مشروع الشبكات

تصميم وتطبيق شبكة آمنة وفعالة

إعداد الطالب

توبولوجيا الشبكة والأجهزة المستخدمة

الراوتر المركزي

استخدمت راوتر Cisco 1941 ليكون المركز الرئيسي وبوابة العبور للشبكة.

- يوفر خدمات التوجيه بين الـ VLANs.
- يدير خدمات NAT و VPN.
- يعمل كخادم DHCP أساسي.

السويتشات

تم توزيع المهام على سويتشات متنوعة لضمان كفاءة الأداء:

- سويتش عادي (Switch1) للأجهزة الطرفية.
- سويتشات متعددة الطبقات (Switch0, Switch2).
- توزيع الحمل وتقليل الازدحام.

الأجهزة الطرفية

تتضمن الشبكة أجهزة كمبيوتر تمثل المستخدمين في أقسام مختلفة:

- PC0, PC1, PC2 للموظفين.
- خادم مركزي (Server0).
- توصيل يضمن عزل الأقسام تقنياً.

تقسيم الشبكة (VLANs)

الأهداف التنظيمية

قمت بتقسيم الشبكة إلى عدة VLANs لضمان التنظيم والأمان. يساهم هذا التقسيم في تقليل الازدحام وتسهيل التحكم في الوصول بشكل فعال.

توزيع الـ VLANs

رقم الـ VLAN	الاسم	القسم المستهدف
100	IT_VLAN	تقنية المعلومات
110	FINANCE_VLAN	المالية
200	SERVER_VLAN	الخوادم
999	BLACKHOLE	الحماية (Native)

الفوائد التقنية

- أمان عالٍ عبر عزل الأقسام تقنياً.
- تحسين الأداء بتقليل نطاق البث.
- سهولة إدارة الشبكة والمستخدمين.

توزيع عناوين الـ IP (يدوي وتلقائي)

الإعداد اليدوي (Manual)

اعتمدت في هذه المرحلة ضبط عناوين IP يدوياً لبعض الأجهزة pc1,pc0 لضمان ثبات العناوين وعدم تغيرها.

هذا الإجراء ضروري للخوادم لضمان وصول الأجهزة الأخرى إليها عبر عنوان ثابت ومحدد.

التوزيع التلقائي (DHCP)

تم تفعيل خدمة DHCP لتخصيص العناوين للأجهزة تلقائياً، مما يسهل عملية الإدارة ويقلل الأخطاء.

هذه هي التفاصيل الأساسية التي اعتمدت عليها في ربط الأجهزة ببعضها البعض داخل الشبكة.

نماذج تطبيقية

جهاز PC0: تم ضبطه ليستلم عنوان IP الخاص به عبر DHCP من السيرفر

الخادم: تم ضبطه بعنوان IP يدوي ثابت لضمان استمرارية الخدمات.

التوجيه بين الـ VLANs

أهمية التوجيه

لتمكين التواصل بين الـ VLANs المختلفة، قمت بتفعيل التوجيه (Routing). ساهمت هذه الخطوة في ربط الشبكة بالكامل بشكل متسق ومنظم رغم العزل المنطقي.

Router-on-a-Stick

طبقتها على الراوتر (Router0) لتمكين التوجيه بين الـ VLANs المرتبطة بالسويتش العادي عبر منفذ فيزيائي واحد مقسم منطقياً.

استخدمت Sub-interfaces لكل VLAN.

Layer 3 Switching

استخدمت السويتشات متعددة الطبقات لضمان توجيه أسرع ومباشر داخل السويتش نفسه دون الحاجة للرجوع إلى الراوتر في كل عملية.

اعتمدت على واجهات SVI للسرعة.

خدمة الـ DHCP في الشبكة

الراوتر (Router0)

الراوتر مسؤول عن:

- إدارة عناوين قسم تقنية المعلومات.
- توفير البوابة الافتراضية تلقائياً.

السويتش (Switch0)

استخدمت قدرات السويتش متعدد الطبقات لتوزيع العناوين داخلياً:

- إدارة عناوين قسم المالية.
- تقليل حركة البيانات الموجهة للراوتر.

الخادم (Server0)

الخادم مخصص لتوزيع العناوين لشبكة الخوادم والأجهزة المرتبطة بها:

- توزيع العناوين لـ VLAN 200.
- ضمان استقرار توزيع العناوين.
- سهولة مراقبة الأجهزة المتصلة.

حماية الشبكة (NAT & ACL)

خدمة الـ NAT

تم تفعيل NAT على الراوتر لتحويل العناوين الداخلية إلى عناوين عامة عند الخروج للإنترنت.

- إخفاء تفاصيل البنية التحتية للشبكة.
- توفير استهلاك عناوين IP العامة.
- توفير طبقة حماية إضافية من الخارج.

قوائم الـ ACL

طبقت قوائم التحكم بالوصول (ACLs) لتحديد الصلاحيات ومنع الوصول غير المصرح به للأقسام.

- منع الوصول غير المصرح به تقنياً.
- تصفية حركة البيانات (Traffic Filtering).
- تأمين الخوادم والبيانات الحساسة.

الـ VPN الآمن

تم إعداد VPN لتوفير اتصال آمن ومشفر للمستخدمين المصرح لهم من خارج الشبكة.

- تشفير كامل لكافة البيانات المنقولة.
- اتصال آمن عبر شبكة الإنترنت العامة.
- ضمان خصوصية وسلامة البيانات.

بروتوكول ARP

العنصر الأساسي

يعتبر بروتوكول ARP المسؤول الأول عن ربط عناوين IP المنطقية بعناوين MAC الفيزيائية داخل الشبكة المحلية.

بدون هذا البروتوكول، لا يمكن للأجهزة التعرف على مواقع بعضها البعض داخل بيئة Ethernet حتى في نفس الـ VLAN.

آلية العمل

يقوم البروتوكول بعملية مطابقة (Mapping) دقيقة بين العناوين:

IP Address
↓
MAC Address

يكتشف عنوان MAC للجهاز المستهدف لضمان وصول البيانات بدقة تامة.

الأهمية في المشروع

حرصت على تفعيل بروتوكول ARP بشكل صحيح لضمان توجيه البيانات إلى الجهاز المستهدف بدقة وبدون تأخير.

هو البروتوكول التأسيسي الذي يمهد الطريق لعمل كافة الخدمات الأخرى مثل DHCP و NAT.

تأمين الـ VLANs ضد الهجمات

التهديدات الأمنية

تم التركيز بشكل مكثف على الحماية من هجمات VLAN Hopping و Double Tagging التي قد تمنح المهاجم وصولاً غير مصرح به للشبكات الأخرى.

الإجراءات الوقائية

تم تعطيل خاصية التفاوض التلقائي (DTP) وضبط كافة منافذ المستخدمين على وضع الوصول (Access Mode) الصريح.

```
switchport mode access
switchport nonegotiate
```

عزل الـ Native VLAN

تغيير الـ Native VLAN إلى 999 (BLACKHOLE) لمنع محاولات الاختراق عبر التلاعب بالـ Tagging وضمان عزلها التام.

```
switchport trunk native vlan 999
```

التحقق من الإعدادات

أوامر التحقق

استخدمت مجموعة من الأوامر لفحص الشبكة والتأكد من سلامة التكوين لكافة المنافذ والـ VLANs:

```
show ip int brief #
show vlan brief #
show ip route #
```

استقرار النظام

تمت مراجعة حالة المعالج والذاكرة في الأجهزة الأساسية لضمان عدم وجود أي ضغط ناتج عن الإعدادات الجديدة.

```
show processes cpu #
show memory #
```

تظهر النتائج أن البنية التحتية مهيأة للعمل وفق المعايير المطلوبة.

مراجعة التكوين

تمت مراجعة ملف الإعدادات الجاري (Running Config) للتأكد من عدم وجود تعارض بين الخدمات المطبقة.

```
show running-config #
show ip dhcp binding #
```

كافة الإعدادات موثقة ومستقرة داخل النظام.

الخلاصة والتعلم من المشروع

نتائج المشروع

تم بفضل الله تصميم شبكة متكاملة، آمنة، وفعالة تلبي كافة المتطلبات التقنية التي تم التخطيط لها في البداية.

الشبكة الآن مهيأة للتعامل مع المستخدمين وتأمين بياناتهم وفق أعلى المعايير المتبعة.

الخبرات المكتسبة

اكتسبت من خلال هذا المشروع خبرة عملية في الربط بين العناوين الثابتة والتلقائية وتأمين الشبكات من الثغرات.

أظهر المشروع أهمية التخطيط السليم للـ VLANs والتوجيه في بناء بنية تحتية قوية ومستدامة.

خاتمة

كانت تجربة تقنية ثرية ومفيدة جداً في مجال هندسة الشبكات.

شكراً لحسن استماعكم