جهاز الـ Switch .. أهميته وطرق تأمين الوصول الإداري له

م. هاشم بن مسعّر الشريف

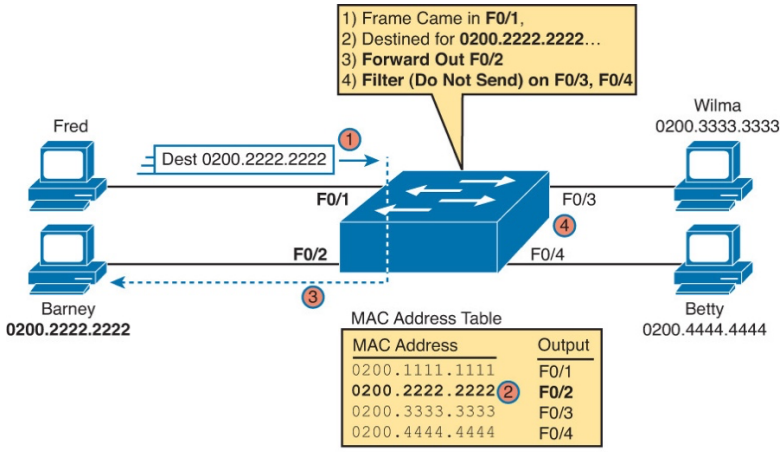
عضو هيئة التدريب بالكلية التقنية بحائل

محاضر معتمد لدى أكاديمية سيسكو

يلعب الـ Switch دوراً هاماً جداً في ربط الأجهزة في شبكات الـ LAN ويعتبر هذا الجهاز ذكياً مقارنةً بسلفه الـ hub والذي كان يسبب الكثير من الإشكالات في نطاق الشبكة الترددي، فمما تميز به الـ Switch أنه يقوم **بثلاثة مهام رئيسية هي:**

١. إيصال الرسائل الى وجهتها الصحيحة داخل الشبكة المحلية بكل دقة وبدون الاعتماد على رسائل البث العام بشكل كلي.
٢. بناء جدول للعناوين خاص به ويسمى هذا الجدول بالـ MAC Address Table بحيث يحوي هذا الجدول على جزئين أساسيين و مهمين في نقل البيانات:
   a. عناوين الـ MAC Address للأجهزة الموجودة.
   b. أرقام المنافذ (Port number) والتي توصل للأجهزة المرتبطة بها.
٣. يمنع التكرار غير المنتهي من دوران الرسائل داخل الشبكة وهو ما يسمى بالـ Looping مستخدماً في ذلك تقنية تسمى بالـ STP.

في المثال أدناه توضيح لكيفية أيصال جهاز الـ Switch للرسالة إلى وجهتها الصحيحة وبدون أخطاء وبناءً على جدوله الخاص بعناوين الـ MAC Address Table

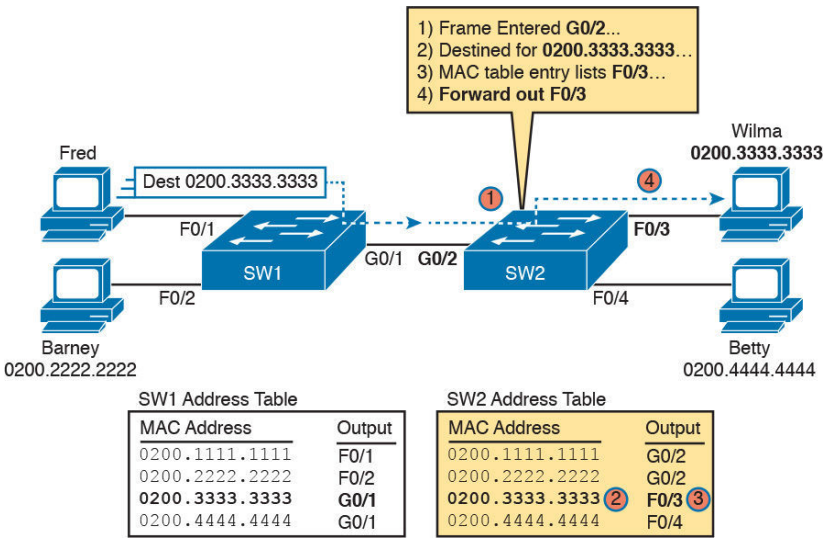


يحاول هنا Fred ارسال رسالة لـ Barney وفي إطار الرسالة يوجد عنوان الـ Mac Address لـ Barney وهو كما هو واضح من الشكل أعلاه 0200.2222.2222 عندها يقوم الـSwitch بالخطوات التالية لإيصال الرسالة لوجهتها:

١. استقبال الرسالة الواردة من المنفذ F0/1
٢. العودة لجدول الـ MAC Address Table الخاص به لتحديد المنفذ المستخدم لتمرير هذه الرسالة.
٣. تمرير الرسالة عبر المنفذ الصحيح وهو في هذه الحالة F0/2.
٤. منع الرسالة من المرور عبر أي منفذ آخر غير المنفذ المؤدي للوجهة الصحيحة.

وهذا ما يميز جهاز الـ Switch عن جهاز الـ hub والذي لم يكن لديه جدول خاص بالعناوين وبالتالي كان يقوم ببث الرسالة لجميع المنافذ عند كل إرسال وهو ما كان يسبب إشكالات نطاق البث الترددي للشبكة.

وعند وجود أكثر من جهاز Switch في الشبكة المحلية فإنها تتعاون فيما بينها لإيصال الرسائل إلى وجهتها الصحيحة، ففي المثال أدناه يحاول Fred ارسال رسالة لـ Wilma ولأن بينهما جهازي Switch فيقوم كل منها باستخدام جدوله للـ MAC Address Table لضمان وصول الرسالة لوجهتها.

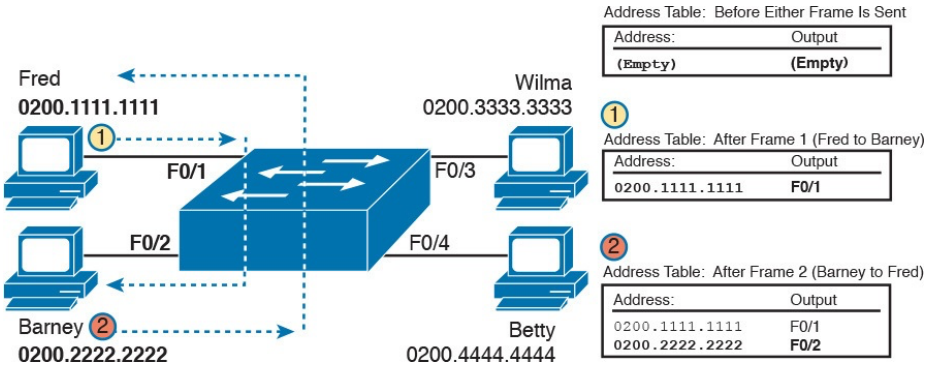


جدول الـ MAC Address Table وكيفية بناؤه:

ذُكر سابقاً أن جهاز الـ Switch يعتبر جهازاً ذكياً لوجود هذا الجدول لديه ولأنه يستخدمه في إيصال الرسائل الى وجهتها فكيف يتم بناء هذا الجدول من الأساس وفي بداية عمل الـ Switch.

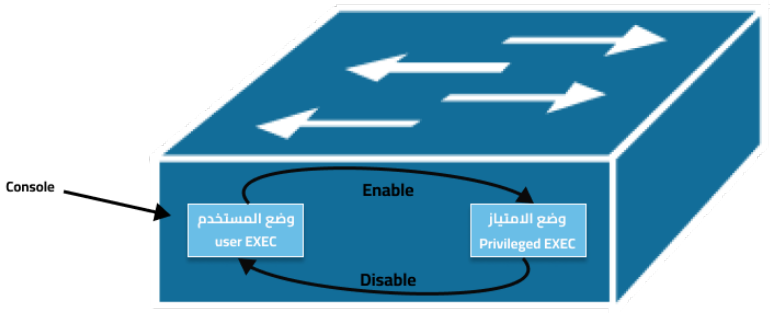
عند ربط جهاز الـ Switch بالأجهزة لأول مرة يكون جدول الـ MAC Address Table خالي من أي مدخلات ويقوم الـ Switch بتعبئته وتحديثه للإستفادة منه ويقوم بذلك متبعاً الخطوات التالية:

١. بمجرد أن تصل اليه رسالة من جهاز معين داخل الشبكة يقوم بتدوين الـ MAC Address له ورقم المنفذ الذي وصل منه في جدوله الخاص.
٢. يقوم بإرسال هذه الرسالة لجميع المنافذ المتصلة به ماعدا المنفذ الذي وصلت منه تلك الرسالة وذلك لأنه لا يعرف الى الآن عناوين الأجهزة المرتبطة.
٣. تتجاهل هذا الرسالة جميع الاجهزة غير المعنية به والتي ليس لديها العنوان الموجود في الرسالة ولا يرد الا الجهاز صاحب العنوان المطلوب.
٤. عند وصول الرد يقوم الـ Switch بتدوين معلومات الرسالة والتي تحوي عنوان المنفذ الذي وصلت منه ويكون بذلك حصل على معلومات جديدة هي العنوان الجديد والمنفذ التابع له.
٥. وهكذا حتى يكمل بناء هذا الجدول

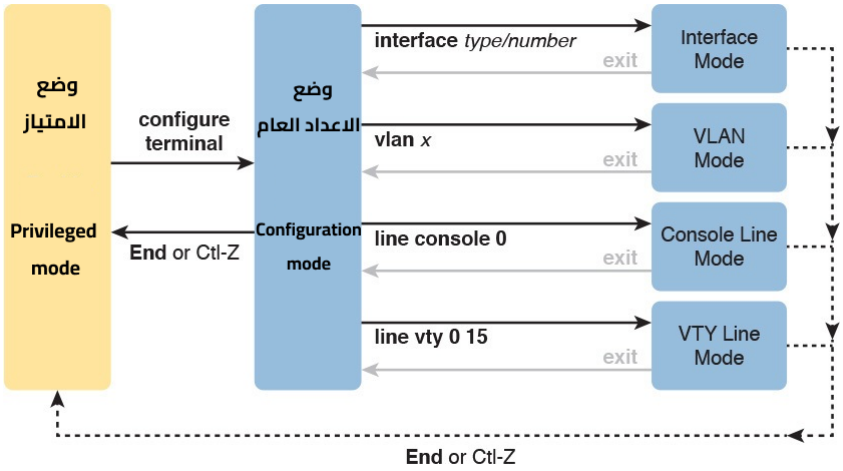


أمان الـ Switch:

يعتبر تأمين أجهزة الـ Switch خطوة مهمة وأساسية لتأمين الشبكة ككل والتهاون في هذا الأمر يعرض الشبكة وجميع مواردها لخطر الاختراق وما يترتب عليه من آثار سلبية. يسمح الوضع الافتراضي لأجهزة سيسكو لأي شخص بالدخول لمنفذ الـ Console والوصول الى وضع المستخدم (user EXEC) بدون كلمة مرور ومن ثم الانتقال لوضع الامتياز (Privileged EXEC) وذلك باستخدام أمر واحد وبسيط هو enable ويكون الخروج للوضع السابق أيضاً بكل سهولة باستخدام الأمر disable ولا يتطلب هذا أي كلمة مرور.



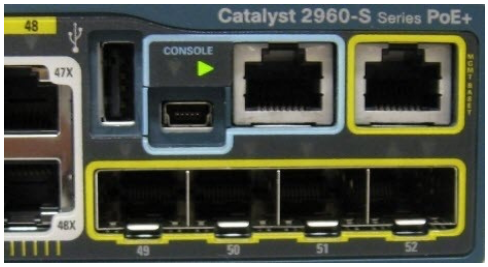
ومن ثم يستطيع المستخدم الانتقال لوضع الاعداد العام (Configuration mode) والذي يمكنه من إجراء أي تعديلات يرغب بها على الجهاز وذلك فقط باستخدام الأمر Configure terminal وذلك بدون أي كلمات مرور.



ومن هنا كانت أحد أهم مهام مهندس الشبكة هو القيام بتأمين الوصول لهذه الأجهزة وقبل الحديث عن آلية وكيفية تأمينها من المهم معرفة الطرق التي يمكن بها الوصول الإداري لهذه الأجهزة وذلك للبدء في خطوات تأمينها.

هناك ثلاث طرق للوصول الإداري لهذا الجهاز وهي:

١. **منفذ الـ Console:** وهو منفذ مادي موجود في نفس الجهاز ويستخدم بدايةً لإجراء الإعدادات الخاصة بالجهاز فهو يسبق الطرق الأخرى.

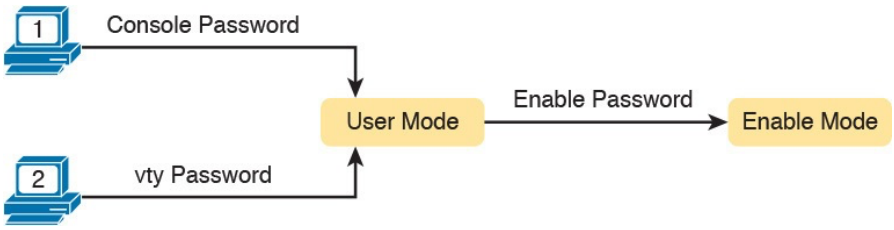


٢. **بروتوكول Telnet:** وهو بروتوكول الوصول عن بعد ويعيبه أنه غير آمن فهو ينقل البيانات بطريقة مكشوفة وغير مشفرة.

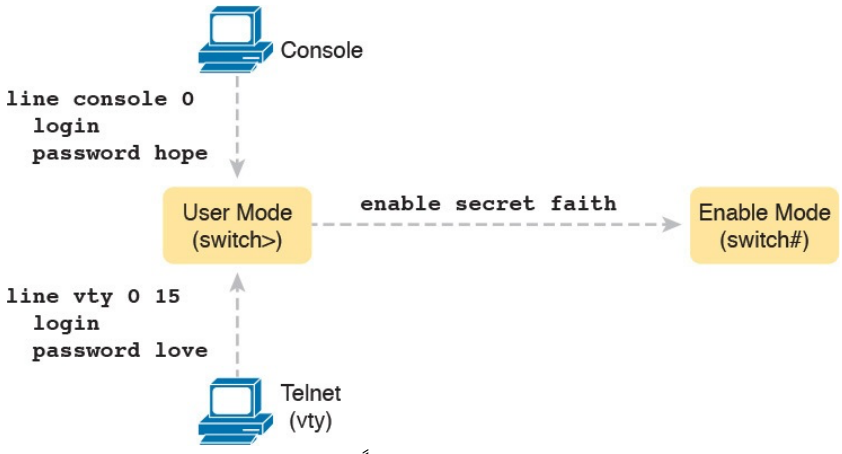
٣. **بروتوكول SSH:** وهو بروتوكول الوصول عن بعد ويتميز بأنه آمن فهو ينقل البيانات بطريقة مشفرة.

طرق تأمين جهاز الـ Switch هي:

١. **كلمة السر المشتركة والبسيطة:** هناك الكثير ممن يستخدم هذه الطريقة لتأمين الأجهزة والتي تتكون من كلمات المرور فقط ولا تتطلب أسم للمستخدم بحيث يمكن وضع كلمة مرور للولوج لمنفذ الـ Console وكلمة مرور أخرى للولوج عن بعد وهو ما يسمى بالـ vty وكلاهما يوصلان لوضع المستخدم العادي ثم كلمة مرور اخرى للولوج لوضع المستخدم صاحب الصلاحيات.

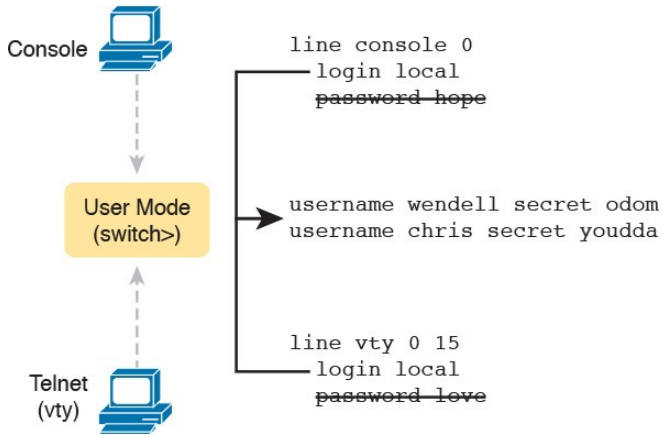


والأوامر المستخدمة لتعيين كلمات المرور المشتركة والبسيطة هي بكل بساطة الموضحة أدناه

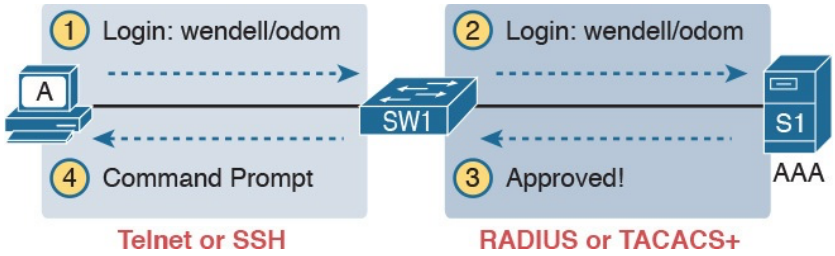


هذه الطريقة هي خطوة للتأمين لكنها غير كافية أبداً لأن المهاجمين سيلجؤون لتخمين كلمات المرور مستخدمين العديد من الأدوات التي تسهل الوصول لكلمة المرور الصحيحة ومن ثم الولوج للجهاز وبالتالي للشبكة. ولذلك يفضل تجنب هذه الطريقة واستخدام الطرق الأخرى لتأمين الأجهزة.

٢. **أسم المستخدم وكلمة المرور المحلية:** تعتمد هذه الطريقة على وجود اسم للمستخدم وكلمة للمرور بحيث يتم حفظ بيانات اسم المستخدم وكلمة المرور في نفس الجهاز (محلياً) وفي هذه الحالة يتم ادخال اسماء المستخدمين وكلمات مرورهم بشكل يدوي لكل جهاز وذلك في وضع الإعداد العام (Configuration mode) ووفق البنية الموضحة في الصورة أدناه. لكن يعيب هذه الطريقة أنها متعبة ومرهقة حيث سيتم إدخال بيانات أسماء المستخدمين وكلمات مرورهم في كل جهاز Switch موجود في الشبكة.



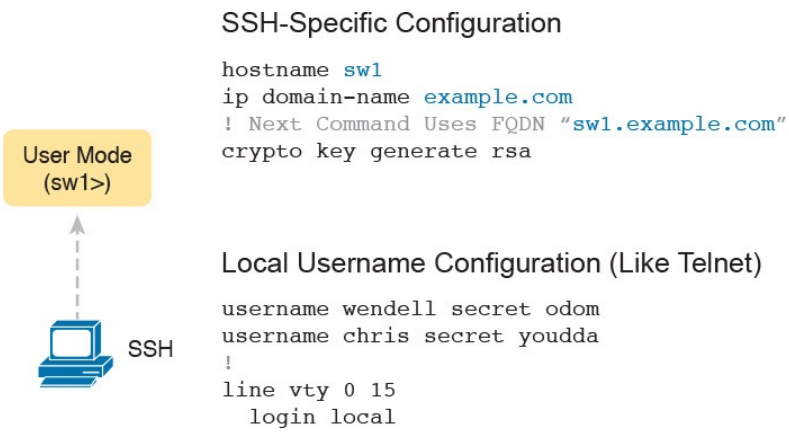
٣. **أسم المستخدم وكلمة المرور الخارجية:** هي طريقة مماثلة للطريقة السابقة إلا أن حفظ بيانات أسماء المستخدمين وكلمات المرور يتم بشكل مركزي ويستخدم لجميع الأجهزة في هذه الشبكة وبالتالي هي طريقة توفر الجهد والوقت في إدارة أجهزة الشبكات. وعمل هذه الطريقة يتطلب تفعيل خدمة الـ AAA server والتي تقوم من التحقق من البيانات الخاصة بالمستخدمين.



ملاحظات مهمة:

<u>أولاً : متطلبات تفعيل الـ SSH:</u> ذُكر سابقاً أن بروتوكول الوصول عن بعد SSH هو أكثر أماناً من Telnet لذا نجدر الإشارة لبعض خصائص هذا البروتوكول والتي تميزه عن نظيره غير الآمن:

١. هذا البروتوكول لا يدعم وسائل التحقق التي لا تحوي كلمة مرور مثل "كلمة السر المشتركة".
٢. يحتاج هذا البروتوكول الى ثلاثة أوامر إضافية على تلك المستخدمة مع الـ Telnet وهي (وجود اسم للجهاز، وجود اسم للمجال (domain)، وجود مفتاح للتشفير)
٣. يُفضّل تفعيل الإصدار الثاني من الـ SSH وفق الأمر ip ssh version 2



من المهم معرفة أنه بالإمكان تعطيل بروتوكول Telnet والاكتفاء بالـ SSH كإجراء أمني بحيث يفرض الوصول عن بعد فقط باستخدام البروتوكول SSH ولتفعيل ذلك يستخدم الأمر transport input بحيث يكون استخدامه كالتالي:

transport input all: support both Telnet & SSH
transport input none: support neither
transport input telnet: support only Telnet
transport input ssh: support only SSH

ثانياً : تشفير كلمات المرور: كلمات المرور المستخدمة للولوج لمنفذ الـ Console أو المستخدمة للوصول عن بعد تكون محفوظة بشكل غير مشفر بمعنى أنه عند استخدام بعض الأوامر مثل show run أو show start تظهر بشكل واضح ويمكن أن تمثل تهديد أمني للشبكة ولرفع درجة الأمان وجب استخدام خدمة تشفير جميع كلمات المرور وفق الأمر service password-encryption

ثالثاً : كيفية إعطاء جهاز الـ Switch عنوان الـ IP address لأجل التحكم فيه عن بعد: هناك طريقتين لفعل ذلك الأولى هي الإسناد اليدوي للعنوان والثانية استخدام خدمة الـ DHCP
للإسناد اليدوي:

Sw1 # configure terminal
Sw1 (config)# interface vlan 1
Sw1 (config-if)# ip address 192.168.10.200 255.255.255.0
Sw1 (config-if)# no shutdown
Sw1 (config-if)# exit
Sw1 (config)# ip default-gateway 192.168.1.1

وعند الرغبة في استخدام خدمة الـ DHCP يشترط أولاً أن تكون الخدمة مفعلة في الشبكة:

Sw1# configure terminal
Sw1 (config)# interface vlan 1
Sw1 (config-if)# ip address dhcp
Sw1 (config-if)# no shutdown
Sw1 (config-if)# ^z
Sw1 #