الخبرة العملية لاحتراف أوامر

CISCO

CCNA & CCNP

By

Eng. Mohamed Omar

الكورس العملي لإحتراف أوامر سيسكو

General Commands

الدخول على المود	Sw#En
الدخول على configuration mode	Sw#Conf t Sw(config)#
للرجوع للمود السابق للتراجع خطوة للخلف للتراجع لأول المود	Sw#Ctrl + Z Sw#exit Sw#end
لرؤية فرجن الروتر	Sw#Sh version Sw#Sh flash
لرؤية switch configuration	Sw#sh run
لمشاهدة الوقت والتاريخ	Sw#Sh clock
لضبط الوقت	Sw#Clock set time day month year Sw#Clock set 11:10:30 1 Feb 2002

لتسجيل الأوامر المخزنة في الـ run والتي لم يتم حفظها نهائيا على الروتر إلى الروتر فعليا	Sw#Copy run start or Sw#wr
لرؤية البورتات على الروتر	Sw# Sh ip int brief
لرؤية port configuration	Sw#sh run int fa 0/23
لإغلاق بورت معين	Sw(config)#int fa 0/23 Sw(config-if)#shut
لفتح بورت مغلق	Sw(config)#int fa 0/23 Sw(config-if)#no shut
لفتح مجموعة بورتات مرة واحدة	Sw#conf t Sw(config)#int range fa 0/1 - 24 Sw(config-if)#no shut
لعمل رستارت للروتر او السويتش	SW#reload
لإعطاء السويتش IP للوصول إليه عن طريق الـ Telnet	Sw(config)#int vlan 1 Sw(config-if)#ip address 10.0.0.1 255.255.255.0 Sw(config-if)#no shut
لإعطاء السويتش أسم جديد	SW(config)#hostname SVS-Switch

SW1#sh mac-address-table	لعرض جميع ماكات الأجهزة على السويتش MAC-Table
SW1#sh mac-address-table address 000.221c.00.sddd	للبحث عن جهاز على السويتش من خلال الـ MAC address
SW#traceroute mac 1200156a25e1 0012544se554se	للبحث عن جهازين على السويتش من خلال ماك أدريس
SW#traceroute mac ip 10.1.2.10 details	للبحث عن جهاز من خلال الـ IP
SW1#sh mac-address-table int fa 1/21	لرؤية من هو الماك المتصل بهذا البورت
SW1#sh mac-address-table vlan 2	لرؤية كل الناس المتصلة بالفيلان 2
SW1#sh mac-address-table count	لعد كم جهاز على الفيلان
SW1#clear mac-address-table dynamic	لمسح الماك ادرس تابل
SW1#clear mac-address-table dynamic int fa 1/12	لمسح ماك ادرس بعينة على بورت معين
SW1#clear mac-address-table dynamic vlan 2	لمسح الماك ادرس على كل الفيلان
Sw1(config)#mac-address-table aging-time 600	مدة الاحتفاظ بالماك ادرس 300 ثانية وهذا امر تغيير هذا الوقت
Sw1(config)#mac-address-table static FC-4D-D4-53-D2-E4 vlan 2 interface fa 1/15	أمر إعطاء السويتش الماك ادرس بتاع جهاز معين وفي أي فيلان وعلى أي بورت لعدم مسحه نهائاً
Sw1(config)#no mac-address-table static FC-4D-D4-53-D2-E4 vlan 2 interface fa 1/15	إعادة وضع الماك ادرس اللي دخلته static إلى dynamic مرة أخرى
Sw1(config)#default int fa 0/23	لإسترجاع البورت إلى وضعه الرئيسي

لرؤية اللوج على السويتش مرئية	Sw#ter mon
تغيير الـ speed على البورت	Sw1(config)#Int gi 1/0/36 Sw1(config)#Speed 10 Sw1(config)#Duplex auto
لإعادة السويتش إلى Default Factory	Sw1(config)#erase startup-config Sw1(config)#reload
لتفعيل الـ Logging	Sw1(config)#Conf t Sw1(config)#Logging monitor debugging Sw1(config)#Logging on Sw1(config)#Exit Sw1(config)#Terminal monitor

Password Configuration

SW #conf t SW(config)#line console 0 SW(config-line)#login SW(config-line)#password $M@rt SW(config-line)#exit	لعمل Consol Password
SW(config-line)#line vty 0 ? <1-871> last line number SW(config-line)#line vty 0 871 SW(config-line)#login SW(config-line)#password $M@rt	لعمل Telnet Password
SW#conf t SW(config)#enable password V	لعمل privilege mode password غير مشفرة
SW#conf t SW(config)#enable secret $M@rt	عمل privilege mode password مشفرة ويجد ألا تكون مشابهة للباص ورد الغير مشفرة في حالة الانتقال من user mode إلى Privilege mode

تكون الباص ورد المشفرة هي الأقوى في الاستخدام	Sw(config)#Exit
لإلغاء الـ Password	SW(config-line)#no password
للدخول على السويتش في حالة نسيان Password أي عن طريقة عمل Password Recovery	**Recovery password on switch** نقوم بغلق وتشغيل السويتش و الضغط على ذر mod لحد ما يعطي switch: - Switch: flash_init تعني حمل الفلاش - لرؤية الفلاش الموجود - Switch: dir flash: - لو السويتش مش عليه معلومات هامة يمكن حذف ملف config.text - لو عليه معلومات هامة غير اسمه فيقوم السويتش من غير تحميل هذا الملف اللي فيه الباسورد - ولتغير اسم هذا الملف - Switch:rename flash:config.text flash:thm - Switch:boot - After restarting - نقوم بجعل الفلاش يستخدم الـ thm كونفجراشن - Switch#copy thm run - بعد ذلك نقوم بعمل باسورد جديدة - Conf t - Enable secret Cisco **Recovery password on Router**

- **Reboot the router and** press the Break key (Alt + Break)
- **Type** confreg 0x2142
- **Type** reset **to reboot the router**
- **Type** copy start run
- **type a** show run config
- **Change the enable secret - "**enable secret new_password**"**
- **Change the register back to 0x2102:** config-register 0x2102
- **When the router reboots it will load the old configuration with the new password.**

Save the password so that it will be persistent during reboots, type copy run start

Reboot the router by typing reload **at the enable prompt.**

VLAN Configuration

لرؤية الـ **Vlans** الموجودة على السويتش	**Sw#sh vlan**
لرؤية كل البورتات اللي على فيلان معينة	**Sw#sh vlan id 2** حيث 2 هي رقم الفيلان
لرؤية ملخص عن كل الفيلان المتواجدة	**Sw#sh vlan brief**
لعمل **VLAN** جديدة	**SW#vlan d** **Sw(vlan)#vlan 2 name SVS-Vlan2** **Sw(vlan)#exit** للخروج **Or** **Sw#conf t** **SW(config)#vlan 3** **SW(config-vlan)#name SVS-vlan3**

لعمل VLAN جديدة بـ default name والتي ستصبح VLAN0004	Sw#conf t SW(config)#vlan 4 SW(config-vlan)#end
لعمل تعديل في VLAN بعد إنشاءها مثل تغيير الأسم سيتم تغيير اسم Vlan2 إلى Sales	Sw#conf t Sw(config)#vlan 2 Sw(config-vlan)#name Sales Sw(config-vlan)#exit
لإضافة Port واحد إلى Vlan2	Sw#conf t Sw(config)#int fa 0/1 Sw(config-if)#switchport mode access Sw(config-if)#switchport access vlan 2 Sw(config-if)#no shut

Sw(config)#int range fa 0/1 – 0/24 Sw(config-if)#switchport mode access Sw(config-if-range)#switchport access vlan 2 Sw(config-if-range)#no shut	لإضافة مجموعة Ports إلى Vlan2
Sw(config)#int vlan 2 Sw(config-if)#ip address 10.0.2.1 255.255.255.0 Sw(config-if)#no shut	لإعطاء الفيلان interface IP Address وهو بمسابة الـ Gateway للفيلان
Sw(config)#no vlan 2	لمسح Vlan
Sw(config)#ip routing Sw(config)#ip default gateway 10.1.1.1	لتفعيل الـ Routing بين كل الـ VLANs حيث 10.1.1.1 هو Core Switch IP

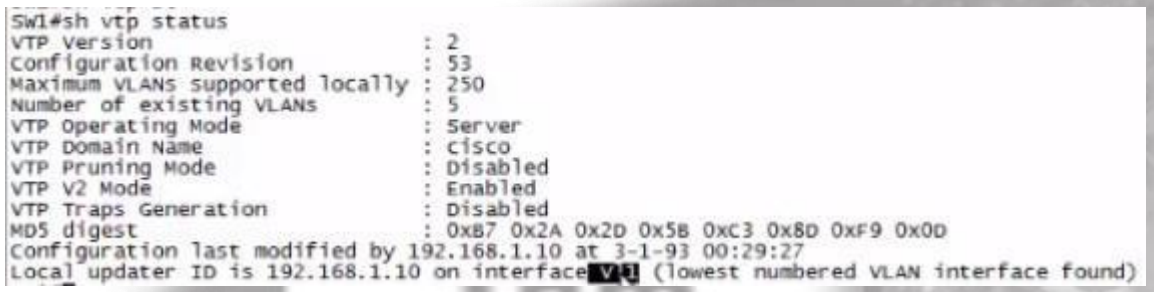
VTP Configuration

المسئول عن إنشاء الفيلانات بشكل أوتوماتيك على السويتشات الأخرى وله ثلاثة أشكال

Server , Client , Transparent

- Switch# **show vtp status**
- Switch(config)# **vtp version {1 | 2 | 3}**
- Switch(config)# **vtp domain** *domain-name*
- Switch(config)# **vtp mode {server | client | transparent | off}**
- Switch(config)# **vtp password** *password* **[hidden | secret]**

ملحوظة : يجب جعل الكور سويتش VTP mode Server وباقي السويتشات VTP mode client

لرؤية الـ **VTP** وخصائصه على السويتش	**SW#sh vtp status** 
لتغيير الـ **VTP** على السويتش من **server** إلى **Client** أو **transparent**	**Sw#conf t** **Sw(config)#vtp mode server** **Sw(config)#vtp mode client** **Sw(config)#vtp mode transparent** **Or** **Sw#vlan d** **Sw(vlan)#vtp server** **Sw(vlan)#exit**

```
SW1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 53
Maximum VLANs supported locally : 250
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB7 0x2A 0x2D 0x5B 0xC3 0x8D 0xF9 0x0D
Configuration last modified by 192.168.1.10 at 3-1-93 00:29:27
Local updater ID is 192.168.1.10 on interface Vl1 (lowest numbered VLAN interface found)
```

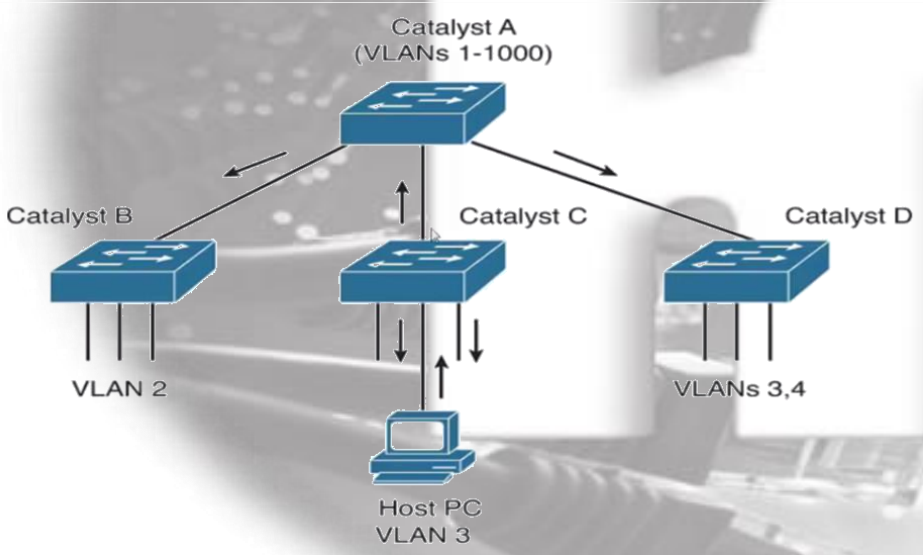
الفرق بين أنواع الـ VTP	**Server :** Create , Modify , Delete , Send / forward Advertisement to another server, Sync **Transparent :** Create , Modify , Delete Locally , forward to client , Can't sync but send Adv. **Client :** Can't Create , Modify , delete , Can sync **Off :** Not sync , not vtp relay
ادخال ال Vlan على الـ Domain	SW1#vlan database SW1(vlan)#vtp domain SVS SW1(vlan)#exit SW1#sh vtp status

ملحوظة : عند شراء سويتش مستعمل يجب أن نعيد VTP Configuration Revision = 0 وذلك لإلغاء كل الفيلان المتواجدة وذلك بجعل السويتش **transparent** فيصبح **0= Configuration Revision**

VTP Prunning

يستخدم لمنع وصول ترافيك إلى فيلان ليس لها بورت على السويتش وذلك لتقليل الهدك على السويتش

بمعنى لو جهاز في فيلان 3 ترسل باكت لجهاز في فيلان 3 على سويتش آخرى لن يتم ارسال هذه الباكت إلى السويتش الغير متصل بأي جهاز في هذه الفيلان وذلك لتوفير الباندويتس والترافيك على السويتش



Enabling VTP Pruning

- Switch(config)# **vtp pruning**
- Switch(config)# **interface** *type member/module/number*
- Switch(config-if)# **switchport trunk pruning vlan** {{{**add** | **except** | **remove**}*vlan-list*} | **none**}

Sw#sh vtp status	لرؤية عمل الـ **vtp pruning**

Trunk Configuration

لعمل بورت Trunk	**Sw1#conf t** **Sw1(config)# int fa 0/23** **Sw1(config-if)# switchport mode trunk** **Sw1(config)# switchport trunk encapsulation dot1q** **Sw1(config)# exit** يتم تنفيذ نفس الخطوات على السويتش الآخر لنفس البورت
لعمل مجموعة بورتات Trunk	**Sw1# conf t** **Sw1(config)# int range fa 0/23 – 24** **Sw1(config)# switchport mode trunk** **Sw1(config)# switchport trunk encapsulation dot1q** يتم تنفيذ نفس الخطوات على السويتش الآخر لنفس البورتات
لعدم ارسال رسالة dtp **بين الترنكين كل 3 ثواني** **Dtp=dynamic trunk protocol**	**Sw# conf t** **Sw# switchport negotiate**

لجعل الترنك native vlan	Sw#switchport trunk native vlan 3
جعل الـ trunk يسمح لعدد معين من الفيلان لرؤية بعضها وحجب البعض الآخر ملحوظة : يجب السماح فقط للفيلان المتواجد فقط على السويتش وليس كل الفيلان المتواجدة على جميع السويتشات	Sw1#conf t Sw1(config)#int fa 0/23 Sw1(config)#switchport trunk allowed vlan 1-9 Or Sw1(config)#switchport trunk allowed vlan 2-4,7 من غير مسافة
لإضافة كل الـ VLANs ما عدا Vlan واحدة	Sw1#conf t Sw1(config)#int fa 0/23 Sw1(config)#switchport trunk allowed vlan except 1 بمعني ضيف كل الفيلان ما عدا فيلان 1
لإضافة فيلان مع الـ trunk للسماح لها بالدخول مع المجموعة السابقة	Sw1#conf t Sw1(config)#int fa 0/23 Sw1(config)#switchport trunk allowed vlan add 1
لإلغاء فيلان من الـ trunk لعدم السماح لها بالدخول مع المجموعة السابقة	Sw1#conf t Sw1(config)#int fa 0/23 Sw1(config)#switchport trunk allowed vlan remove 5

لتشغيل البورت وجعله حسب الطرف الثاني المتصل به بمعني أن السويتش يجعل البورت ترنك إن كان الطرف الثاني ترنك أو جعله mode access عادي إن كان متصل بجهاز ملحوظة : يجب أن يكون على الأقل طرف واحد desirable أما إن كان الطرفان auto فلن يعمل	Sw1#conf t Sw1(config)#int fa 0/23 Sw1(config)#switchport mode dynamic desirable يتم تنفيذ هذه الخطوة على سويتش واحد والطرف الآخر حسب استخدامة إما Trunk or mode access
يجب الأخذ في الاعتبار عن جعل السويتش Trunk Dynamic	SW1 / SW2 / mode Trunk Desirable / Desirable / work Desirable / Auto / work Auto / Desirable / work Auto / Auto / not work
لرؤية الـ trunk بين السويتشات	Sw#show int trunk
لرؤية الـ trunk على البورت والفيلان المسموح بها	Sw#show int fa 0/23 trunk
للتأكيد أن البورت اصبح ترنك	Sw#sh int fa 1/24 switchport
لمشاهدة السويتشات والأجهزة بموديل سيسكو أو hp المرتبطة بهذا السويتش	Sw#Sh cdp neighbor Sw#Sh cdp ne detail

سواء كانت راوترات سويتشات ، تليفونات ، أكسس بوينت	**Sw#no cdp enable** لإلغائه على بورت معينه **SW#sh cdp** لمعرفة إن كان مفعل أم لا **Sw# cdp run** لتفعيله
هناك بروتوكول يسمى **LLDP** يقوم هو الآخر باكتشاف الاجهزة المرتبطة بالسويتش أيا كانت سيسكو أو غيرها ولكنه **disabled by default** ولهذا يجب تفعليه	**SW# lldp run** لتفعيله على كل البورتات **SW(config-if)# lldp transmit** لتفعيله على بورت معين وهنا يقوم بإرسال معلومات عن نفسه **SW(config-if) # lldp receive** لتفعيله على البورت وهنا يقوم باستقبال معلومات من الغير ولا يعطي معلومات عن نفسه **SW#sh lldp ne** **SW#sh lldp ne detail**

DTP Combinations

Administrative Mode	Auto	Desirable	Trunk (on)	Access (off)	Non-Negotiate (access)	Non-Negotiate (trunk)
Auto	Static access (NT)	Trunk	Trunk	Static access	Static access	Unexpected Results
Desirable	Trunk	Trunk	Trunk	Static access	Static access	Unexpected Results
Trunk (on)	Trunk	Trunk	Trunk	Unexpected Results	Unexpected Results	Trunk
Access (off)	Static access	Static access	Unexpected Results	Static access	Static access	Unexpected Results
Non-Negotiate (access)	Static access	Static access	Unexpected Results	Static access	Static access	Unexpected Results
Non-Negotiate (trunk)	Unexpected Results	Unexpected Results	Trunk	Unexpected Results	Unexpected Results	Trunk

Link Aggregation

- هو عبارة ربط سويتشين ببعض عن طريق عدة كابلات وجعلهم كأنهم كابل واحد وذلك بعمل channel-group
- هناك ثلاثة أنواع On , PAGP , LACP
- لا يحبذ استخدام الـ mode on مع الـ Fastethernet بل يفضل استخدام واحد من البروتوكولين الآخرين وذلك لتفادي بعض المشاكل
- ملحوظة : يستخدم بروتوكول PAgP مع سويتشات سيسكوا فقط أما LACP فهو Standard Protocol أي يستخدم على أي سويتش آخر ولهذا يفضل استخدام الـ LACP كبروتوكول لكل السويتشات

لعمل Mode ON	
	Sw1(config)#int fa 0/23 Sw1(config-if)#channel-group 1 mode on Sw1(config)#int fa 0/24 Sw1(config-if)#channel-group 1 mode on ############ على السويتش الآخر Sw2(config)#int fa 0/23 Sw2(config-if)#channel-group 1 mode on Sw2(config)#int fa 0/24 Sw2(config-if)#channel-group 1 mode on

لرؤية عمل الـ **configuration** صح	**Sw1#sh etherchannel summary**
لإلغاء الـ **Channel-Group ON**	**Sw1(config)#int fa 0/23** **Sw1(config-if)#no channel-group 1 mode on**
لإلغاء الـ **Port-Channel** نهائيا	**Sw1(config-if)#no int port-channel 1**
لرؤية إن كان موجود الـ **Port-Channel**	**Sw1#sh run int port-channel 1**
لإسترجاع البورت إلى وضعه الرئيسي	**Sw1(config)#default int fa 0/23**
لالغاء الـ **channel group** وهذا الأمر يقوم بالغاء الشانيل جروب وعودة **SPANNING TREE PORT FAST**	**Sw1#conf t** **Sw1(config)#int fa 0/23** **Sw1(config-if)#switchport host** **Sw1(config-if)#exit**

PAGP Link Aggregation

```
Sw1(config)#int  fa 0/23
Sw1(config-if)#channel-protocol pagp
Sw1 (config-if)#channel-group 1 mode desirable
```
يعني المسئول عن ارسال الباكت

```
Sw1(config)#int  fa 0/24
Sw1(config-if)#channel-protocol pagp
Sw1(config-if)#channel-group 1 mode desirable
##########################
```
على السويتش الآخر

```
Sw2(config)#int  fa 0/23
Sw2(config-if)#channel-protocol pagp
Sw2(config-if)#channel-group 1 mode auto
```
يعني المسئول عن استقبال الباكت

```
Sw2(config)#int  fa 0/24
Sw2(config-if)#channel-protocol pagp
Sw2(config-if)#channel-group 1 mode auto
```

`Sw1(config)#int  fa 0/23` `Sw1(config-if)#no channel-protocol pagp`	لإلغاء الـ PAgP

LACP Link Aggregation

Sw1(config)#int fa 0/23 Sw1(config-if)#channel-protocol lacp Sw1 (config-if)#channel-group 1 mode active ← Sw1(config)#int fa 0/24 Sw1(config-if)#channel-protocol lacp Sw1(config-if)#channel-group 1 mode active ########## Sw2(config)#int fa 0/23 Sw2(config-if)#channel-protocol lacp Sw2(config-if)#channel-group 1 mode passive ← Sw2(config)#int fa 0/24 Sw2(config-if)#channel-protocol lacp Sw2(config-if)#channel-group 1 mode passive	لعمل جروب للكابل عن طريق Protocol LACP يعني المسئول عن ارسال الباكت يعني المسئول عن استقبال الباكت
Sw1(config)#int fa 0/23 Sw1(config-if)#no channel-protocol LACP	لإلغاء الـ LACP

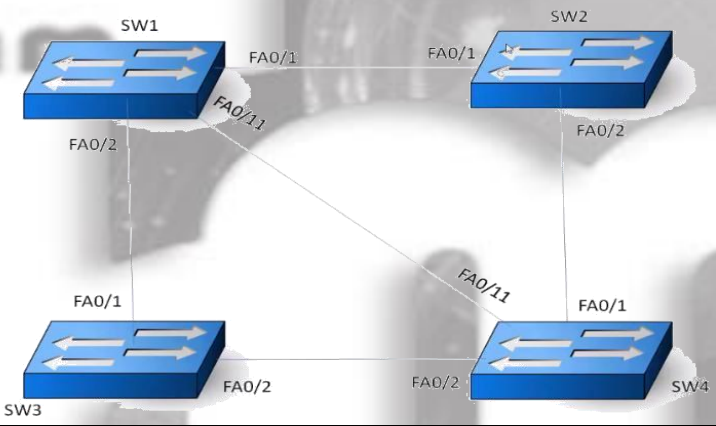
Uplink Fast

لو هناك سويتشين متصلين ببعض عن طريق 2 كابل نتورك وعند انقطار كابل منهم يتم تحويل الباكت إلى الآخر في خلال 30 ثانية أو أكثر ولاختصار هذا الوقت يتم استخدام uplink fast فعند انقطاع الاتصال من الأول ينتقل للأخر مباشرة ولعمل هذا :

لتفعيل هذه الخاصية	SW# conf t Sw(config)# spanning-tree uplinkfast
لإلغائها	SW# conf t Sw(config)# no spanning-tree uplinkfast
لرؤية الـ uplink	Sw#sh spanning-tree uplinkfast

Spanning Tree

هو البروتوكول المسئول عن استخدام مسار واحد فقط بين السويتشات وهو افضل مسار بين سويتش واخر ويقوم بإغلاق المسارات الأخرى إن وجدت



أمر معرفة البورتات المتصلة بالسويتش الآخر وتأخذ designated path cost 0 ملحوظة : البورت المتصل بالأجهزة عن طريق كابل Ethernet يكون الكوست بتاعته بـ 19 أما البورت المتصل designated path cost عن طريق كابل فيبر giga يكون الكوست بتاعته بـ 4	Sw1#sh spanning-tree SW1#sh spanning-tree vlan 2
Spanning tree portfast للبورت المتصل بجهاز وليس سويتش لإلغاء وقت الاتصال في حالة إنقطاع الأتصال وعودته مرة أخرى	Sw1#conf t Sw1(config)#int fa 0/23 Sw1(config-if)#spanning-tree portfast

بمعني ليس الجهاز في حالة لـ learning , listening , forwording **حتى تعود الترافيك** **ولجعل البورت spanning tree portfast**	**Sw1(config-if)#exit** **Or** **Sw1# int fa 0/23** **Sw1#switchport host** هذا الأمر يقوم باختصار أمرين **Mode access / protfast**
ولجعل عدة بورتات spanning tree portfast	**Sw1#conf t** **Sw1(config)#int range fa 0/1 - 24** **Sw1(config-if)#spanning-tree portfast** **Sw1(config-if)#exit**
لعمل Spanning-Tree Rapid	**SW1#conf t** **Sw1(config)#spanning-tree mode rapid-pvst**

DHCP Configuration

هناك طريقتين لعمل DHCP الأولى وهي توجيه الفيلان لأخذ الـ IP من Microsoft Server DHCP وتسمى DHCP Relay وهي كالتالي :

توجيه السويتشات للسيرفر dhcp	Core#conf t Core(config)#int vlan 2 Core(config-if)# ip helper-address 10.0.0.21 وهكذا على جميع الفيلانات
لإلغاء الـ ip helper-address	Core#conf t Core(config)#int vlan 2 Core(config-if)#no ip helper-address 10.0.0.21 وهكذا على باقي الفيلان

الطريقة الثانية لعمل الـ DHCP هي إعداد كونفجراشن الـ DHCP على الكور سويتش نفسه وهي كالتالي :

لتفعيل الـ DHCP على الكور سويتش لفيلان واحدة تحديد اسم Pool تحديد VLAN Subnet تحديد اسم الدومين تحديد VLAN IP interface تحديد الـ DNS تحديد فترة الـ Expiration استثناء عدد معين من الـ IPs	Core#conf t Core(config)#service dhcp Core(config)#ip dhcp pool SVS-Phase1 Core(dhcp-config)#network 10.0.2.0 255.255.255.0 Core(dhcp-config)#domain-name svs.local Core(dhcp-config)#default-router 10.0.2.1 Core(dhcp-config)#dns-server 10.0.0.21 8.8.8.8 Core(dhcp-config)#lease 8 Core(dhcp-config)#exit Core(config)#ip dhcp excluded-address 10.0.2.1 10.0.2.10
لحجز أو إعطاء ip معين لجهاز معين عن طريق الـ MAC Address بتاعه وهي ما تسمى بـ RESERVATION	Core#Conf t Core(config)#ip dhcp pool SVS-Phase1 Core(config)#host 10.0.2.2 255.255.255.0 Core(config)#client-identifier 0100.50b6.5bc0.11ed Core(config)#exit

Core#sh ip dhcp pool Core#sh ip dhcp server statistics	لرؤية dhcp pool
Core#sh ip dhcp binding	لرؤية الاجهزة اللي أخذت IP
Core#conf t Core(config)# no ip dhcp pool svs-phase1	لإلغاء الـ DHCP من على الكور سويتش
Core#clear ip dhcp binding 10.0.2.15	لمسح ip من الـ DHCP
Core#clear ip dhcp binding *	لمسح كل الأيبيهات من على ال dhcp
Core#ip dhcp pool IP-PHONES Core(config)# network 10.1.200.0 255.255.255.0 Core(config)# default-router 10.1.200.1 Core(config)# option 150 ip 10.1.200.10 10.1.200.11 Core(config)# dns-server 8.8.8.8 Core(config)# ip dhcp excluded-address 10.1.200.11 Core(config)# ip dhcp excluded-address 10.1.200.1 Core(config)# ip dhcp excluded-address 10.1.200.10	لعمل بول خاصة بتليفونات سيسكو IP Phone عمل الإعدادات لفيلان 200 وإستثناء 10.1.200.10 , 10.1.200.11 الخاصين بالـ Call Managers

Access Control List (ACL)

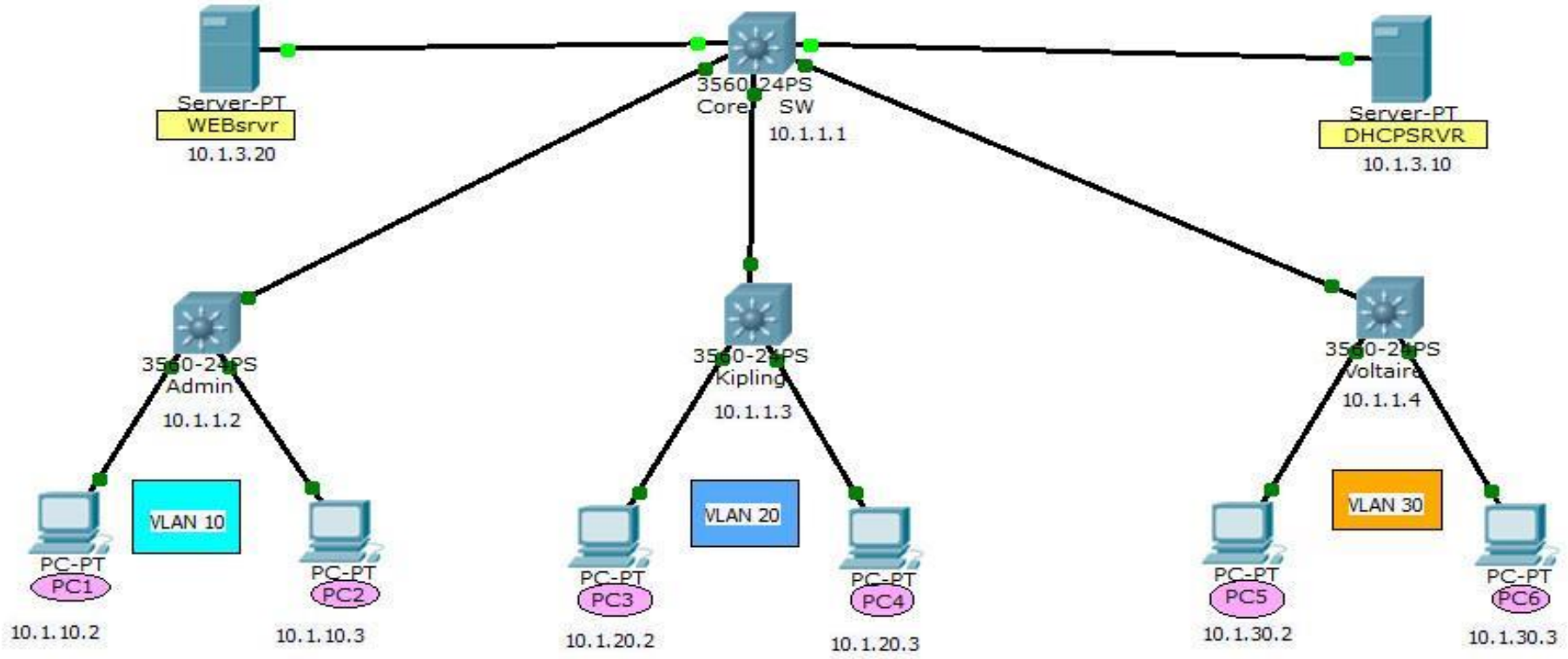
Extended	Standard
(100 – 199)	(1 – 99)
محددة Specific	غير محددة Unspecific
تستخدم لمنع أو السماح بجزء معين في الشبكة جهاز أو عدة أجهزة أو بروتوكول معين مثل http , https , ftp , telnet , وهكذا	تستخدم للمنع أو السماح لشبكة بكاملها دون قيود
أكثر شمولا وتتعامل مع : Source IP Address , Destination IP Address Protocol (TCP , UDP) , Port Number	تعتمد على Source IP بمعني عند منع يجب منع الـ Source Address وتسمى Deny وكذلك عند السماح يسمح لـ Source Address وتسمى Permit

لمنع أو السماح لشبكة كاملة يكون الـ subnet هكذا 192.168.1.0 0.0.0.255

لمنع جهاز واحد بعينه يكون الـ subnet هكذا 172.16.3.5 0.0.0.0

لمنع أو السماح للكل نكتب any ولمنع أو السماح لجهاز معين نكتب Host قبل رقم الجهاز 10.1.3.10 Host

يجب أن نأخذ في الحسبان أن الـ Default **Deny any** ولهذا يجب وضع **Permit** أولا	
يجب ربط الـ ACL بـ Interface ويجب تحديد أتجاهها IN / OUT	
ACL Extented تكون أقرب ما يكون من الـ Source ودائما يكون IN	ACL Standard تكون أقرب ما يكون من الـ Destination ودائما يكون OUT
لرؤية الأكسس ليست المتواجدة	Core# sh access-lists



Core#conf t Core(Config)#int vlan 30 Core(Config-if)#ip access-group 1 out Core(Config-if)#exit Core(Config)#access-list 1 deny 10.1.10.0 0.0.0.255 Core(Config)#access-list 1 permit any	EX1: Deny VLAN 10 (Source) to access VLAN 30 (Destination)
Core#conf t Core(Config)#int vlan 30 Core(Config-if)#no ip access-group 1 out Core(Config-if)#exit Core(Config)#no access-list 1	لإلغاء الـ Access List
core#conf t core(config)#int vlan 10 core(config-if)#ip access-group 100 in core(config-if)#exit core(config)#access-list 100 deny ip host 10.1.10.2 host 10.1.30.2 core(config)#access-list 100 permit ip any any	EX2: Deny PC1 from (VLAN 10) to access PC5 from Network C (VLAN30)

Core#conf t Core(config)#int vlan 10 Core(config-if)#ip access-group 100 out Core(config-if)#exit Core(Config)#access-list 100 permit tcp host 10.1.10.2 host 10.1.3.20 eq 80 Core(Config)#access-list 100 deny tcp any host 10.1.3.20 eq 80 Core(config)#access-list 100 permit ip any any	**EX3: Permit only PC1 from VLAN 10 to access Internet (http) from server 10.1.3.20 and deny other networks but permit any traffic**
TCP : 80 **telnet : 23** **FTP : 20 / 21**	

VLAN Access-Map (VACL)

تستخدم لعمل منع أو سماح ترافك من جهاز في فيلان لباقي الأجهزة في نفس الفيلان

VLAN Access Lists

- Switch(config)# **vlan access-map** *map-name* [*sequence-number*]
- Switch(config-access-map)# **match ip address** {*acl-number* | *acl-name*}
- Switch(config-access-map)# **match mac address** *acl-name*
- Switch(config-access-map)# **action** {**drop** | **forward** [**capture**] | **redirect** *type mod/*
- *num*}
- Switch(config)# **vlan filter** *map-name* **vlan-list** *vlan-list*

مثال 1: منع الفيلان 130 من الوصول لأي مكان في الشبكة ما عدا الدخول على الانترنت

- **Setp 1**

#conf t

#vlan access-map THM-map 10

#match ip address THM-ACL

#action drop

#vlan access-map THM-map 20

#action forward

- **Step 2**

#Conf t

#ip access-list extended THM-ACL

#permit ip 10.1.130.0 0.0.0.255 host 10.1.2.2

#permit ip 10.1.130.0 0.0.0.255 10.1.1.0

لتطبيق هذه Access-list على فيلان معينة

#conf t

#vlan filter THM-map vlan-list 130

مثال2 : منع الترافيك من جهاز 99.17 للوصول لباقي الفيلان

VLAN Access Lists

- VLAN access lists (VACLs) are filters that directly can affect how packets are handled *within* a VLAN

- Switch(config)# ip access-list extended local-17
- Switch(config-acl)# permit ip host 192.168.99.17 192.168.99.0 0.0.0.255
- Switch(config-acl)# exit
- Switch(config)# vlan access-map block-17 10
- Switch(config-access-map)# match ip address local-17
- Switch(config-access-map)# action drop
- Switch(config-access-map)# vlan access-map block-17 20
- Switch(config-access-map)# action forward
- Switch(config-access-map)# exit
- Switch(config)# vlan filter block-17 vlan-list 99

Port-Security Configuration

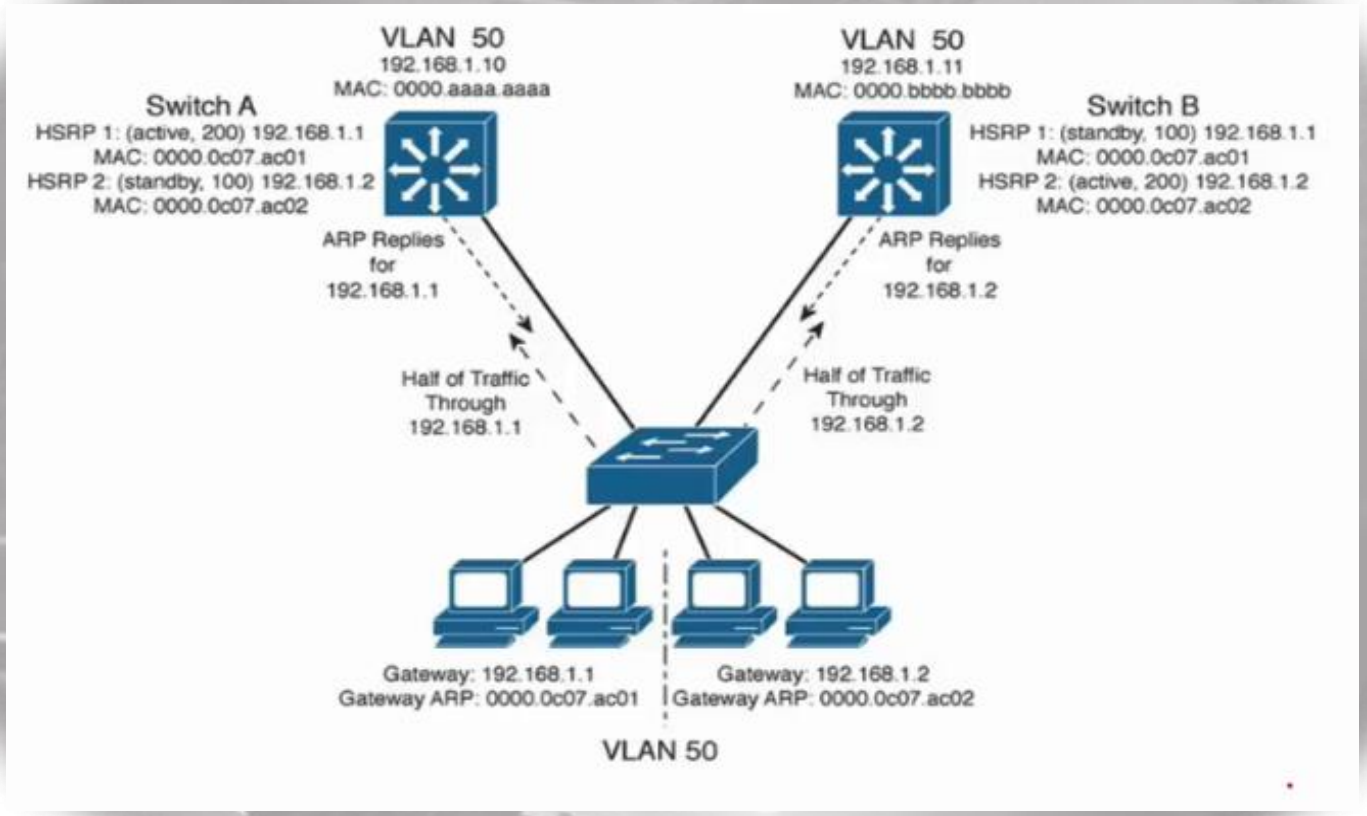
هو عبارة تحديد ماكات الأجهزة المستخدمة بالشركة وتحديد أماكن البورتات المستخدمة لكل ماك وفي حالة دخول أي جهاز غير مصرح له يتم إغلاق البورت أو منع الترافيك للجهاز الغير مرغوب فيه ولعمل هذه الإعدادات :

تحديد البورت تحديد عدد الماكات المستخدمة على هذا البورت وليكن جهازين فهم البورت لأول وثاني ماك يتم توصيلهم بالبورت وضع ماك يدوي على البورت في حالة وجود ماك غير مصرح له قم بالتالي : • إغلاق البورت • منع كل الترافيك على الماك الغير مصرح له • منع كل الترافيك وإرسال رسالة تحذيرية	**#Int gi 1/0/1** **#Switchport port-security maximum 2** **# Switchport port-security mac-address sticky** **# Switchport port-security mac-address 0000.0000.0000** **# Switchport port-security violation (shutdown / restrict / protect)** • Shutdown = close the port • Protect = drop all packet if it isn't the right mac • Restrict = drop all packet and send message alert
لرؤية port security على البورت	# show port-security int gi 1/0/1
لإلغاء port-security	#clear port-security {all / configured / dynamic / sticky}

بعض الإعدادات لزيادة الـ Security في مجال العمل :

لمنع الدخول على السويتش من خلال **Web Browser**	# no ip http server
للسماح لجهاز معين الدخول على السويتش من خلال صفحة الويب	#ip http secure server #Access-list 1 permit 10.1.10.62 255.255.255.255 #ip http access-class 1
لإلغاء الـ **Telnet & SSH** على السويتش	**Sw#** conf t **Sw(config)#** line vty0 15 **Sw(config)#** transport input none **Sw(config)#** exit
لتحديد جهاز معين يقوم بالدخول على السويتش من خلال الـ **Telnet**	**Sw#** conf t **Sw(config)#** Access-list 10 permit 10.1.10.62 **Sw(config)#**Line vty 0 15 **Sw(config)#**Access-class 10 in **Sw(config)#**end
إغلاق جميع البورتات الغير مستخدمة	
لرؤية البورتات الغير مستخدمة port statistics	**Sw#** Sh int stat
لرؤية البورتات المغلقة	**Sw#** Sh int stat err-dis

Gateway Load Balancing Protocol



Active core with the greatest number الرقم الأكبر

GLBP , HSRP for Cisco switches only

VRRP for any vendor for example hp , jenuper , …..

GLBP Protocol

Switch A	Switch B
SwitchA#interface vlan 50	Switch-B#Interface vlan 50
Switch A(config)#Ip add 192.168.1.10 255.255.255.0	Switch-B(config)#ip add 192.168.1.11 255.255.255.0
Switch A(config)#Glbp 1 priority 200	Switch-B(config)#Glbp 1 priority 150
Switch A(config)#Glbp 1 preempt	Switch-B(config)#Glbp 1 preempt
Switch A(config)#Glbp 1 ip 192.168.1.1	Switch-B(config)#Glbp 1 ip 192.168.1.1

Switch-A# Show glbp brief

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Vl50	1	-	200	Active	192.168.1.1	local	192.168.1.11
Vl50	1	1	7	Active	0007.b400.0101	local	-
Vl50	1	2	7	Listen	0007.b400.0102	192.168.1.11	-
Vl50	1	3	7	Listen	0007.b400.0103	192.168.1.12	-

Switch-B# Show glbp brief

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Vl50	1	-	150	Standby	192.168.1.1	192.168.1.10	local
Vl50	1	1	7	Listen	0007.b400.0101	192.168.1.10	-
Vl50	1	2	7	Active	0007.b400.0102	local	-
Vl50	1	3	7	Listen	0007.b400.0103	192.168.1.12	-

Standby Protocol (HSRP)

Switch A	Switch B
Switch-A#conf t Switch-A(config)#int vlan 50 Switch-A(config-if)#ip add 192.168.1.10 255.255.255.0 Switch-A(config-if)#no shut Switch-A(config-if)#standby 1 ip 192.168.1.1 وده الـ Gateway اللي هيكون عند جهاز اليوزر Switch-A(config-if)#standby 1 priority 200 الرقم الأعلى للأولوية Switch-A(config-if)#standby 1 preempt Switch-A(config-if)#standby 1 authentication P@ssw0rd Switch-A(config-if)#standby 2 priority 150 Switch-A(config-if)#standby 2 ip 192.168.1.2 Switch-A(config-if)#standby 2 authentication P@assw0rd	Switch-B#conf t Switch-B(config)#int vlan 50 Switch-B(config-if)#ip add 192.168.1.10 255.255.255.0 Switch-B(config-if)#no shut Switch-B(config-if)#standby 1 ip 192.168.1.1 Switch-B(config-if)#standby 1 priority 150 رقم أقل لأنه هيكون الـ **backup** Switch-B(config-if)#standby 1 preempt Switch-B(config-if)#standby 1 authentication P@ssw0rd Switch-B(config-if)#standby 2 priority 200 Switch-B(config-if)#standby 2 ip 192.168.1.2 Switch-B(config-if)#standby 2 authentication P@assw0rd

Switch-A# Show standby vlan 50 brief

```
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active addr     Standby addr    Group addr
V150        1    200  P Active   local           192.168.1.11    192.168.1.1
V150        2    100    Standby  192.168.1.11    local           192.168.1.2
```

Switch-B# int vlan 50 Switch-B# Standby 1 priority 210	لجعل السويتش رقم 2 هو الأكتف نقوم بزيادة رقم الـ Priority عن الرقم اللي موجود في السويتس رقم 1
Switch-B# Standby 1 track 0/15 50	بمعنى اعمل تراك على الإنترفيس 15 لو وقعت اخصم 50 درجة من الـ standby علشان يحول للسويتش الآخر ويجعله Active

Redundancy Protocol (VRRP)

Switch A	Switch B
Switch-A#conf t	Switch-B#conf t
Switch-A(config)#int vlan 50	Switch-B(config)#int vlan 50
Switch-A(config-if)#ip add 192.168.1.10 255.255.255.0	Switch-B(config-if)#ip add 192.168.1.11 255.255.255.0
Switch-A(config-if)#no shut	Switch-B(config-if)#no shut
Switch-A(config-if)#vrrp 1 priority 200	Switch-B(config-if)#vrrp 1 priority 100
Switch-A(config-if)#vrrp 1 ip 192.168.1.1	Switch-B(config-if)#vrrp 1 ip 192.168.1.1
Switch-A(config-if)#vrrp 2 priority 100	Switch-B(config-if)#vrrp 2 priority 200
Switch-A(config-if)#no vrrp 2 preempt	Switch-B(config-if)#no vrrp 1 preempt
Switch-A(config-if)#vrrp 2 ip 192.168.1.2	Switch-B(config-if)#vrrp 2 ip 192.168.1.2

Switch-A# Show vrrp brief

```
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vlan50             1   200 3218        Y  Master  192.168.1.10    192.168.1.1
Vlan50             2   100 3609           Backup  192.168.1.11    192.168.1.2
```

Backup and Restor Configuration

- Install CiscoKits.TFTPServer program
  - To backup configuration

```
Sw#conf t
Sw(config)#copy run tftp
Sw(config)#copy running-configt tftp
Sw(config)#Address or name of remote host []? 10.1.3.30
Sw(config)#Destination filename [running-configt]?
```

  - To Restore Configuration File

```
Sw#conf t
Sw(config)#copy tftp run
Sw(config)#Address or name of remote host []? 10.1.3.30
Sw(config)#Source filename []?svs-core-sw-confg
```

تم بحمد الله الكورس العملى لإحتراف أوامر سيسكو

نسأل الله أن ينفعنا وإياكم بهذا العمل وأن يجعله فى ميزان حسناتنا يوم القيامة

نسألكم الدعاء