الأكاديمية العربية الدولية
Arab International Academy

شبكات الحاسوب المتقدمة

Advanced Computer Networks

عبدالقادر العبدالله

كلية العلوم – تخصص البرمجة

المحاور

1. **مقدمة إلى شبكات الحاسوب المتقدمة**
   - نظرة عامة على المقرر وأهدافه.
   - منهجية سيسكو في الشبكات المتقدمة ومسارات الشهادات.
2. **بروتوكولات التوجيه المتقدمة**
   - EIGRP، OSPF، BGP.
   - إعادة توزيع المسارات وتقنيات التصفية.
3. **بروتوكول الإنترنت الإصدار السادس (IPv6)**
   - حتمية IPv6 وخصائصه.
   - آليات الانتقال من IPv4 إلى IPv6.
4. **تبديل الملصقات متعدد البروتوكولات (MPLS)**
   - بنية MPLSومكوناتها.
   - تطبيقات MPLSمثل VPN وهندسة حركة المرور.
5. **الشبكات المعرفة بالبرمجيات (SDN) والمحاكاة الافتراضية**
   - مقدمة إلى SDN ومبادئها.
   - Cisco ACI و Cisco DNA.

المخرجات المتوقعة من الدرس

- فهم البروتوكولات المتقدمة مثل EIGRP، OSPF، و BGP وتطبيقاتها في الشبكات المعقدة.
- فهم تصميم وتنفيذ شبكات تعتمد على IPv6 وفهم آليات الانتقال من IPv4.
- فهم تطبيق تقنيات MPLS في إنشاء شبكات VPN وهندسة حركة المرور.
- استيعاب مفاهيم SDN والمحاكاة الافتراضية وتطبيقاتها في الشبكات الحديثة.
- فهم مشكلات الشبكات المتقدمة وحلها باستخدام الأدوات والبروتوكولات المناسبة.

الوحدة الاولى

مقدمة إلى شبكات الحاسوب المتقدمة

نظرة عامة على المقرر وأهدافه

يهدف هذا المقرر إلى توفير فهم عميق للتقنيات المتطورة في مجال شبكات الحاسوب. يركز المحتوى على دراسة البروتوكولات المتقدمة، وتصميم الشبكات، وإدارة الشبكات على مستوى متقدم، وذلك لتمكين المشاركين من تصميم وتنفيذ شبكات حاسوبية قوية وموثوقة. يتناول المقرر التقنيات المتقدمة المستخدمة في شبكات الحاسوب، مع التركيز على تصميم الشبكات وإدارتها باستخدام تقنيات حديثة. يشمل المحتوى دراسة البروتوكولات المتقدمة مثل IPv6 وMPLS ، فضلاً عن تطبيقات الحوسبة السحابية في الشبكات. كما يتم تدريب الطلاب على كيفية التعامل مع قضايا الأمان في الشبكات وحمايتها من الهجمات، بالإضافة إلى التعرف على أساليب تشخيص الشبكات وحل المشكلات المتقدمة.

تتمحور الأهداف الرئيسية لهذا المقرر حول تطوير مهارات المشاركين في عدة مجالات حيوية. تشمل هذه الأهداف فهم بروتوكولات الشبكات المتقدمة مثل IPv6 وMPLS ، وتعلم تصميم وتنفيذ شبكات حاسوبية متقدمة باستخدام التقنيات الحديثة. بالإضافة إلى ذلك، يسعى المقرر إلى إكساب المشاركين المهارات اللازمة لإدارة شبكات الحاسوب بكفاءة وفعالية، ودراسة تقنيات الشبكات المعرفة بالبرمجيات (SDN) وتطبيقاتها. كما يهدف إلى تعريفهم بأساليب حماية الشبكات من الهجمات والتهديدات الأمنية، وتطوير مهارات تشخيص مشكلات الشبكات وحلها بشكل فعال.

منهجية سيسكو في الشبكات المتقدمة ومسارات الشهادات

تعتمد سيسكو منهجية شاملة في تعليم الشبكات المتقدمة، تتدرج من المفاهيم الأساسية إلى المستويات الاحترافية والخبيرة، مما يوفر مسارًا منظمًا لإتقان تقنيات الشبكات. يبدأ هذا المسار ببرنامج Cisco Certified Network Associate (CCNA) ، الذي يغطي أساسيات الشبكات والوصول إليها، واتصالIP ، وخدماتIP ، وأساسيات الأمان، والأتمتة وقابلية البرمجة. يتضمن منهج أكاديمية سيسكو تدريس مهارات تقنية الإنترنت مثل الشبكات، وUNIX، وأساسيات تكنولوجيا المعلومات، والكابلات، وJava، ويُعد الطلاب لشهادات الصناعة مثلCCNA ، وCisco Certified Network Professional (CCNP)، وشهادات أمان الشبكة من سيسكو. يمتد المنهج ليشمل موضوعات واسعة، من أساسيات بناء وصيانة الشبكة إلى مفاهيم تكنولوجيا المعلومات الأكثر تعقيدًا مثل تطبيق أدوات استكشاف الأخطاء وإصلاحها المتقدمة.

تتطور الخبرة مع برنامج Cisco Certified Network Professional (CCNP) ، الذي يركز على مجالات مثل البنية المعمارية، والمحاكاة الافتراضية، والبنية التحتية، وضمان الشبكة، والأمان، والأتمتة. تشمل الموضوعات الرئيسية في CCNP Enterprise مثل امتحان (ENCOR) الشبكات المعرفة بالبرمجيات(SDN) ، والشبكات اللاسلكية، ومختبرات التكوين، وبروتوكولات OSPF و BGP. هذه المستويات تؤكد على أن الشبكات المتقدمة، من منظور سيسكو، لا تقتصر على معرفة المزيد من البروتوكولات فحسب، بل تتعلق بإتقان تطبيق هذه البروتوكولات في سيناريوهات معقدة وواقعية. يبرز هذا التركيز من خلال عناصر "العملي" و"استكشاف الأخطاء وإصلاحها" في الشهادات، مما يشير إلى أن الخبرة المتقدمة تتطلب فهمًا عميقًا لكيفية عمل التقنيات في الممارسة العملية، والقدرة على حل المشكلات المعقدة.

مسارات شهادات سيسكو

يصل المسار إلى ذروته مع شهادة Cisco Certified Internetwork Expert (CCIE) Enterprise Infrastructure ، التي تتناول موضوعات على مستوى الخبراء في تقنيات الطبقة الثانية والثالثة، وخدمات الشبكة، والأمان، والبنية التحتية المعرفة بالبرمجيات، وتقنيات النقل، والأتمتة وقابلية البرمجة. يؤكد هذا التقدم المنظم على أن الخبرة المتقدمة في الشبكات هي عملية تراكمية، حيث تُبنى المهارات العملية والقدرة على حل المشكلات على أساس متين من المعرفة النظرية والتطبيقية. يضمن هذا النهج أن المتخصصين في الشبكات ليسوا مجرد خبراء في البروتوكولات، بل هم مهندسون قادرون على تصميم وتنفيذ وإدارة شبكات قوية وموثوقة تلبي متطلبات الأعمال المتطورة.

مراجعة أساسيات الشبكات (من منظور متقدم)

على الرغم من أن هذا المقرر يركز على المفاهيم المتقدمة، إلا أن مراجعة سريعة للأساسيات من منظور يبرز أهميتها للموضوعات المتقدمة أمر بالغ الأهمية. يتضمن ذلك مكونات الشبكة، وهياكل الطوبولوجيا، والكابلات، ومفاهيم التبديل والتوجيه الأساسية. يُعد الفهم العميق لهذه الأساسيات أمرًا بالغ الأهمية للتصميم المتقدم واستكشاف الأخطاء وإصلاحها. على سبيل المثال، يشمل ذلك فهم دور ووظيفة مكونات الشبكة مثل الموجهات، ومحولات الطبقة الثانية والثالثة، وجدران الحماية من الجيل التالي، وأنظمة منع الاختراق (IPS)، ونقاط الوصول، ووحدات التحكم Cisco DNA Center) و(WLC، ونقاط النهاية، والخوادم، وتقنية الطاقة عبر الإيثرنت (PoE).

تُعد خصائص هياكل طوبولوجيا الشبكة، مثل الطبقتين والثلاث طبقات، وطوبولوجيا Spine-leaf ، وشبكاتWAN ، وشبكات المكاتب الصغيرة/المنازل(SOHO) ، والشبكات المحلية والسحابية، جزءًا لا يتجزأ من التصميم المتقدم. كما أن فهم الأنواع المادية للواجهات والكابلات، مثل الألياف أحادية الوضع، والألياف متعددة الوضع، والنحاس، ووصلات الإيثرنت المشتركة ونقطة إلى نقطة، أمر ضروري. يمكن أن يؤدي تحديد مشكلات الواجهة والكابلات، مثل الاصطدامات والأخطاء وعدم تطابق الازدواج و/أو السرعة، إلى مشاكل أداء كبيرة. بالإضافة إلى ذلك، فإن مقارنة بروتوكولي TCP وUDP، وفهم مفاهيم التبديل مثل تعلم MAC وتقادمه، وتبديل الإطارات، وفيضان الإطارات، وجدول عناوينMAC ، يشكل أساسًا لا غنى عنه. إن الفهم الدقيق لهذه الأساسيات، بما في ذلك سبب سلوكها بهذه الطريقة وحدودها وكيف تتفاعل في سيناريوهات معقدة، أمر بالغ الأهمية للتصميم المتقدم واستكشاف الأخطاء وإصلاحها بفعالية. على سبيل المثال، فهم قيود تعلم MAC أمر حيوي لتصميم هياكل الشبكة الكبيرة.

نموذج تصميم الشبكة الهرمي

يُعد نموذج سيسكو لتصميم الشبكات الهرمي مبدأ تصميم أساسيًا لبناء شبكات قابلة للتوسع، ومرنة، وقابلة للإدارة. يقسم هذا النموذج الشبكة منطقيًا إلى طبقات مميزة، لكل منها وظائف محددة. يتكون النموذج التقليدي من ثلاث طبقات: طبقة الوصول، وطبقة التوزيع، وطبقة النواة.

- **طبقة الوصول (Access Layer):** تُعد هذه الطبقة نقطة اتصال المستخدمين النهائيين والخوادم بالشبكة. ينصب التركيز الأساسي في هذه الطبقة على تقليل "التكلفة لكل منفذ". تشمل وظائفها توفير اتصال تبديل من الطبقة الثانية، وضمان أمان المنافذ، وتوفير الطاقة عبر الإيثرنت (PoE) للأجهزة المتصلة، وتطبيق علامات جودة الخدمة(QoS) ، والتعامل مع دخول حركة المرور الأولية.
- **طبقة التوزيع (Distribution Layer):** تُعرف هذه الطبقة بالطبقة "الذكية" في النموذج ثلاثي الطبقات. تقع بين طبقتي الوصول والنواة، والغرض منها هو تحديد حدود الشبكة من خلال تطبيق قوائم الوصول (ACLs) والمرشحات الأخرى، وبالتالي تحديد سياسة الشبكة. تضمن طبقة التوزيع توجيه الحزم بشكل صحيح بين الشبكات الفرعية وشبكات VLAN داخل المؤسسة. غالبًا ما تدير أجهزة طبقة التوزيع اتصالات WAN للمكاتب الفرعية الفردية.
- **طبقة النواة (Core Layer):** تُعد طبقة النواة العمود الفقري للشبكة، حيث تقع بوابات الإنترنت (الشبكة البينية). توفر هذه الطبقة خدمات إعادة توجيه عالية السرعة وذات توفر عالٍ لنقل الحزم بين أجهزة طبقة التوزيع في مناطق مختلفة من الشبكة. تتكون أجهزة طبقة النواة عادةً من أكبر وأسرع وأقوى الموجهات والمحولات، وتدير اتصالات بأعلى سرعة مثل 10 جيجابت إيثرنت أو 100 جيجابت إيثرنت.

فوائد النموذج الهرمي وتصميم النواة المدمجة

تتعدد فوائد نموذج سيسكو الهرمي ثلاثي الطبقات، حيث يساعد في تصميم ونشر وصيانة شبكة إنترنت هرمية قابلة للتوسع وموثوقة وفعالة من حيث التكلفة. تشمل هذه الفوائد أداءً أفضل للشبكة، وإدارة واستكشاف أخطاء أفضل، وتطبيقًا أفضل للسياسات والمرشحات، وقابلية توسع محسّنة لاستيعاب النمو المستقبلي، وتوفرًا أعلى من خلال روابط متعددة عبر أجهزة متعددة.

بالإضافة إلى النموذج ثلاثي الطبقات، يوجد تباين شائع يُعرف بتصميم "النواة المدمجة(Collapsed Core Design) "، حيث تُدمج وظائف طبقتي التوزيع والنواة في طبقة واحدة من المحولات. يُعد هذا الهيكل ثنائي الطبقات مناسبًا للحرم الجامعي الأصغر (على سبيل المثال، الذي يخدم أقل من 1000-1500 مستخدم) أو البيئات التي لا يُتوقع فيها نمو كبير في المستقبل. على الرغم من الدمج، تظل المبادئ الأساسية لطبقة النواة - السرعة العالية، والموثوقية، والتوفر - حاسمة في تصميم النواة المدمجة. يجب أن توفر المحولات التي تؤدي الأدوار المدمجة اتصالًا قويًا وعالي السرعة بين كتل الوصول والتوزيع المختلفة التي تخدمها، مع توفير التكرار بين هذه المحولات المدمجة غالبًا من خلال تقنيات الشبكات الكاملة أو التراص/التجميع عالي التوفر. يؤكد هذا النموذج أن تصميم الشبكة ليس مجرد مخطط ثابت، بل هو قرار استراتيجي يؤثر على مرونة المنظمة وقدرتها على التكيف مع المتطلبات المستقبلية. إن فهم سبب هذا النموذج الهرمي – قدرته على عزل الأعطال، وتبسيط الإدارة، وتسهيل النمو – أمر أساسي لمتخصصي الشبكات المتقدمين، مما يمكنهم من اختيار وتكييف البنية المناسبة لمتطلبات العمل المحددة.

فوائد النموذج الهرمي وتصميم النواة المدمجة

اسم الطبقة	الوظائف الأساسية	الخصائص الرئيسية	الأجهزة النموذجية
الوصول(Access)	اتصال المستخدمين النهائيين والأجهزة، أمان المنافذ، PoE، تحديدQoS ، دخول حركة المرور الأولية.	تكلفة منخفضة لكل منفذ، اتصال تبديل من الطبقة الثانية.	محولات الوصول، نقاط الوصول اللاسلكية.
التوزيع(Distribution)	تحديد سياسة الشبكة، التوجيه بين الشبكات الفرعية وشبكاتVLAN ، التصفية، QoS، إدارة اتصالات WAN.	الطبقة "الذكية"، توجيه الطبقة الثالثة، تجميع طبقة الوصول.	محولات الطبقة الثالثة المتطورة.
النواة(Core)	إعادة توجيه الحزم عالية السرعة، توفير عالٍ، العمود الفقري للشبكة، دمج الشبكات المتباعدة جغرافيًا.	أسرع وأكبر الموجهات/المحولات، اتصالات عالية السرعة(10G ، 100G).	موجهات ومحولات عالية الأداء) مثل Cisco Catalyst 9000).

فوائد النموذج الهرمي وتصميم النواة المدمجة

تتعدد فوائد نموذج سيسكو الهرمي ثلاثي الطبقات، حيث يساعد في تصميم ونشر وصيانة شبكة إنترنت هرمية قابلة للتوسع وموثوقة وفعالة من حيث التكلفة. تشمل هذه الفوائد أداءً أفضل للشبكة، وإدارة واستكشاف أخطاء أفضل، وتطبيقًا أفضل للسياسات والمرشحات، وقابلية توسع محسّنة لاستيعاب النمو المستقبلي، وتوفرًا أعلى من خلال روابط متعددة عبر أجهزة متعددة.

بالإضافة إلى النموذج ثلاثي الطبقات، يوجد تباين شائع يُعرف بتصميم "النواة المدمجة(Collapsed Core Design) "، حيث تُدمج وظائف طبقتي التوزيع والنواة في طبقة واحدة من المحولات. يُعد هذا الهيكل ثنائي الطبقات مناسبًا للحرم الجامعي الأصغر (على سبيل المثال، الذي يخدم أقل من 1000-1500 مستخدم) أو البيئات التي لا يُتوقع فيها نمو كبير في المستقبل. على الرغم من الدمج، تظل المبادئ الأساسية لطبقة النواة - السرعة العالية، والموثوقية، والتوفر - حاسمة في تصميم النواة المدمجة. يجب أن توفر المحولات التي تؤدي الأدوار المدمجة اتصالًا قويًا وعالي السرعة بين كتل الوصول والتوزيع المختلفة التي تخدمها، مع توفير التكرار بين هذه المحولات المدمجة غالبًا من خلال تقنيات الشبكات الكاملة أو التراص/التجميع عالي التوفر. يؤكد هذا النموذج أن تصميم الشبكة ليس مجرد مخطط ثابت، بل هو قرار استراتيجي يؤثر على مرونة المنظمة وقدرتها على التكيف مع المتطلبات المستقبلية. إن فهم سبب هذا النموذج الهرمي – قدرته على عزل الأعطال، وتبسيط الإدارة، وتسهيل النمو – أمر أساسي لمتخصصي الشبكات المتقدمين، مما يمكنهم من اختيار وتكييف البنية المناسبة لمتطلبات العمل المحددة.

Q1

ما هو الهدف الرئيسي من دراسة بروتوكولات الشبكات المتقدمة؟

أ) تحسين سرعة الإنترنت المنزلي

ب) تصميم شبكات قوية ومؤثوقة

ج) تقليل تكلفة الأجهزة

ما هي الشهادة التي تقدمها سيسكو للمبتدئين في مجال الشبكات؟

أ) CCIE

ب) CCNA

ج) CCNP

صح أم خطأ: يركز نموذج سيسكو الهرمي على تقسيم الشبكة إلى طبقتين فقط.

الاجوبة

ما هو الهدف الرئيسي من دراسة بروتوكولات الشبكات المتقدمة؟

أ) تحسين سرعة الإنترنت المنزلي

ب) تصميم شبكات قوية ومؤثوقة

ج) تقليل تكلفة الأجهزة

ما هي الشهادة التي تقدمها سيسكو للمبتدئين في مجال الشبكات؟

أ) CCIE

ب) CCNA

ج) CCNP

صح أم خطأ: يركز نموذج سيسكو الهرمي على تقسيم الشبكة إلى طبقتين فقط. × يقسم الشبكة الى 3 طبقات

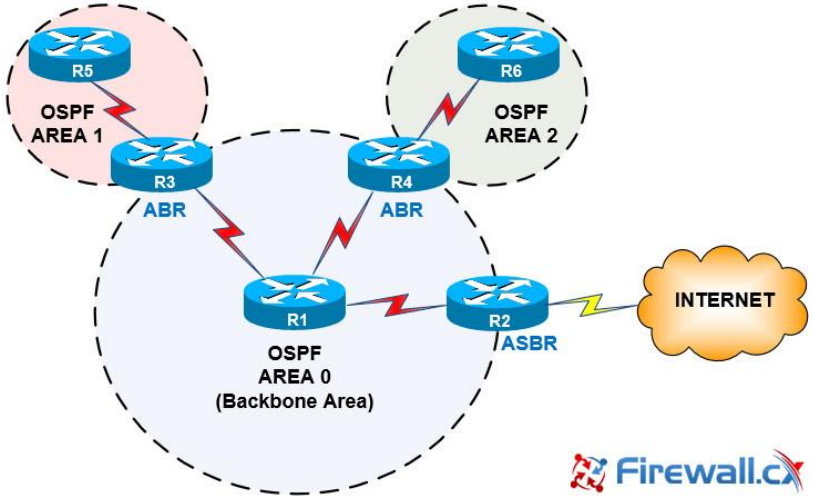
الوحدة الثانية

بروتوكولات التوجيه المتقدمة

مقدمة إلى التوجيه المتقدم

تُعد بروتوكولات التوجيه المتقدمة حجر الزاوية في تصميم وتشغيل الشبكات الحديثة، سواء كانت شبكات مؤسسات كبيرة أو شبكات مزودي الخدمة. تتجاوز هذه البروتوكولات التوجيه الأساسي لتمكين قابلية التوسع، والكفاءة، والمرونة، والتحكم الدقيق في تدفق حركة المرور.

تركز هذه الوحدة على بروتوكولات البوابة الداخلية المتقدمة (IGPs) مثل EIGRP وOSPF، وبروتوكول البوابة الخارجية(BGP) ، بالإضافة إلى تقنيات معالجة التوجيه والتكرار التي لا غنى عنها في البيئات الشبكية المعقدة.



بروتوكول التوجيه الداخلي المحسّن (EIGRP) – مفاهيم متقدمة

يُعد EIGRP (Enhanced Interior Gateway Routing Protocol) بروتوكول توجيه خاص بسيسكو، يوفر تقاربًا سريعًا واستخدامًا فعالًا لعرض النطاق الترددي، مما يجعله خيارًا شائعًا في بيئات المؤسسات. تتجاوز المفاهيم المتقدمة لـ EIGRP مجرد التكوين الأساسي لتشمل تفاصيل عملياته، واختيار المسار، وتقنيات التحسين التي تضمن الأداء الأمثل للشبكة.

فيما يتعلق بـ العلاقات المجاورة (Adjacencies)، يعتمد EIGRP على تبادل حزم EIGRP لإنشاء جداول الجيران والطوبولوجيا. يتضمن ذلك تكوينات EIGRP الأساسية، وتحديد الجيران الثابتين، وواجهات الوضع السلبي (Passive Interface) للتحكم في تبادل التحديثات، وتقنيات التلخيص (Summarization) لتقليل حجم جداول التوجيه. أما بالنسبة لـ اختيار أفضل مسار(Best Path Selection)، فيستخدم EIGRP مقاييس واسعة (Wide Metrics) لتحديد المسار الأمثل، مما يوفر مرونة أكبر في اختيار المسارات مقارنة بالبروتوكولات التقليدية.

بروتوكول التوجيه الداخلي المحسّن (EIGRP) – العمليات والتحسين

تتضمن **العمليات العامة (General Operations)** لـ EIGRP فهم آلة الحالة المحدودة (Finite State Machine - FSM) التي تحكم سلوكه، وأوقات الانتظار (Hold Time) وحزم Hello للحفاظ على العلاقات المجاورة، وقيم (K values) K التي تحدد كيفية حساب المقياس، بالإضافة إلى آليات مثل (SIA) "Stuck in Active" التي تشير إلى مشاكل في التقارب، و "Graceful Shutdown" لإغلاق EIGRP بشكل منظم. تُعد هذه التفاصيل حاسمة لاستكشاف الأخطاء وإصلاحها وضمان استقرار الشبكة.

في سياق **موازنة التحميل(Load Balancing)** ، يدعم EIGRP موازنة التحميل غير المتساوية التكلفة (Unequal Cost Load Balancing)باستخدام ميزةVariance ، مما يسمح بتوزيع حركة المرور عبر مسارات متعددة ذات تكاليف مختلفة، مما يزيد من استخدام عرض النطاق الترددي المتاح. كما يدعم EIGRP Named Mode لتبسيط التكوين في الشبكات الكبيرة.

بالنسبة لـ **التحسين والتقارب وقابلية التوسع(Optimization, Convergence, and Scalability)** ، يوفر EIGRP ميزات متقدمة مثل Stub EIGRP للتحكم في انتشار معلومات التوجيه، و "Loop Free Alternate (LFA) Fast Reroute (FRR)"لتوفير مسارات بديلة خالية من الحلقات لتقارب سريع في حالة الفشل. كما تتضمن تقنيات مثل "Leak-Map Summary" و "EIGRP Stub Leak-map"تحكمًا دقيقًا في تصفية المسارات. يضمن هذا التركيز على التحسين والتقارب وقابلية التوسع أن EIGRP يمكنه التكيف بسرعة مع التغيرات في الطوبولوجيا وتوفير موازنة تحميل مرنة، مما يجعله مناسبًا لبيئات المؤسسات المعقدة التي تتطلب استعادة سريعة للخدمة واستخدامًا فعالًا للموارد.

تُعد **المصادقة (Authentication)** جانبًا أمنيًا مهمًا فيEIGRP ، حيث يدعم EIGRP Authentication و SHA Authentication لضمان أن تحديثات التوجيه تأتي من مصادر موثوقة. هذه الميزات ضرورية لحماية بروتوكول التوجيه من الهجمات الخبيثة.

بروتوكول فتح أقصر مسار أولاً (OSPF) – المناطق المتعددة والتحسين

يُعد OSPF (Open Shortest Path First) بروتوكول توجيه من نوع Link-State ، وهو أساسي للشبكات الكبيرة والقابلة للتوسع. تتضمن النشر المتقدم لـ OSPF تصميمات متعددة المناطق وتقنيات تحسين متنوعة لضمان الكفاءة والاستقرار.

فيما يتعلق بـ **العلاقات المجاورة(Adjacencies)** ، يشمل OSPF التكوين الأساسي ومتعدد المناطق، بالإضافة إلى استكشاف أخطاء العلاقات المجاورة بين الجيران. أما بالنسبة لـ **أنواع الشبكات والمناطق(Network and Area Types)** ، فيقدم OSPF فهمًا عميقًا لأنواع
LSA (Link-State Advertisement) المختلفة، وأنواع الشبكات مثلNon-Broadcast ، وBroadcast، وPoint-to-Point، وPoint-to-Multipoint، وPoint-to-Multipoint Non-Broadcast. تُعد هذه الأنواع حاسمة لتصميم الشبكات المعقدة وتكييف OSPFمع بيئات مختلفة.

تتضمن **تفضيل المسار (Path Preference)** في OSPF تلخيص OSPF واختيار المسار الأمثل. أما **العمليات (Operations)** فتشمل تحديد عرض النطاق الترددي المرجعي، وفيضان LSA وLSDB (Link-State Database)، وفترات Hello وDead، ومعرف الموجه(Router ID) ، وانتخاب(DR/BDR (Designated Router/Backup Designated Router ، وواجهة الوضع السلبي (Passive Interface)، والإغلاق المنظم(Graceful Shutdown) ، وآلية أمان TTL العامة (Generic TTL Security Mechanism - GTSM).

بروتوكول فتح أقصر مسار أولاً (OSPF) – التحسين والأمان

في سياق **التحسين والتقارب وقابلية التوسع(Optimization, Convergence, and Scalability)** ، يوفر OSPF ميزات مثل LSA Throttlingلتقليل تكرار تحديثاتLSA ، وضبط جدولة SPF (SPF Scheduling Tuning) لتحسين أداء حسابات أقصر مسار. كما يدعم OSPF مناطق Stub (Stub, Totally Stub, NSSA, Totally NSSA) للتحكم في انتشار معلومات التوجيه وتقليل حجم جداول التوجيه. تُعد ميزات مثل Loop Free Alternate (LFA) Fast Reroute (FRR) و Remote LFA FRRحاسمة للتقارب السريع في حالة الفشل، بينما يساعد Prefix Suppression في تقليل عدد البادئات المعلن عنها.

تُعد **المصادقة (Authentication)** جزءًا لا يتجزأ من أمانOSPF ، حيث يدعمOSPF Plain-text Authentication ، و MD5 Authentication، وHMAC-SHA Extended Authentication، بالإضافة إلى مصادقة وتشفير .OSPFv3 يضمن هذا أن تحديثات التوجيه موثوقة ومحمية. إن قوة OSPF في الشبكات الكبيرة تنبع من تصميمه متعدد المناطق، الذي يحد من نطاق قواعد بيانات Link-State وحسابات SPF ، مما يحسن من قابلية التوسع والاستقرار. تسمح القدرة على تقسيم مجال OSPF إلى أنواع مناطق مختلفة مثل Stub و NSSA لمهندسي الشبكات بالتحكم في تدفق معلومات التوجيه، وتقليل استهلاك الموارد على الموجهات، وتعزيز استقرار الشبكة، مما يبرز دور OSPF في بناء شبكات مؤسسية مرنة وفعالة على نطاق واسع.

بروتوكول البوابة الحدودية (BGP) – الأساسيات والسياسات المتقدمة

يُعد BGP (Border Gateway Protocol) بروتوكول التوجيه الأساسي للإنترنت، ويُستخدم للتوجيه بين الأنظمة المستقلة (Autonomous Systems).
يتضمن الفهم المتقدم لـ BGP علاقات النظراء، وسمات اختيار المسار، والسياسات التوجيهية المعقدة التي تتيح التحكم الدقيق في تدفق حركة المرور على مستوى الإنترنت.

فيما يتعلق بـ **علاقات النظراء IBGP وEBGP (IBGP and EBGP Peer Relationships)**، يتناول BGP مقدمة عن البروتوكول، وحالات تجاور الجيران، والفرق بين الوضع النشط والسلبي، وأنواع رسائلBGP ، ومجموعات النظراء(Peer Groups) ، واستخدام أرقام الأنظمة المستقلة ذات 4 بايت، ونطاقات الأنظمة المستقلة الخاصة والعامة.
تُعد **سمات اختيار المسار (Path Selection Attributes)** في BGP حاسمة للتحكم في كيفية اختيار المسارات وتفضيلها. تشمل هذه السماتWeight :، وLocal Preference، وLocally Originated، وAS Path Prepending، وOrigin Code، و MED (Metric).كما يتضمن ذلك تفضيل eBGP علىiBGP ، وموازنة التحميل متعددة المسارات (Multipath Load Sharing) لكل من IBGPوEBGP، والمسارات الإضافية، وسمة مقياس IGP التراكمي.(AIGP)

بروتوكول البوابة الحدودية (BGP) – السياسات والتحسين والأمان

في سياق **السياسات التوجيهية(Routing Policies)** ، يُعد BGP أداة قوية لتطبيق سياسات معقدة. يتضمن ذلك استكشاف أخطاء إعلان مساراتBGP ، ومجتمعات (BGP Communities) BGP مثلNo-Advertise ، وNo-Export، وLocal AS، وتصميمات الشبكات أحادية/ثنائية الربط ومتعددة الربط. أما **معالجات AS Path (AS Path Manipulations)** فتشمل MPLS L3 VPN BGP Allow AS in،
وBGP Remove Private AS، والتعبيرات المنتظمة لـ (BGP Regular Expressions) BGP للتحكم الدقيق في المسارات.

لتحسين **التقارب وقابلية التوسع(Convergence and Scalability)** ، يستخدم BGP مفاهيم مثل BGP Route Reflector لتقليل عدد اتصالات BGP في الشبكات الكبيرة، و BGP Aggregate AS-Set لتلخيص المسارات. تشمل **ميزات BGP الأخرى** BGP Soft Reset Reconfigurationو BGP Route Refresh Capability لتحديث جداول التوجيه دون إعادة تعيين الجلسات

بروتوكول البوابة الحدودية (BGP) – السياسات والتحسين والأمان

يُعد **الأمان (Security)** جانبًا حيويًا فيBGP ، حيث يتضمن مصادقة موجه الجوار BGP (BGP Neighbor Router Authentication)، ودعم BGP لـTTL Security Check ، وتصفية المسارات الصادرة المستندة إلى البادئة-BGP Prefix) Based Outbound Route Filtering).على عكس بروتوكولات IGP التي تركز على إيجاد أفضل مسار داخل نظام مستقل، فإن مجموعة سمات المسار وقيم المجتمع الواسعة في BGP تتيح تحكمًا دقيقًا في إعلان المسارات واختيارها.

هذا يشير إلى دور BGP كمحرك لتطبيق السياسات، وليس مجرد بروتوكول توجيه، مما يجعله الأداة الأساسية لمهندسي الشبكات المتقدمين لتنفيذ سياسات توجيه معقدة وهندسة حركة المرور والاتصال بين المنظمات، وهو أمر بالغ الأهمية لمزودي الخدمة والمؤسسات الكبيرة ذات الاتصالات المتعددة المتطلبات.

إعادة توزيع المسارات وتقنيات التصفية

في الشبكات المعقدة، غالبًا ما تتعايش بروتوكولات توجيه مختلفة، مما يتطلب آليات لتبادل معلومات التوجيه بينها. تسمح إعادة التوزيع (Redistribution)بإعلان المسارات التي تعلمها بروتوكول واحد في بروتوكول آخر، بينما تضمن التصفية (Filtering) التحكم الدقيق في المسارات المعلن عنها والمستقبلة.

تُعد **إعادة التوزيع (Redistribution)** عملية حاسمة لتمكين التشغيل البيني بين مجالات التوجيه المختلفة. تشمل هذه العملية مقدمة عن إعادة التوزيع، وكيفية إجرائها بين EIGRP وOSPF، بالإضافة إلى استكشاف أخطاء إعادة توزيع المقاييس (Metric Redistribution)والمسافة الإدارية .(AD Redistribution) كما تتناول إعادة توزيعIPv6 ، مما يضمن التوافق في البيئات المختلطة.

للحفاظ على التحكم في تدفق معلومات التوجيه، تُستخدم **تقنيات تصفية المسارات .(Route Filtering Techniques)** تشمل هذه التقنيات:

- **Distribute-list**: تُستخدم لتصفية المسارات بناءً على قوائم الوصول.(Access Lists)
- **Prefix-list**: توفر طريقة أكثر مرونة وقوة لتصفية المسارات بناءً على بادئات.IP
- **Route-map filtering**: تُعد الأداة الأكثر شمولاً ومرونة، حيث تسمح بتطبيق قواعد متعددة ومجموعات شروط لتصفية وتعديل سمات المسارات.

إعادة توزيع المسارات وتقنيات التصفية

تُطبق هذه التقنيات عبر بروتوكولات التوجيه المختلفة. على سبيل المثال، في OSPF ، يمكن استخدام Distribute-list Filtering ، وتصفية LSA Type 3 لـ ABR (Area Border Router) ، وتصفية LSA Type 5. أما في BGP ، فتُستخدم BGP Extended Access-list Filtering و BGP IPv6 Route Filtering للتحكم في المسارات. بالإضافة إلى ذلك، تُعد **التلخيص اليدوي (Manual Summarization)**، مثل تلخيص IPv6 ، أداة مهمة لتقليل حجم جداول التوجيه وتحسين قابلية التوسع.

تُعد إعادة التوزيع ضرورية للتشغيل البيني بين مجالات التوجيه المختلفة، ولكنها تُدخل تعقيدًا كبيرًا واحتمال حدوث حلقات توجيه أو مسارات غير مثالية. يؤكد التركيز على التصفية (قوائم التوزيع، قوائم البادئات، خرائط المسارات) واستكشاف الأخطاء وإصلاحها أن التحكم الدقيق والتحقق أمران بالغا الأهمية.

يتطلب تصميم الشبكات المتقدمة ليس فقط معرفة كيفية إعادة التوزيع، بل متى وكيفية تطبيق التصفية الصارمة والتلخيص للحفاظ على التحكم، ومنع الثقوب السوداء في التوجيه، وضمان تدفق حركة المرور الأمثل عبر مجالات التوجيه المتباينة، خاصة في بيئات متعددة البائعين أو متعددة البروتوكولات.

بروتوكولات التكرار للقفزة الأولى FHRPs

تُعد بروتوكولات التكرار للقفزة الأولى (FHRPs) ضرورية لضمان استمرارية الوصول إلى الشبكة للأجهزة النهائية، حتى في حالة فشل الموجه الأساسي. توفر هذه البروتوكولات بوابة احتياطية، مما يمنع نقطة فشل واحدة في طبقة الوصول.
تشمل **مقدمة إلى تكرار البوابة (Introduction to Gateway Redundancy)** الغرض من FHRPs وكيفية حلها لمشكلة نقطة الفشل الواحدة في البوابة الافتراضية. تُعد سيسكو رائدة في هذا المجال من خلال بروتوكولاتها الخاصة والمعايير المفتوحة:

- **Hot Standby Routing Protocol (HSRP)**: بروتوكول خاص بسيسكو، يوفر تكرارًا للبوابة الافتراضية عن طريق تعيين موجه نشط وموجه احتياطي.
- **Virtual Router Redundancy Protocol (VRRP)**: بروتوكول مفتوح المعيار، يؤدي وظيفة مماثلة لـHSRP ، مما يتيح التوافق بين أجهزة البائعين المختلفين.
- **Gateway Load Balancing Protocol (GLBP)**: بروتوكول خاص بسيسكو يوفر تكرار البوابة مع موازنة التحميل، مما يسمح باستخدام جميع الموجهات في مجموعة FHRP بشكل نشط.

بروتوكولات التكرار للقفزة الأولى FHRPs

بالنسبة لـ **تفضيل إعلان موجه(IPv6 Router Advertisement Preference) IPv6** ، يحتوي IPv6 على آليات FHRP مدمجة مثل
Neighbor Unreachability Detection (NUD) ، ويمكن أيضًا استخدام بروتوكولات FHRP التقليدية مثل HSRP و GLBP و VRRP في بيئات
IPv6.
بينما تضمن بروتوكولات التوجيه اكتشاف المسار عبر الشبكة، فإن FHRPs تعالج مشكلة "الميل الأخير" الحاسمة مثل ضمان أن الأجهزة النهائية لديها دائمًا بوابة نشطة.

يشير وجود FHRPs متعددة بقدرات مختلفة مثل موازنة التحميل في GLBP إلى أنه يجب على المهندسين المعماريين اختيار الحل المناسب بناءً على متطلبات التوفر والأداء المحددة.
تُعد FHRPs ضرورية لتحقيق توفر عالٍ في طبقة الوصول، ومنع نقاط الفشل الفردية لاتصال المستخدم النهائي. إن تنفيذها الصحيح أمر بالغ الأهمية لاستمرارية الأعمال وضمان تجربة مستخدم سلسة، خاصة للتطبيقات الحيوية.

توجيه البث المتعدد عبر بروتوكول الإنترنت ((IP Multicast Routing

يُمكن توجيه البث المتعدد عبر بروتوكول الإنترنت (IP Multicast) من الاتصال الفعال من نقطة إلى عدة نقاط، وهو أمر حيوي لتطبيقات مثل مؤتمرات الفيديو، وتلفزيون بروتوكول الإنترنت(IPTV) ، وتوزيع البيانات في الوقت الفعلي.
تتضمن **مقدمة إلى البث المتعدد (Introduction to Multicast)** المفاهيم الأساسية لكيفية عمل البث المتعدد، حيث يتم إرسال حزمة واحدة إلى مجموعة من المستلمين بدلاً من إرسال نسخ متعددة لكل مستلم على حدة.
في **البث المتعدد للطبقة الثانية(Layer 2 Multicast)** ، تُستخدم بروتوكولات مثل IGMP (Internet Group Management Protocol)بإصداريه الثاني والثالث (v2, v3) لإدارة عضويات المجموعات على الشبكات المحلية.

تُعد ميزات مثل IGMP Snooping و IGMP Querierضرورية لتمكين المحولات من توجيه حركة مرور البث المتعدد فقط إلى المنافذ التي تحتوي على مستمعين، مما يوفر عرض النطاق الترددي. كما تُستخدم Multicast PIM Snooping و IGMP Filter و Embedded RP IPv6 Multicast لإدارة حركة مرور البث المتعدد بشكل فعال.

توجيه البث المتعدد عبر بروتوكول الإنترنت IP Multicast Routing – PIM وأنماطه

يُعد **توجيه المسار العكسي (Reverse Path Forwarding - RPF)** آلية أمان وتوجيه أساسية في البث المتعدد، حيث تضمن أن حزم البث المتعدد تصل من مصدر موثوق به عبر أقصر مسار عكسي إلى المصدر. أما **PIM (Protocol Independent Multicast)**، فهو بروتوكول توجيه البث المتعدد الذي يعمل بشكل مستقل عن بروتوكول التوجيه الأساسي) مثل OSPF أو EIGRP). تتعدد أنماط PIMلتناسب سيناريوهات الشبكة المختلفة:

- **PIM Dense-Mode**:يستخدم نموذج الفيضان والقطع.(Flood-and-Prune)
- **PIM Sparse Mode**:يعتمد على نقطة الالتقاء (Rendezvous Point - RP) لتوجيه حركة المرور.
- **PIM Sparse-Dense Mode**:يجمع بين خصائص النمطين الكثيف والخفيف.
- **PIM Auto RP** و **PIM Bootstrap (BSR)** و **PIM Accept RP** : آليات لاكتشاف وتوزيع معلومات نقطة الالتقاء.
- **IPv6 PIM MLD** :دعم PIM لـ IPv6 باستخدام.Multicast Listener Discovery
- **Bidirectional PIM**و **Source Specific Multicast (SSM)**و **Boundary Filtering**و **Anycast RP** :ميزات متقدمة توفر مرونة وتحكمًا إضافيًا في توجيه البث المتعدد.

توجيه البث المتعدد عبر بروتوكول الإنترنت IP Multicast Routing – PIM وأنماطه

تنشأ الحاجة إلى البث المتعدد من التطبيقات التي تستهلك عرض نطاق ترددي مكثف مثل الفيديو. يتيح البث المتعدد تسليم البيانات بكفاءة إلى مستلمين متعددين دون تكرار حركة المرور على قطاعات الشبكة، وبالتالي تحسين موارد الشبكة. تشير أوضاع PIM المختلفة إلى الحاجة إلى تصميم دقيق. إن تنفيذ IP Multicast بفعالية يُعد مهارة متقدمة تُحسن بشكل كبير من كفاءة الشبكة لتطبيقات معينة. يتطلب فهمًا عميقًا لـRPF ، وأنماطPIM ، و IGMPلضمان تسليم حركة المرور بشكل صحيح وتجنب ازدحام الشبكة، خاصة في بيئات توزيع الفيديو واسعة النطاق أو البيانات في الوقت الفعلي.

Q2

أي من البروتوكولات التالية يستخدم للاتصال بين الأنظمة المستقلة (?AS)
أ) OSPF
ب) BGP
ج) EIGRP

ما هي الوظيفة الرئيسية لبروتوكول HSRP؟
أ) موازنة التحميل
ب) توفير بوابة افتراضية احتياطية
ج) تصفية المسارات

صح أم خطأ: يمكن استخدام OSPF في شبكات WAN فقط.

الاجوبة

أي من البروتوكولات التالية يستخدم للاتصال بين الأنظمة المستقلة (?AS)
أ) OSPF
ب) BGP
ج) EIGRP

ما هي الوظيفة الرئيسية لبروتوكول HSRP؟
أ) موازنة التحميل
ب) توفير بوابة افتراضية احتياطية
ج) تصفية المسارات

صح أم خطأ: يمكن استخدام OSPF في شبكات WAN فقط. × يمكن استخدامه في LAN و WAN

الوحدة الثالثة

بروتوكول الإنترنت الإصدار 6 (IPv6)

حتمية IPv6

لم يعد IPv6 مجرد تقنية مستقبلية، بل أصبح انتقالًا ضروريًا للإنترنت لمعالجة القيود المتزايدة لـIPv4 ، خاصة مع استنفاد مساحات العناوين المتاحة. لقد حان الوقت أخيرًا لـ IPv6 بعد 24 عامًا من ظهوره، مما يؤكد على الطبيعة المتأصلة للشبكات التي تجعل كل شيء يعمل معًا، في أي مكان، وفي أي وقت.

تؤكد الولايات المتحدة على هذه الحتمية من خلال **التفويضات الحكومية**، حيث تهدف الحكومة الفيدرالية الأمريكية إلى تقديم خدماتها، وتشغيل شبكاتها، والوصول إلى خدمات الآخرين باستخدام IPv6 فقط. يُعتبر نهج "Dual Stack" الذي يشغل IPv4 و IPv6معًا" معقدًا للغاية للصيانة وغير ضروري" على المدى الطويل، مما يشير إلى توجه نحو بيئات IPv6-Only. وقد وضعت الحكومة **بوابات نشر** محددة، تستهدف 20% من الأصول التي تدعم IP بحلول نهاية السنة المالية 2023، و50% بحلول نهاية السنة المالية 2024، و80% بحلول نهاية السنة المالية 2025. تتضمن هذه الأهداف أيضًا تحديد وتبرير الأنظمة النهائية التي لا يمكن تحويلها والتخطيط لاستبدالها.

حتمية – IPv6 مساحة العناوين وتأثيرها

السبب الجذري لهذه الحتمية يكمن في **مساحة العناوين الهائلة** التي يوفرها IPv6. بينما يبلغ إجمالي عدد عناوين IPv4 حوالي 4.3 مليار، يوفر IPv6 مساحة عناوين ضخمة تصل إلى حوالي 3.4 × 10^38 عنوانًا. هذه المساحة الشاسعة تتيح نماذج تصميم جديدة تمامًا، مثل تخصيص بادئة /64 (التي تحتوي على 18.4 كوينتليون عنوان) لكل مقطع شبكة محلية (LAN). إن هذا التحول الجذري من ندرة العناوين في IPv4 إلى وفرتها في IPv6 يعني أن المهندسين يجب أن يتخلوا عن "تفكير IPv4" الموجه نحو الحفاظ على العناوين.

تتيح هذه الوفرة تبسيط العنونة من طرف إلى طرف، مما يقلل من الحاجة إلى آليات معقدة مثل ترجمة عناوين الشبكة(NAT) ، ويفتح الباب أمام إمكانيات معمارية جديدة، مثل تخصيص عنوان Global Unicast Address (GUA) لكل حاوية في مجموعة Kubernetes. هذا التحول ليس تقنيًا فحسب، بل هو تحول مفاهيمي في كيفية التفكير في تصميم الشبكات وقابليتها للتوسع لدعم النمو الهائل لأجهزة إنترنت الأشياء (IoT) والتطبيقات السحابية الأصلية.

بنية وعنونة IPv6

يُعد فهم تنسيق عنوان IPv6 ذي 128 بت، وأنواعه المختلفة، والترميز المختصر أمرًا بالغ الأهمية للنشر الفعال. تُعد عناوين IPv6 معرفات (عناوين) 128 بت للواجهات ومجموعات الواجهات، وتُخصص للواجهات وليس للعقد.

يتكون **تنسيق العنوان** من ثماني قطع 16 بت، كل قطعة ممثلة بأربعة أرقام سداسية عشرية مفصولة بنقطتين رأسيتين (X:X:X:X:X:X:X:X).لتبسيط كتابة العناوين الطويلة التي تحتوي على سلاسل طويلة من الأصفار، تم تطوير قواعد ضغط:

- **القاعدة 1 :**يمكن حذف الأصفار البادئة في أي قطعة (على سبيل المثال، 0001 تصبح 1).
- **القاعدة 2 :**يمكن استبدال مجموعة واحدة متتالية من الأصفار بـ "::" (على سبيل المثال، FEDC:0001:0000:0000:0000:0000:ABDC:0FF0 يمكن ضغطها إلى (FEDC:1::ABDC:FF0) . لا يمكن أن يظهر "::" مرتين في نفس العنوان.
- **القاعدة 3 :**يمكن استخدام "::" لضغط الأصفار البادئة أو اللاحقة في العنوان (على سبيل المثال، 0000:0000:0000:0000:0001:FEDC:ABDC:0FF0يمكن ضغطها إلى .(::1:FEDC:ABDC:FF0
- **القاعدة 4 :**في البيئات المختلطة IPv4 وIPv6، يُستخدم التنسيق X:X:X:X:X:X.d.d.d.d حيث تمثل X القيم السداسية عشرية لست قطع عالية الترتيب 16 بت، وتمثل d القيم العشرية لأربع قطع منخفضة الترتيب (8 بت) عنوان IPv4 الفعلي 32 بت.

يُكتب **ترميز البادئة** بطريقة مماثلة لترميزCIDR: ipv6-address/prefix-length ، حيث prefix-lengthهي قيمة عشرية تحدد عدد البتات المتجاورة الأقصى من اليسار التي تشكل البادئة.

أنواع وعناوين IPv6 الخاصة

تُصنف **أنواع العناوين** في IPv6 إلى:

- **Unicast عنوان أحادي :** معرف لواجهة واحدة، ويتم تسليم الحزم إلى تلك الواجهة.
  - **Global Unicast Address (GUA):** قابل للتوجيه عبر الإنترنت (2000::/3). يُشبه عناوين IPv4 العامة القابلة للتوجيه، ويُخصص في كتل لمزودي خدمة الإنترنت.
  - **Unique Local Address (ULA):** قابل للتوجيه داخل مجال إداري .(fc00::/7) تنصح سيسكو عمومًا بعدم استخدام ULAs كبديل حقيقي لـ RFC1918 بسبب التعقيدات المحتملة في عمليات الدمج والاستحواذ.
  - **Link-Local Address:** غير قابل للتوجيه، ويوجد فقط على مجال الطبقة الثانية واحد.(fe80::/10)

- **Anycast عنوان أي نقطة :** معرف لمجموعة من الواجهات، ويتم تسليم الحزمة المرسلة إلى عنوان Anycast إلى أقرب واجهة تحددها تلك المجموعة، وفقًا لبروتوكول التوجيه. تُؤخذ عناوين Anycast من مساحة عناوين Unicast.

- **Multicast عنوان متعدد النقاط :** معرف لمجموعة من الواجهات، ويتم تسليم الحزمة المرسلة إلى عنوان Multicast إلى جميع الواجهات المحددة بهذا العنوان. يستخدم IPv6 البث المتعدد على نطاق واسع بدلاً من البث العام في (Broadcast)

أنواع وعناوين IPv6 الخاصة

تشمل **عناوين الاستخدام الخاص :(Special Use Addresses)** العنوان غير المحدد (::)، وعنوان(1::) Loopback ، وبادئة التوثيق(2001:0db8::/32) ، وبادئة التخلص.(0100::/64)

تُعد **عملية تعيين معرف الواجهة (Interface ID Assignment)** في IPv6 مرنة وتدعم طرقًا مختلفة: يدوية، وتكوين العنوان التلقائي عديم الحالة(SLAAC) ، و SLAAC مع امتدادات الخصوصية (RFC 8981) للعناوين المؤقتة، و SLAAC مع العناوين المستقرة (RFC 7217)، و DHCPv6. كما يمكن تحويل عنوان MAC ذي 48 بت إلى معرف واجهة ذي 64 بت بتنسيق EUI-64. إن العدد الهائل من عناوينIPv6 ، وخاصة معيار /64 لشبكات LAN ، يغير بشكل أساسي استراتيجيات تقسيم الشبكة والعنونة.

ينتقل هذا من تقسيم الشبكة المعقد الذي يحركه ندرة IPv4 إلى نموذج الوفرة، مما يبسط تخطيط الشبكة على مستوى القطاع. تتيح هذه الوفرة تصميمات شبكة أكثر وضوحًا وأقل تقييدًا، مما يسهل العنونة المباشرة للأجهزة مثل (IoT) دون طبقات NATالمعقدة. يحول هذا التركيز تصميم الشبكة من الحفاظ على العناوين إلى التقسيم المنطقي وتطبيق السياسات، مما يجعل إدارة الشبكة أبسط على المدى الطويل ولكنه يتطلب عقلية مختلفة.

أنواع وخصائص عناوين IPv6

نوع العنوان	البادئة/النطاق	الوصف	نظير IPv4 (إن وجد)
Global Unicast Address (GUA)	2000::/3	قابل للتوجيه عالميًا عبر الإنترنت.	عنوان IP عام.
Unique Local Address (ULA)	fc00::/7	قابل للتوجيه داخل مجال إداري خاص.	عناوين RFC1918 الخاصة (لكن مع تحذيرات سيسكو).
Link-Local Address	fe80::/10	غير قابل للتوجيه، صالح فقط على رابط محلي واحد.	لا يوجد نظير مباشر، لكن يُستخدم للتواصل المحلي.
Anycast	من مساحةUnicast	معرف لمجموعة من الواجهات، يتم تسليمه لأقرب واجهة.	لا يوجد نظير مباشر، لكن يُستخدم لخدمات التوفر العالي.
Multicast	ff00::/8	معرف لمجموعة من الواجهات، يتم تسليمه لجميع أعضاء المجموعة.	عناوين البث المتعدد.
Loopback Address	::1	يستخدم لاختبار الاتصال بالذات على الجهاز.	127.0.0.1
Unspecified Address	::	يستخدم كعنوان مصدر عندما لا يكون للجهاز عنوان بعد.	0.0.0.0

عمليات رابط IPv6

يُدخل IPv6 آليات جديدة لاتصال الأجهزة على الرابط المحلي، لتحل محل بروتوكول تحليل العناوين (ARP) واكتشاف موجه ICMP في IPv4.

في طبقة **الإيثرنت(Ethernet)** ، يمتلك IPv6 معرف نوع إيثرنت خاص به (0x86DD) ويعتمد بشكل كبير على البث المتعدد (Multicast)بدلاً من البث العام (Broadcast) المستخدم في IPv4. هذا التحول من البث العام إلى البث المتعدد يحسن الكفاءة وقابلية التوسع على الروابط المحلية، حيث تستمع الأجهزة فقط إلى مجموعات البث المتعدد ذات الصلة.

تُعد **رسائل ICMPv6** حاسمة لعمليات IPv6 (النوع 58). تشمل هذه الرسائل:

- **رسائل الخطأ:**مثل Destination Unreachable الوجهة غير قابلة للوصول، و Packet Too Bigالحزمة كبيرة جدًا، و Time Exceededانقضاء الوقت، و Parameter Problemمشكلة في المعاملات.
- **الرسائل المعلوماتية:**مثل Neighbor Discovery اكتشاف الجيران، وRouter Discovery كتشاف الموجهات، و Multicast Listener Discoveryاكتشاف مستمعي البث المتعدد، وPing، و.Traceroute

يعتمد **اكتشاف المسارMTU (Path MTU Discovery)** في IPv6 على رسائل ICMPv6 Packet Too Big لتحديد أكبر وحدة نقل قصوى (MTU) يمكن إرسالها عبر المسار دون تجزئة. يتم التعامل مع التجزئة بواسطة المصدر فيIPv6 ، على عكس IPv4 حيث يمكن للموجهات تجزئة الحزم.

بروتوكول اكتشاف الجيران (NDP) في IPv6

يُعد **بروتوكول اكتشاف الجيران (Neighbor Discovery Protocol - NDP)** بديلاً لـ ARP و ICMP Router Discovery.
يستخدم NDP عناوين Link-Local كمصدر ويعتمد على البث المتعدد. تشمل رسائل NDP الرئيسية:

- **Router Solicitation (RS)**: تُستخدم لاكتشاف الموجهات على الرابط.
- **Router Advertisement (RA)**: تُستخدم من قبل الموجهات لإعلان وجودها وتقديم معلومات التكوين.
- **Neighbor Solicitation (NS)**: تُستخدم لطلب عنوان MAC لجهاز معين أو للتحقق من وجود عنوان.
- **Neighbor Advertisement (NA)**: استجابة لرسالة NS ، تحتوي على عنوان MAC للجهاز المطلوب.
- **Redirect**: تُستخدم لإبلاغ المضيفين بمسار أفضل لوجهة معينة.

تستخدم العقد **البث المتعدد للعقدة المطلوبة (Solicited Node Multicast)** للانضمام إلى عناوين بث متعدد محددة لعناوينها الأحادية وأي نقطة، مما يسهل اكتشاف الجيران. أما **اكتشاف العناوين المكررة (Duplicate Address Detection - DAD)** فيستخدم رسائل NS مع عنوان مصدر غير محدد للتحقق من تفرد العنوان على الرابط المحلي قبل استخدامه. إن استبدال ARP و ICMP Router Discovery بـ NDP هو تغيير معماري جوهري. هذا التحول من البث العام (ARP) إلى البث المتعدد (NDP) يحسن الكفاءة وقابلية التوسع على الروابط المحلية، حيث تستمع الأجهزة فقط إلى مجموعات البث المتعدد ذات الصلة.

إن فهم آليات الطبقة المحلية الجديدة هذه أمر بالغ الأهمية لاستكشاف أخطاء شبكات IPv6 وتأمينها، حيث يؤثر على كيفية اكتشاف الأجهزة للجيران، والحصول على العناوين، والتعامل مع الاتصالات المحلية، مما يتطلب من متخصصي الشبكات تكييف استراتيجيات التشخيص والأمان الخاصة بهم بعيدًا عن نهج IPv4.

آليات الانتقال من IPv4إلى IPv6

تُعد استراتيجيات الهجرة من IPv4 إلىIPv6 ، أو تمكين التعايش بينهما، ضرورية لضمان انتقال سلس وتقليل الاضطرابات في الشبكة.
لا يوجد حل واحد يناسب الجميع، وتعتمد الطريقة المختارة على البنية التحتية الحالية والميزانية وسرعة اعتماد IPv6 المطلوبة.

تُحدد **استراتيجية النشر التدريجي (Incremental Deployment Strategy)** نطاقًا يتراوح من شبكات IPv4 فقط إلى شبكات IPv6فقط بالكامل.

تُعد **وضع التشغيل المزدوج (Dual Stack Mode)** الطريقة المفضلة من سيسكو. يتضمن هذا الوضع تشغيل IPv4 و IPv6بالتوازي على نفس الأجهزة دون الحاجة إلى الأنفاق أو ترجمة عناوين الشبكة(NAT) ، مما يوفر مرونة وقابلية توسع وأداءً عاليًا.
لتحسين تجربة المستخدم في بيئات التشغيل المزدوج، تُستخدم تقنية **Happy Eyeballs (RFC 8305)**. تعمل هذه التقنية على تحسين تجربة المستخدم من خلال محاولة الاتصال عبر كل من IPv4 و IPv6في وقت واحد، واستخدام الاتصال الذي ينجح أولاً، مما يخفف من المشكلات المتعلقة بمسارات IPv6 المعطلة أو البطيئة.
في سيناريوهات مثل **مزودي خدمة الهاتف المحمول الذين يستخدمون IPv6 فقط(Mobile Provider Using IPv6-only)** ، تُستخدم آليات مثل 464xLAT RFC6877 لمعالجة التطبيقات القديمة التي تحتوي على عناوين IPv4 حرفية مضمنة.

آليات ربط مواقع IPv6

لربط مواقع IPv6 عبر بنية تحتية قائمة علىIPv4 ، تُستخدم **آليات ربط مواقع IPv6 (Connecting IPv6 Sites)** المتنوعة. تشمل هذه الآليات:

- **شبكة WAN ذات التشغيل المزدوج (Dual Stack WAN)** :حيث يتم تشغيل IPv4 و IPv6على روابط WAN.
- **الأنفاق المكونة يدويًا (Manually Configured Tunnels)** : مثلIPv6 over GRE ، وIPSec، وDMVPN، التي تغلف حزم IPv6 داخل حزم IPv4.
- **خدمة 6VPEعبر MPLS IPv4 Core** : وهي آلية متقدمة لنقل حركة مرور IPv6 VPN عبر شبكة MPLS الأساسية التي تعمل بـ IPv4.
- **IPv6عبرMPLS :**
  - **6PE (IPv6 Provider Edge)**:يسمح بنقل حركة مرور IPv6 عبر شبكة MPLS أساسية تعمل بـ IPv4.
  - **6VPE (IPv6 VPN Provider Edge)**:يسمح بنقل حركة مرور IPv6 داخل شبكات VPN عبر شبكة MPLS أساسية تعمل بـ IPv4.

إن مجموعة آليات الانتقال التشغيل المزدوج، الأنفاق، 6PE/6VPE تشير إلى عدم وجود حل واحد يناسب الجميع. تعالج كل طريقة سيناريوهات محددة مثل الهجرة التدريجية، وربط جزر IPv6 المعزولة عبر بنية تحتية IPv4

يؤكد تركيز سيسكو على التشغيل المزدوج كخيار "مفضل" على أنه يوازن بين قابلية التشغيل البيني والاستعداد للمستقبل. يتضمن تصميم الشبكات المتقدم الاختيار الاستراتيجي لآلية الانتقال المناسبة بناءً على البنية التحتية الحالية، والميزانية، والسرعة المطلوبة لاعتماد IPv6. يتطلب هذا فهمًا للمقايضات من حيث التعقيد والأداء والأمان لكل طريقة.

اعتبارات أمان IPv6

بينما يوفر **IPv6** مزايا أمنية متأصلة، فإنه يقدم أيضًا نواقل هجوم جديدة تتطلب تدابير مضادة محددة. يتطلب تأمين بيئات IPv6 فهمًا عميقًا لآلياته الفريدة.

تُشدد **سيسكو** على أمان القفزة الأولى لـ (**IPv6 First Hop Security - FHS**) IPv6، الذي يهدف إلى التحكم في حركة مرور IPv6 بطريقة مماثلة لـ IPv4. تشمل ميزات FHS ما يلي:

- **RA Guard حماية إعلانات الموجه:**
  يحمي من إعلانات الموجهات الخبيثة أو الضارة وهجمات الرجل في المنتصف MiM
- **DHCPv6 Guard حماية DHCPv6**
  يحمي من عروض DHCP غير الصالحة، وهجمات حجب الخدمة DoS وهجمات MiM.
- **Destination Guard حماية الوجهة:**
  يحمي من هجمات DoS، والمسح الضوئي، واستخدام عناوين وجهة غير صالحة.
- **ND Multicast Suppression قمع البث المتعدد لاكتشاف الجيران:**
  يقلل من حركة مرور التحكم لعمليات الارتباط الصحيحة لتحسين الأداء.
- **RA Throttle تقييد إعلانات الموجه:**
  يسهل قابلية التوسع عن طريق تحويل حركة مرور إعلانات الموجهات متعددة البث إلى أحادية البث.
- **Source/Prefix Guard حماية المصدر/البادئة:**
  يحمي من عناوين المصدر والبادئات غير الصالحة، وانتحال عنوان المصدر.

اعتبارات أمان IPv6

تُفصل الوثائق الهجمات الشائعة في IPv6 وكيفية تخفيف ميزات FHS لها. تشمل **نواقل الهجوم:(Attack Vectors)**

- **هجمات اكتشاف الموجهات :(Router Discovery Attacks)** يمكن للمهاجمين خداع الضحايا لقبولهم كموجهات افتراضية باستخدام إعلانات موجهات مزيفة.
- **هجمات تكوين العنوان :(Address Configuration Attacks)** يمكن للمهاجمين انتحال إعلانات الموجهات ببادئات خاطئة على الرابط، مما يؤدي إلى مشاكل في تصفية الدخول.
- **هجمات تحليل العنوان :(Address Resolution Attacks)** يمكن للمهاجمين المطالبة بعنوان IP للضحية.
- **هجمات :(DAD (Duplicate Address Detection Attacks** يمكن للمهاجمين تعطيل محاولاتDAD ، مما يمنع الضحايا من تكوين عناوين.IP

تُمكن **واجهة سطر الأوامر لجودة الخدمة (QoS CLI)** من مطابقة خرائط الفئات لكل من حركة مرور IPv4 وIPv6، مما يسمح بسياسات QoS متسقة عبر البروتوكولين. أما **بروتوكولات التكرار للقفزة الأولى (FHRPs)** فيIPv6 ، فتشمل آليات FHRP مدمجة مثل(NUD) Neighbor Unreachability Detection ، ويمكن أيضًا استخدام بروتوكولات FHRP التقليدية مثل HSRP و GLBP و.VRRP

اعتبارات أمان IPv6

تُقدم سيسكو **العديد من الأوراق البيضاء الرسمية** التي تتناول أمان IPv6 بشكل خاص، مثل "IPv6 Security" التي تشرح الإجراءات الوقائية، و"Flexible NetFlow Mappings Specific to IPv6"، و"IPv6 First-Hop Security Concerns"، و"Remotely Triggered Black Hole Filtering in IPv6"، و "IPv6 Extension Headers Review and Considerations"، و "Countermeasures for the Malicious Use of IPv6 Type 0 Routing Headers".

إن التفصيل الدقيق لميزات FHS ونواقل الهجوم المحددة في IPv6 يشير إلى أن مجرد نشر IPv6 دون تدابير أمنية مخصصة ينطوي على مخاطر. العديد من افتراضات أمان IPv4 مثل تسميم ARP لا تُترجم مباشرة، وتنشأ نقاط ضعف جديدة من آليات IPv6 الفريدة مثل الهجمات المستندة إلى RA.
يتطلب أمان الشبكة المتقدم في بيئة IPv6 نهجًا استباقيًا، وتحديدًا تنفيذ ميزات FHS وفهم كيفية استغلال طبيعة IPv6 عديمة الحالة واعتمادها الكبير على ICMPv6 (NDP). يستلزم هذا تحولًا في سياسة الأمان ونشر الأدوات لمعالجة مشهد البروتوكول الجديد بفعالية.

Q3

ما هو طول عنوان IPv6بالبت؟

أ) 32

ب) 64

ج) 128

ما هو نوع العنوان المستخدم للاتصال المحلي فقط (لا يمكن توجيهه)?

أ) Global Unicast

ب) Link-Local

ج) Anycast

صح أم خطأ: IPv6 لا يدعم البث المتعدد (Multicast).

Q3

ما هو طول عنوان IPv6بالبت؟
أ) 32
ب) 64
ج) 128

ما هو نوع العنوان المستخدم للاتصال المحلي فقط (لا يمكن توجيهه)?
أ) Global Unicast
ب) Link-Local
ج) Anycast

صح أم خطأ: IPv6 لا يدعم البث المتعدد (Multicast) . × بل يدعم بشكل موسع

الوحدة الرابعة

تبديل الملصقات متعدد البروتوكولات (MPLS)

تطور MPLS وفوائده

ظهرت تقنية MPLS (Multiprotocol Label Switching) لمعالجة القيود المتأصلة في توجيه IP التقليدي، مقدمة آلية إعادة توجيه عالية الكفاءة والمرونة للشبكات الحديثة. تُعرف MPLS بأنها معيار من مجموعة مهندسي الإنترنت (IETF) لتوجيه حركة المرور، حيث تُرفق ملصقات بالحزم وتُعاد توجيهها على طول مسارات محددة. تجمع هذه التقنية بين سمات تبديل الطبقة الثانية والتوجيه في الطبقة الثالثة في كيان واحد، مما يسمح بإنشاء بنية تحتية شبكية موحدة.

تُقدم كتب سيسكو بريس لمحة تاريخية عن **بروتوكولات ما قبل MPLS** وكيف تطورت **MPLSفي Cisco IOS** من Tag Switching إلى MPLS. هذا التطور كان مدفوعًا بالحاجة إلى تحسينات في الأداء والمرونة.

تطور MPLS وفوائده

تتعدد **فوائد MPLS** وتُعد حاسمة في بيئات الشبكات المعاصرة:

- **هندسة حركة المرور (Traffic Engineering - TE):** تسمح MPLS بتوجيه حركة المرور على طول مسارات محددة مسبقًا، مما يحسن من استخدام موارد الشبكة ويضمن تدفقًا أمثل لحركة المرور، بالإضافة إلى توفير تحسين المسار وحمايته.
- **جودة الخدمة (Quality of Service - QoS):** تُمكن MPLS من تحديد أولويات الحزم ذات الملصقات لضمان جودة الخدمة، وحجز عرض النطاق الترددي للتطبيقات الحيوية مثل الصوت والفيديو.
- **شبكات VPN عبر بروتوكول الإنترنت (IP VPNs):** تُعد MPLS حجر الزاوية في توفير خدمات الشبكات الخاصة الافتراضية (VPNs)لمزودي الخدمة، وذلك باستخدام نموذج VPN من نظير إلى نظير.(Peer-to-Peer VPN Model)
- **بنية تحتية شبكية موحدة:** تتيح MPLS استخدام بنية تحتية شبكية موحدة لتقديم خدمات متنوعة.
- **تكامل أفضل لـ IP عبر ATM:.**
- **نواة خالية من BGP (BGP-Free Core):** تُبسط توجيه النواة عن طريق تقليل الحاجة إلى تشغيل BGP في كل جهاز في النواة.
- **تحسين الإنتاجية وتقليل زمن الوصول:** خاصة لأحجام الملفات الكبيرة.
- **قابلية التوسع:** توفر MPLS قوة وقابلية توسع توجيه IP بالإضافة إلى ميزات تبديل الدوائر.

تطور MPLS وفوائده

إن وصف MPLS بأنه يجمع بين سمات تبديل الطبقة الثانية وتوجيه الطبقة الثالثة، وتمكينه لـ "بنية تحتية شبكية موحدة"، يشير إلى دوره في تقارب الشبكة. هذا يسمح لمزودي الخدمة بتقديم أنواع مختلفة من الخدماتVPN ، TE، QoS عبر عمود فقري واحد وفعال.

إن MPLS ليس مجرد تقنية إعادة توجيه؛ إنه عامل تمكين أساسي لخدمات الشبكة المتقدمة. إن قدرته على توفير هندسة حركة المرور، وضمانات جودة الخدمة، وإمكانيات VPN عبر بنية تحتية مشتركة يعزز بشكل كبير مرونة الشبكة وكفاءتها، مما يجعله لا غنى عنه لشبكات مزودي الخدمة الحديثة والمؤسسات الكبيرة.

بنية ومكونات MPLS

يُعد فهم العناصر المعمارية الأساسية لـ MPLS أمرًا بالغ الأهمية لاستيعاب كيفية عملها. تقع MPLS كطبقة "2.5" بين الطبقة الثانية والثالثة من نموذج OSI.

ملصقات MPLS (MPLS Labels) قيمة 20 بت، تعمل كمؤشر للبحث السريع في جدول إعادة توجيه MPLS. يمكن أن تُكدس **الملصقات (Label Stacking)** ، مما يعني أن حزمة واحدة يمكن أن تحتوي على رؤوس MPLS متعددة.

تشمل المكونات الرئيسية في بنية MPLS:

- **موجه تبديل الملصقات (Label Switch Router - LSR)**: موجه يقوم بإعادة توجيه الحزم بناءً على الملصقات.
- **موجه الحافة لتبديل الملصقات (Label Edge Router - LER)**: موجه LSR يقع على حافة مجال MPLS ، يقوم بتطبيق الملصقات على الحزم الواردة وإزالتها من الحزم الصادرة.
- **مسار تبديل الملصقات (Label Switched Path - LSP)**: مسار أحادي الاتجاه عبر شبكة MPLS يُحدد بواسطة تسلسل من الملصقات.
- **فئة إعادة التوجيه المتكافئة (Forwarding Equivalence Class - FEC)**: مجموعة من حزم IP التي تُعاد توجيهها بنفس الطريقة عبر LSP.

بنية ومكونات MPLS

يُمكن أن يتم **توزيع الملصقات (Label Distribution)** بطريقتين: إما أن تُدمج الملصقات مع بروتوكول توجيه IP موجود مثل BGP أو تُوزع عبر بروتوكول منفصل مثل بروتوكول توزيع الملصقات .(LDP) تُعرف **مساحات ملصقات (MPLS Label Spaces)** بمساحات لكل منصة **MPLS**
(Per-platform) أو لكل واجهة.(Per-interface)

تُحدد **أوضاع MPLS (MPLS Modes)** سلوك توزيع الملصقات والاحتفاظ بها والتحكم في:LSP

- **أوضاع توزيع الملصقات (Label Distribution Modes)**: مستقل (Independent) أو مرتب.(Ordered)
- **أوضاع الاحتفاظ بالملصقات (Label Retention Modes)**: ليبرالي (Liberal) أو محافظ.(Conservative)
- **أوضاع التحكم في LSP (LSP Control Modes)**

رأس MPLS

تُكون رأس **MPLS (MPLS Header)** من عدة حقول مهمة:

- **قيمة الملصق :(Label Value)** قيمة 20 بت تُستخدم كأساس لإعادة توجيه الحزم في سحابة.MPLS
- **حقل EXP (Experimental Bits) : 3** بتات تُستخدم عادةً لدعم Diffserv في شبكةMPLS ، وتحمل عادةً قيمة IP Precedenceمن حزمة.IP
- **بت أسفل المكدس (Bottom of Stack Bit - S-bit)** يُضبط هذا البت على رأس الملصق السفلي للإشارة إلى الوصول إلى أسفل المكدس.
- **حقل Time-To-Live (TTL)** يُستخدم لمنع الحلقات وربما لتتبع المسار في سحابةMPLS ، وتتناقص قيمته مع كل قفزة.

إن الابتكار الأساسي لـ MPLS هو إعادة التوجيه القائم على الملصقات، والذي يسمح بمعالجة الحزم بشكل أسرع عن طريق تجنب عمليات البحث المعقدة عن IP في كل قفزة داخل سحابة .MPLS تتيح آلية "الطبقة 2.5" هذه مسارات حتمية (LSPs) وتبسط قرارات إعادة التوجيه. تُصمم المكونات المعمارية لـMPLS ، وخاصة الملصق وآليات إعادة التوجيه المرتبطة به، لنقل الحزم عالي السرعة وفعاليته. تُعد هذه الكفاءة حاسمة للعمود الفقري لمزود الخدمة الذي يحمل أنواعًا مختلفة من حركة المرور ولتنفيذ ميزات متقدمة مثل هندسة حركة المرور وشبكات VPN بأداء يمكن التنبؤ به.

رأس MPLS

اسم الحقل	الحجم (بت)	الوصف/الغرض
الملصق(Label)	20	قيمة تُستخدم لتحديد مسار التوجيه في شبكة MPLS.
EXP (Experimental)	3	تُستخدم لتحديد جودة الخدمة (QoS) أو فئة الخدمة (CoS) للحزمة.
S-bit (Bottom of Stack)	1	يشير إلى ما إذا كان هذا هو الملصق الأخير في مكدس الملصقات.
TTL (Time-To-Live)	8	يمنع الحلقات ويُستخدم لتتبع المسار، يتناقص عند كل قفزة.

عمليات بروتوكول توزيع الملصقات (LDP)

يُعد بروتوكول توزيع الملصقات (LDP) البروتوكول الأكثر شيوعًا لتوزيع الملصقات في شبكةMPLS ، مما يمكّن موجهات تبديل الملصقات (LSRs) من بناء جداول معلومات إعادة توجيه الملصقات (LFIB) الخاصة بها.

تتضمن **نظرة عامة على LDP وعملياته** اكتشاف موجهات LSRs التي تشغلLDP ، وإنشاء جلسات LDP وصيانتها، وإعلان وسحب تعيينات الملصقات، ومهام الصيانة الدورية. تُعد هذه الخطوات أساسية لضمان أن جميع موجهات LSRs في مجال MPLS لديها معلومات الملصقات اللازمة لإعادة توجيه الحزم.

تُستخدم **جلسة LDP المستهدفة (Targeted LDP Session)** لإقران LDP بين موجهات LSRs غير المتجاورة مباشرةً، مما يوفر مرونة في التصميم. أما **مصادقة(LDP (LDP Authentication** ، فهي ميزة أمنية حاسمة لتأمين جلسات LDP ومنع التلاعب بمعلومات الملصقات.

للحفاظ على التحكم في إعلانات الملصقات، يُستخدم **التحكم في إعلان الملصقات(Controlling Label Advertisement)** ، بما في ذلك تصفية ربط الملصقات الواردة .(Inbound Label Binding Filtering) تُسهم **تكوين LDP التلقائي (LDP Autoconfiguration)**في تبسيط عملية النشر وتقليل الأخطاء اليدوية.

مزامنة وحماية LDP

تُعد **مزامنة MPLS LDP-IGP (MPLS LDP-IGP Synchronization)** ميزة تشغيلية حرجة تضمن أن LDP يعمل بكامل طاقته قبل استخدام مسارات بروتوكول البوابة الداخلية (IGP) لإعادة توجيه حركة المرور ذات الملصقات.
يمنع هذا السيناريو الذي قد يؤدي إلى "ثقوب سوداء" في التوجيه حيث تصل الحزم الموجهة بالملصقات إلى موجه LSR لا يمتلك الملصق الصحيح لإعادة توجيهها.

تُعالج هذه المزامنة التبعيات الحرجة بين البروتوكولات في بيئات الشبكة المعقدة. أما **حماية جلسة MPLS LDP (MPLS LDP Session Protection)** ، فهي تعزز موثوقية جلسات LDP من خلال توفير آليات للحفاظ على الجلسات حتى في حالة فشل الارتباطات المادية المؤقتة.
تُعد المزامنة بين MPLS LDP وبروتوكولات IGP تفصيلاً تشغيليًا بالغ الأهمية. إنها تعالج احتمال حدوث "ثقوب سوداء" في التوجيه إذا لم يتم إنشاء جلسات LDP بالكامل قبل استخدام مسارات IGP لإعادة توجيه حركة المرور الموصوفة. هذا يسلط الضوء على أهمية تبعيات البروتوكولات المتداخلة في بيئات الشبكة المعقدة. تتطلب عمليات نشر MPLS المتقدمة دراسة متأنية للفروق الدقيقة في تشغيل LDP، وخاصة مزامنته مع IGP الأساسي. هذا يضمن استقرار الشبكة ويمنع فقدان حركة المرور أثناء أحداث التقارب، وهو أمر بالغ الأهمية في شبكات مزودي الخدمة.

إعادة توجيه الحزم ذات الملصقات وتكامل CEF

تُعد عملية إعادة توجيه الحزم ذات الملصقات في MPLS محسّنة للغاية، وغالبًا ما تستفيد من تقنية Cisco Express Forwarding (CEF)لتحقيق أداء عالٍ. يضمن هذا التكامل معالجة الحزم بكفاءة عبر شبكة.MPLS

تتضمن **إعادة توجيه الحزم ذات الملصقات (Forwarding of Labeled Packets)** فهم عملية الملصقات والفرق بين بحث IP وبحث الملصقات. تُعد **إزالة الملصق في القفزة قبل الأخيرة (Penultimate Hop Popping - PHP)** سلوكًا افتراضيًا حيث يقوم موجه LSR قبل الأخير في مسار LSP بإزالة رأس MPLS قبل إعادة توجيه الحزمة إلى موجه LER النهائي. يوفر هذا على موجه LER الأخير عبء عمل معالجة رأسMPLS ، مما يحسن الكفاءة.

تُخصص **ملصقات محجوزة (Reserved Labels)** لوظائف خاصة، مثل Implicit NULL Label و Explicit NULL Label و Router Alert Label. وOAM Alert Label.أما **الملصقات غير المحجوزة (Unreserved Labels)** فتُستخدم لإعادة توجيه البيانات العادية.

يُعد **سلوك TTL (Time-To-Live)** في MPLS أمرًا معقدًا، حيث يختلف سلوك TTL في سيناريوهاتIP-to-Label ، وLabel-to-IP، وLabel-to-Label، بالإضافة إلى كيفية التعامل مع انتهاء صلاحية TTL. أما **MPLS MTU (Maximum Transmission Unit)** فيشير إلى أكبر حجم حزمة يمكن إرسالها عبر شبكة MPLS دون تجزئة. يتضمن ذلك فهم أمرMPLS MTU ، وإطارات Giant وBaby Giant، ووحدة الاستقبال القصوى لـMPLS ، وتجزئة حزمMPLS ، واكتشاف.Path MTU

Cisco Express Forwarding (CEF)

تُعد **Cisco Express Forwarding (CEF)** آلية تبديل عالية الأداء في أجهزة سيسكو.

- **نظرة عامة:** تُشرح الحاجة إلى CEF في شبكاتMPLS ، ومكوناته الأساسية مثل جدول التجاور (Adjacency Table) وجدول FIB/CEF.
- **العملية:** تُفصل كيفية معالجة CEF للحزم، بما في ذلك CEF الموزع (DCEF) الذي يسمح بمعالجة الحزم في الأجهزة.(Hardware)
- **موازنة التحميل:** يدعم CEF موازنة التحميل غير المتساوية التكلفة(Unequal Cost Load Balancing) ، وتوسيم حزم IP بواسطة CEF ، وموازنة التحميل للحزم ذات الملصقات.
- **استكشاف أخطاء CEF وإصلاحها:** تُقدم إرشادات لتشخيص المشكلات المتعلقة بـ.CEF

إن التركيز على CEF ودوره في إعادة توجيه MPLS يسلط الضوء على تركيز سيسكو على معالجة الحزم المتسارعة بالأجهزة. يحسب CEFمعلومات القفزة التالية مسبقًا، مما يتيح عمليات بحث أسرع من تبديل العمليات التقليدي. هذا أمر بالغ الأهمية لشبكات الأداء العالي. يعتمد أداء الشبكة المتقدم في بيئات MPLS بشكل كبير على آليات إعادة التوجيه الفعالة مثل .CEF إن فهم كيفية عملCEF ، خاصة بطريقة موزعة(DCEF) ، يسمح للمهندسين بتحسين إنتاجية الشبكة وتشخيص اختناقات الأداء، مما يضمن قدرة الشبكة على التعامل مع كميات كبيرة من حركة المرور الموصوفة.

شبكات MPLS VPN شبكات VPN من الطبقة (3)

تُعد شبكات MPLS Layer 3 VPNs حجر الزاوية لمزودي الخدمة لتقديم خدمات شبكة خاصة آمنة وقابلة للتوسع ومرنة عبر عمود فقري مشترك لـ MPLS.

تتضمن **مقدمة (Introduction)** تعريفVPN ، ونماذج VPN المختلفة، ونموذج MPLS VPN الذي يجمع بين مزايا IP و MPLS لإنشاء شبكات خاصة افتراضية.

فيما يتعلق بـ **نظرة عامة معمارية(Architectural Overview)** ، تعتمد MPLS VPNs على مفاهيم أساسية مثل:

- **Virtual Routing Forwarding (VRF)**: جداول توجيه منفصلة تُمكن من عزل شبكات العملاء منطقيًا على نفس الموجه.
- **Route Distinguishers (RD)**: قيمة 64 بت تُضاف إلى بادئات IP لجعلها فريدة عالميًا داخل شبكةMPLS VPN ، مما يسمح بوجود نفس البادئة في VRFs مختلفة.
- **Route Targets (RTs)**: قيم تُستخدم لتحديد VRFs التي يجب أن تستورد أو تصدر مسارات معينة، مما يتيح التحكم في تبادل المسارات بين VPNs.

ميزات PE-CEالمتقدمة وسيناريوهات النشر

تشمل **ميزات PE-CE المتقدمة (Advanced PE-CE Features)** تكوينOSPF VRF ، وانتشار مقياسOSPF ، ومجتمعات BGP الموسعة لـOSPF ، وتصميم شبكةOSPF ، و) Sham Linkلتحسين اتصال OSPF بين(VRFs ، و Down Bitو Domain Tagلمنع الحلقات، و EIGRP PE-CE مع روابطBackdoor ، وAutonomous System Override، و.allowas-in

تُقدم الوثائق أيضًا سيناريوهات نشر متنوعة مثل **Hub-and-Spoke**، و**SOO (Send Only Once)**، و**VRF Access**، و) **Internet Access**بما في ذلك الإنترنت في VPN أو الوصول عبر جدول التوجيه العام، و **Multi-VRF CE** حيث يقوم موجه CE واحد بتشغيل VRFs متعددة، و **CE Management**. إن شبكات MPLS VPN ، من خلال VRFs وRDs وRTs ، تتيح الفصل المنطقي لشبكات العملاء عبر بنية تحتية مادية مشتركة.

هذا هو أساس تعدد المستأجرين لمزودي الخدمة، مما يسمح لهم بتقديم خدمات VPN مميزة دون تسرب حركة المرور بين العملاء. إن القدرة على إنشاء مجالات توجيه معزولة (VRFs) والتحكم في تبادل المسارات (RD/RT) هي مهارة متقدمة بالغة الأهمية. إنها تتيح تقديم خدمة مرنة للغاية وقابلة للتوسع، وتلبية احتياجات العملاء المتنوعة مع الحفاظ على ضمانات الأمان والأداء على شبكة مشتركة.

هندسة حركة المرور عبر MPLS (MPLS TE)

تُعد هندسة حركة المرور عبر MPLS (MPLS TE) آلية قوية تتيح لمديري الشبكات توجيه حركة المرور على طول مسارات صريحة، مما يحسن من استخدام موارد الشبكة ويضمن جودة الخدمة للتطبيقات الحيوية.

تنشأ **الحاجة إلى MPLS TE** من قصور بروتوكولات التوجيه الداخلية (IGPs) التقليدية، التي تعتمد فقط على أقصر مسار (أو أقل تكلفة) وقد لا تأخذ في الاعتبار عوامل مثل عرض النطاق الترددي المتاح أو الازدحام.

تتضمن **نظرة عامة على عملية MPLS TE** عدة خطوات رئيسية:

- **توزيع معلومات TE (Distribution of TE Information):** يتطلب ذلك امتدادات لبروتوكولات IGP مثل OSPF و IS-IS لتبادل معلومات هندسة حركة المرور، مثل عرض النطاق الترددي المتاح، وسمات الارتباط، ومجموعات الارتباط ذات المخاطر المشتركة (SRLGs). تُستخدم آليات الفيضان في IGP لنشر هذه المعلومات.
- **توجيه وتكلفة LSP TE (Routing and Cost of a TE LSP):** تُحدد سمات ارتباط TE، مثل الحد الأقصى لعرض النطاق الترددي القابل للحجز، وأعلام السمات، ومقياس TE، و SRLGs. تُحدد سمات نفق TE، مثل أولوية الإعداد والاحتفاظ، وإعادة التحسين (Reoptimization) الدوري أو القائم على الأحداث أو اليدوي، وخيارات إعداد المسار مثل استبعاد عنوان IP الصريح (Explicit Address Exclusion).

تُستخدم **مقاييس TE المزدوجة (Dual TE Metrics)** و PCALC (Path Computation Element - PCE) لتعقيد حسابات المسار واختيار المسارات المثلى. يُعد **RSVP (Resource Reservation Protocol)** بروتوكول الإشارة المستخدم لإنشاء وصيانة مسارات LSP TE وحجز الموارد على طولها. يُسهم **Link Manager** في إدارة الارتباطات.

إعادة التوجيه السريع وتطبيقات MPLS TE

تُعد **إعادة التوجيه السريع (Fast Reroute - FRR)** ميزة حاسمة في MPLS TE لتعزيز مرونة الشبكة. توفر FRR حماية للارتباط (Link Protection)وحماية للعقدة(Node Protection) ، مما يضمن تقاربًا سريعًا في حالة الفشل. يمكن استخدام SRLGs بواسطة أنفاق النسخ الاحتياطي، ويمكن تكوين أنفاق نسخ احتياطي متعددة.

تتضمن **إعادة توجيه حركة المرور إلى أنفاق MPLS TE (Forwarding Traffic onto MPLS TE Tunnels)** آليات مختلفة مثل التوجيه الثابت، والتوجيه القائم على السياسات(Policy-Based Routing) ، وإعلان المسار التلقائي(Autoroute Announce) ، والتجاور الأمامي(Forwarding Adjacency) ، واختيار النفق القائم على الفئة(Class-Based Tunnel Selection) ، وحساب التكلفة لمسارات IGP عبر أنفاق TE. يُمكن أيضًا دمج **MPLS TE معMPLS VPN** ، مما يسمح بأنفاق TE بين موجهات PE وتوجيه VRFإلى نفق TE. يركز توجيه IP التقليدي (IGPs) على إيجاد أقصر مسار. ومع ذلك، تتيح" MPLS TE مسارات صريحة" و"توجيه حركة المرور" بناءً على معايير تتجاوز مجرد عدد القفزات، مثل توفر عرض النطاق الترددي أو السياسات الإدارية. هذا يتجاوز التوجيه الأساسي إلى تحسين الشبكة المتطور. يعزز FRR المرونة بشكل أكبر. تُعد MPLS TE أداة حاسمة لإدارة حركة المرور المتقدمة، مما يسمح لمهندسي الشبكات بضمان جودة الخدمة لحركة المرور ذات الأولوية العالية، وتجنب الازدحام في قطاعات شبكة معينة، وبناء شبكات مرنة للغاية بقدرات تجاوز الفشل السريع. إنها تحول الشبكة من نظام تفاعلي إلى بنية تحتية استباقية تعتمد على السياسات.

تطبيقات MPLS الأخرى

تدعم MPLS مجموعة متنوعة من التطبيقات الأخرى، مما يوسع فائدتها بما يتجاوز شبكات VPN وهندسة حركة المرور، ويجعلها تقنية متعددة الاستخدامات لمزودي الخدمة والمؤسسات الكبيرة.

IPv6عبر MPLS 6PE و 6VPE تم تناول هذا التطبيق في الوحدة 3، حيث يسمح بنقل حركة مرور IPv6 عبر شبكة MPLS أساسية تعمل بـIPv4 ، سواء لشبكات IPv6 المستقلة (6PE) أو شبكات IPv6 VPN (6VPE).

أي نقل عبر(Any Transport over MPLS - AToM) MPLS :

- **الحاجة إلى AToM:** تنشأ الحاجة إلى AToM من الرغبة في نقل إطارات الطبقة الثانية) مثل إيثرنت، Frame Relay، (ATMعبر عمود فقري لـMPLS.
- **البنية المعمارية :**تتضمن AToM مستوى البيانات (Data Plane) وإشارةPseudowire ، والتي تحدد نوعPseudowire ، والمعرفات، ومعلمات الواجهة، وإشارة الحالة.
- **كلمة التحكم :(Control Word)** تُستخدم كلمة التحكم في AToM لوظائف مثل حشو الحزم الصغيرة، وحمل بتات التحكم من رأس الطبقة الثانية للبروتوكول المنقول، والحفاظ على تسلسل الإطارات المنقولة، وتسهيل موازنة التحميل الصحيحة لحزمAToM ، وتسهيل التجزئة وإعادة التجميع.
- **بروتوكولات الطبقة الثانية المنقولة :**يدعم AToM نقل مجموعة واسعة من بروتوكولات الطبقة الثانية مثلHDLC ، وPPP، و Frame Relay، وATM، والإيثرنتEoMPLS)) ، وإعادة كتابة معرفVLAN ، و QinQعبر.(AToM
- **اختيار نفق AToM وجودة الخدمة.:(QoS)**

تطبيقات MPLS الأخرى

- **خدمة شبكة LAN الخاصة الافتراضية:(Virtual Private LAN Service - VPLS)**
  - **الحاجة إلى VPLS:** تتيح VPLS توسيع خدمات الطبقة الثانية عبر منطقة واسعة، مما يجعل الشبكات المحلية تبدو وكأنها متصلة مباشرة عبر شبكة MPLS.
  - **البنية المعمارية:** تتضمن مستوى بيانات VPLS وإشاراتها.
  - **التكوين الأساسي والتحقق:.**
  - **بروتوكولات الطبقة الثانية للأنفاق:** تدعم VPLS أنفاق بروتوكولات الطبقة الثانية مثل Cisco Discovery Protocol و Spanning Tree Protocol.
  - **VPLS الهرمية (H-VPLS):** تُستخدم لإنشاء شبكات VPLS قابلة للتوسع، مع خيارات مثل QinQ في طبقة الوصول أو MPLS في طبقة الوصول.
  - **جودة الخدمة(QoS) ، تحديد عناوينMAC ، نظير التوجيه:.**
- **MPLS وجودة الخدمة:(QoS)**
  - **DiffServ مع حزم IP و MPLS:** تُشرح كيفية عمل خدمات DiffServ مع كل من حزم IP و MPLS.
  - **سلوك QoS الافتراضي لـ MPLS في Cisco IOS:.**
  - **نماذج أنفاق DiffServ:** Pipe ، وShort Pipe، وUniform.
  - **أوامر MQC لـ MPLS QoS:.**
  - **نقل MPLS QoS من موجه PE إلى موجه CE:.**
  - **ميزة Table-Map:.**
  - **استخدام MPLS QoS لـ Ethernet over MPLS:.**

Q4

ما هي الطبقة التي تعمل فيها تقنية MPLS حسب نموذج OSI؟

أ) الطبقة الثانية
ب) الطبقة 2.5
ج) الطبقة الثالثة

ما هو البروتوكول المستخدم لتوزيع الملصقات في MPLS؟

أ) OSPF
ب) LDP
ج) BGP

صح أم خطأ: MPLS لا يدعم جودة الخدمة .(QoS)

Q4

ما هي الطبقة التي تعمل فيها تقنية MPLS حسب نموذج OSI؟

أ) الطبقة الثانية

ب) الطبقة 2.5

ج) الطبقة الثالثة

ما هو البروتوكول المستخدم لتوزيع الملصقات في MPLS؟

أ) OSPF

ب) LDP

ج) BGP

صح أم خطأ: MPLS لا يدعم جودة الخدمة (QoS). × بل يدعم QoS

الوحدة الخامسة

الشبكات المعرفة بالبرمجيات (SDN) والمحاكاة الافتراضية للشبكة

مقدمة إلى الشبكات المعرفة بالبرمجيات (SDN)

تُعد الشبكات المعرفة بالبرمجيات (SDN) بنية شبكية تحويلية تفصل مستوى التحكم عن مستوى إعادة التوجيه، مما يتيح الإدارة المركزية وقابلية البرمجة. يُمكن تعريف SDN كنهج معماري للشبكات يتيح التحكم في الشبكة وإدارتها باستخدام تطبيقات البرامج. يكمن المفهوم الأساسي في برمجة سلوك الشبكة بالكامل وأجهزتها بطريقة مركزية عبر تطبيقات البرامج باستخدام واجهات برمجة التطبيقات (APIs) المفتوحة.

تتكون SDN من ثلاثة مكونات رئيسية:

- **مستوى البيانات (Data Plane):** المسؤول عن إعادة توجيه حركة مرور الشبكة.
- **مستوى التحكم (Control Plane):** يدير البنية التحتية للشبكة ويتخذ القرارات حول كيفية التعامل مع حركة مرور الشبكة.
- **طبقة التطبيق (Application Layer):** تتكون من تطبيقات البرامج التي تعمل فوق بنية SDN التحتية.

يُعد **وحدة التحكم المركزية (Centralized Controller)** إدخالًا رئيسيًا فيSDN ، حيث توفر رؤية عالمية للشبكة وتستخدم بروتوكول إدارة مشتركًا لتكوين أجهزة البنية التحتية للشبكة. يمكن لوحدة التحكم هذه حساب معلومات قابلية الوصول ودفع التدفقات داخل المحولات لإعادة التوجيه.

فوائد SDN

تقدم SDN العديد من **الفوائد** مقارنة بنهج الشبكات التقليدية:

- **الكفاءة :**إدارة شبكة أكثر كفاءة، حيث يمكن لمديري الشبكات أتمتة العديد من المهام التي كانت تُؤدى يدويًا.
- **المرونة وقابلية التخصيص :**يمكن إعادة تكوين البنية التحتية للشبكة بسرعة.
- **الأتمتة :**تقلل من الحاجة إلى التدخل البشري في العديد من قرارات إدارة الشبكة.
- **الفعالية من حيث التكلفة :**تزيد من الوصول وتقلل من الظروف التي تتطلب أجهزة وبرامج متخصصة.
- **قابلية التوسع :**شبكات SDN مرنة وقابلة للتوسع بشكل لا يصدق، وتتكيف بسهولة مع احتياجات العمل المتزايدة.

إن فصل مستويات التحكم والبيانات وإدخال وحدة تحكم مركزية يغيران بشكل أساسي كيفية إدارة الشبكات. بدلاً من تكوين الأجهزة الفردية، تسمح SDN ببرمجة *الشبكة بأكملها* عبر البرامج، والتعامل معها بشكل أكبر كمورد أو خدمة قابلة للبرمجة. تُشكل SDN تحولًا نموذجيًا من التكوين التقليدي القائم على الجهاز إلى نهج رشيق، يعتمد على السياسات، ومؤتمت. هذا يتيح نشر خدمة أسرع، ويقلل من التكاليف التشغيلية، ويزيد من القدرة على التكيف مع متطلبات العمل المتغيرة، وهو أمر بالغ الأهمية لبيئات تكنولوجيا المعلومات الحديثة والديناميكية.

SDN مقابل الشبكات التقليدية (مقارنة)

الميزة	الشبكة التقليدية	الشبكة المعرفة بالبرمجيات(SDN)
البنية المعمارية	صلبة، هرمية، يصعب تعديلها أو تكييفها مع احتياجات العمل المتغيرة.	مرنة، معرفة بالبرمجيات، يمكن إعادة تكوين البنية التحتية بسرعة.
مستوى التحكم	موزع، يتم التحكم في الأجهزة بشكل فردي.	مركزي، وحدة تحكم مركزية ذات رؤية عالمية للشبكة.
التكوين والإدارة	يدوي، شاق، عرضة للأخطاء.	مؤتمت، يعتمد على السياسات، مبسط.
قابلية البرمجة	غير قابلة للبرمجة.	قابلة للبرمجة عبر تطبيقات البرامج وواجهات برمجة التطبيقات المفتوحة.
الواجهات	مغلقة.	مفتوحة (واجهات برمجة التطبيقات).
اقتران مستوى البيانات/التحكم	مستوى البيانات ومستوى التحكم مثبتان على نفس المستوى.	مستوى البيانات ومستوى التحكم مفصولان بواسطة البرامج.
قابلية التوسع	تحدٍ كبير، يتطلب غالبًا إصلاحًا شاملاً.	مرنة وقابلة للتوسع بشكل لا يصدق، تتكيف بسهولة.
الأمان	يعتمد عادةً على الدفاعات القائمة على المحيط.	يوفر تجزئة دقيقة تعتمد على الهوية.
التكاليف الأولية	أقل في البداية.	قد تكون أعلى في البداية وتكاليف التحويل.
مخاطر الأمان	مخاوف أمنية مثل الوصول غير المصرح به.	التحكم المركزي يمكن أن يكون نقطة ضعف إذا لم يتم تأمينه جيدًا.

بنية Cisco Application Centric Infrastructure (ACI)

Cisco ACI (Application Centric Infrastructure)هو حل SDN مصمم لمراكز البيانات، ويوفر نهجًا يعتمد على السياسات لأتمتة تكوينات وخدمات الشبكة. يهدف ACI إلى تبسيط إدارة الشبكة من خلال ترجمة احتياجات العمل إلى سياسات شبكية، مما يضمن اتصالًا وأمانًا سلسين عبر كل من السحابات الخاصة والعامة.

يعتمد ACI على **إدارة السياسات والتكوين المركزية**. تُعد **طوبولوجيا Leaf-and-Spine** هي البنية الأساسية لـ:Cisco ACI

- **عقد :(Spine Nodes) Spine** تشكل العمود الفقري عالي السرعة، وتربط أجهزةLeaf ، وتخزن إدخالات تعيين نقطة النهاية إلى VTEP (Virtual Tunnel Endpoint).لا يُسمح بالاتصال المباشر بين عقد Spine أو بين عقد.Leaf
- **محولات :(Leaf Switches) Leaf** هي محولات(Top-of-the-Rack (ToR ، تتصل بجميع عقدSpine ، وتتصل بأعباء العمل الخوادم، وأجهزةHypervisor ، وأجهزة خدمة الشبكة، وتوفر وظيفةVTEP ، وتطبق سياسات ACI

APIC - عقل Cisco ACI

يُعد **APIC (Application Policy Infrastructure Controller)** المكون المعماري الرئيسي و"عقل" حل Cisco ACI. يعمل APICكمركز قيادة مركزي، ويوفر إدارة مركزية وأتمتة، ويتعامل مع تعريف السياسات وتطبيقها عبر الشبكة.

- **الوظائف :**يدير مستودع السياسات الموزع المسؤول عن تعريف ونشر التكوين القائم على السياسات لبنية ACI التحتية. كما يدير معلومات الطوبولوجيا والمخزون لجميع الأجهزة داخل.ACI pod
- **وظائف APIC الإضافية :**وظيفة "المراقب" التي تراقب صحة وحالة وأداءACI pod ، ووظيفة "مدير التمهيد" المسؤولة عن عملية التمهيد وتحديثات البرامج الثابتة لمفاتيح Spine و Leafومكونات .APIC. كما يدير "مدير الأحداث" ويخزن جميع الأحداث والأخطاء الصادرة من APIC وعقد.ACI fabric
- **التفاعل :**يدعم APIC واجهةREST API ، وCLI، وواجهة المستخدم الرسومية (GUI) للتفاعل.

إن نهج" ACI المتمحور حول التطبيق" و"القائم على السياسات" يشير إلى تحول من تكوين أجهزة الشبكة بناءً على موقعها الفعلي أو عنوان IP إلى تحديد سلوك الشبكة بناءً على متطلبات التطبيق. يترجم APIC هذه السياسات عالية المستوى إلى تكوينات شبكة أساسية. يُبسط هذا التجريد شبكات مراكز البيانات المعقدة، مما يسمح لفرق تكنولوجيا المعلومات بالتركيز على احتياجات التطبيقات بدلاً من تكوينات الشبكة منخفضة المستوى. إنه يسرع بشكل كبير نشر التطبيقات ويضمن تطبيقًا متسقًا للسياسات، وهو أمر بالغ الأهمية لمراكز البيانات الحديثة والديناميكية

مفاهيم Cisco Application Centric Infrastructure (ACI) الرئيسية

بالإضافة إلى البنية المادية، يقدم ACI مفاهيم منطقية تمكن من أتمتة السياسات. هذه المفاهيم ضرورية لتحقيق التحكم الدقيق والمرونة في بيئة مركز البيانات.

- **ملفات تعريف شبكة التطبيقات (Application Network Profiles - ANPs):** تُعد ANPs بمثابة مخططات لاتصال التطبيقات وأمانها. تتيح نمذجة التطبيقات في APIC وترجمة هذه النماذج إلى تكوينات شبكة، مما يوفر نهجًا منظمًا ومتسقًا لإدارة الشبكة وتطبيق السياسات.
- **مجموعات نقاط النهاية (Endpoint Groups - EPGs):** هي تجميعات منطقية لنقاط النهاية (مثل الأجهزة الافتراضية، والخوادم، والتطبيقات) التي تشترك في سياسات مماثلة. تُحدد EPGs سياسات الأمان وجودة الخدمة (QoS) والشبكة لحركة المرور بين المجموعات، مما يتيح تحكمًا دقيقًا وتجزئة دقيقة (Micro-segmentation) داخل ACI fabric.
- **العقود والمرشحات (Contracts and Filters):** تتحكم العقود والمرشحات في الاتصال بين EPGs ، وتُحدد سياسات الأمان وجودة الخدمة (QoS) والشبكة مثل قوائم التحكم في الوصول (ACLs) وقواعد QoS.
- **مجالات الجسر (Bridge Domains - BDs) و VRFs (Virtual Routing and Forwarding):** تُعد BDs مجالات إعادة توجيه من الطبقة الثانية تحتوي على شبكات فرعية، مما يسمح بتجزئة وإدارة الشبكة بكفاءة. تُعزل VRFs شبكات الطبقة الثالثة، مما يتيح تعدد المستأجرين والفصل الآمن لقطاعات الشبكة المختلفة.

مفاهيم VXLAN – ACI والتجزئة الدقيقة وتكامل السحابة

- **VXLANوتراكبات الشبكة:(VXLAN and Network Overlays)**
  - **VXLAN (Virtual Extensible LAN):**تقنية افتراضية للشبكة تُغلف إطارات إيثرنت للطبقة الثانية داخل حزمUDP ، مما يوسع مجالات الطبقة الثانية عبر شبكة الطبقة الثالثة. تستخدم VXLAN معرف شبكة VXLAN (VNID) لتمثيل مجال بث منطقي للطبقة الثانية.
  - **تراكبات الشبكة :(Overlays)** تُستخدم لتحقيق موازنة التحميل، وقابلية التوسع، والمرونة، والتقارب الأسرع في الشبكات ومراكز البيانات الحديثة.
- **التجزئة الدقيقة :(Micro-segmentation)** هي القدرة على فرض تجزئة الشبكة على مستوى الجهاز الافتراضي (VM) أو الحاويات، بشكل مستقل عن شبكات VLAN أو الشبكات الفرعية. تُعد "واعية للتطبيق"، مما يعني أن عملية التجزئة تبدأ وتنتهي بالتطبيق، وغالبًا ما تستخدم نموذج "عدم الثقة.(Zero-trust model) "
- **اكتشاف الشبكة والأتمتة :(Fabric Discovery and Automation)** تتيح قدرات اكتشاف الشبكة والأتمتة في Cisco ACI اكتشاف الأجهزة الجديدة تلقائيًا عند الاتصال، ويدفع APIC التكوينات ديناميكيًا إلى عناصر الشبكة.
- **تكامل السحابة المتعددة :(Multicloud Integration)** يتكامل ACI معNexus Dashboard ، ويدعم الإدارة الآمنة والمؤتمتة لموارد السحابة العامة والخاصة.

إن الجمع بين EPGs والعقود والتجزئة الدقيقة يتيح تحكمًا دقيقًا للغاية في الاتصال، متجاوزًا الأمان التقليدي القائم علىVLAN/ الشبكة الفرعية. هذا يتيح نموذج "عدم الثقة" حيث يُرفض الاتصال ما لم يُسمح به صراحةً، مما يعزز أمان مركز البيانات بشكل كبير. توفر البنى المنطقية لـ ACI الأدوات اللازمة لتنفيذ أوضاع أمان متقدمة داخل مركز البيانات، مما يتيح تحكمًا دقيقًا ويقلل من سطح الهجوم. هذا أمر بالغ الأهمية لحماية التطبيقات والبيانات الحساسة في البيئات الديناميكية والافتراضية للغاية.

رؤية وأركان Cisco Digital Network Architecture (DNA)

Cisco Digital Network Architecture (DNA)هو حل للشبكات القائمة على النوايا (Intent-Based Networking) يوسع مبادئ SDN عبر شبكات الحرم الجامعي، وشبكاتWAN ، والمكاتب الفرعية، مما يوفر الأتمتة، والضمان، والأمان المتكامل.
تتمثل **رؤية Cisco DNA** في أن تكون بنية مفتوحة، قابلة للتوسيع، ومدفوعة بالبرمجيات، وتسرع وتبسط عمليات شبكة المؤسسة، مع تقليل التكاليف والمخاطر. إنها جسر فريق تكنولوجيا المعلومات إلى شبكة قائمة على النوايا.
تتكون Cisco DNA من أربعة **أركان رئيسية**، يمثل كل منها مجالًا رئيسيًا في شبكة المؤسسة:

- **WAN شبكة المنطقة الواسعة:** مدعومة بحلول مثل.Cisco Software-Defined WAN (SD-WAN)
- **Campus الحرم الجامعي:** مدعومة بحلول مثل.Cisco Software-Defined Access (SD-Access)
- **Data Center مركز البيانات:** مدعومة بحلول مثل.Cisco Application Centric Infrastructure (ACI)
- **Cloud Edge حافة السحابة:** مدعومة بحلول مثل.Cisco Secure Agile Exchange (SAE)

مبادئ وأمان Cisco DNA

في جوهرها، تسترشد Cisco DNA بـ **مبادئ أساسية**:

- **مدفوعة بالنوايا :**تترجم نوايا العمل إلى سياسات شبكية.
- **مستنيرة بالسياق :**توفر رؤية مستمرة لجميع أنماط حركة المرور.
- **تتعلم باستمرار :**تستفيد من التعلم الآلي على نطاق واسع لتوفير ذكاء متزايد.
- **تحمي باستمرار :**تُمكّن الشبكة من رؤية وتوقع المشكلات والتهديدات للاستجابة السريعة.

يُعد **Cisco DNA Center (DNAC)** العنصر الأساسي للقيادة والتحكم، ويوفر إدارة مركزية عبر لوحات المعلومات وواجهات برمجة التطبيقات.(APIs)

يُعد **الأمان المتكامل (Integrated Security)** جانبًا محوريًا في Cisco DNA. فالأمان متأصل في كل حل من حلول Cisco DNA ، وليس مجرد إضافة. يُمكن لـ Cisco DNA تحويل الشبكة بأكملها إلى مستشعر لاكتشاف حركة المرور الضارة والشذوذ في السلوك. كما توفر مجموعة كاملة من الحلول المحلية والسحابية لزيادة الحماية للمؤسسات. إن فلسفة "القائمة على النوايا" في Cisco DNA تمثل تطورًا كبيرًا يتجاوز إدارة الشبكة التقليدية. بدلاً من التكوين اليدوي، تُبرمج الشبكة *لفهم نوايا العمل وتلبيتها*، وتتكيف ديناميكيًا مع التغييرات. هذا يقلل من التعقيد التشغيلي ويتيح تسليم خدمة أسرع. يُعد هذا التحول إلى الشبكات القائمة على النوايا أمرًا بالغ الأهمية للتعامل مع النمو الهائل للأجهزة والتطبيقات. إنه يسمح للمنظمات بأن تكون أكثر مرونة، وأتمتة المهام المعقدة، ومعالجة مشكلات الأمان والأداء بشكل استباقي، مما يحول عمليات الشبكة من تفاعلية إلى تنبؤية.

الشريحة 52: حلول Cisco Digital Network Architecture (DNA) الرئيسية

تضم Cisco DNA حلولًا رئيسية معرفة بالبرمجيات تمتد عبر المؤسسة، مما يوسع الأتمتة القائمة على السياسات.

Cisco SD-Access (SDA):

- **الغرض:** نهج يعتمد على السياسات لشبكات الحرم الجامعي، يبسط العمليات ويقلل التكاليف.
- **البنية المعمارية:** تستخدم الشبكة الأساسيةIPv4 ، بينما تُنقل حركة مرور IPv6 المتراكبة في أنفاق VXLAN عبر IPv4. تستخدم Cisco DNA Center للتصميم والتوفير والسياسات والضمان.
- **الميزات الرئيسية:** تجزئة قائمة على الهوية لأمان دقيق. كفاءة معززة من خلال الأتمتة. تعديلات شبكة مرنة وقابلة للتوسع.

Q5

ما هو المكون الرئيسي في بنية SDNالذي يفصل مستوى التحكم عن مستوى البيانات؟

أ) الموجه

ب) وحدة التحكم المركزية

ج) المحول

أي من الحلول التالية تقدمه سيسكو للشبكات القائمة على النوايا (?Intent-Based Networking)

أ) Cisco ACI

ب) Cisco DNA

ج) كليهما

صح أم خطأ: SDN تعتمد على تكوين الأجهزة بشكل فردي. × تعتمد على التحكم المركزي لا التكوين الفردي

Q5

ما هو المكون الرئيسي في بنية SDNالذي يفصل مستوى التحكم عن مستوى البيانات؟

أ) الموجه

ب) وحدة التحكم المركزية

ج) المحول

أي من الحلول التالية تقدمه سيسكو للشبكات القائمة على النوايا (?Intent-Based Networking)

أ) Cisco ACI

ب) Cisco DNA

ج) كليهما

صح أم خطأ: SDN تعتمد على تكوين الأجهزة بشكل فردي. × تعتمد على التحكم المركزي لا التكوين الفردي

المصادر

تُعد **Cisco Systems, Inc.** من أبرز الشركات العالمية في مجال تقنيات الشبكات والاتصالات.
تأسست عام 1984، وقد لعبت دورًا رياديًا في تطوير بنى الشبكات الحديثة وحلول الأمان والبنية التحتية للإنترنت.
توفر سيسكو مجموعة واسعة من المنتجات والخدمات التي تُستخدم في المؤسسات الكبرى حول العالم، وتُعتبر مرجعًا أساسيًا في تعليم شبكات الحاسوب من خلال برامج مثل **CCNA, CCNP, CCIE** وغيرها.
اعتمدنا في تجهيز هذه المحاضرة على منهجيات سيسكو

يمكن زيارة الموقع الرسمي للشركة لمزيد من المعلومات:
https://www.cisco.com

شكرا لكم