2021-2022

جامعة البعث

الكلية التطبيقية – السنة الرابعة – تقنيات الحاسوب

الفصل الثاني 2022-2021

Networks Security

Lecture 1

:SUPERVISED BY

ENG. ALI MUSTAFA

Academic Year 2021-2022

Layer 2 Security

الهجمات المُمكنة في الطبقة الثانية

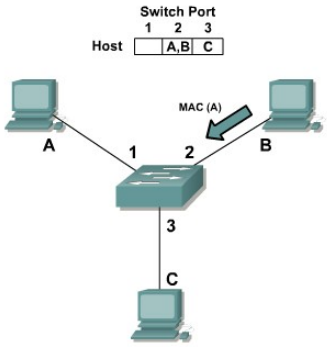
إنّ المُبدّلات (Switches) عرضة للعديد من الهجمات تماما مثل الموجّهات (Routers) ولكن معظم هذه الهجمات تكون من المستخدمين الذين لديهم وصول داخليّ إلى الشبكة.

هجمات الطبقة الثانية

سنتعرّف في هذا الفصل على أكثر الهجمات انتشاراً ونناقش بعض الأساليب المتبعة لحماية الشبكة الخاصة بنا من الهجمات المحتملة على المُبدّلات.

1. انتحال العنوان الفيزيائيّ MAC Address Spoofing

يقوم المهاجم هنا باستخدام برمجية معينة كي يقوم بتغيير عنوانه الفيزيائيّ (MAC) وانتحال عنوان يملكه جهاز اخر ضمن الشبكة المحليّة.



MAC Spoofing

2. هجوم طفحان جدول MAC (MAC Address Table Overflow Attack)

يقوم المهاجم بتوليد عدة رزم تحوي عناوين MAC وهمية غير موجودة خلال فترة قصيرة من الزمن بهدف ملء جدول العناوين في المبدلة وعندها لن تستطيع استقبال عناوين أخرى.

عند إغراق المبدلة بالعناوين الوهمية يتم إرسال الإطارات أو الرزم على كل المنافذ وبالتالي وصول رزم الى العقدة لم تكن سابقا تتمكن من الوصول إليها.

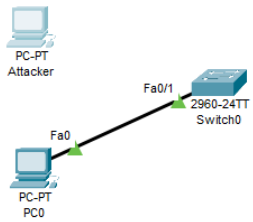
من الحلول المتبعة لحل هجمات العنوان الفيزيائيّ: **Port Security**

هي عملية التحكم بالوصول للمنفذ بحسب العنوان الفيزيائي للجهاز الموصول مع المبدلة.

يمكن أن نحدد عنوان محدد **أو** أن يتم تعلمه بشكل ديناميكيّ "أول عنوان يتم ربطه مع المنفذ" **أو** السماح لعدد معين من العناوين على كل منفذ.

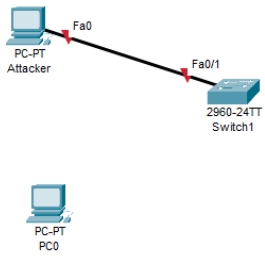
لتفعيل الخدمة على منفذ معين ندخل للواجهة (Interface) المطلوب تفعيل الخدمة عليها ونكتب التعليمات التالية:

```
switchport port-security
switchport port-security mac-address {‘device_mac_address’}
switchport port-security maximum 1
switchport port-security violation shutdown
```




```
Switch(config)#
Switch(config)#int f0/1
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0001.4340.323B
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#
Switch(config-if)#do wr
Building configuration...
[OK]
```

وستتغيّر حالة المنفذ إلى Shutdown عند حدوث خرق في سياسة الحماية:



ونقوم لإعادة تشغيل المنفذ بإعادة وصل جهاز الحاسوب النظامي وبعدها ندخل للمنفذ الذي تم إغلاقه ونطبّق التعليمة shutdown وبعدها التعليمة no shutdown.

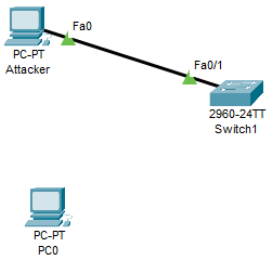
يمكن أن نميز 3 حالات للسياسة التي يتبعها المنفذ عند عملية الاختراق وهي:

1. **Shutdown :**

يصبح المنفذ بحالة errdisable (Error Disable) ولا يعمل حتى يتم إعادة تفعيلهُ.

2. **Protected:**

يبقى المنفذ بحالة عمل لكن كل الرزم التي يرسلها المهاجم يتم إهمالها دون الاحتفاظ بسجلات عن عملية التجاوز الحاصلة.



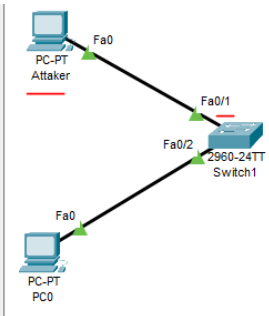

```
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#do wr
Building configuration...
[OK]
Switch(config-if)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------
       Fa0/1        1           1               0          Protect
---------------------------------------------------------------------
```

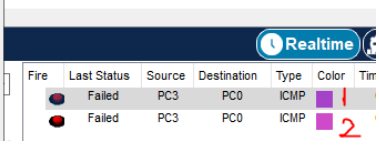
3. Restrict:

هنا السياسة مشابهة للنوع السابق ولكن تقوم المبدلة بإرسال رسالة SNMP trap تحوي معلومات عن عملية التجاوز أو الاختراق الحاصلة **ويحفظ عدد الرزم التي يتم إرسالها من المهاجم.**

```
Switch(config-if)#do show port security
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

show port security
     ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------
       Fa0/1        1           1               2          Restrict
---------------------------------------------------------------------
Switch(config-if)#
```

Ctrl+F6 to exit CLI focus — Copy — Paste





كما أن هناك امكانية ترك العنوان الفيزيائي كي تتعلمهُ المُبدّلة تلقائياً ويتم ذلك عن طريق وضع كلمة **sticky** بدلا من عنوان MAC، وكمثال على ذلك يمكن تنفيذ التعليمات التالية:

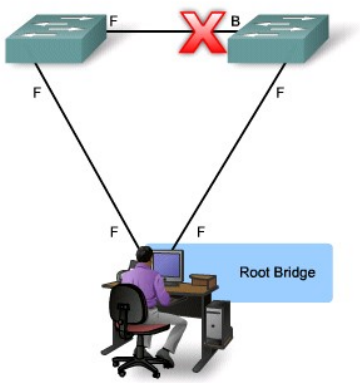
```
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
```

❖ **تعاني طريقة port security من عدة مشاكل مثل:**

1. سهولة انتحال العنوان الفيزيائيّ MAC.
2. من الصعب تحديد الأجهزة اللاسلكية التي تتصل مع المُبدّلة لأن المُبدّلة ترى فقط عناوين MAC.

لذا تم التوسّع واستخدام تقنية التحقّق من هوية المستخدم من خلال المنفذ **port-based authentication** التي تعتمد على استخدام مُخدّمات توثّق مثل مُخدّمي RADIUS وTACACS+ (والتي سنراها ضمن محاضرة لاحقاً).

3. هجمة STP Attack



يهدف هذا النوع من الهجمات إلى إنشاء مُبدّلة جذر مزوّرة (Bogus Root bridge).

يقوم المهاجم ببث رسائل BPDUs ليعلن وجود مبدلة ذات أولوية أصغر بهدف إعادة انتخاب المُبدّلة الجذر.

إعادة انتخاب المُبدّلة الجذر بحد ذاته يمكن أن يؤدي إلى حالة منع خدمة denial-of-service (DoS) لأن بناء شجرة STP جديدة بحاجة لمدة تتراوح من 30 إلى 45 ثانية كل مرة تتغير فيها المبدلة الجذر.

إذا نجح الهجوم يمكن للمهاجم أن يصبح المُبدّلة الجذر root bridge وبالتالي يُتاح له الوصول إلى إطارات (Frames) غير متاحة له في الحالة العادية.

✓ **التنصّل والحماية من التعديل ضمن STP (Mitigating STP Manipulations)**

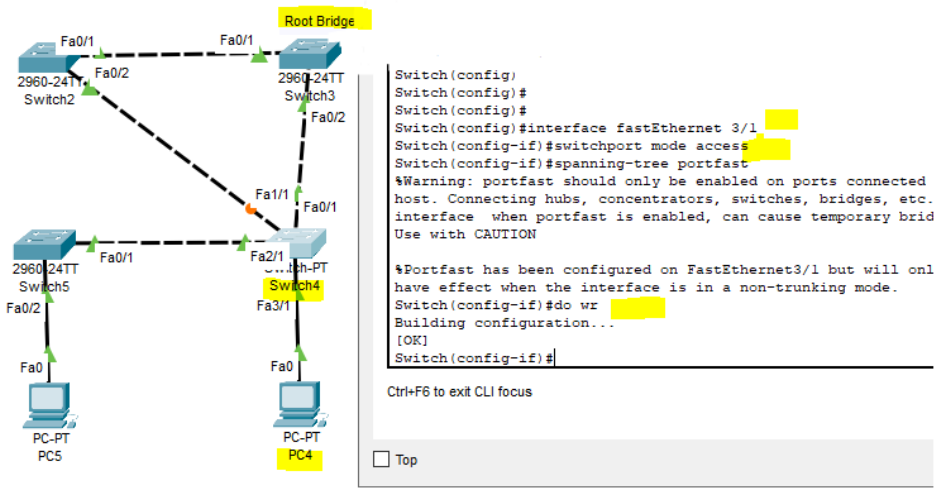
1) Portfast

ليست تقنية حماية وإنما ميّزة من أجل تسريع عملية تحوّل البورت لحالةforwarding دون الانتظار (لا تشارك بعملية ال STP) و نستخدم هذه الميّزة للمنافذ المتصلة مع PCs.

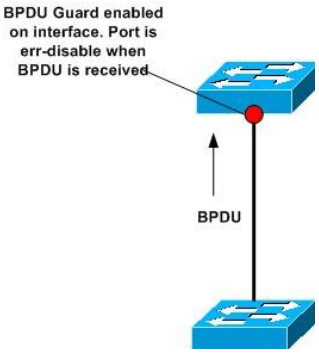
تُعرّف عن طريق الأمر:

- **spanning-tree Portfast**

ويجب تطبيقها على Access ports حصراً.

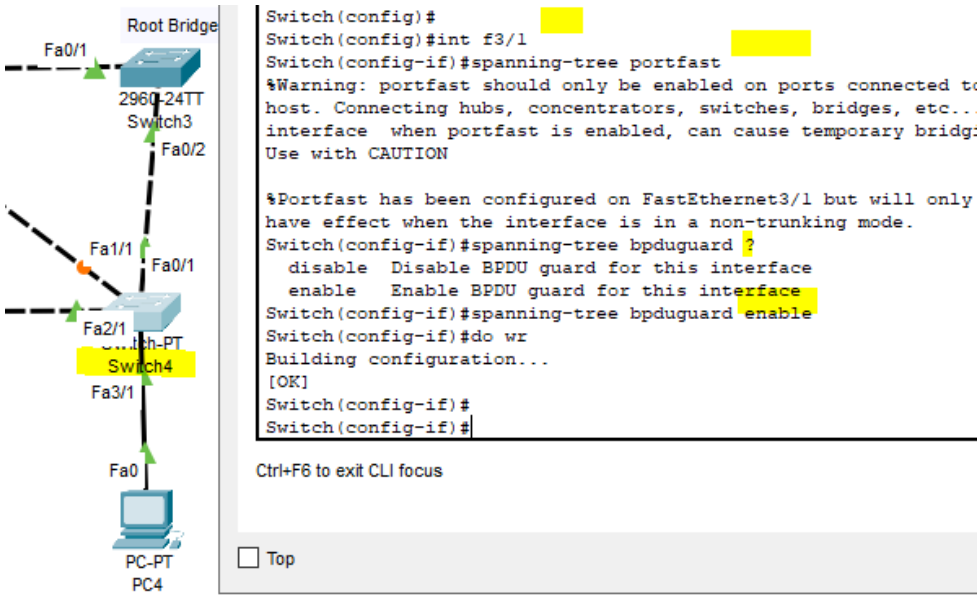


2) BPDU Guard



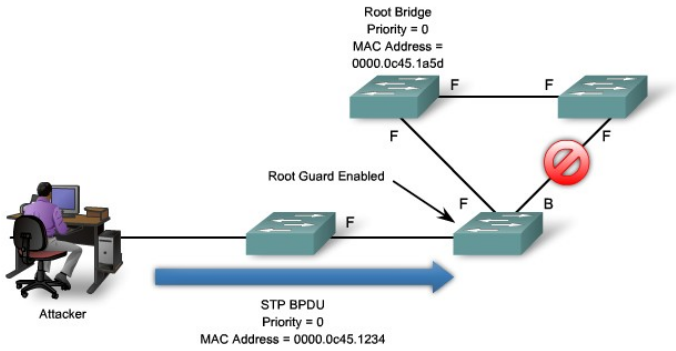
هي خاصية تُستخدم حتى نخبر **المنفذ** ألا يستقبل أي نوع من رسائل الـ BPDU وفي حال استلام المنفذ لأية BPDU سوف يقوم بتحويل حالة المنفذ إلى errdisable أي سوف يتم اغلاق المنفذ بشكل كامل.

يتم تفعيل BPDU Guard على منفذ ما كالتالي (وغالباً ما يتم تفعيلها بعد تعلية Portfast):



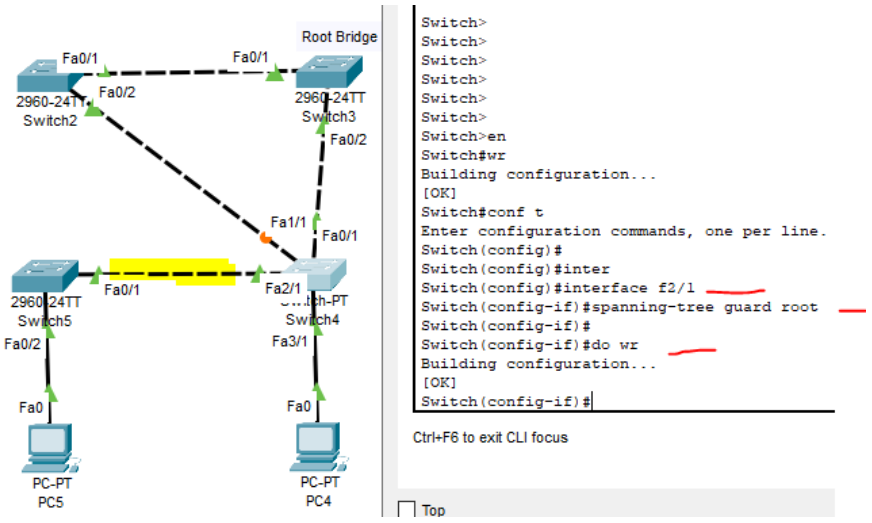
3) Root Guard

هي خاصية تضمن أن العقدة التي نريدها جذراً في الشبكة تبقى كذلك، بحيث أنه عندما تستقبل مُبدّلة على الواجهة التي عرّفنا عليها خاصية Rootguard أية رسائل BPDU من مبدلة تعلن رقم مُعرّف أصغر من مُعرّف الجذر الحالي يتم وضع تلك الواجهة في حالة تدعى **root-inconsistent** ويتم إعادة المنفذ إلى حالته الطبيعية عندما تتوقف الرسائل التي تعلن معرف أصغر.



إن أفضل مكان لتفعيل هذه الخاصية هو على المنافذ التي تتصل بمُبدّلات لا ينبغي أن تُصبح Root Bridge حتى لو أعلنت عن رسائل BPDU ذات أولوية أقل من المُبدّلة الجذر:

(إذاً حافظنا بذلك على المُبدّلة الجذر بأن تبقى في سلطتها كجذر وحمايتها من أن تأتي مُبدّلة أُخرى وتنتزع دورها)



ولعرض المنافذ التي سبق وتعرّضت لخرق يؤذي ال Root Bridge، نكتب التعليمة التالية:

```
Switch#show spanning-tree inconsistentports
Name                 Interface            Inconsistency
-------------------- -------------------- ------------------

Number of inconsistent ports (segments) in the system : 0
```

4. هجوم العاصفة (LAN Storm Attacks)

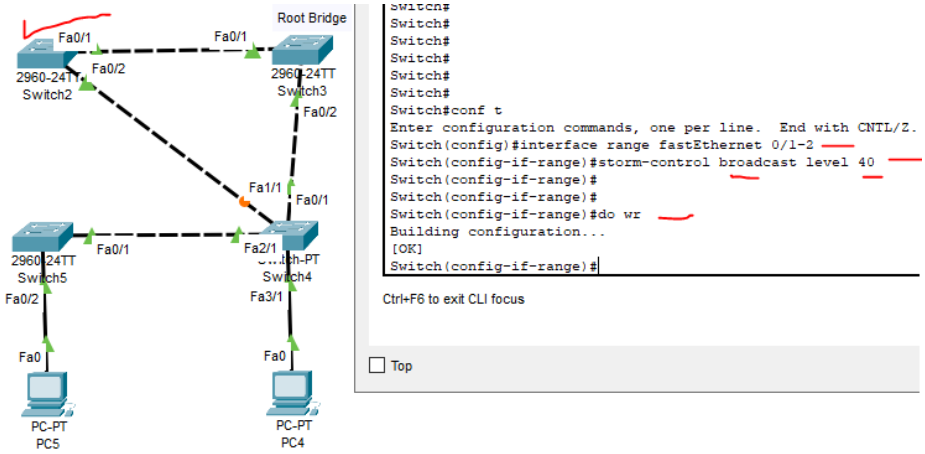
تحدث عاصفة LAN Storm عندما تملأ الإطارات (Frames) شبكة ال LAN مُسببةً حركة بيانات زائدة عن المعقول (excessive traffic) وانخفاض في أداء الشبكة.

- من أسباب حدوث هذه العاصفة:
  - × أخطاء ضمن إعدادات الشبكة.
  - × هجوم منع الخدمة (DoS).

نستطيع تحديد نسبة مئوية من عرض الحزمة المُتاح والتي تستطيع حركة البينات (Traffic) استخدامهُ منها كالتالي:

(تُفعّل على مستوى ال Interface)

- **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[.*fraction*]



وضعنا هنا إمكانية استخدام 40% من عرض الحزمة كحد أقصى لأي بيانات Broadcast وفي حال تجاوز هذه النسبة سيتم تخفيض ال Traffic وإهمال البيانات الزائدة.

المراجع

- جامعة البعث -كلية الهندسة المعلوماتيّة -السنة الخامسة / مُقرّر أمن الشبكات الحاسوبيّة – مُحاضرة (Layer 2 Security) / **الدُكتورة زينب خَلوف.**

???Any Questions