الـ VLANs ماهي وكيف يتم إعدادها

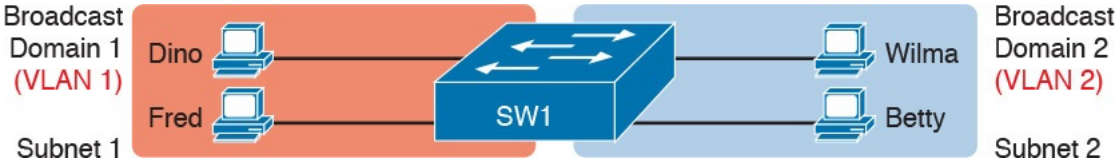
م. هاشم بن مسنور الشريف

عضو هيئة التدريب بالكلية التقنية بحائل

محاضر معتمد لدى أكاديمية سيسكو

من المهم قبل التعرف على الـ VLAN معرفة الـ LAN وفهم المقصود منه، الـ LAN هي الإختصار لـ Local Area Network والتي تعني الشبكة المحلية وعليه فالبعض يعرفها بأنها أجهزة المستخدمين والخوادم (Servers) والـ Switches والـ Routers والكيابل ونقاط الوصول (Access Points) الموجودة في مكان واحد. والبعض الآخر يعرفها بأنها جميع الأجهزة الموجودة في نفس مجال البث (Broadcast domain) والذي يقصد به جميع الأجهزة المرتبطة مع بعضها والتي لو قام أحدها بإرسال رسالة بث سوف تصل لجميع هذه الأجهزة. وجهاز الـ Switch يعتبر أن جميع منافذه موجودة في نفس مجال البث (Broadcast domain) فعندما يصل له رسالة بث يقوم بتمريرها لجميع منافذه وبناءً على هذا عند الرغبة في وجود أكثر من مجال بث واحد في الشبكة المحلية لابد من وجود أكثر من جهاز Switch واحد.

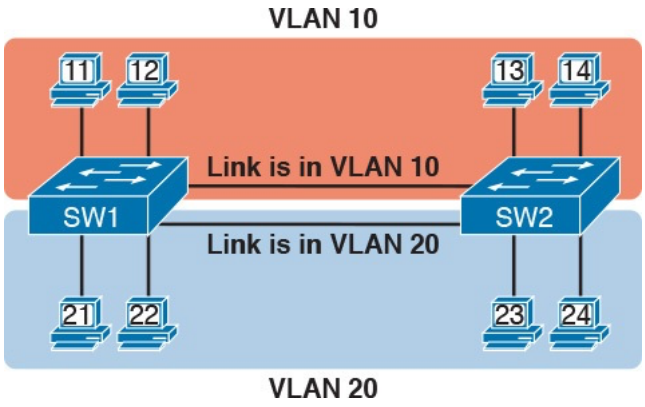
وهنا تأتي أهمية الـ VLAN بحيث أن جهاز Switch واحد يتم تفعيل الـ VLAN عليه سيحقق لنا نفس الهدف المحقق من وجود أكثر من جهاز Switch واحد الشبكة المحلية، بمعنى أنه بالإمكان تحديد بعض منافذ الـ Switch لتكون موجودة على مجال بث واحد وتحديد منافذ أخرى لتكون هي الأخرى موجودة على مجال بث آخر.



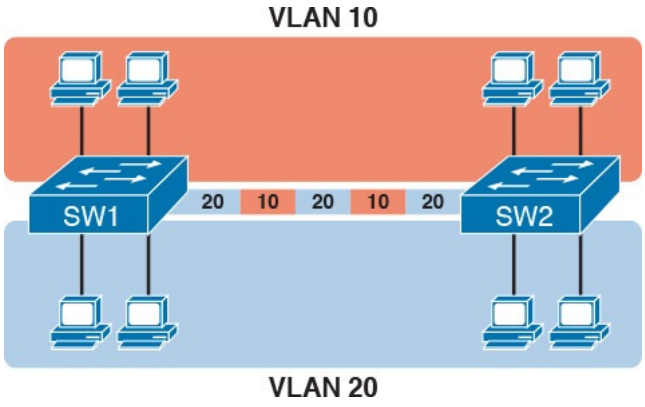
وجود أكثر من مجال بث في الشبكة المحلية مفيد في تقليل عدد الأجهزة في كل مجال بث مما يعني كفاءة أفضل في أداء الشبكة ومفيد كذلك في تأمين الشبكة بحيث لا يستطيع جهاز ما في الشبكة من مراقبة جميع رسائل الشبكة وحركة بياناتها. وهي أيضاً تساعد مهندس الشبكة في تحديد اللوائح والقيود الأمنية الخاصة بكل VLAN بحسب طبيعة العاملين في مجال البث وهذا أيضاً يضيف طبقة حماية للشبكة. كما أنها مفيدة جداً في إطار حل المشاكل بشكل سريع فهي مفيدة في تحديد مكان المشكلة وبالتالي سرعة معالجتها. أخيراً هي تخفف من الجهد الذي يقوم به بروتوكول الـ STP.

إعداد VLANs على جهاز Switch واحد يعتبر سهل جداً فلا يتطلب سوى جهد بسيط لتفعيله حيث إننا باختصار نقوم بإعداد المنافذ وتوزيعها على الـ VLANs المراد إنشاؤها. بينما نحتاج مزيد من الإعدادات بشأن كيفية نقل البيانات عند وجود أكثر من جهاز Switch واحد في الشبكة المحلية. ففي حال وجود أكثر من جهاز Switch في الشبكة المحلية يبرز لنا مصطلح الـ VLAN trunking وهو المعني بنقل البيانات بين جهازي الـ Switch. الـ VLAN trunking هو ما يجعل أجهزة الـ Switch تستخدم إجراء يسمى VLAN tagging والذي يعني باختصار وضع وإضافة ترويسة على الرسالة حتى يستطيع جهاز الـ Switch الآخر معرفة وجهة الرسالة القادمة لأي VLAN تتبع.

لتوضيح فكرة عمل الـ VLAN trunking المثال أدناه يمثل وجود جهازي Switch في كل منها منافذ تتبع لـ VLAN 10 وأخرى تتبع لـ VLAN 20 ويتضح أن الربط بين جهازي الـ Switch تم بأكثر من كبل واحد وذلك لتمكين الأجهزة الموجودة في كل VLAN من التواصل مع نظرائها في جهاز الـ Switch الآخر



هذا الإجراء يؤدي المهمة لكنه غير عملي إذ لو تطلب العمل في الشبكة وجود عدد ٢٠ VLAN فهذا يعني وجود ٢٠ كبل فقط لربط الـ VLANs بين كل Switch و آخر وهنا تأتي أهمية الـ VLAN trunking والذي يمكننا من توصيل أجهزة الـ Switch فيما بينها بكبل واحد فقط مهما كان عدد الـ VLANs الموجودة في الشبكة المحلية والمثال أدناه يوضح الفكرة.

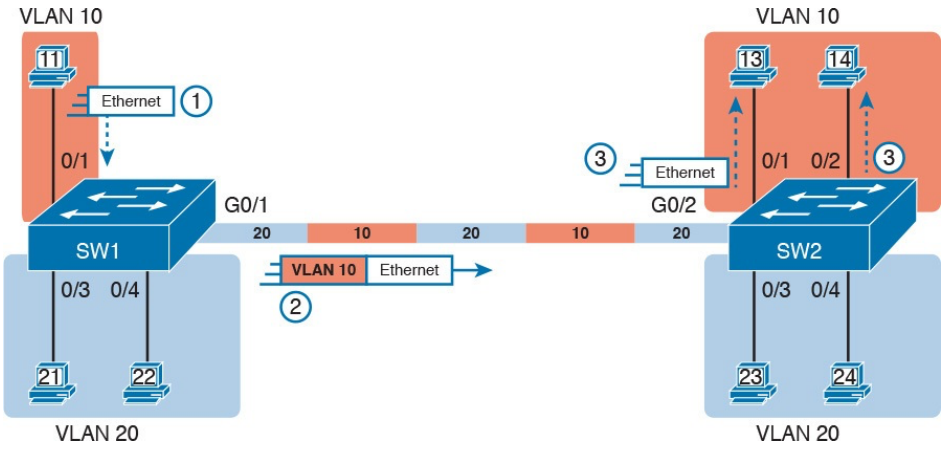


ذُكر سابقاً أن الـ VLAN trunking يدفع أجهزة الـ Switch لاستخدام الـ VLAN tagging وذلك لأجل إيصال الرسائل من أجهزة موجودة في VLAN محدد لنظرائها على جهاز Switch آخر. ففي المثال أدناه يتضح أن الجهاز PC11 قام بإرسال رسالة بث يرغب في وصولها لجميع الأجهزة الموجودة في نفس مجال بثه فالخطوات التي تمت هي:

١- وصول رسالته للمنفذ /1Fa0 والموجود في SW1

٢- يقوم SW1 بتمرير الرسالة الى SW2 وذلك بعد إضافة ترويسة تمكن SW2 من معرفة وجهة الرسالة ولأي VLAN تتبع.

٣- تصل الرسالة لـ SW2 عبر المنفذ /2G0 والتي تتعرف على وجهتها من خلال الترويسة ثم تقوم بإزالة الترويسة وارسالها لـ VLAN 10.

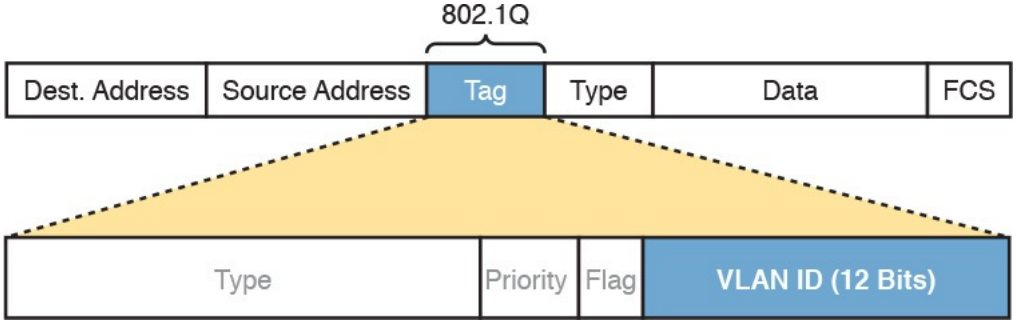


تدعم Cisco بروتوكولين مختلفين من بروتوكولات الـ VLAN trunking هما:

1- Inter-Switch Link (ISL)

2- IEEE 802.1Q

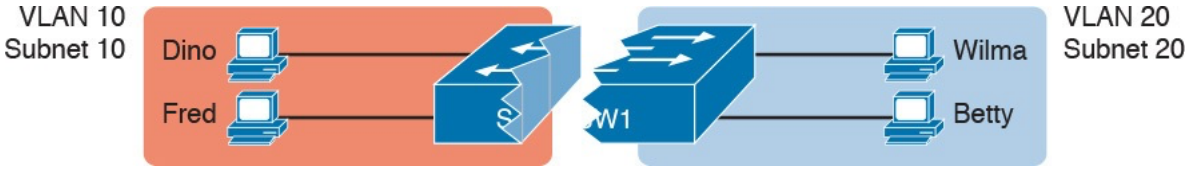
السبب في وجود البروتوكول هو أن الأول قامت Cisco بإنشائه والعمل به على أجهزتها قبل أن تنشئ IEEE بروتوكولها لنفس الهدف. حالياً يعتبر بروتوكول 802.1Q هو الأشهر والأكثر استخداماً حتى أن غالبية أجهزة Cisco من السلسلة التابعة للموديل Catalyst لا تدعم الا هذا المعيار. كلى البروتوكولين يقومان بإضافة الترويسة على الرسالة كما ذكر سابقاً مع وجود بعض الاختلافات في تفاصيل هذه الترويسة.



في حال دعم أجهزة الـ Switches والتابعة لـ Cisco لكلى البروتوكولين فإنه بالإمكان تفعيل خاصية التفاوض بينهما لاختيار أحدهما وهو ما يسمى Dynamic Trunking Protocol (DTP) وفيما عدا ذلك فتقوم الأجهزة باستخدام البروتوكول المدعوم من قبلهما.

نقل البيانات بين الـ VLANs المختلفة:

من الطبيعي في الشبكات المحلية وجود الحاجة لتبادل البيانات بين الـ VLANs المختلفة وأجهزة الـ Layer 2 Switches لا تدعم نقل البيانات بين الـ VLANs المختلفة وهو ما يسمى بالتوجيه (Routing)

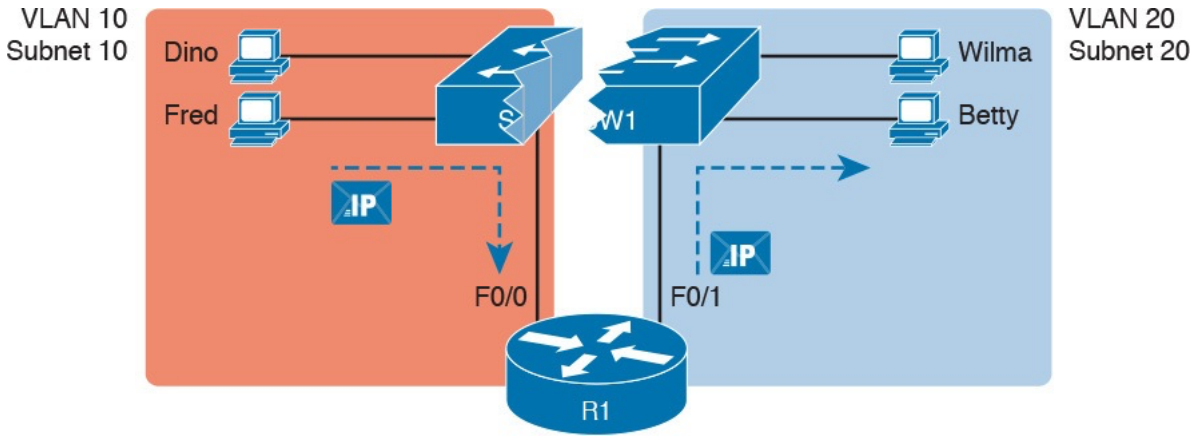


فكما يظهر في الصورة أعلاه عندما يتم إعداد بعض منافذ الـ Layer 2 Switches للتبع مثلاً الـ VLAN 10 وأخرى للتبع الـ VLAN 20 فإن الـ Switch يتصرف وكأنه جهازي Switch مختلفين لكل منهما مجال بثه الخاص ولا يسمح أبداً بنقل البيانات بين الـ VLANs المختلفة فلا يسمح مثلاً بتوصيل الرسالة من Dino لـ

Betty. ولمعالجة هذه المشكلة وتمكين الأجهزة في الـ VLANs المختلفة من التواصل مع بعضهما لابد من استخدام أحد الجهازين:

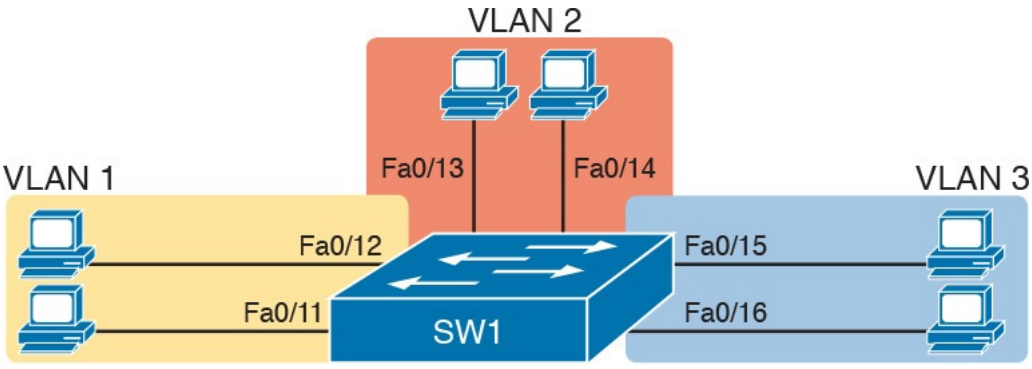
1- Layer 3 Switches (multilayer switches)
2- Router

يقوم الـ Layer 3 Switches بعمل كلاً من الـ Layer 2 Switch والـ Router في نفس الوقت وهذه تعتبر ميزة له إلا أن أسعار هذا النوع من الـ Switches يعتبر الأغلى والأكثر كلفة وأما الحل الثاني فهو استخدام جهاز الـ Router لربط الـ VLANs المختلفة وهذا الحل يتضمن أكثر من سيناريو لتنفيذه فمثلاً من الصورة أدناه تم استخدام منفذين من منافذ الـ Router للربط بين الـ VLANs المختلفة وهناك سيناريو آخر وهو استخدام منفذ واحد فقط في كل من الـ Switch والـ Router وسنذهب الآن مع السيناريو الأول والذي نمثله الصورة للقيام بكامل الإعدادات المطلوبة وذلك لأنه الأسهل لفهم الموضوع ومن ثم يمكن الانتقال للسيناريوهات الأخرى.



أمثلة لتوضيح آلية الإعداد:

المثال الأول: سنقوم هنا بإعداد وتعريف الـ VLANs على جهاز الـ Switch الموجود وكما يظهر من الصورة فهناك ثلاثة VLANs وموضح أرقامها وأرقام المنافذ المرتبطة بها



من المهم في البداية تذكر أن الوضع الافتراضي لأي Switch هو وجود VLAN ترتبط به جميع منافذ الجهاز وهذا VLAN يكون رقمه بشكل افتراضي VLAN1 ويكون أسمه default. وعند الدخول على نظام التشغيل لهذا الجهاز وكتابة الأمر show vlan brief لاستعراض الـ VLANs الموجودة على الجهاز يظهر التالي:

```
SW1# show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

يوجد VLAN واحد ترتبط به جميع منافذ الجهاز وهذا هو الوضع الافتراضي الذي تكون عليه جميع الأجهزة، وعليه يتم بدأ الإعداد للـ VLAN2

```
SW1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)# vlan 2
SW1(config-vlan)# name Freds-vlan
SW1(config-vlan)# exit
```

تم الدخول على وضع الاعداد العام ثم كتابة vlan 2 للدخول على وضع الاعداد الخاص به و من ثم إعطاؤه الاسم المناسب والذي يختلف بحسب طبيعة الشبكة الافتراضية المحلية والتي يجب أن تعكس الغاية والمقصود من وجوده.

```
SW1(config)# interface range fastethernet 0/13 - 14
SW1(config-if)# switchport access vlan 2
SW1(config-if)# switchport mode access
SW1(config-if)# end
```

بعد الخروج من وضع أعداد الـ VLAN تم الدخول على الوضع الخاص لإعداد المنافذ التي يراد إسنادها للـ VLAN2 وهي في مثالنا هذا Fa0/13 و Fa0/14 ونجدر الإشارة أنه بالإمكان الدخول على المنافذ بشكل فردي وبالإمكان كذلك اختيار نطاق المنافذ والتي يراد إجراء الإعدادات لها وما تم هنا هو الخيار الثاني، وبعد الدخول على وضع الإعداد الخاص بالمنفذين يتم إسنادهما للـ VLAN2 عن طريق الأمر switchport access vlan 2 والأمر الذي يليه هو أمر اختياري ولكنه مهم جداً لأسباب أمنية تخص الشبكة سنتطرق لها لاحقاً ويقصد به بقاء المنفذ على الخيار access وعدم الانتقال للخيار trunk.

```
SW1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gi0/1, Gi0/2
2    Freds-vlan                        active    Fa0/13, Fa0/14
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

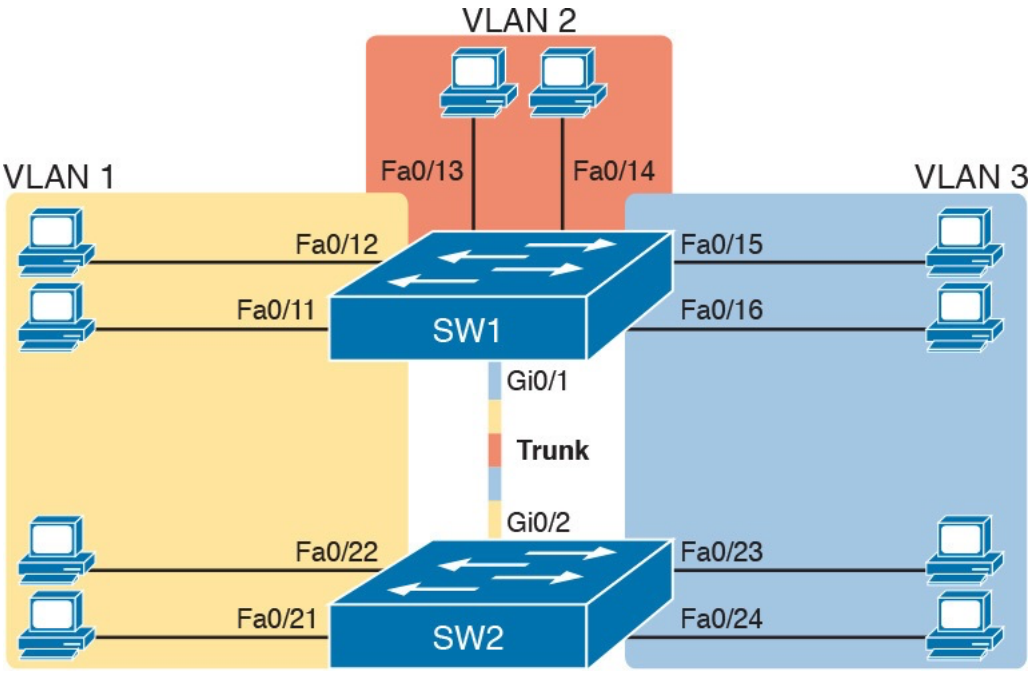
بعد إعادة الأمر show vlan brief كما هو موضح أعلاه يظهر أنه تم إنشاء الـ VLAN2 ويظهر كذلك الاسم الذي تم إعطاؤه له والمنافذ المسندة اليه. من الجدير بالذكر أن خطوات إعداد الـ vlan هي خطوات متتابعة بشكل منطقي إلا أن جهاز الـ Switch يقوم بشكل آلي بإنشاء VLAN في حال تمت إضافة وإسناد منافذ معينة لـ vlan غير موجود كما هو واضح من المثال أدناه مع المنفذين Fa0/15 و Fa0/16

```
SW1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)# interface range Fastethernet 0/15 - 16
SW1(config-if-range)# switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SW1(config-if-range)# ^Z

SW1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
2    Freds-vlan                        active    Fa0/13, Fa0/14
3    VLAN0003                          active    Fa0/15, Fa0/16
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

المثال الثاني: الإعداد الكلي للـ VLANs وذلك على جهازي Switch وكما يظهر من الصورة أدناه سيكون الربط بين جهازي الـ Switch بنظام الـ VLAN Trunking والمطلوب هو إعداد ثلاثة VLANs وموضح أرقامها وأرقام المنافذ المرتبطة بها.



بالنسبة لـ SW1 فقد تم إعداد الـ VLANs له في المثال الأول، ولأجل عدم التكرار سيكون إعداد الـ VLANs للـ SW2 بنفس الطريقة التي تمت في المثال السابق مع مراعاة تعريف VLAN1 و VLAN3 فقط، أما الجديد في هذا المثال فهو آلية وكيفية ربط جهازي الـ Switch ببعضهما

```
SW1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)# interface gigabit 0/1
SW1(config-if)# switchport mode dynamic desirable
SW1(config-if)# ^Z
SW1#
```

استخدام الأمر switchport mode dynamic desirable يمكن جهازي الـ Switch من بدء التفاوض بينهما حول البروتوكول المستخدم في نقل البيانات.

```
SW1# show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

وعند إدخال الأمر show interface gigabit 0/1 switchport يظهر أنه تم التفاوض وتم الإتفاق على mode trunk وكذلك على البروتوكول 802.1Q.

يوجد أكثر من أمر عند إجراء إعدادات الـ VLAN Trunking وهي:

- **switchport mode access**

يقوم بضبط المنفذ ليكون على الوضع access فقط

- **switchport mode dynamic auto**

يجعل المنفذ قادر على التحول والتغيير ليصبح على الوضع trunk وذلك في حال كون منافذ الأجهزة الأخرى معدة على الأوضاع trunk أو desirable

- **switchport mode trunk**

يقوم بضبط المنفذ على الوضع trunk ويكون قادر على التفاوض مع الجهاز الآخر لتحويله للوضع trunk

- **switchport mode dynamic desirable**

يجعل المنفذ يحاول بشكل نشط للتحول للوضع trunk ويتم ذلك في حال اذا كانت منافذ الأجهزة المجاورة الأخرى معدة على الأوضاع trunk أو desirable أو auto

- **switchport mode nonegotiate**

يمنع المنفذ من التفاوض أبداً ويستخدم فقط عندما يكون المنفذ على أحد الوضعين access أو trunk

الجدول أدناه يوضح كيف سيكون فعلياً طريقة نقل البيانات بناءً على إعدادات جهازي الـ Switch:

الوضع الإداري	access	dynamic auto	trunk	dynamic desirable
access	access	access	Do Not Use[1]	access
dynamic auto	access	access	trunk	trunk
trunk	Do Not Use[1]	trunk	trunk	trunk
dynamic desirable	access	trunk	trunk	trunk

[1] عندما يكون جهازي الـ Switch أحدهما معد ليكون access والآخر trunk نحدث إشكالية لذا يجب تجنبها

خطوات استكشاف وإصلاح الأخطاء في الـ VLANs:

١. التأكد من كون الـ VLAN معرف ويعمل على جهاز الـ Switch ويتم ذلك ببساطة عن طريق الأمر show vlan brief حيث ستظهر جميع الـ VLANs وأمام كل منها أحد الحالتين active أو act/lshut وتعني الأخيرة منهما إيقاف الـ VLAN ولتشغيله يستخدم الأمر no shutdown بعد الدخول على وضع الاعداد الخاص للـ VLAN المقصود كما هو موضح أدناه

```
SW2# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
10   VLAN0010                         act/lshut Fa0/13
20   VLAN0020                         active
30   VLAN0030                         act/lshut
40   VLAN0040                         active
SW2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)# no shutdown vlan 10
SW2(config)# shutdown vlan 20
SW2(config)# vlan 30
SW2(config-vlan)# no shutdown
SW2(config-vlan)# vlan 40
SW2(config-vlan)# shutdown
SW2(config-vlan)#
```

٢. تأكد من قوائم الـ VLANs المفعلة على كلى منافذ أجهزة الـ Switch والتي تعمل على الوضع trunk وأنها معدة بشكل صحيح لأن هناك حالات تتعطل فيها إمكانية نقل البيانات وهي التي يكون فيها كلى الطرفين على غير وضع الـ trunk أو أحدهما على الأقل على غير وضع الـ trunk. والأمر الذي يوضح ذلك هو show interface *portnumber* switchport كما هو موضح أدناه

```
SW2# show interfaces gigabit0/2 switchport
Name: Gi0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
```

وجود الوضع على static access يسبب خلل في هذه الحالة والمفترض أن يكون trunking.

ملاحظات هامة:

١. **تعطيل خاصية الـ (DTP):** لدواعي أمنية يفضل تعطيل خاصية التفاوض بشأن الـ VLAN Trunking في غالبية المنافذ وذلك لأن معظم منافذ الـ Switch تكون مرتبطة بأجهزة كمبيوتر والتي تحتاج فقط أن تكون على الوضع access والتي يتم إعدادها عن طريق الأمر switchport mode access وهذا الأمر يعطل تلقائياً خاصية التفاوض (DTP) بينما المنافذ التي تم إعدادها لتكون الى الوضع trunk عن طريق الأمر switchport mode trunk فإن خاصية التفاوض (DTP) فيها تبقى مفعلة لذا يفضل تعطيلها عن طريق الأمر switchport nonegotiate والذي يتم تنفيذه على نفس وضع الاعداد الخاص بالمنفذ.

٢. **من المهم التعرف على الـ VLAN Trunking Protocol (VTP):** تعتبر أحد أدوات Cisco المتميزة والتي تمكن أجهزة الـ Switch والموجودة في نفس الشبكة المحلية من تبادل نفس إعدادات الـ VLANs فبدلاً من إجراء الإعدادات على جميع أجهزة الـ Switches يكفي القيام بها على أحدها وهو يقوم بتوزيعها على البقية. وهذا يعني أنه لابد أن يكون أحد هذه الـ Switches هو المسؤول عن ذلك ويسمى (server Switch) وفيه يتم إنشاء وإعداد الـ VLANs والبقية تسمى (client Switches) وهي لا تملك صلاحية إعداد أي VLAN.

٣. **VLAN hopping:** كما هو معروف أن الوضع الافتراضي لكل Switch هو وجود جميع المنافذ الخاصة به على الـ VLAN1 وهو ما يسمى Native VLAN. يمكن تغييره وإعطاؤه أي رقم آخر ولكن من المهم مراعاة ذلك عند وضع الـ trunking لأن هذا قد يسبب مشكلة تسمى الـ VLAN hopping وفكرتها عندما يرسل SW1 رسالة تابعة لـ VLAN1 والي تمثل في حالته الـ Native VLAN الى SW2 والذي قام بتغيير الـ Native VLAN له وجعلها مثلاً VLAN2 فعندما يستلم الـ SW2 الرسالة ولا يجد فيها ترويسة الـ 802.1Q سيفترض أنها تتبع الـ Native VLAN خاصته ومن ثم يرسلها للـ VLAN2 في حين أن المفترض أنها تخص الـ VLAN1 وهذا ما يسمى بالـ VLAN hopping.