المؤسسة العامة للتدريب التقني والمهني بالمدينة المنورة

قسم الحاسب وتقنية المعلومات

تصميم البنية الأساسية لشبكات الاتصالات الحاسوبية الآمنة والقابلة للتوسع وعالية الاعتمادية

إعداد المتدربين:

عبدالرحمن العنزي - عبدالرحمن النجار - جواد المحمدي

محمد الحارثي - محمد وائل - محمد الحربي

إشراف المهندس:

محمد عبدالكريم اسكندر

1447هـ - 2026م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

صفحة الشكر والتقدير

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، نبينا محمد وعلى آله وصحبه أجمعين.. أما بعد:

فإن الشكر والامتنان يظلان عاجزين أمام كل من مدّ لنا يد العون والمساندة طوال مسيرتنا الأكاديمية والتدريبية، وفي هذا المقام، نتقدم بخالص الشكر والتقدير والعرفان إلى **الكلية التقنية بالمدينة المنورة**، وتحديداً إلى **قسم الحاسب وتقنية المعلومات** بكافة منسوبيه من أعضاء هيئة التدريب الأفاضل، الذين لم يدخروا جهداً في تزويدنا بالمعارف والمهارات التي أنارت لنا طريق التميز والنجاح.

كما نخص بالشكر والامتنان الجزيل سعادة المهندس والمشرف على مشروع التخرج:

والذي كان لتوجيهاته السديدة، ونصائحه القيمة، ومتابعته المستمرة والدقيقة طوال فترة العمل على هذا المشروع، الأثر البالغ والدور الأساسي في تذليل العقبات وإخراج هذا البحث والهيكل الشبكي بهذه الصورة المتميزة. نسأل الله أن يجزيه عنا خير الجزاء.

فهرس المحتويات

الفصل الأول: البحث والتصميم 7
1.1 المقدمة 8
1.2 مشكلة المشروع 8
1.3 أهداف المشروع 9
1.4 نطاق المشروع 9
1.5 المنهجية المتبعة 10
1.6 التصميم الإفتراضي 10
1.7 التصميم الفيزيائي 12
الفصل الثاني: التنفيذ 14
2.1 مقدمة الفصل 15
2.2 توزيع العناوين - IP Addressing 15
2.3 إعداد الشبكة المحلية - VLANs & Inter-VLAN Routing 20
2.4 خدمات DHCP وHSRP 20
2.5 بروتوكولات التوجيه والاعتمادية 20
2.6 تأمين الشبكة 21
2.7 خدمات VoIP والشبكة اللاسلكية 21
2.8 بروتوكولات DTP، VTP، STP في المحولات 22
الفصل الثالث: الإختبار والتقييم 23
3.1 مقدمة الفصل 24
3.2 اختبار الاتصال والتوجيه الداخلي - Testing Connectivity & OSPF 24
3.3 اختبار الموثوقية والجاهزية العالية - Testing High Availability & Failover 25
3.4 اختبار الخدمات الأمنية وحماية البيانات - Testing Security & VPN 26
3.5 اختبار منظومة الاتصالات الصوتية - Testing VoIP 27
3.6 تقييم الأداء العام وخلاصة الفصل 28
الخاتمة 30
قائمة المراجع: 31

فهرس الجداول

الوصف	الشكل	الصفحه
القسم الرئيسي	1-2	15
القسم الثاني	2-2	17

فهرس الأشكال

الوصف	الشكل	الصفحه
التصميم الإفتراضي الكامل	1-1	11
الأجهزة التي أستعملت في الشبكة	2-1	11
التصميم الفيزيائي المملكة العربية السعودية	3-1	12
التصميم الفيزيائي الفرع الرئيسي	4-1	13
التصميم الفيزيائي الفرع الثاني	5-1	13

الفصل الأول: البحث والتصميم

1.1 المقدمة

أصبحت الشبكات جزءاً أساسياً من البنية التحتية للمنشآت الحديثة، حيث تعتمد عليها المؤسسات في تبادل البيانات وتشغيل الخدمات المختلفة مثل الاتصالات الصوتية عبر الإنترنت (VoIP). ومع ازدياد الاعتماد على الشبكات، أصبحت الحاجة إلى توفير الاستمرارية والأمان أمراً ضرورياً لضمان عدم توقف الأعمال وحماية البيانات من التهديدات السيبرانية.

يهدف هذا المشروع إلى تصميم شبكة آمنة وعالية الاعتمادية تعتمد على مزودي خدمة إنترنت متعددين، مع تطبيق تقنيات التوجيه والحماية الحديثة لضمان استقرار الشبكة واستمرارية الخدمات.

1.2 مشكلة المشروع

تعاني بعض المنشآت من عدة مشكلات تؤثر على أداء الشبكة وأمنها، من أهمها:

- الاعتماد على مزود خدمة إنترنت واحد مما يؤدي إلى توقف الخدمات عند حدوث أي عطل.
- نقل البيانات بين الفروع عبر الإنترنت دون حماية كافية مما يعرضها للاختراق أو التنصت.
- ارتفاع تكاليف الاتصالات التقليدية بين الفروع.
- ضعف إدارة الشبكة بسبب عدم فصل الخدمات والأقسام المختلفة، مما يؤثر على الأداء والأمان.

1.3 أهداف المشروع

يهدف المشروع إلى تصميم ومحاكاة شبكة آمنة وقابلة للتوسع من خلال:

- تحقيق الجاهزية العالية باستخدام مزودي خدمة إنترنت وتفعيل بروتوكول HSRP.
- تأمين الاتصال بين الفروع باستخدام تقنية Site-to-Site IPSec VPN.
- توفير خدمة الاتصالات الصوتية عبر الإنترنت (VoIP) باستخدام Cisco CME.
- تحسين الأداء والأمان من خلال تقسيم الشبكة باستخدام VLANs وتطبيق ACLs.
- توفير الوصول إلى الإنترنت باستخدام تقنية NAT/PAT مع ترشيد استخدام العناوين العامة.

1.4 نطاق المشروع

ما يشمله المشروع

- تحليل متطلبات الشبكة.
- تصميم المخطط الشبكي باستخدام Cisco Packet Tracer.
- إعداد خطة العنونة (IP Addressing).
- تفعيل بروتوكولات Routing و Switching و OSPF.
- إعداد VPN و HSRP و VoIP.

- اختبار الشبكة والتحقق من عمل جميع الخدمات.

ما لا يشمله المشروع

- شراء الأجهزة الفعلية وتنفيذ المشروع على أرض الواقع.
- أعمال التمديدات والكابلات الفيزيائية.
- إدارة وصيانة الشبكة بعد انتهاء المشروع.

1.5 المنهجية المتبعة

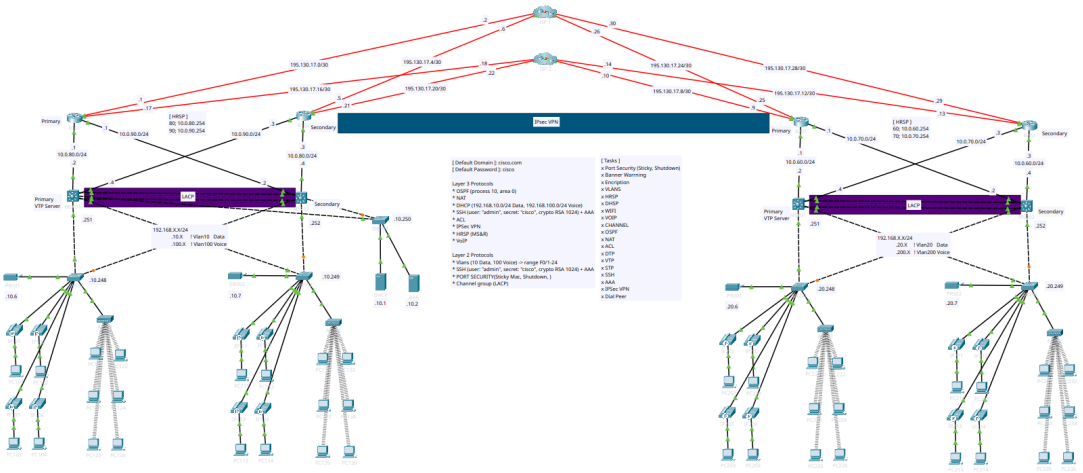
تم تنفيذ المشروع وفق المراحل التالية:

1. **البحث وجمع المعلومات:** دراسة تقنيات الشبكات المطلوبة مثل OSPF و VPN و VoIP.
2. **التخطيط والتصميم:** إعداد مخطط الشبكة وحساب العناوين وتحديد الأجهزة المناسبة.
3. **التنفيذ والمحاكاة:** تطبيق الإعدادات باستخدام أوامر Cisco CLI داخل Packet Tracer.
4. **الاختبار والتحقق:** إجراء اختبارات الاتصال وفحص البروتوكولات للتأكد من تحقيق أهداف المشروع.

1.6 التصميم الإفتراضي

هذا التصميم الذي يوضح ويختصر لي المهندس بنية الشبكة والأجهزة المستخدمة وكيفية ربط الشبكة ببعضها البعض.

صورة من التصميم الكامل:



شكل (1-1)

الأجهزة التي أستعملت في الشبكة:

أجهزة الشبكة

2811
موجه (راوتر)، يربط الشبكات المختلفة
ويعمل في الطبقة الثالثة (الشبكة)

3650-24PS
محول متعدد الطبقات، يربط الأجهزة
داخل الشبكة المحليةويعمل في
الطبقة الثانية (ربط البيانات)

2960-24TT
محول لإدارة الاتصال داخل الشبكة
ويعمل في الطبقة الثانية (ربط البيانات)

AccessPoint-PT
نقطة وصول تربط الأجهزة اللاسلكية عبر Wi-Fi
ويعمل في الطبقة الثانية (ربط البيانات)

أجهزة النهاية

Server-PT
خادم لتخزين البيانات وتوفير الخدمات
ويعمل في الطبقة السابعة (التطبيق)

PC-PT
حاسوب شخصي، يستخدمه المستخدم ويعمل
في الطبقة السبعة (التطبيق)

7960
هاتف IP الإجراء المكالمات الصوتية
ويمل في الطبقة السابعة (التطبيق)

Primer-PT
طابعة المستندات ويعمل في الطبقة السابعة
(التطبيق)

شكل (2-1)

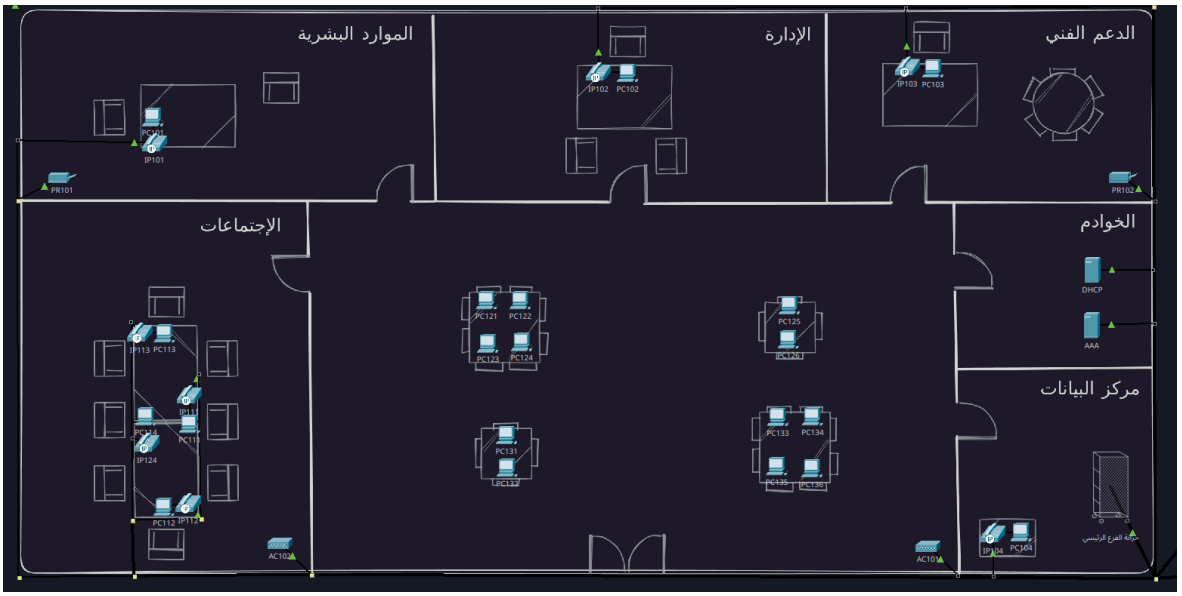
1.7 التصميم الفيزيائي

قمنا بالتصميم على انها شركة متخصصة في الحلول التقنية

المملكة العربية السعودية

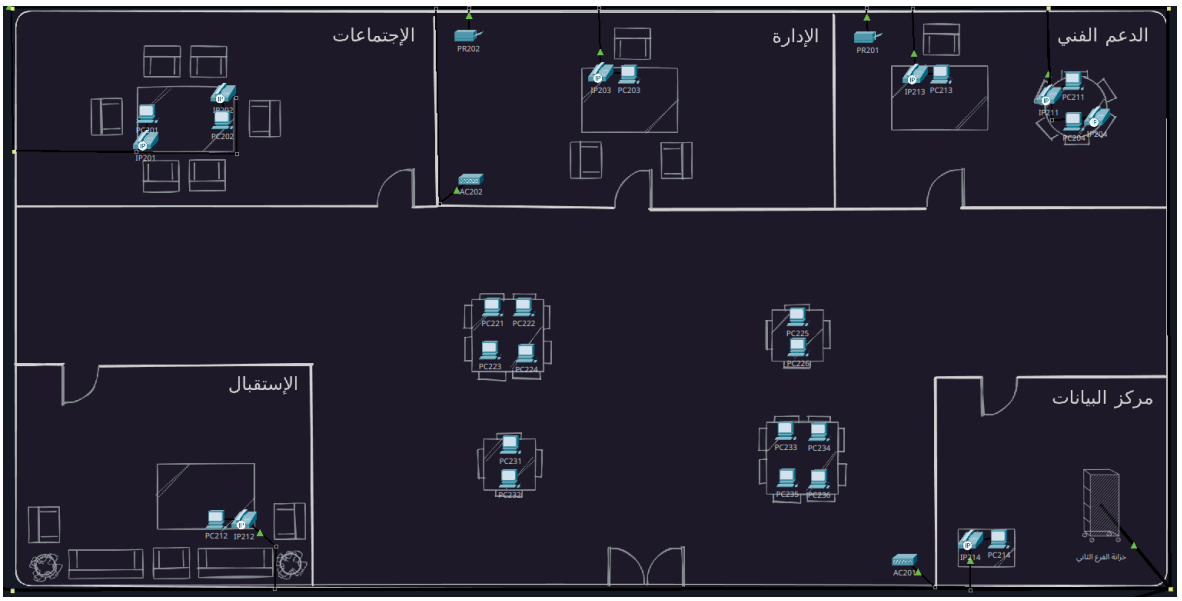
شكل (1-3)

الفرع الرئيسي (المدينة)



شكل (1-4)

الفرع الثاني (الرياض)



شكل (1-5)

الفصل الثاني: التنفيذ

2.1 مقدمة الفصل

يتناول هذا الفصل تنفيذ وتصميم الشبكة باستخدام برنامج Cisco Packet Tracer، من خلال إعداد الموجهات والمحولات وتفعيل بروتوكولات التوجيه والأمان والخدمات المختلفة لتحقيق شبكة آمنة وعالية الاعتمادية.

2.2 توزيع العناوين - IP Addressing

القسم الرئيسي

الجهاز	الواجهة	VLAN	النطاق	المخرج الافتراضي
حواسيب الفرع الرئيسي (DATA10)	F0	10	192.168.10.0/24	192.168.10.254
الصوت 1 (VOICE100)	N/A	100	192.168.100.0/24	192.168.100.254
الخادم (DHCP)	F0	10	192.168.10.1/24	192.168.10.254
الخادم (AAA)	F0	10	192.168.10.2/24	192.168.10.254
الطابعة 101	F0	10	192.168.10.6/24	192.168.10.254
الطابعة 102	F0	10	192.168.10.7/24	192.168.10.254

المحول 101	Vlan10	10	192.168.10.248/24	192.168.10.254
المحول 102	Vlan10	10	192.168.10.249/24	192.168.10.254
المحول 103	Vlan10	10	192.168.10.250/24	192.168.10.254
المحول متعدد الطبقات 101	Vlan10	10	192.168.10.251/24	10.0.80.254
...	Vlan100	100	192.168.100.251/24	...
...	G1/0/24	...	10.0.80.2/24	...
...	G1/0/23	...	10.0.90.4/24	...
المحول متعدد الطبقات 102	Vlan10	10	192.168.10.252/24	10.0.80.254
...	Vlan100	100	192.168.100.252/24	...
...	G1/0/24	...	10.0.80.3/24	...
...	G1/0/23	...	10.0.90.2/24	...
الموجه 101	F0/0	N/A	10.0.80.1/24	S0/0/0-1

...	F0/1	...	10.0.90.1/24	...
...	S0/0/0	...	195.130.17.1/30	...
...	S0/0/1	...	195.130.17.17/30	...
الموجه 102	F0/0	N/A	10.0.80.1/24	S0/0/0-1
...	F0/1	...	10.0.90.1/24	...
...	S0/0/1	...	195.130.17.5/30	...
...	S0/0/0	...	195.130.17.21/30	...

جدول (2-1)

القسم الثاني

الجهاز	الواجهة	VLAN	النطاق	المخرج الافتراضي
حواسيب الفرع الثاني (DATA20)	F0	20	192.168.20.0/24	192.168.20.254

الصوت 2 (VOICE200)	N/A	200	192.168.200.0/24	192.168.200.254
الطابعة 201	F0	20	192.168.20.6/24	192.168.20.254
الطابعة 202	F0	20	192.168.20.7/24	192.168.20.254
المحول 201	Vlan20	20	192.168.20.248/24	192.168.20.254
المحول 202	Vlan20	20	192.168.20.249/24	192.168.20.254
المحول متعدد الطبقات 201	Vlan20	20	192.168.20.251/24	10.0.80.254
...	Vlan200	200	192.168.200.251/24	...
...	G1/0/24	...	10.0.60.2/24	...
...	G1/0/23	...	10.0.70.4/24	...
المحول متعدد الطبقات 202	Vlan20	20	192.168.20.252/24	10.0.80.254
...	Vlan200	200	192.168.200.252/24	...
...	G1/0/24	...	10.0.60.4/24	...

...	10.0.70.2/24	...	G1/0/23	...
S0/0/0-1	10.0.60.1/24	N/A	F0/0	الموجه 201
...	10.0.70.1/24	...	F0/1	...
...	195.130.17.25/30	...	S0/0/1	...
...	195.130.17.9/30	...	S0/0/0	...
S0/0/0-1	10.0.60.1/24	N/A	F0/0	الموجه 202
...	10.0.70.1/24	...	F0/1	...
...	195.130.17.1/30	...	S0/0/0	...
...	195.130.17.17/30	...	S0/0/1	...

جدول (2-2)

2.3 إعداد الشبكة المحلية - VLANs & Inter-VLAN Routing

تم إنشاء شبكتين VLAN واحد للبيانات والثاني للصوت في كل قسم لفصل أقسام الشبكة وتحسين الأداء والأمان. كما تم تفعيل التوجيه بين الشبكات باستخدام محولات الطبقة الثالثة (Layer 3 Switches) عبر واجهات SVI لتوفير الاتصال بين الأقسام المختلفة.

2.4 خدمات - DHCP وHSRP

- تم إعداد خادم DHCP لتوزيع عناوين IP تلقائيًا على الأجهزة.
- تم استخدام الأمر `ip helper-address` على محولات متعددة الطبقات لتمرير طلبات DHCP بين الشبكات المختلفة.
- تم تفعيل بروتوكول HSRP على أجهزة (الموجهات، المحولات متعددة الطبقات) لتوفير بوابة افتراضية احتياطية وضمان استمرارية الخدمة عند تعطل أحد الأجهزة.

2.5 بروتوكولات التوجيه والاعتمادية

- تم تفعيل بروتوكول OSPF لتبادل جداول التوجيه واختيار أفضل المسارات داخل الشبكة.
- تم إعداد مسارات افتراضية احتياطية (Floating Static Routes) باستخدام مزودي خدمة إنترنت لضمان استمرار الاتصال عند فشل المسار الرئيسي.

- تم تفعيل EtherChannel على بروتوكول LACP لزيادة سرعة الاتصال وتوفير مسارات احتياطية بين المحولات.

2.6 تأمين الشبكة

- تم تهيئة أجهزة الشبكة بل أعدادات الأساسية (التسمية + كلمات المرور المشفرة + رسالة التحذير القانونية).
- تم تطبيق تقنية NAT/PAT لتمكين الأجهزة الداخلية من الوصول إلى الإنترنت باستخدام عنوان عام واحد.
- تم استخدام قوائم التحكم بالوصول (ACLs) للتحكم بحركة المرور بين الشبكات.
- تم إنشاء نفق IPSec VPN لتأمين الاتصال بين الفروع وتشفير البيانات المتبادلة عبر الإنترنت.
- تم تفعيل بروتوكول SSH للإدارة الآمنة ومنع استخدام Telnet.
- تم تفعيل كلمات المرور المشفرة وخدمة TACACS على خادم AAA وربطها بجميع أجهزة الشبكة.
- تم تفعيل PorSecurity على وضع اغلاق المنفذ وSticky MAC.

2.7 خدمات VoIP والشبكة اللاسلكية

- تم إعداد خدمة Cisco CME لتوفير الاتصالات الصوتية عبر بروتوكول VoIP.
- تم تخصيص أرقام داخلية للهواتف وتفعيل الاتصال بين الفروع.

- تم إعداد الشبكة اللاسلكية (WLAN).

2.8 بروتوكولات STP، VTP، DTP في المحولات

- تم تهيئة STP الأساسي في محول متعدد الطبقات الأول في كل قسم و الاحتياطي في الثاني لمنع حدوث حلقات التكرار.
- تم تفعيل بروتوكول VTP لتوزيع VLANS
- تم تهيئة DTP وتفعيل وضع "Access" بين المحولات وأجهزة النهاية وتعطيل المفاوضات بين المحولات والمحولات والموجهات وتهيئتها على وضع "Trunk"

الفصل الثالث: الإختبار والتقييم

3.1 مقدمة الفصل

بعد الانتهاء من مرحلة التنفيذ والتهيئة البرمجية لكافة أجهزة ومكونات الشبكة، تأتي مرحلة **الاختبار والتقييم** كخطوة حاسمة لضمان أن البنية التحتية المصممة تعمل وفقاً للمعايير الهندسية المطلوبة. يهدف هذا الفصل إلى التحقق الفعلي من كفاءة بروتوكولات التوجيه، وآلية التحويل التلقائي عند الفشل (Failover)، وتأمين نفق الـ VPN، وسلامة الاتصالات الصوتية (VoIP). تم الاعتماد في هذا الفصل على أدوات الفحص الأساسية مثل (Ping & Traceroute) بالإضافة إلى أوامر التحقق الإدارية من خلال واجهة السطر البرمجي (CLI) داخل برنامج **Cisco Packet Tracer**.

3.2 اختبار الاتصال والتوجيه الداخلي - Testing Connectivity & OSPF

أولاً: اختبار التوجيه بين الشبكات الوهمية - Inter-VLAN Routing Test

للتأكد من نجاح محولات الطبقة الثالثة (Layer 3 Switches) في توجيه البيانات بين الأقسام المختلفة المعزولة منطقياً، تم إجراء فحص اتصال (Ping) من جهاز كمبيوتر يقع في شبكة الموظفين (VLAN 10) إلى جهاز آخر في شبكة الإدارة (VLAN 20).

- **النتيجة:** تم نجاح الاتصال (Success Rate is 100%)، مما يثبت صحة إعدادات الواجهات الافتراضية (SVIs) وتفعيل خاصية `ip routing`.

ثانياً: التحقق من جدول توجيه الـ OSPF

تم تنفيذ أمر التحقق `show ip route` على الموجهات (Routers) للتأكد من أن بروتوكول OSPF قد قام بتبادل المسارات وبناء جدول التوجيه ديناميكياً.

- **النتيجة:** ظهرت الشبكات البعيدة في الجدول مسبوقة بالحرف **(O)**، مما يعني أن الموجهات استطاعت التعرف على طوبولوجيا الشبكة الكاملة وحساب أفضل المسارات بنجاح.

3.3 اختبار الموثوقية والجاهزية العالية - Testing High Availability & Failover

أولاً: اختبار بروتوكول HSRP للبوابات الافتراضية

تم التحقق من حالة الموثوقية للمحولات الأساسية باستخدام الأمر `show standby brief`.

- **النتيجة:** أظهر الأمر أن أحد المحولات يعمل كجهاز أساسي **(Active)** يمر عبره البيانات، بينما المحول الآخر في وضع الاستعداد **(Standby)**. عند القيام بفصل كابل الطاقة عمداً عن المحول

الأساسي، تحول المحول الاحتياطي فوراً وبشكل تلقائي إلى حالة (Active) دون أن يشعر المستخدمون بانقطاع الخدمة.

ثانياً: اختبار المسارات الافتراضية العائمة (Floating Static Routes)

تم محاكاة سقوط الرابط المتصل بمزود الخدمة الأول (ISP-1) عبر إغلاق المنفذ (Shutdown).

- **النتيجة:** اختفى المسار الثابت الأساسي ذو المسافة الإدارية (AD=1) من جدول التوجيه، وظهر مكانه تلقائياً المسار الاحتياطي الموجه نحو (ISP-2) ذو المسافة الإدارية (AD=10)، وتحولت حركة البيانات للإنترنت عبر المنفذ الاحتياطي بسلاسة كاملة.

3.4 اختبار الخدمات الأمنية وحماية البيانات - Testing Security & VPN

أولاً: التحقق من عمل نفق الـ Site-to-Site VPN

لمعرفة ما إذا كانت البيانات المتبادلة بين فرع المدينة المنورة والفرع الآخر تمر مشفرة عبر الإنترنت، تم إرسال حزم بيانات وتنفيذ الأوامر التالية على الموجه الأساسي:

1. الأمر `show crypto isakmp sa`: أظهر الحالة **(QM_IDLE)**، وهي الحالة النموذجية التي تعني نجاح المرحلة الأولى (Phase 1) وتطابق كلمات المرور المشتركة.

2. الأمر `show crypto ipsec sa`: أظهر إحصائيات دقيقة لعدد الحزم التي تم تشفيرها (Encapsulated) وفك تشفيرها (Decapsulated)، مما يؤكد أن البيانات لا تمر كنص واضح بل يتم حمايتها عبر خوارزمية AES.

ثانياً: اختبار قوائم التحكم بالوصول (ACL) وترجمة العناوين (NAT)

- **اختبار الـ ACL:** تم محاولة الدخول من شبكة الزوار أو الاستضافة إلى خادم البيانات الحساس، وظهرت رسالة (Destination host unreachable)، مما يثبت أن القائمة الممتدة (Extended ACL) تقوم بفلترة وحظر الحزم غير المصرح لها بدقة.
- **اختبار الـ NAT/PAT:** عند خروج الأجهزة الداخلية للإنترنت، تم تنفيذ الأمر `show ip nat translations` وظهرت العناوين الداخلية الخاصة (Private IPs) وهي تترجم وتتحول إلى العنوان العام المشترك (Public IP) مع أرقام منافذ (Ports) مختلفة، مما يؤكد نجاح حجب الهوية الداخلية للشبكة وترشيد العناوين العامة.

3.5 اختبار منظومة الاتصالات الصوتية - Testing VoIP

لتقييم نجاح منظومة الاتصال الصوتي المعتمدة على خدمة Cisco CME، تم إجراء الاختبارات التالية:

1. **اختبار تسجيل الهواتف:** بعد ربط الهواتف بالشبكة، تم التحقق من سحبها لأيبيهات تلقائية من نطاق الـ Voice DHCP، وظهور الأرقام المكونة من 3 خانات المخصصة لها على شاشات الهواتف (IP Phones) بناءً على جدول توزيع الأقسام.
2. **اختبار الاتصال الداخلي وبين الفروع:** تم إجراء مكالمة تجريبية من الهاتف رقم (101) في الفرع الرئيسي إلى الهاتف رقم (201) في الفرع الآخر.

- **النتيجة:** ظهرت حالة الاتصال **(Connected)** على الشاشتين، مما يثبت صحة برمجة الـ `dial-peer voice` وقدرة الموجهات على تحويل وتمرير حزم الصوت (VoIP Packets) عبر المسارات الشبكية المتاحة بنجاح وكفاءة عالية.

3.6 تقييم الأداء العام وخلاصة الفصل

أثبتت نتائج جميع الاختبارات السابقة أن التصميم الهندسي المقترح للبنية التحتية قد حقق الأهداف التشغيلية والأمنية بنسبة 100%. الشبكة الآن تتمتع بـ:

- **صمود عالٍ ضد الأعطال (Resilience):** بفضل تفعيل بروتوكولات التكرارية HSRP و Floating Static Routes.

- **أمان متكامل وموثوقية:** بفضل عزل الشبكات عبر VLANs وتأمين خطوط الربط بنفق VPN المشفر وفلترة البيانات بالـ ACLs.
- **خدمات مدمجة وذكية:** بفضل التشغيل الناجح لمنظومة الهواتف الصوتية والشبكات اللاسلكية المؤمنة.

تؤكد هذه النتائج أن الشبكة جاهزة تماماً للانتقال من مرحلة المحاكاة والتصميم الافتراضي إلى مرحلة التطبيق الفعلي على أرض الواقع في أي منشأة حيوية.

الخاتمة

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه تتحقق الغايات، والصلاة والسلام على نبينا محمد وعلى آله وصحبه أجمعين.. وبعد:

في ختام هذا المشروع المتميز بفضل الله، نكون قد استكملنا رحلة هندسية متكاملة ركزت على "**تصميم وبناء بنية تحتية شبكية آمنة، متطورة، وعالية الاعتمادية**". لقد كان هذا العمل تطبيقاً عملياً حقيقياً لكافة المعارف والمهارات التقنية التي اكتسبناها طوال فترة دراستنا وتدريبنا في الكلية التقنية بالمدينة المنورة، حيث نجحنا في تحويل المفاهيم والنظريات الهندسية المعقدة إلى بيئة محاكاة واقعية وذكية عبر برنامج **Cisco Packet Tracer**.

وفي النهاية، نرجو من الله العلي القدير أن نكون قد وُفّقنا في تقديم مشروع هندسي ذي قيمة علمية وفنية ملموسة، وأن يكون هذا التقرير مرجعاً مفيداً لزملائنا المتدربين والباحثين في قسم الحاسب وتقنية المعلومات. نكرر شكرنا لكل من ساندنا، ونخص بالشكر مهندسنا ومشرفنا الفاضل، سائلين الله عز وجل التوفيق والنجاح في مسيرتنا المهنية القادمة لخدمة ديننا ووطنا الغالي.

والسلام عليكم ورحمة الله وبركاته.

قائمة المراجع:

"دليل كتابة تقرير مشروع التخرج"، الكلية التقنية بالمدينة المنورة، 1442هـ.

الحقيبة التدريبية لمقرر "مشروع شبكات"، الكلية التقنية بالمدينة المنورة.