكن استخدامها لاحقاً في قواعد الحظر أو السماح، مما يُسimplify عملية التحكم في حركة البيانات ويعزز من أمان الشبكة بين المواقع

الشكل 3.2.10 ip firewall mangle

```
[admin@MikroTik] > ip firewall mangle print detail
Flags: X - disabled, I - invalid, D - dynamic
  0  chain=prerouting action=mark-connection new-connection-mark=conn_voip
    passthrough=yes protocol=udp dst-address-list=SITE1
    connection-mark=conn_voip dst-port=5060,10000-20000 log=no
    log-prefix=""
  1  chain=prerouting action=mark-packet new-packet-mark=pkt_voip
    passthrough=no connection-mark=conn_voip log=no log-prefix=""
  2  chain=prerouting action=mark-routing new-routing-mark=VOIP_PATH
    passthrough=no packet-mark=pkt_voip log=no log-prefix=""
  3  chain=prerouting action=mark-routing new-routing-mark=DATA_PATH
    passthrough=no dst-address-list=SITE1 connection-mark=!conn_voip log=no
    log-prefix=""
  4  chain=prerouting action=mark-packet new-packet-mark=pkt_icmp
    passthrough=no protocol=icmp log=no log-prefix=""
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات قواعد Mangle ضمن الجدار الناري على جهاز MikroTik في موقع Site B، وذلك بهدف تصنيف حركة البيانات وتوجيهها حسب نوع الخدمة.

تم تنفيذ الأمر `ip firewall mangle print detail` داخل واجهة الطرفية، ويُظهر الناتج مجموعة من القواعد التي تُستخدم لتحديد نوع الاتصال، ووضع علامات على الحزم، وتوجيهها عبر المسارات المناسبة. نلاحظ ما يلي:

- القاعدة 0: تُستخدم لتحديد الاتصالات الخاصة بـ VoIP عبر بروتوكول UDP، وتعطيها علامة اتصال باسم `conn_voip`، بناءً على قائمة العناوين SITE1 والمنفذ 5060 و 10000-20000.

- القاعدة 1: تُستخدم لوضع علامة على الحزم المرتبطة بالاتصالات التي تحمل العلامة `.pkt_voip`، وتعطيها علامة حزمة باسم `conn_voip`.

- القاعدة 2: تُستخدم لتوجيه الحزم التي تحمل العلامة `pkt_voip` عبر المسار المخصص لخدمة الصوت `VOIP_PATH`.

- القاعدة 3: تُستخدم لتوجيه باقي الحزم المرتبطة بـ SITE1 والتي لا تحمل علامة `.DATA_PATH` عبر المسار المخصص للبيانات.

- القاعدة 4: تُستخدم لوضع علامة على الحزم من نوع ICMP، وتُعطيها علامة باسم .pkt_icmp.

هذه القواعد تُعد من الأدوات المتقدمة في MikroTik، وتُستخدم لتحقيق فصل منطقي بين أنواع الحركة داخل الشبكة، مما يُسهم في تحسين الأداء، وتطبيق سياسات QoS، وضمان توجيه الحزم عبر المسارات المناسبة حسب نوع الخدمة، خاصة في بيئة الربط بين موقع Site A وموقع Site B.

الشكل 3.2.11 firewall nat for voip and data

```
[admin@MikroTik] > ip firewall nat print detail
Flags: X - disabled, I - invalid, D - dynamic
0  chain=srcnat action=masquerade out-interface=MPLS_VOIP log=no
log-prefix=""
1  chain=srcnat action=masquerade out-interface=mpls_data log=no
log-prefix=""
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات ترجمة العناوين (NAT) على جهاز MikroTik في موقع Site B، وذلك باستخدام واجهات MPLS المخصصة لكل نوع من أنواع الحركة.

تم تنفيذ الأمر ip firewall nat print detail داخل واجهة الطرفية، ويُظهر الناتج وجود قاعدتين مفعّلتين ضمن سلسلة srcnat، وتفاصيلهما كالتالي:

- القاعدة الأولى: تُطبق على الحزم الخارجة عبر واجهة MPLS_VOIP، ويتم تنفيذ إجراء masquerade لإخفاء عنوان المصدر الداخلي، مما يُمكّن من التواصل مع الشبكات الخارجية دون الكشف عن تفاصيل الشبكة المحلية.

- القاعدة الثانية: تُطبق على الحزم الخارجة عبر واجهة mpls_data، بنفس الإجراء، وذلك لتؤمن حرمة البيانات العامة.

عدم وجود أعلام مثل X أو I يدل على أن القواعد مفعّلة وصحيحة، وتعمل كما هو متوقع.

هذه الخطوة تُعد ضرورية لضمان أن الأجهزة داخل الشبكة المحلية في موقع Site B يمكنها الوصول إلى الشبكات الأخرى بشكل آمن، مع الحفاظ على خصوصية العناوين الداخلية، مما يعزز من مستوى الأمان في التصميم العام للشبكة، خاصة في بيئة الربط بين الموقع عبر

الشكل 3.2.12 queue tree for priority and service

```
[admin@MikroTik] > queue tree print detail
Flags: X - disabled, I - invalid
0  name="VOIP_TOTAL" parent=MPLS_VOIP packet-mark="" limit-at=0
queue=default-small priority=1 max-limit=5M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

1  name="VOIP_Q" parent=VOIP_TOTAL packet-mark=pkt_voip limit-at=0
queue=default-small priority=1 max-limit=2M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

2  name="DATA_TOTAL" parent=mpls_data packet-mark="" limit-at=0
queue=default-small priority=8 max-limit=10M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

3  name="ICMP_Q" parent=DATA_TOTAL packet-mark=pkt_icmp limit-at=0
queue=default-small priority=1 max-limit=1M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1

4  name="DATA_Q" parent=DATA_TOTAL packet-mark="" limit-at=0
queue=default-small priority=8 max-limit=9M burst-limit=0
burst-threshold=0 burst-time=0s bucket-size=0.1
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات شجرة الانتظار (Queue Tree) على جهاز MikroTik في موقع Site B، وذلك بهدف تنظيم حركة البيانات وتحديد أولويات الخدمة حسب نوع الحزم.

تم تنفيذ الأمر `queue tree print detail` داخل واجهة الطرفية، ويُظهر الناتج مجموعة من القواعد التي تُستخدم لتوزيع عرض النطاق الترددية وتحديد الأولوية لكل نوع من أنواع الحركة. نلاحظ ما يلي:

- `VOIP_TOTAL`: تم ربطها بواجهة `MPLS_VOIP`، وتُستخدم كمجموعة رئيسية لحركة الصوت، بحد أقصى M5 وأولوية 1.

- `VOIP_Q`: تدرج تحت `VOIP_TOTAL`، وتُطبق على الحزم التي تحمل العلامة `pkt_voip`، بحد أقصى M2 وأولوية 1.

- `DATA_TOTAL`: تم ربطها بواجهة `mpls_data`، وتُستخدم كمجموعة رئيسية لحركة البيانات، بحد أقصى M10 وأولوية 8.

8. - DATA_Q - تدرج تحت DATA_TOTAL، وتُطبق على الحزم العامة، بحد أقصى M9 وأولوية .

- ICMP_Q - أيضاً تحت DATA_TOTAL، وتُطبق على الحزم التي تحمل العلامة pkt_icmp، بحد أقصى M1 وأولوية 1، مما يدل على أنها تُعطى أولوية عالية في المعالجة.

عدم وجود إعدادات للـ burst يدل على أن التوزيع ثابت، مما يُسهم في استقرار الأداء.

هذه الخطوة تُعد من أهم مراحل تحسين جودة الخدمة داخل موقع Site B، حيث يتم التحكم في توزيع الموارد حسب نوع الحركة، مما يُقلل من التأخير ويساعد تجربة المستخدم، خاصة في الخدمات الحساسة مثل VoIP و ICMP.

الشكل 3.2.13 mpls interfaces (voip+data+lan)

```
[admin@MikroTik] > mpls interface print detail
Flags: X - disabled, * - default
0 X* interface=all mpls-mtu=1508
1     interface=MPLS_VOIP mpls-mtu=1508
2     interface=mpls_data mpls-mtu=1508
[admin@MikroTik] >
```

في هذا الشكل، يتم عرض إعدادات واجهات MPLS على جهاز MikroTik في موقع Site B، مع توضيح حالة كل واجهة وقيمة MTU الخاصة بها.

تم تنفيذ الأمر mpls interface print detail داخل واجهة الطرفية، ويُظهر الناتج ثلاث واجهات كما يلي:

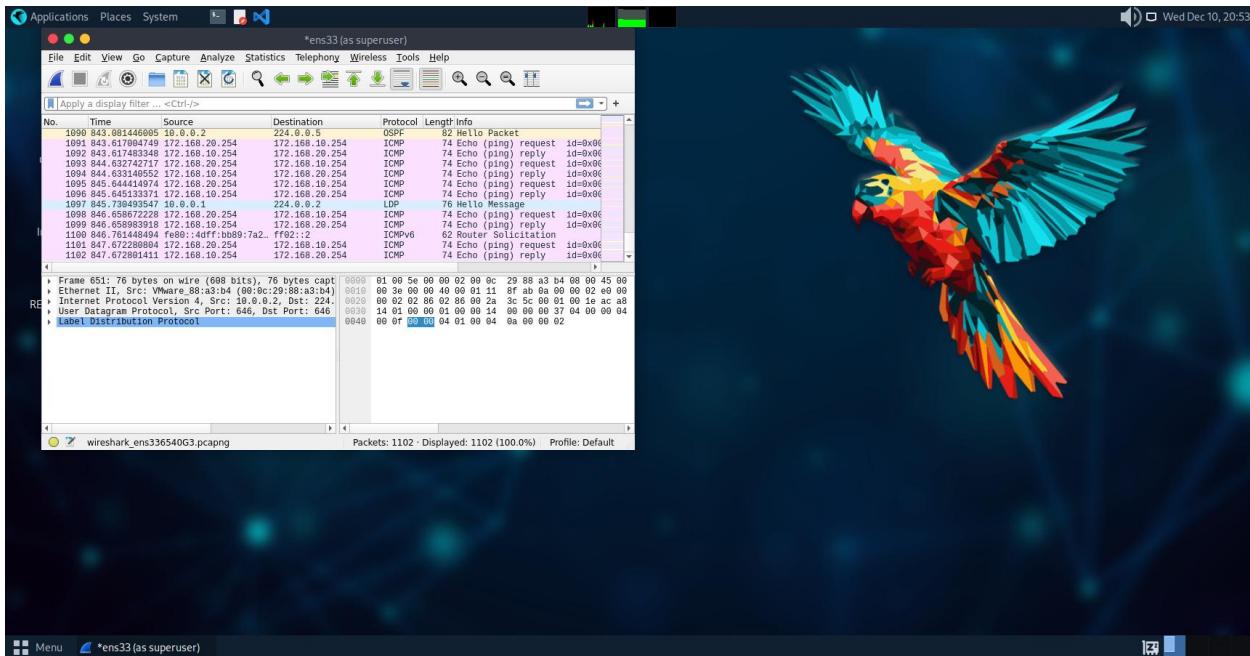
- interface=all: وهي الواجهة الافتراضية، ولكنها تظهر بعلم X* مما يدل على أنها مُعطلة رغم كونها الإعداد الافتراضي.

MTU، بقيمة `interface=MPLS_VOIP` –
واجهة مخصصة لنقل حركة الصوت عبر MPLS، تبلغ 1508.

MTU –
واجهة مخصصة لنقل البيانات العامة عبر MPLS، بنفس قيمة `interface=mpls_data` –
وهي 1508.

تفعيل واجهات MPLS بهذه الطريقة يُعد خطوة أساسية لضمان أن الحزم تُنقل بكفاءة دون تجزئة، خاصة في بيئة الربط بين المواقع. كما أن تعطيل الواجهة الافتراضية "all" يُشير إلى تخصيص التوجيه فقط للواجهات المحددة، مما يعزز من التحكم في حركة البيانات ويقلل من احتمالية التداخل أو التوجيه غير المرغوب فيه

الشكل 3.1.14 تحليل حركة الشبكة باستخدام Wireshark



يعرض لقطة شاشة من أداة Wireshark تم التقاطها أثناء مراقبة حركة البيانات بين الموقعين Site A و Site B. يُظهر هذا الشكل تفاصيل الحزم المنقولة عبر رابط MPLS، مع إبراز حركة بروتوكولات ICMP و LDP و OSPF و (ping) ICMP.

1. جدول الحزم (Packet List):

يظهر الجدول سلسلة من الحزم المرسلة والمستقبلة بين العناوين التالية:

العناوين الظاهرة:

Site A (MPLS Interface) → 10.0.0.1

Site B (MPLS Interface) → 10.0.0.2

Site A → مضيف في 172.168.10.254

Site B → مضيف في 172.168.20.254

: OSPF حركة

الحزمة 1090: (OSPF Hello عنوان 224.0.0.5 → 10.0.0.2)

التفسير: إرسال حزمة OSPF Hello للجوار، مما يدل على أن OSPF يعمل بنجاح ويحافظ على الجوار بين الموجهين.

حركة ICMP (اختبار الاتصال):

الحزم 1091-1102: طلبات Ping وردودها بين 172.168.20.254 و 172.168.10.254

التفسير: تأكيد الاتصال الناجح بين المضيفين في كل المواقع عبر شبكة MPLS.

حركة LDP:

الحزمة 1097: (LDP Hello عنوان 224.0.0.2 → 10.0.0.1)

التفسير: إرسال رسالة LDP Hello لتبادل معلومات العلامات (Labels) بين الموجهين، مما يدل على تفعيل MPLS/LDP بنجاح.

2. تفاصيل الحزمة : (Frame Details)

تم تفصيل الحزمة 1097 (LDP Hello) لإظهار بنيتها:

الإطار 651:

الحجم: 76 بايت.

المصدر الفعلي: .(VMware واجهة c:29:88:a3:b400:0)

.IP المصدر: (Site B) 10.0.0.2

.IP الوجهة: (عنوان 224.0.0.2 multicast)

البروتوكول: UDP على المنفذ 646 (منفذ LDP القياسي).

بيانات LDP: تحتوي على معرف الموجه (LSR-ID) (المقابل لـ 172.168.20.1) ac a8 14 01.

3. التحليل التقني:

نجاح OSPF: وجود حزم Hello يؤكد أن OSPF في حالة "FULL" بين الموقعين.

نجاح MPLS/LDP: إرسال واستقبال حزم LDP يدل على تبادل العلامات وإنشاء مسارات.

اختبار الاتصال: استمرارية طلبات Ping وردودها تؤكد أن البيانات تنتقل عبر MPLS بدون NAT، مع الحفاظ على العناوين الأصلية.

4. الأهمية في إطار المشروع:

يؤكد هذا الشكل النجاح العملي لجميع الإعدادات الموضحة في الفصول السابقة، حيث:

يتم توجيه البيانات عبر MPLS باستخدام العلامات.

يعمل OSPF كبروتوكول توجيه ديناميكي.

يتم الحفاظ على الاتصال بين الشبكات المحلية مع تطبيق قواعد الأمان والجودة.

3.3 ملخص فصل الثالث :

إعدادات الشبكة وتكامل الخدمات في موقعي Site B و Site A

يتناول هذا الفصل عرضاً شاملأً للإعدادات الأساسية والمتقدمة التي تم تطبيقها على أجهزة MikroTik في كل من موقعي Site A و Site B، بهدف إنشاء بنية شبكية متراقبة تعتمد على بروتوكولات OSPF و MPLS، مع تطبيق سياسات QoS وإدارة حركة البيانات لضمان جودة الخدمة واستقرار الاتصال بين الموقعين.

1. إعداد واجهات MPLS في كلا الموقعين

تم تفعيل واجهات MPLS المخصصة لنقل البيانات والصوت في كل من Site B و Site A، مع ضبط قيمة mpls-mtu = 1508 لضمان عدم تجزئة الحزم أثناء انتقالها عبر الشبكة.

كما تم تعطيل الواجهة الافتراضية "all" لضمان تخصيص MPLS فقط للواجهات المطلوبة.

2. تفعيل بروتوكول LDP

تم تفعيل بروتوكول Label Distribution Protocol (LDP) في كلا الموقعين، مما يسمح بتبادل العلامات بين أجهزة التوجيه، وبالتالي إنشاء مسارات MPLS ديناميكية وفعالة.

3. توزيع عناوين IP على الواجهات

تم توزيع عناوين IP على الواجهات في كلا الموقعين وفقاً لتقسيم شبكي موحد يشمل:

- شبكة MPLS الخاصة بالصوت (VOIP)

- شبكة MPLS الخاصة بالبيانات (DATA)

- الشبكة المحلية LAN لكل موقع

هذا التقسيم يضمن الفصل بين أنواع الحركة وتحسين الأداء.

4. إعداد بروتوكول OSPF

تم تفعيل OSPF على الواجهات في كلا الموقعين، مع إدراج الشبكات ضمن منطقة backbone، مع تبادل معلومات التوجيه بشكل ديناميكي.

جميع الواجهات تعمل بنمط broadcast، مع قيمة cost = 10 وأولوية 1.

5. إعداد NAT

تم تطبيق قواعد NAT من نوع masquerade في كلا الموقعين على واجهات MPLS، وذلك لإخفاء العناوين الداخلية عند التواصل بين المواقع، مما يعزز الأمان ويضمن توافق الاتصال.

6. تصنیف الحزم باستخدام Mangle

تم استخدام قواعد Mangle في كلا الموقعين لتصنیف الحزم حسب نوع الخدمة:

- تحديد اتصالات VoIP ووضع علامة conn(voip)

- وضع علامة للحزم الصوتية pkt(voip)

- وضع علامة لحزم ICMP

- توجيه الحزم عبر المسارات المناسبة (DATA_PATH و VOIP_PATH)

هذه الخطوة ضرورية لتطبيق سياسات QoS لاحقاً.

7. إدارة عرض النطاق باستخدام Queue Tree

تم إنشاء شجرة انتظار في كلا الموقعين لتوزيع عرض النطاق الترددی:

- مجموعات رئيسية لحركة الصوت والبيانات

- تحديد أولويات عالية لحركة VoIP و ICMP

- تحديد حدود قصوى للسرعات لضمان جودة الخدمة

هذا يضمن عدم تأثر حركة الصوت بحركة البيانات الثقيلة.

8. إعداد قوائم العناوين (Address Lists)

تم إدراج شبكات كل موقع ضمن قوائم عناوين في الموقع الآخر، مثل:

Site B في SITE1 -

(إن وجدت) Site A في SITE2 -

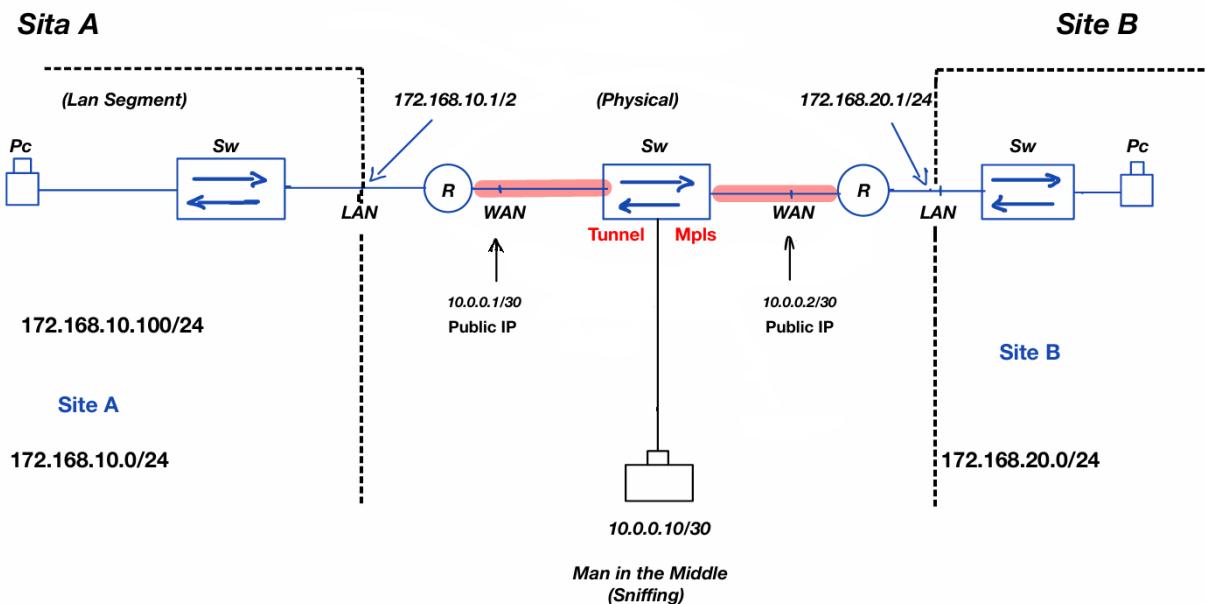
وذلك لتسهيل تطبيق قواعد NAT و Mangle والجدار النارى.

4.1 الفصل الرابع : المقارنات والتحليل

4.1.1 التحليل النتائج المحققة

لقد نجح المشروع في تحقيق الهدف الرئيسي المتمثل في تصميم وتنفيذ شبكة MPLS آمنة وموثوقة تربط موقعين منفصلين باستخدام أجهزة MikroTik CHR في بيئة محاكاة واقعية تم التحقق من صلاحية الشبكة من خلال مجموعة شاملة من الاختبارات تضمنت:

الشكل 4.1 مخطط التدفقي لـ MPLS



اتصال ناجح بين المضيفين في الموقعين عبر أوامر ping.

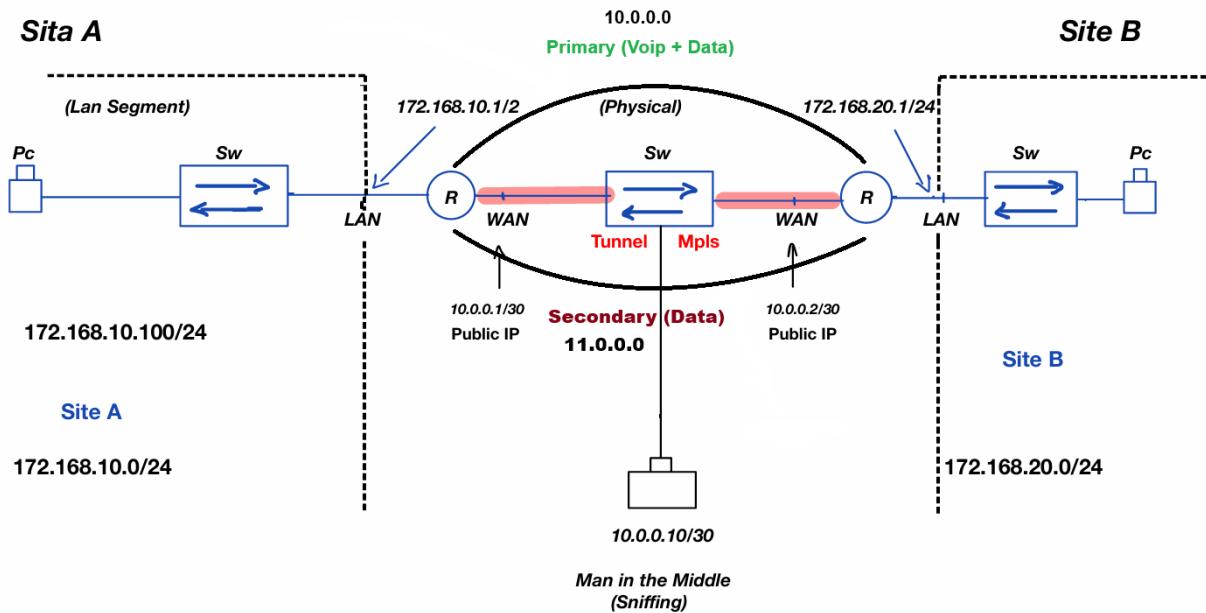
تبادل فعال لعلامات MPLS عبر بروتوكول LDP.

توجيه ديناميكي عبر OSPF مع حالة جوار FULL.

فصل حركة المرور بين خدمات VOIP والبيانات العادية.

تطبيق سياسات أمنية عبر الجدار النارى وقواعد NAT.

الشكل 4.2 تطبيق Traffic Engineer + QOS



4.1.2 التوجهات المستقبلية والمفترضات

بناءً على النجاح المتحقق في هذا المشروع، يمكن التوجه نحو تطويرين رئيسيين لتعزيز قدرات الشبكة:

4.1.3 التطوير الأول: مسارات هجينة ذكية (Hybrid Intelligent Paths)

بدلاً من الاعتماد على مسارين ثابتين (أساسي وبديل)، يمكن تطوير نظام توجيه ذكي يتكيف ديناميكياً مع ظروف الشبكة سيقوم هذا النظام باختيار المسار الأمثل بناءً على نوع حركة المرور (صوت، بيانات، فيديو) وجودة الروابط المتاحة (التأخير، الاهتزاز، فقدان الحزم)، مما يحسن كفاءة استخدام النطاق التردددي ويزيد من موثوقية الخدمة.

4.1.4 التطوير الثاني: نظام اتصال صوتي متكامل (VOIP)

يمكن تطبيق نظام اتصال صوتي عملي يحاكي عمل تطبيقات المراسلة مثل واتساب، حيث يتم إضافة خادم VOIP (مثل Asterisk) في أحد المواقعين وعملاء (Softphones) في الموقع الآخر هذا التطوير سيمكن من إجراء مكالمات صوتية عالية الجودة بين الموقع مع ضمان أولوية حركة الصوت عبر سياسات QoS متقدمة، مما يحول الشبكة من مجرد ناقل بيانات إلى منصة اتصال متكاملة.

4.2 الخلاصة

يمثل هذا المشروع نموذجاً عملياً متكاملاً لبناء شبكة MPLS بين موقعين، حيث نجح في الجمع بين الجوانب النظرية والتطبيقية لتقنيات الشبكات المتقدمة تم تحقيق جميع الأهداف المخطط لها بما في ذلك التوجيه الديناميكي، تبديل العلامات، وإدارة حركة المرور المفترضات المستقبلية المقدمة تفتح آفاقاً لتطوير الشبكة نحو أنظمة أكثر ذكاءً وشمولية، مما يثبت قابلية التوسيع والتحسين المستمر للبنية التحتية الشبكية المطبقة.

Reference :

- [1] E. Rosen et al., "Multiprotocol Label Switching Architecture," IETF RFC 3031, 2001.
- [2] B. Davie and Y. Rekhter, "MPLS: Technology and Applications," Morgan Kaufmann Publishers, 2000.
- [3] L. De Ghein, "MPLS Fundamentals," Cisco Press, 2007.
- [4] A. Farrel et al., "A Path Computation Element (PCE)-Based Architecture," IETF RFC 4655, 2006.
- [5] D. Awduche et al., "Requirements for Traffic Engineering Over MPLS," IETF RFC 2702, 1999.
- [6] J. Moy, "OSPF Version 2," IETF RFC 2328, 1998.
- [7] A. Retana et al., "OSPF Stub Areas and Not-So-Stubby Areas (NSSA)," IETF RFC 3101, 2003.
- [8] T. Szigeti and C. Hattingh, "End-to-End QoS Network Design," Cisco Press, 2004.
- [9] L. Martini et al., "Encapsulation Methods for Transport of Ethernet over MPLS Networks," IETF RFC 4448, 2006.

[10] S. Bryant and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture," IETF RFC 3985, 2005.

[11] S. Khan et al., "Performance Evaluation of MPLS Networks with QoS," International Journal of Computer Networks, 2019.

[12] A. Al-Saadi and H. Al-Raweshidy, "Improving MPLS Traffic Engineering Using OSPF Extensions," Journal of Network Systems, 2020.

[13] E. Mulyana et al., "Implementation of MPLS and OSPF on RouterOS for Site-to-Site Connectivity," International Journal of Advanced Computer Science, 2021.

[14] K. Myers, "MPLS Network Design and Implementation for WISPs," MikroTik MUM Presentation, 2025.

[15] Network Berg, "Configuring MPLS VPN Services on MikroTik RouterOS v7," Class Central, 2025.

[16] L. Andersson, I. Minei, and B. Thomas, *LDP Specification*, IETF RFC 5036, October 2007.