الشبكات الافتراضية

THE VLANs

تقديم : الحسن حوكان

تاريخ : 2016/2015

ملخص

يقدم هذا البحث مفهوم شامل عن الشبكات الافتراضية وتطبيقاتها بالإضافة إلى نقاط ضعف هذه التقنية ومحاولة إصلاحها.

المقدمة:

منذ ما يقارب سبعة آلاف سنة مضت ،بدأ الإنسان في ترك حياته البدائية البسيطة واتجه إلى صنع الحضارة في مجالات مختلفة ، مثل الزراعة وتشييد المساكن وغير ذلك. و نتيجة لهذا تحوّل المجتمع البشري تحولاً جذرياً من كونه مجتمعاً بدائّياً ليغدو مجتمعاً حكوميّاً بيروقراطيّاً تسوده النّظم والقوانين ،بدلاً من الأعراف ومنذ نهاية القرن السابع عشر إلى وقتنا الحاضر دأب الإنسان في استخدام مصطلح "ثورة Revolution " للتعبير عن التحولات الجذرية في المجتمع والناجمة عن مخرجات الفكر البشري المتمثل في الابتكار والإبداع التكنولوجي الذي يمس كل نواحي الحياة من ثورة المحركات البخارية و قطارات السكك الحديدية وانتهاء بثورة الحاسبات والمعلومات وكان لابد من مواكبة التطور والسرعة وشمل ذلك نقل البيانات فتفجرت ثورة الشبكات وانتشرت بشكل كبير وتعددت أشكالها وقد سهلت العديد من النواحي الحياتية.

إشكالية البحث :

ماهي ال VLANs؟؟؟

ماهي فوائد ال VLANs وما هي استخداماتها ؟؟؟

هل هي على مستوى عالٍ أم يوجد فيها ثغرات؟؟؟

هل يمكن معالجة تلك الثغرات في حال وجودها ؟؟؟

الأهداف :

التعرف على ال LANs وما علاقتها بال VLANs .

التعرف على عمل ال VLANs وكيفية إنشائها .

البحث في نقاط ضعف الVLANs ومحاولة إصلاحها .

الفصل الأول:

LANs and WANs

Network: هي مجموعة من الأجهزة المتصلة مع بعضها ويتم نقل data بينها إما سلكياً أو لاسلكياً بالإضافة إلى إمكانية تحكم أحد الأجهزة بالأجهزة الأخرى وتتكون من أربع عناصر مهمة وهي: أجهزة ووسيط وحزم وبروتوكولات ويجد نوعان رئيسيان للشبكات وهما:

LANs (Local Area Network): وهي عبارة شبكة صغيرة تقوم بتغطية مساحة عمل مكتبية أو منزلية وامتدادها قصير المدى أي أنها تعمل عل نطاق ضيق بالإضافة إلى أنها تحكم وتنظم وتدار من قبل شخص واحد.

WANs (Wide Area Network): وهي عبارة عن شبكة كبيرة جداً تقوم بتغطية مساحات كبيرة تشمل الشركات الكبرى وتعمل على نطاق واسع وتعد شبكة الإنترنيت أهم تطبيقات الWANs بالإضافة إلى أنها قد تكون مؤلفة من مجموع من شبكات الLANs وإن الوسيط الذي يجمع شبكات الLANs لتشكيل شبكة الWANs يدعى Router وهي غالباً لا تنظم من قبل شخص واحد إنما من عدة أشخاص.

قبل البدأ بOSI[1] يجب معرفة جزئين مهمين هما:

1-IP: وهو عنوان الجهاز الذي يحمله يمكن الجهاز من الولوج إلى الشبكة ويجعل الأجهزة المتصلة بالشبكة قابلة للتمييز ويسمح بنقل المعلومات ويعرف بالعنوان المنطقي ويوجد في كرت الشبكة في قسم الرام ويتم الحصول عليها من الخادم أو يدوياً ويتألف من أربع أجزاء وكل جزء يتكون من 8 بيت وكل قسم يمكن أن يأخذ قيم من 0 إلى 255 .

2-MAC: وهو أيضاُ عنوان الجهاز ولكن تكون الشركة هي التي كتبته على قسم الروم ولا يمكن تغييره يتألف من12 رمز وينكون من48 بيت.

[1] Odom, W. (2013). Cisco CCENT/CCNA: 187.

أما بعد ذلك فعلينا أن نتعرف على OSI (Open System Interconnection):

7-Application:وهي الطبقة التي تحتوي على البروتوكولات وتتمثل بالمتصفح الموجود على الحاسب ومن أمثلة تلك البروتوكولات:HTTP-FTP-SMTP-SNMP-DNS-DHCP

6-Presentation:وهي الطبقة التي تقوم بتشفير وضغط الملفات من صور وفيديوهات وملفات نصية وما إلى ذلك ومنها:

خوارزميات التشفير:AES-3DES-DES ومن خوارزميات الضغط:JPEG-LZW-RLC

5-session: وهي باختصار طبقة الفرز أو بعبارة أخر هي TAP في المتصفح أو اللسان.

4-Transport: تتم هنا مرحلة التقطيع وبعده الترقيم لكل قطعة تلي الخطوتان السابقتان عملية إعادة التجميع بعد وصولها إلى الوجهة المطلوبة وهنا يتم تحديد الPort الذي تمر منه الData مثال على ذلك:

HTTP➔Port 80➔FTP Port (20, 21) Port ويعطى الPort نمطان هما: Destination Port and Source Port

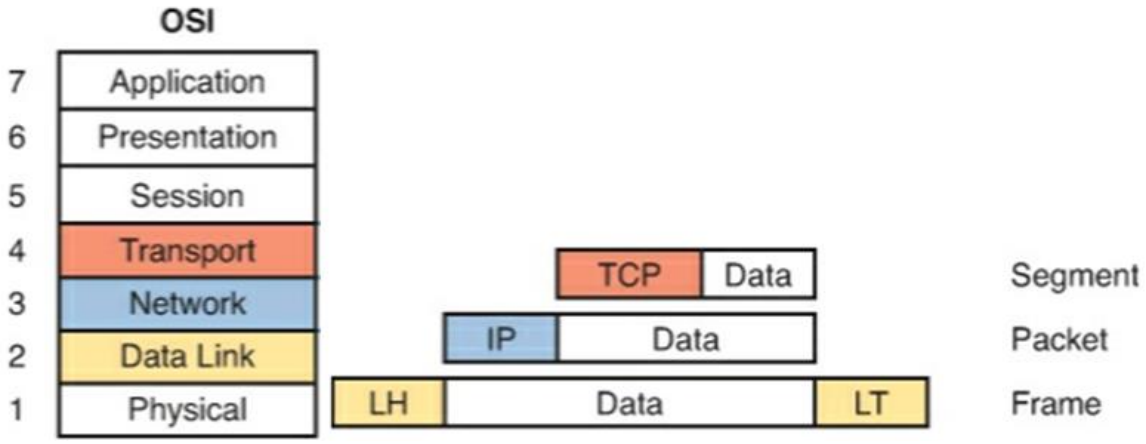
3-Network: هنا تعطى الرسالة أو الملف... Address IP (Internet Protocol) وهو له نمطان أيضاً وهما: Destination address and Source address.

2-Data Link: في هذه الطبقة يضاف الMAC Address وله نمطان مثل الIP ويتم ذلك عن طريق: Ethernet Wired LAN إذا كان الوسط سلكي أما إذا كان لاسلكي فيتم عن طريق:

IEEE 802.11 أما في حال كان الوسط WAN فتكون: PPP, HDLC

1-Physical: وهي المرحلة التي تمر بها ال Data في الكبل على شكل أصفار وواحدات.

في الطبقات 7و6و5 لاتتغير الdata ولا يضاف عليها شئ أم في الطبقة 4 يضاف المنفذ وتسمى عندها الdata "Segment" وفي الطبقة 3 تسمى Packet وفي الطبقة 2 تسمى Frame.



الصورة 1 شرح طبقات ال OSI

الفصل الثاني:Virtual LANs concept

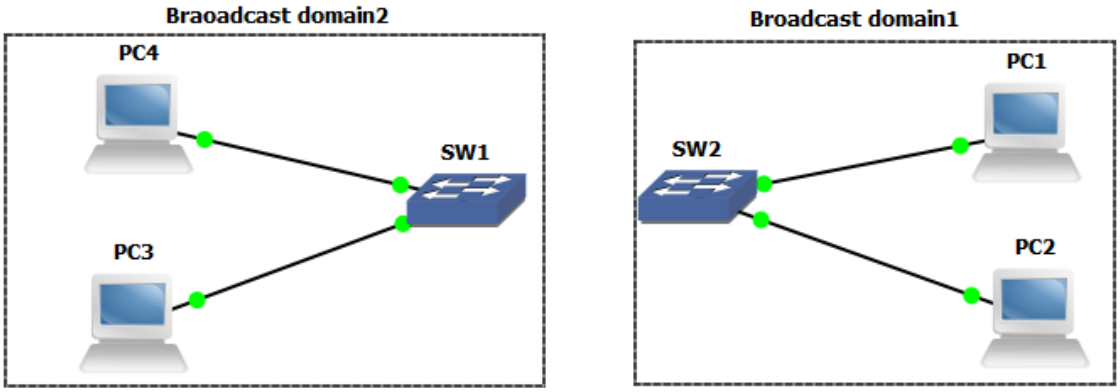
قبل البدء في الVLANs يجب أن نفهم مصطلح الBroadcast domain[1] والمقصود بهذا المصطلح أنه عندما يتم بث LAN من أي جهاز إرسال سواء أكانت شبكة حاسب أم شبكة ناشر فإن مايتم بثه يدعى Broadcast domain أي أنه الحيز الذي يمكن للأجهزة أن تصل من خلاله إلى الشبكة ودائماً يحتوي على كل الأجهزة المتصلة بLANs وبما أن جميع الأجهزة موجودة ضمن Broadcast domain

فإنه عندما يقوم أي جهاز متصل بLANs بإرسال حزمة ضمنها فإن جميع الأجهزة المتصلة الأخرى يمكن أن تنسخ هذه الحزمة ومما سبق نجد أنه عندما جهاز واحد يبث LANs يكون في هذه الحالة ال Broadcast domain وLAN نفس الشيء لهذا فإن الSwitch سوف تعتبر كل الواجهات موجودة ضمن Broadcast domain واحدة بعبارة أخرى عند مرور Frame عبر منفذ Switch

ومنه ستقوم هي الأخرى بإرسالها إلى بقية المنافذ وماسبق لإنشاء two LAN في نفس Broadcast

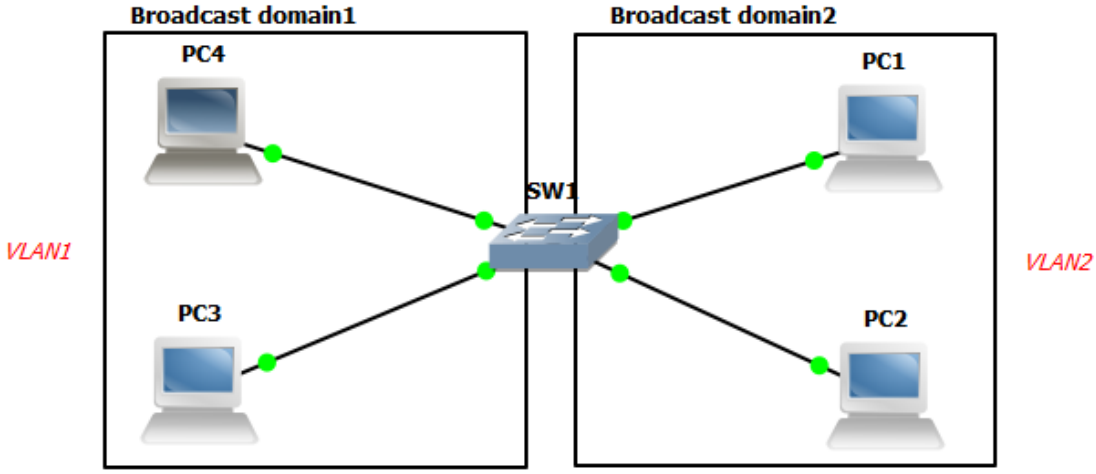
فإنه يجب علينا شراء Switch أخرى

[1] Odom, W. (2013). Cisco CCENT/CCNA: 357.



الصورة 2

من هنا ظهرت فكرة الVLANs التي تستطيع انجاز ذلك العمل باستخدام Switch واحدة أي أنها تستطيع إنشاء أكثر من Broadcast domain في آن واحد حيث يمكن لSwitch واحدة تشكيل عدة واجهات وبثها ضمن Broadcast domain وتشكيل واجهات أخرى بثها في Broadcast domain أخرى بالإضافة إلى أنشاء Multiple Broadcast domain وكل واحدة منشأة من Switch تسمى(VLANs) Virtual LANs حيث تعمل الSwitch الواحدة على خلق شبكتين افراضيتين وتقوم بمعاملة كل Ports في كل VLAN على أنه موزع مستقل عن البقية وفي هذه الحال Switch سوف لن توزع أي Broadcast frame في حال وصولها إليها إلى كل المنافذ.



الصورة 3 ، توضح استخدام vlan

وببساطة يمكن تشكيل VLANs على Switch.

ويوجد العديد من الفوائد والميزات التي تتمع بها VLANs ومنها:

1- التقليل من الاخطار الأمنية المحتملة وذلك بتخفي عدد المستضيفين الذين يستقبلون نسخ من الحزم المرسلة ضمن النطاق التي تبثه (Broadcast ,multicast ,Unicast) Switch.

2- إنشاء تصاميم بمرونة تامة لتوزيع المستخدمين حسب الأقسام وذلك يعد بديل عن تقسيمهم حسب المكان الفيزيائي.

3- حل المشكلات بسرعة أكبر وذلك لأن إصلاح مشكلة لجهاز في Broad cast domain يقوم بحل هذه المشكلة لبقية الأجهزة الموجودة بنفس VLANs.

4- تخفيض العمل الواجب على (Spanning Tree Protocol (STP.

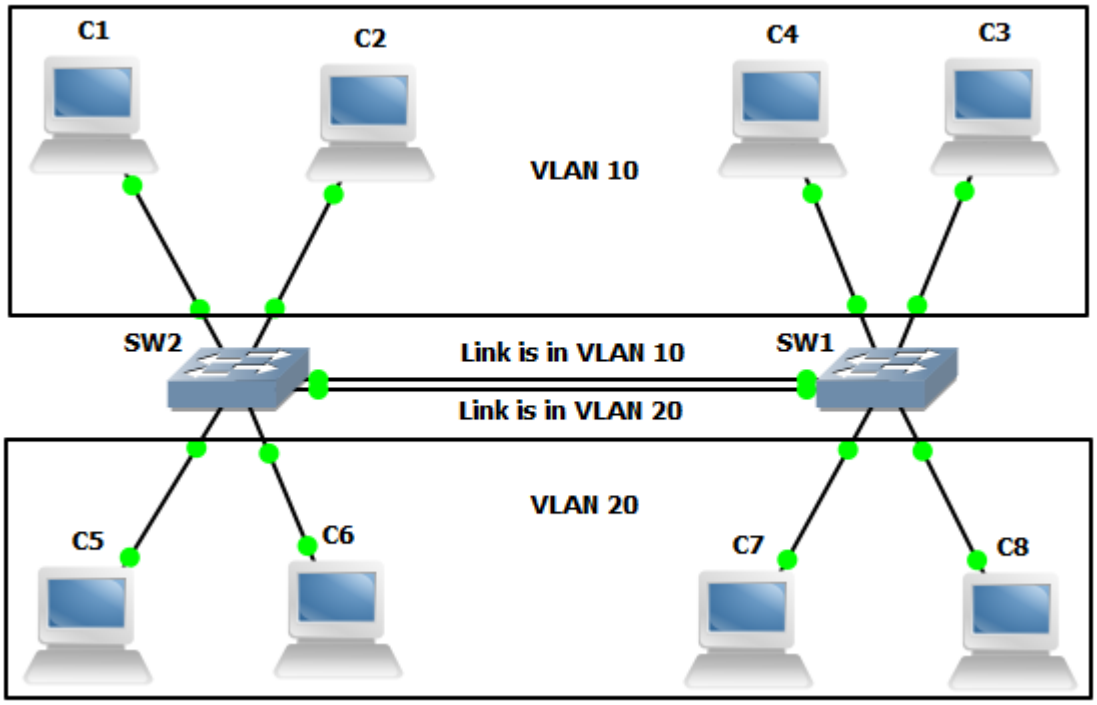
5-تحسين الحماية للأجهزة المستضيفة التي تقوم بإرسال بيانات حساسة وذلك بإبقاء أولئك المستخدمين في VLANs منفصلة.

ويتم برمجة VLANs وذلك عن طريق إعلام كل منفذ موجود ضمن Switch عن رقم كل VLANs وإلى أي منفذ ينتمي.

لدينا في المثال التالي:

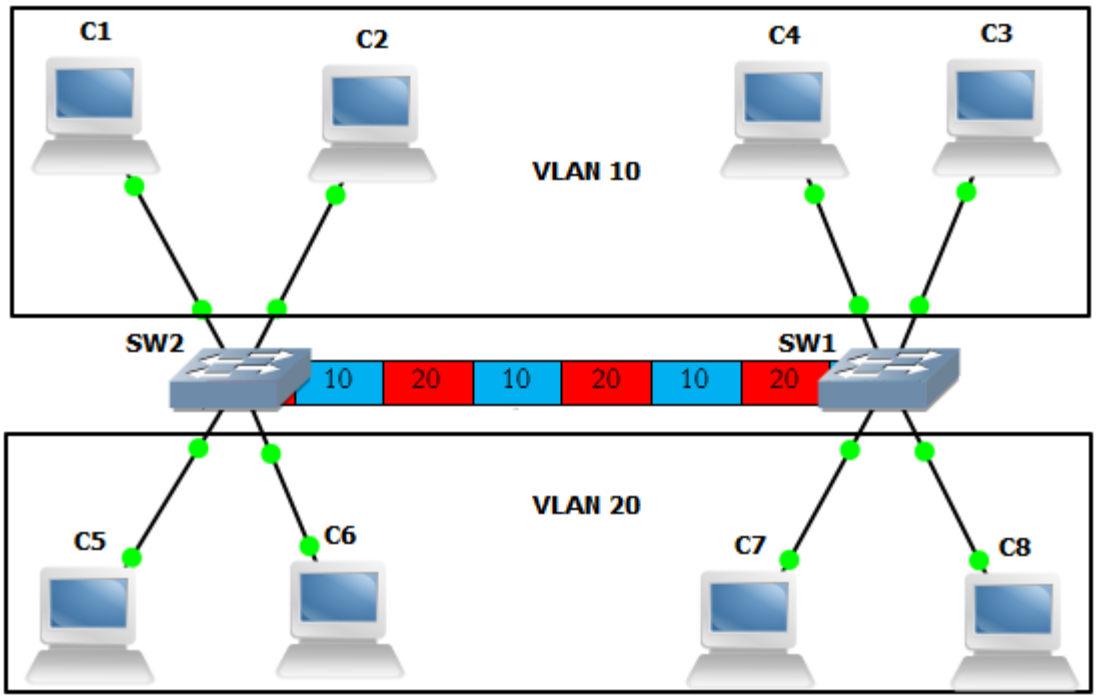
يمكن للجهاز رقم أربعة أن يرسل حزمة إلى الجهاز رقم واحد حيث تنتقل الحزمة ضمن VLAN 10 لتعبر Switch 1 حتى تصل إلىSwitch 2.

ولكن هذه الطريقة عديمة الجدوى وذلك لأنها تحتاج إلى وصلة بين Switches لكل VLANs فإذا كان نمط الشبكة التي نحتاجها يحتوي على ما يقارب من 10 إلى VLAN 20 فسوف نحتاج إلى عدد من الوصلات يساوي عدد VLANs وإلى عدد مماثل من المنافذ وهذه مشكلة بحد ذاتها.



الصورة 4، توضح عدم استخدام الtrunk

من هنا ظهرت فكرة VLAN Trunking التي قامت بحل تلك المشكلة وذلك يكون على الشكل التالي: يلزم لذلك وصلة واحدة بين كل Switch وذلك يكفي ليدعم ما يلزم من VLAN حيث تقوم Switchبمعاملة الوصلة على أنها جزء من كل VLAN وفي نفس الوقت تقوم بفصل كل VLAN عن الأخرى عندما يكون لدينا اثنين VLAN واثنين وتكون كل VLAN موصولة مع Switch عبر منفذ بذلك تصبح كل VLAN موجودة على كل Switch وتكون آلية عملها على النحو التالي: تسمح عملية Trunk للSwitch بإرسال حزم بث مباشر وذلك عن طريق إرفاق الحزم ب Header فعل سبيل المثال: إذا أراد الجهاز c1 إرسال Broadcast frame إلى الجهاز c3 عبر interface Fa0/1 في خطوة أولى حيث تقوم Switch1 بإرسال Broadcast frame إلى Switch2 ولكن يتوجب على Switch1 إعلام Switch2 بأن الحزمة تابعة ل VLAN 10 بحيث عندما تصل إليها الحزمة ترسلها فقط إلى VLAN 10 يتم ذلك قبل إرسال الحزمة من قبل Switch1 إذ تقوم بإضافة VLAN Header إلى الحزم الأصلية وبعد أن تستلمها Switch2 تقوم بتجريدها من VLAN Header وإرسالها إلى VLAN 10 دون غيرها.



الصورة 1، توضح استخدام الvlan

يوجد نوعان أساسيان من البروتوكولات التي تدعم عملية The Trunking هما: Inter-Switch Link(ISL)[1] و IEEE 802.1Q وكلاهما إنتاج شركة سيسكو وقد ظهر بروتوكول ISL قبل بروتوكول IEEE 802.1Q ولكن الأكثر انتشاراً في وقتنا الحاضر هو بروتوكول 802.1Q حيث أنه على الرغم من أنه كل من 802.1Qو ISL يؤديان نفس الوظيفة إلا أنهما يختلفان ببعض التفاصيل حيث أن بروتوكول 802.1Q قد زيد عليه 4-Byte على VLAN ID Header علاوة على Header الموجودة في الحزمة الأصلية.

جميع قطع Switches تقوم بتقسيم حلقة (0-4094) VLAN IDs إلى حلقتان هما حلقة عادية وحلقة موسعة حيث أن أي Switch تستطيع أن أن تستخدم الحلقة العادية التي تأخذ قيم من 1 إلى 1005 حيث أنه فقط بعض الSwitches تستطيع استخدام الحلقة الموسعة الت تأخذ قيم من 1005 إلى 4094 وإن تحديد إذا ما كانت ال Switch تستطيع استخدام الحلقة الموسعة أو لا يتوقف على مايسمى ب VLAN Trunking Protocol (VTP).

[1] Odom, W. (2013). Cisco CCENT/CCNA: 369.

توضيح كيفية برمجة VLAN:

SW1# **Configure terminal**

Enter configuration commands, on per line. End with CNTL/Z.

SW1 (config) # **vlan 2**

SW1 (config-vlan) # **name Freds-vlan**

SW1 (config-vlan) # **exit**

SW1 (config) # **interface range fastethernet 0/13-14**

SW1 (config-if) # **switchport access vlan 2**

SW1 (config-if) # **end**

! Below, the **show running-config** command lists the interface subcommands on

! interfaces Fa0/13 and Fa0/14.

SW1 # **show running-config**

! Many lines omitted for brevity

! Early in the output:

Vlan 2

Name Freds-vlan

!

! more lines omitted for brevity

Interface Fastethernet0/13

Switchport access vlan 2

Switchport mode access

!

SW1 # **show vlan brief**

بعدها سو فتظهر لدينا قائمة تظهر فيها جميع المنافذ وإلى أين تنتمي كما تظهر جميع VLANs وإذا كان مفعلة أم لا كما في الشكل التالي:

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, Fa/22
			Fa0/23, Fa/24, Fa0/25, Fa0/26
2	Freds-vlan	active	Fa0/13, Fa0/14
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	faddinet-default	act/unsup	
1005	trnet-default	act/unsup	

أما إذا أردنا أن نعلم جميع خصائص ال VLAN التي أنشأناها فيجب أن نكتب التعليمة التالية:

SW1 # **show vlan id 2**

هكذا نكون قد أنشأنا VLAN ووسمناها إلى المنافذ التي نحتاج أن تكون مسندة إليها.

أما بالنسبة ل VLAN Trunking Configuration فيتم ذلك على الشكل التالي:

> vlan 10

> name Freds

> exit

> interface range fastethernet 0/13-14

vlan 10

exit

> interface fastethernet 0/14

Switch port mode trunk

الفصل الرابع: The security of VLAN

بعد أن تحدثنا عن VLAN وقمنا بتعريفها وبيّنا كيفية عملها فسوف نتحدث الآن عنا آمن الشبكات الافتراضية وعن بعض الثغرات الموجودة فيها وعن حلول لتلك المشاكل, وبما أن عزل المستخدمين يعد من أهم وظائف الشبكات الافتراضية فإن انتقال أحد المستخدمين من VLAN إلى VLAN آخرى فإن هذا يعتبر خرق للشبكة الافتراضية ومن أهم المشاكل هي الهجمات على الشبكات الافتراضية أو ما يسمى بالهجمات التي تستهدف الطبقة الثانية وإن أهم تلك الهجمات:

VLAN Hopping[1] وينقسم إلى قسمين هما:

1-Switch spoofing: هنا يقوم المخترق إما بعمل Switch وهمية باستخدام برامج مثل GNS3 or Packet tracer أو بوصل Switch حقيقية بالSwitch الأصلية مخبراً أياها بأنه Trunk Port وهذه الخطوة تعطيه الصلاحيات في الوصول إلى جميع الأجهزة المتصلة بال Switch الأصلية بغض النظر إلى أي VLAN تنتمي، بالإضافة إلى القدرة على التنصت على جميع الحزم المرسلة بين الأجهزة وذلك في حال كانت جميع ال Ports في وضع "auto" حيث أن جميع المنافذ تستجيب للمخترق إذا أخبرها أنه Switch وأنه Trunk Port

أما بالنسبة لكيفية التصدي لهذا الهجوم فهي أن أن نقوم بكتابة التعليمة التالية في كل Interface متصلة مع Host:

Switch A# conf t

[1] Dolgij, S. (2011). "Set Network." from https://www.network set .com/security/VLAN Hopping.

Switch A(config)#interface fastethernet 0/1

Switch A(config-if)#switchport mode access[1]

بهذا الأمر نكون قد أوقفنا نصف الهجوم لان السويتش يحوي ثغرة آخرى تتم عن طريق بروتوكول الـ DTP أو Dynamic Trunk Protocol وظيفة هذا البروتوكول بأختصار هي تحديد نوع الـ Trunk Protocol الذي يجب أستخدامه بشكل أوتماتيكي أي تحديد هل يجب أستخدام802.1Q أو ISL وهو يعمل Be defaultعلى كل البورتات الموجودة على السويتش وهذا مايستغله المخترق بشكل جيد فهو يقوم بأرسال DTP Packetإلى السويتش مخبرا ايأه بأنه يستخدم بروتوكول802.1Q مثلا ليتحول الـ Port إلى Trunk Portبشكل أوتماتيكي حتى لو كنا قد طبقنا الأمر السابق ولأيقاف هذه البروتوكول عن العمل نقوم بتنفيذ الأمر التالي:

SwitchA(config)#interface fastethernet 0/1

SwitchA(config-if)#switchport mode trunk

SwitchA(config-if)#switchport nonegotite

هكذا نكون قد متعنا المنفذ من التفاوض مع الطرف الآخر حول نوع البروتوكول الذي يجب استخدامه.

1-Double Tagging: تعتبر هذه الطريقة أقوى من التي سبقتها وذلك لأنه تسمح للمخترق بالانتقال من VLAN إلى آخرى حتى لو قمنا بكل الخطوات والتعليمات السابقة وذلك بإرسال حزمة مرتين تم تحديدها أو تأشيرها ب 802.1Q tags فعندما تصل هذه الحزمة للSwitch الأولى تقوم بإزالة الHeader الخارجي فقط وترسله إلى الSwitch الآخرى وعندما تصلها وهي تحمل الHeader الدخلي الذي تم إعداده من قبل ليوجه الSwitch ومنه إرسال الحزمة إلى المكان المطلوب.

أما بالنسبة للحل فيتم بإنشاء VLAN غير مستخدمة وإرسال الحزم التي لاتحتوي Header وذلك كما يلي:

SwitchA(config)#interface fastethernet 0/1

SwitchA(config-if)#switchport trunk native vlan 210

[1] Smith, J. (2007). LANs and security.

الخاتمة:

بعد أن انتهينا من هذا البحث المتواضع الذي قمنا به بالشرح عن الشبكات المحلية والواسعة واستخداماتها بالإضافة إلى شرح مفصل عن الشبكات الافتراضية وعن مجالات استخدامها بالإضافة إلى الإشارة إلى بعض الأخطار الأمنية التي قد تهدد آمن الشبكات الافتراضية ووضنا الحلول المناسبة لهذه المشاكل.

النتائج والتوصيات:

بعد أن شرحنا أهمية الشبكات الافتراضية وبين دورها في تخفيف النفقات وتقليص حجم العتاد الفيزيائي اللازم لهيكلة العديد من الخدمات المكتبية والمحلية والتجارية ليتعدى الأمر ذلك ويصل إلى الشركات الضخمة والعملاقة فإنه يجب:

1-السعي لتطوير هذا النموذج التقني والاحترافي بالإضافة إلى زيادة الوعي الثقافي اتجاه هذا المجال الواسع.

2-توظيف الشبكات الافتراضية وتفعيلها في المؤوسسات الحكومية.

English References:

1-Odom.Wendell.Cisco CCENT/CCNA ICND1 100-101 official Cert Guide.

2-Odom.Wendell.Cisco CCNA Routing and Switching ICND2 200-101 official Cert Guide.

المراجع العربية:

1-القبيلي.مثنى.تقانة المعلومات والانترنيت.OSI and TCP/IP Reference Models. Chapter 2.

فهرس الصور:

الفهرس العام