Introduction

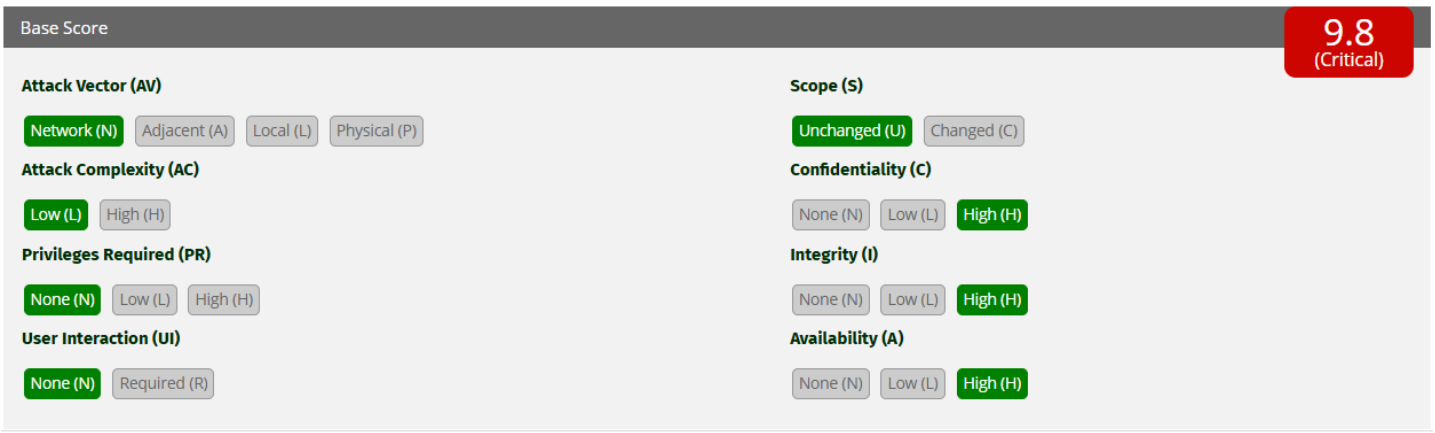
- Information security يختص بدراسة كيفية حماية الdata
- Cyber security يختص بدراسة الهجمات على الOS و الاجهزة والnetworks و الapplication وكيفية الحماية منها
- عند التحدث عن الdata المراد حمايتها فيوجد نوعان من الdata وهم :
  1. At rest وتعنى الdata عندما تكون مخزنة
  2. In motion وتعنى الdata عندما تكون على الnetwork اى انها ترسل

CIA triad

- هو واحد من اهم المصطلحات فى الinformation security والتى يعبر عن الخصائص التى يجب ان تكون متوفرة عند حماية الdata
- CIA هو اختصار ل confidentiality, integrity, availability
- Confidentiality هى تعنى سرية الdata اى ان الdata لا تظهر الا للusers المسموح لهم فقط
- تتحقق الconfidentiality من خلال اضافة encryption للdata المرسلة
- Integrity وهى سلامة data وتعنى التاكد من ان الdata لايمكن التلاعب فيها والتعديل عليها
- يتحقق الintegrity من خلال ارسال hash لdata عند ارسالها
- الخطوة السابقة تتم كتالى :
  1. يقوم الsource بارسال الdata ومعها الhash الخاص بها
  2. يقوم الdestination باستلام الdata ويقوم بعمل hash لها
  3. يقارن قيمة الhash المرسلة مع الdata والقيمة التى قام بانشائها
  4. اذا كانت القيم واحدة فهذا يعنى ان الdata لم تتغير فى مسارها الى destination
- Availability وهى تعنى ان الdata يجب ان تكون متاحة على الاقل فى level معين مثل وجود backup لها

Vulnerability

- اى ثغرة لها unique number ويعرف كا CVE
- CVE اختصار ل Common Vulnerability and Exposure
- من الdatabases المشهورة التى تحتوى على العديد من الCVEs هم https://www.exploit-db.com و https://nvd.nist.gov
- CVSS هو عبارة عن نظام يتم من خلاله حساب خطورة الثغرة بناء على العوامل الخاصة بها



Security terms

- Asset وهو مصطلح يطلق على اى resource يجب حمايته
- Thread ويعنى خطر وقد يكون attacker او software ضار
- Risk المقصود به احتمالية حدوث thread
- Exploit هى الطريقة او الاداة التى يستخدمها الattacker لاستغلال الثغرة
- Countermeasure الخطواط الازم اخدها لتقليل الrisk

- حدوث vulnerability يمكن ان تحدث من خلال الاتى :
  1. Physical access
     - وتعنى الوصول الى الاجهزة بشكل physical لذالك يجب ان يتم وضع اجهزة الnetwork داخل غرفة مخصصة او ان يتم اغلاق الrack بشكل جيد
     - كميرات المراقبة والalarms تعتبر من الphysical security ايضا
  2. Hardware and software
     - وتعنى حدوث ثغرة بسبب الsoftware المستخدم او من الhardware
  3. Human factors
     - وتعنى حدوث ثغرة بسبب التصميم الخاطئ او بسبب حدوث misconfiguration
     - من امثلة التصميم الخاطئ عدم وضع الservers فى منطقة الDMZ
  4. Weakness in protocol, application or systems

Common attacks

- Reconnaissance وهو native attack ويعنى انه لايحدث attack بشكل فعلى وانما يكون عبارة عن تجميع معلومات عن الtarget
  - من امثلة البرامج التى تقوم بتجميع معلومات عن الشبكة (ip scanner – port scanning)
- Social engineering وهى تقوم على خداع الاشخاص مثل خداع الموظفين عند محاولة اختراق شاركة
- Privilege escalation وتعنى الحصول على صلحيات اعلى مثل التحول من user الى admin
- Code execution وتعنى حدوث attack من خلال تشغيل code ضار
- Backdoor وهو باب خلفى يقوم الattacker بانشائه فى حالة اراد الدخول على الsystem مرة اخرى وتنفيز اوامر عليه
- Convert channels تحويل مسار الcommination بعرض سرقة البينات
- Trust exploitation استغلال وجود صلاحية معينة للحصول على access اعلى
- Man in the middle attack(MITM)
- Zero day exploit وهى عبارة عن ثغرة تم اكتشافها ولم يصدر اصلاح لها بعد
- Password crack وهى تحدث من خلال طريقتان :
  1. Brute force attack وهو يقوم على تجربة كل الاحتملات الممكنة
  2. Dictionary attack وهو يقوم على تجربة اشهر الكليمات المستخدمة
- Information disclose وهو thread قائم على سرقة البينات مثل الdata او حتى الsource code
- SQL injection
- HTML injection
- Denial of service(DOS) يقوم على ايقاف service معينة ويكون الهجوم من مصدر واحد
- Distributed DOS وهو مثل الDOS ولاكن مصدر الهجوم يكون عدة اجهزة وغالبا ما تكون هذه الاجهزة مخترقة وتسمى zombie
- يوجد عددة انواع من DOS مثل :
  1. Ping flood
  2. Mail bomb
  3. SYN attack
- يوجد نوع اخر من الDOS يسمى reflected DDOS وهو اخطر حيث يرى الserver ان الهجوم اتى من الip الخاص به وبتالى لايمكنه وضعه فى blacklist

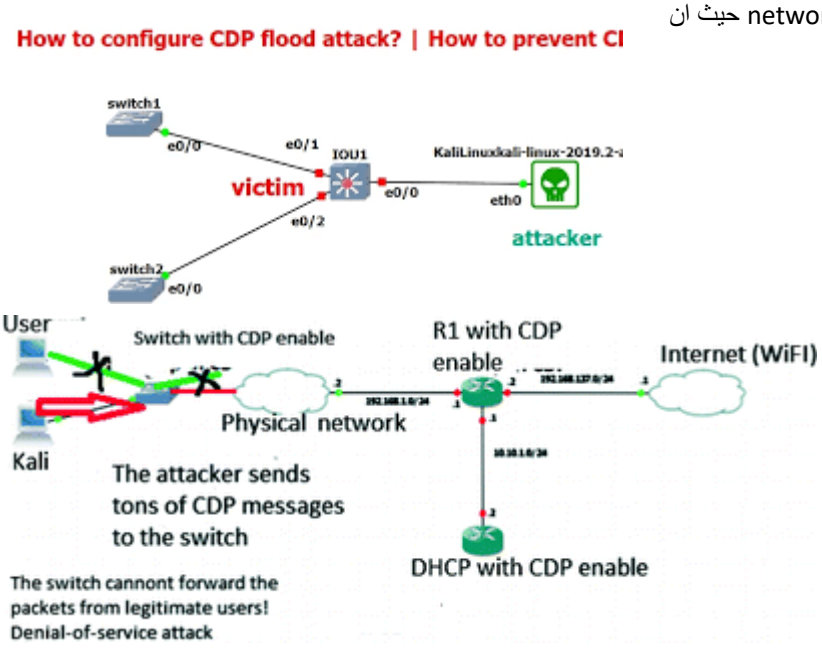
Malwares

- Virus هو كود ضار ومن خصائصه ان يحتاج تفاعل من الuser لكى يعمل
- Worm هى كود ضار ايضا ولاكنها لاتحتاج الى تفاعل الuser وايضا تقوم بالانتشار بمفردها
- Spyware وهو كود ضار غرضة التجسس وسرقة البينات
- Trojan horse هو كود ضار يكون مدموج مع بينات قابلة للاستخدام وله الكثير من الانواع حسب الاستخدام كتالى :
  1. RAT(remote access Trojan) يستخدم لتنفيذ اوامر على الsystem
  2. E-banking اى ان وظيفته سرقة الحسابات البنكية
  3. DOS or DDOS
  4. Ransom ware وهو يقوم بتشفير الdata على الجهاز
  5. Proxy يسمح للattacker ان يستخدم الجهاز المصاب كا proxy لتنفيز الهجمات من عليه
  6. FTP attack اى يمكن استخدام الجهاز المصاب لتحميل ملفات عليه او اخذ من ملفات
  7. Security software disabler اى ان الTrojan يكون وظيفته اطفاء الsecurity software مثل الanti-virus
  8. Backdoor
- عملية تشغيل الكود الضار مثل الTrojan يمكن ان تتم بسهولة من خلال دمج الكود مع ملف مستخدم ويتم ذالك من خلال wrapper or binder او packers و dropper او crypters

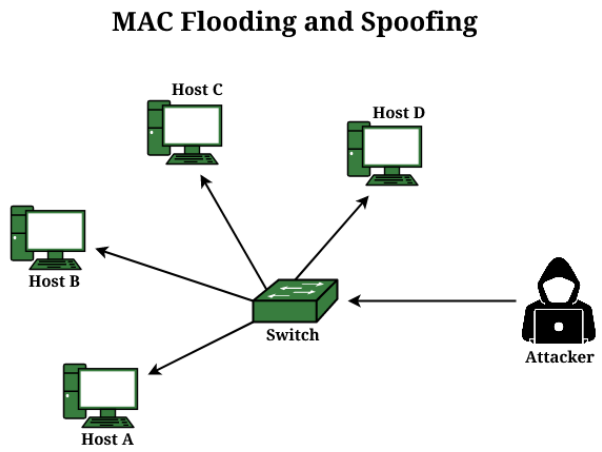
LAN security attack

CDP attack

- CDP هو واحد من البروتوكولات المهمة والتى تقوم بكتشاف الاجهزة المحيطة من routers و switches ويكون مفعل بشكل تلقائى
- يتم استخدامه ايضا فى الtrouble shooting حيث انه L2 protocol لذالك يستخدم فى التحقق من كون الاتصال صحيح بشكل physical
- يمكن استغلال الCDP من خلال معرفة information عن الnetwork حيث ان انه يقوم بارسال البينات كا clear text
- يمكن عمل CDP flood لهدفان :
  1. استخدامها كا DOS لايقاف الdevice
  2. تعطيل الuser من استخدام هذه الfeature
- لتجنب هذا الattack فاننا بتعطيل CDP على :
  1. PCs port
  2. WAN ports
  3. الports الغير متصلة باجهزة ليست لcisco لان الprotocol لن يعمل عليها
- يتم ايقاف الCDP من خلال الدخول على الport وتطبيق امر **no cdp enable**
- لبدأ تجميع البينات من خلال الCDP نقوم باستعمال اداة **cdpsnarf**
- فى حالة قمنا بكتابة **cdpsnarf** فقط سيقوم بتجميع معلومات من كل الinterfaces ويمكننا تحديد الinterface من خلال امر **cdpsnarf -i eth0**
- لكى نتمكن من رؤية جميع الinterfaces الموجودة على الجهاز نستخدم امر **ip add show**
- لكى نقوم بعمل CDP flood فاننا نقوم باستخدام اداة yersinia وهى اداة لها graphic interface ونقوم بتشغيلها من خلال امر **yersinia -G**
- جميع المعلومات القادمة من CDP يتم تخزينها فى CDP table واذا اردنا تنظيفه بعد عمليه cdp flood نقوم باستخدام امر **clear cdp table**



Mac spoofing



- Mac spoofing هو attack يتم على الswitch كتالى :
- يقوم الattacker بارسال رسالة الى الswitch وفى هذه الرسالة يقوم بتزييف الmac address ويضع address خاص بdevice اخر مما يجعل الswitch يقوم بجعل الdata الذاهبة الى الجهاز الاصلى تصل الى جهاز الattacker
- بنسبة للswitch لايمكن ان يتصل نفس الmac address فى two ports مختلفين وبذالك عندما يجد ان device يحمل نفس ال mac address فى port اخر فانه يقوم باذالة الport الاول من ال mac address table ويعتمد الport الجديد
- هذه الهجوم ليس له فاعلية كبيرة بسبب ان الdevice الاصلى اذا قام بارسال رسالة اخرى سيقوم الswitch بعدم ارسال الdata الى الattacker وسيقوم بارسالها الى الجهاز الاصلى

Mac address table overflow

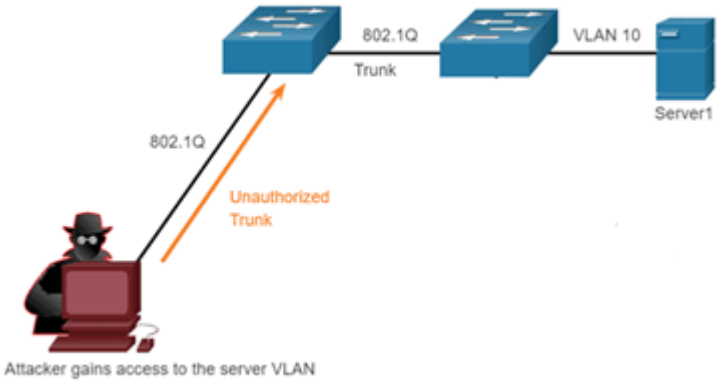
- يقوم هذا الattack على جعل الmac address table الخاص بالswitch يمتلئ مما يجعله يعمل كا hub وبتالى يتم ارسال جميع الpacket فى شكل broadcast
- يكمن خطورة هذا الهجوم فى ان الattacker سيكون لديه نسخة من اى data يتم ارسالها وانه قد يتسبب فى بطئ الnetwork بسبب كثرة الbroadcast
- يتم تنفيز هذا الهجوم من خلال اداة **macof** من خلال هذا الامر **macof -i eth0**

- فى حالة لم نقم بتحديد الinterface واكتفينا بكتابة **macof** سيقوم بتطبيق الهجوم على جميع الinterfaces

Port security

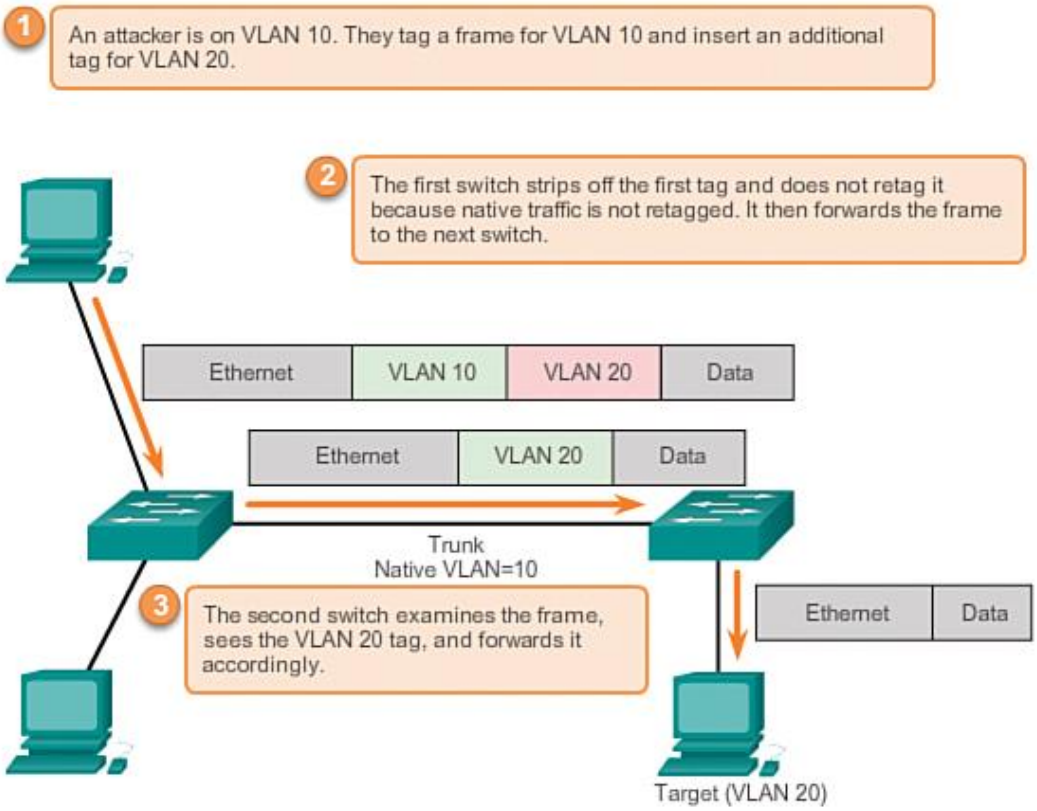
- يتم الحماية من الmac spoofing و من mac table overflow من خلال port security
- يتم الحماية من الmac address spoofing من خلال تطبيق port security violation وله ثلاث اشكال :
  1. Protected
  2. Restricted
  3. (default) Shutdown
- الفرق بين protected و restricted هو ان كلاهما يقوموا بمنع ارسال او استلام data فى حالة كان الmac address مختلف ولاكن restricted يقوم باظهار رسالة فى الconsole عن حدوث port security violation attack
- فى الshutdown يقوم بعرض الرسالة على الconsole ويقوم بوضع ال port فى حالة error disable
- للخروج من حالة الerror disable يتم الدخول على الinterface وعمل shutdown ثم no shutdown
- عند تنفيذ الport security يفضل ايقاف الinterface وهذا لمجموعة من الاسباب وهم :
  1. عند عمل shutdown للinterface يتم فقد كل الmac addresses التى تم تعلمها من خلال هذا الinterface وهذا جيد لازالة الmac addresses الاتية من mac table overflow attack
  2. عند تطبيق الviolation لن يحدث مشكلة عدم اختيار الmac الصحيح
- لتفعيل الport security يلزم تحويل الinterface الى access او trunk اولا ويحدث ذالك من خلال امر **switchport mode access** ثم يتم تنفيذ امر **switchport port-security**
- يتم تحديد الmac المسموح له الاتصال على هذه الport من خلال امر **switchport port-security mac-address** ويتم كتابة الmac address او يتم كتابة sticky وتعنى ان اول mac سيقوم بتواصل على هذا الswitch هو من سيتم السماح له بالاتصال
- فى حالة كان هناك ip phone متصل على هذ الinterface مع pc فيمكننا السماح باتصالهم من خلال جعل الmaximum 2
- يتم تحديد الviolation من خلال هذا الامر **switchport port-security violation** ثم يكتب نوع الviolation
- فى حالة عدم وجود امكانية لعملshutdown للport فيفضل عمل جميع الconfiguration واخر خطوة تكون امر switchport port-security
- لارؤية معلومات عن الport-security التى تمت نستخدم امر **show port-security**
- الport-security violation عند تطبيقه بالprotected او بالrestricted لايحمى من mac table overflow
- توجد طريقة اخرى لاخراج الport من حالة الerror disable وهى من خلال عمل recovery ويحدث ذالك من خلال امرين :
  1. **errdisable recovery interval 30** وهنا قمنا بتحديد المدة التى سيقوم الport بالرجوع للعمل مرة اخرة
     - اذا لم نقم بتحديد المدى سيقوم بالعمل بعد 5 دقائق
  2. **errdisable recovery cause psecure-violation** وهو يقوم بتحديد سبب وقوع الport وبعد ذالك يتم انتظار الinterval ويعاد تشغيله مرة اخرى
- عند وجود two switch متصلين معا فانه يكفى عمل maximum وتحديد الaging وهى المدة التى سيحمل الswitch الmac addresses
- لتحديد aging يتم ذالك من خلال امر **switchport port-security aging time** ثم نكتب المدة وتكون بالدقائق
- تظل الحماية السابقة غير مجدية فى حالة ان الattacker قام بتغير الماك الخاص به الى الmac المطلوب للاتصال ولاكن يمكن منع ذالك ايضا عند استخدام dot 1x

Vlan hopping



- يشمل نوعان من الattack وهم :
  1. switch spoofing
  2. double tagging
- vlan hopping attack بشكل عام يشمل الوصول الى vlan مختلفة
- switch spoofing يقوم على فكرة ان الport فى الشكل الdefault يكون dynamic بنسبة لDTP protocol وبتالى يمكن لجهاز الattacker ايهام الswitch انه switch وان الport الذى بينهم يكون trunk مما يسمح للattacker بارسال اى packet الى اى vlan
- يتم الحماية من هذا الattack من خلال تشغيل امر switchport mode access على الinterface المقابلة للPCs

- double tagging هو attack يقوم على فكرة ان :
  1. الportالمتصل يجب ان يكون فى الnative vlan
  2. ثم يقوم الattacker بوضع two tag على الpacket الtagالداخلى يكون خاص بvlan الPC المراد الهجوم عليه والtag الخارجى يكون الخاص بالnative vlan
  3. عند وصول الpacket الى الswitch يقوم الswitch باذالة الtag الخاص بالnative vlan لان الdefault يكون ان native vlan لا يوضع لها tag وبتالى سيتم اعتبار الpacket خاصة بالvlan الداخلية



- يعد هذا الattack اقل درجة فى الخطورة من switch spoofing بسبب :
  1. يلزم ان يكون الattacker فى native vlan
  2. يتم ارسال الpacket الى الجهاز المستهدف ولاكن الresponse لا يرجع الى الattacker وبتالى لايصلح لجميع الهجمات
     - يمكنه ان يصلح لهجمات مثل الDOS
- يمكن الحماية من هذا الattack من خلال جعل الswitch يقوم بعمل tagging لnative vlan ولاكن يجب تطبيق هذا الامر على جميع الswitches بالضافة الى ان ليس جميع الموديلات لديها هذا الoption وبتالى لايعد هذا حلا مناسبا
- الحل الافضل وهو ان نقوم بتغيير الnative vlan الى vlan اخرى ولانجعل لها اى port
- لو اختلفت الnative vlan فى الswitches فيمكنها التواصل معا لذالك اهم شئ فى الحماية من الattack هو عدم جعل لها اى ports
- لكى نرى معلومات عن الport مثل هل هو dynamic ام لا نستخدم امر **show int e0/0 switchport**
- يمكن تطبيق الswitch spoofing بسهولة من خلال اداة **yersinia** من خانة الDTP ويمكن تطبيق double tagging من خلال خانة 802.1q
- لتغير الnative vlan فاننا نستخدم امر **switchport trunk native vlan 999**

DHCP spoofing

- عند وجود اكثر من DHCP فى LAN واحدة فان من يعطى الIPs الى الاجهزة على الشبكة يعتمد على مدى سرعته وقربه من الجهاز الطالب للconfiguration
- لذالك فا هجوم DHCP spoofing يقوم الattacker فيه بتحويل جهازه الى DHCP ويسمى DHCP rogue
- يمكن للattacker ان يقوم بتوزيع IPs غير الموجودة فى الشبكة وذالك يجعل الdevices التى اخت منه IP غير قادرة على التواصل مع باقى الاجهزة ولاكن هذا السيناريو يعد بسيطا

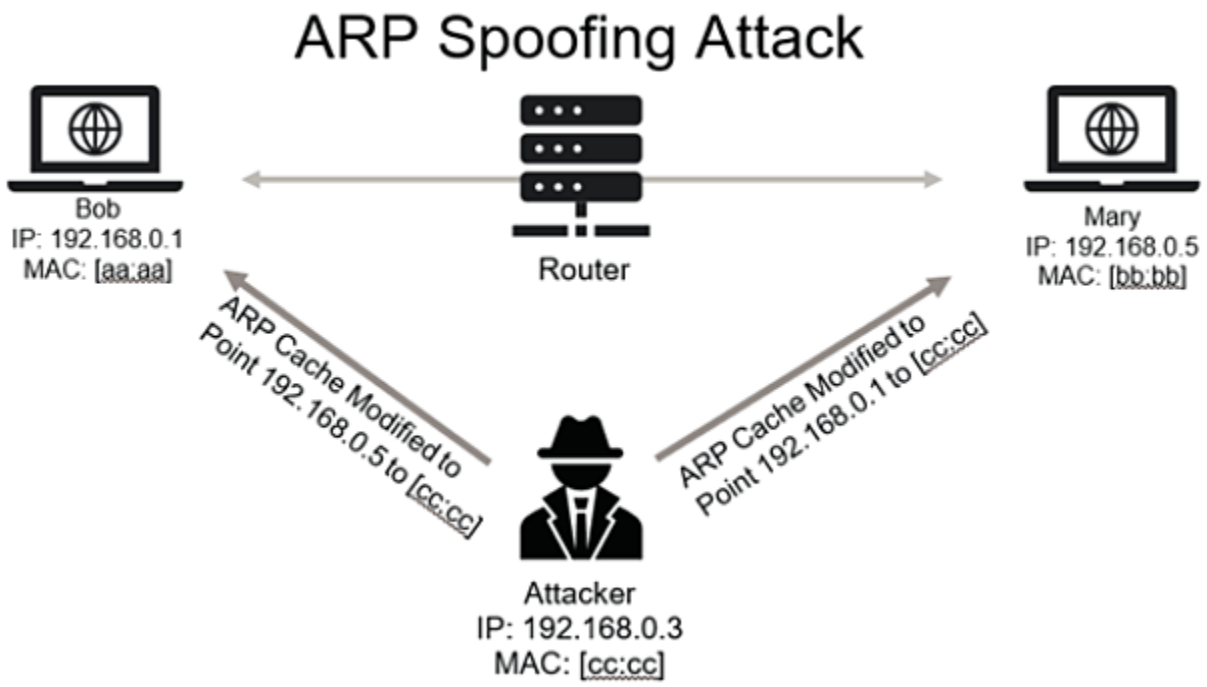
- سيناريو الattack الافضل هو :
  1. ان يقوم الattacker بعمل ما يسمى ب DHCP starvation وهو ان يقوم باخذ كل الIPs التى يوزعها الDHCP
  2. يقوم هو بتوزيع الIPs ويجعل نفسه الgateway
  3. يقوم بارسال الdata الى الgateway الحقيقة وبتالى فهو اصبح man in the middle
- يتم الحماية من هذا الattack من خلال الDHCP snooping باستخدام هذا الامر **ip dhcp snooping vlan 1**
- عدم تحديد الvlan فى الامر السابق قد يؤدى الى عمل load ضخم على الswitch
- بعد تحديد الvlan الذى سيعمل عليه الDHCP snooping فانه يجب تشغيله لكى يبدا العمل ويحدث ذالك من خلال امر **ip dhcp snooping**
- الامر السابق يقوم بجعل جميع الports لا تنقل DHCP discover request لذالك يجب ان نقوم بجعل الports المؤدية الى DHCP server تكون trusted وذالك من خلال الدخول على الport وتنفيذ هذا الامر **ip dhcp snooping trust**
- الاوامر السابقة تمنع اى device من ان يعمل كا DHCP غير الDHCP الحقيقى ولاكنها لاتمنع DHCP starvation
- لكى نمنع الDHCP starvation فننا نحدد عدد الrequests التى يمكن للPC عملها للDHCP وفى الطبيعى تكون 2 (discover, request) لزالك نستخدم الامر الاتى **ip dhcp snooping limit rate 3**
- فى الامر السابق قمنا بتحديد عدد الrequests الى 3 وليس 2 لان اول discover غالبا ما تفقد ولاتصل الى الDHCP
- بعد تطبيق الlimit اذا قام الattacker بعمل starvation فان الport سيقع فى حالة الerror disable
- الاداة المستخدمة فى هذا الattack تسمى ettercap ولتشغيلها فى واجهة رسومية نستخدم امر **ettercap –G**
- فى حالة وجود DHCP فى LAN فا من الطبيعي ان الاجهزة الموجود فى LAN مختلفة ان لا تحصل على IP منه لان رسالة الdiscover تكون broad cast والroutersلايقومو بتمريرها
- لحل المشكلة السابقة فاننا نقوم بكتابة هذا الامر على الrouter فى الinterface المواجهة للاجهزة التى ستحتاج ip **ip helper-address 11.0.0.10** وهو يجعل الrouter عندما يجد رسالة discover فانه يقوم بتحويلها الى single cast ويقوم بارسالها الى الDHCP صاحب الIP المعطى فى الامر
- عندما يقوم الrouter بتحويل رسالة الdiscover الى unicast ويرسها الى الDHCP فانه يقوم باضافة معلومة تسمى GIADDR او relay agent ويقوم بوضع فيها الip الخاص بinterface router التى استقبلت رسالة الdiscover وهى ما تقوم بتعريف الDHCP اى pool سيعطى منه ip
- اغلب الswitches عند تفعيل عليها الDHCP snooping فانها تبدأ بوضع GIADDR ب 0 بالاضافة الى ان CISCO routers عندما تجده له قيمة ب0 فانه يقوم بعمل drop للpacket
- حل المشكلة السابقة يمكن ان يتم بستخدام اكثر من حل كتالى :
  1. ناتى على الswitch ونمنعه من وضع GIADDR من خلال هذا الامر **no ip dhcp snooping information option**
  2. ناتى على الrouter ونجعله يقبل الرسائل التى ب GIADDR 0 من خلال هذا الامر **ip dhcp relay information trusted**
- عند تفعيل الDHCP snooping فانا الswitch يقوم باستخدام جدول يسمى DHCP snooping binding table وهو يحتوى على الdevices التى اخذت IP من الDHCP والports الخاصة بها والمذيد من المعلومات ونقوم بعرضه من خلال امر **show ip dhcp snooping binding**

```
IOU1#show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  ----------
00:50:79:66:68:00   10.0.0.2        86283       dhcp-snooping   1     Ethernet0
/2
Total number of bindings: 1
```

- هذا الtable يعد مهما فى الحماية من انواع attacks اخرى لذالك يجب ان يكون له backup لذالك نستخدم هذا الامر **ip dhcp snooping database** ونقوم باضافة disk او TFTP server
- لعمل DHCP starvation فاننا نستخدم اداة الYersinia

ARP spoofing and DAI

- ARP protocol يستخدم للاتيان بالmac الخاص بجهاز فى الLAN وعند الاتيان به يتم حفظه فى cache
- يمكن رؤية الcache الخاصة بالARP من خلال امر **arp -a** على الpc
- عند تغير الNIC الخاصة بdevice معين فان الdevices التى تريد الاتصال به يجب ان تعرف الMAC الجديد وتقوم باذالة القديم فى الARP cache لذالك نستخدم protocol يقوم بهذه المهمة يسمى gratuitous ARP
- هنا الattacker يقوم باستعمال هذا الprotocol لكلى يوهم الdevices ان الmac الخاص به هو الخاص بالdefault gateway وهنا يمكنه :
  1. الاكتفاء بهذا وسيكون قد منع الاجهزة من الاتصال على الinternet وسيصبح الوحيد القادر على ذالك



2. ان يقوم بتحويل الtraffic الى الdefault gateway وبتالى يصبح man in the middle

- للحماية من هذا الattack نستخدم DAI وهو اختصار ل dynamic arp inspection
- DAI يعتمد على binding table الخاص بالDHCP snooping حيث انه يقوم بالتحقق من كون معلومات الgratuitous arp صحيحة من خلال معلومات binding table واذا لم تكن سمينع مرورها وسيقوم بعرض رسالة على الconsole
- يتم هذا الattack من خلال اداة ettercap
- امر **show arp** يقوم بعرض الarp cache فى الrouter ولازالته نستخدم امر **clear arp**
- لتفعيل الDAI نستخدم امر **ip arp inspection vlan** ونقوم بتحديد الvlan
- فى حالة اردنا الاتصال على device غير معلوم الmac الخاص به وايضا لديه static ip فابسبب الDAI لن نستطيع لان عند الاتيان بالmac الخاص به من خلال الarp سيقوم بمقارنة الpacket بالمعلومات الموجودة فى binding table ولن يجدها وبتالى لن تمر arp packet وبتالى لن يحدث اتصال
- السيناريو السابق يحدث عند الاتصال بserver او بgateway او اى device ياخذ ip static
- يمكن حل المشكلة السابقة من خلال واحد من الاتى :
  1. جعل الport المتصل به الstatic ip يكون trusted وذالك من خلال الدخول على الport واستخدام امر **ip arp inspection trust**
     - هذا الحل مفيد جدا عند وجود two switches متصلين معا فنجعل الports التى بينهم trusted
  2. نقوم بتطبيق ARP access list على الswitch
     - هذا الحل فى حالة كان الجهاز صاحب الstatic ip هو server لانه يمكن للattack الاتيان منه وبتالى جعله trusted سيكون مشكلة
  3. اضافة الhost الى الbinding table بشكل يدوى
- لعمل arp access list نستخدم امر **arp access-list list1** وهنا list1 هو اسم الlist
- لسمح للجهاز صاحب static ip نستخدم امر **permit ip host 192.168.1.1 mac host F801.19A2.FF2A** حيث ان 192.168.1.1 هو ip الجهاز و F801.19A2.FF2A هو الmac الخاص بالجهاز ثم نستخدم امر **ip arp inspection filter list1 vlan 1** حيث list1 اسم الlist المرد تطبيقها على DAI
- امر الpermit يكتب داخل الarp access list وامر تطبيق الlist يحدث فى الconfiguration mode
- لرؤية الarp access list نستخدم امر **show arp access-list**
- عند تفعيل الDAI فان جميع الinterfaces التى ليست trusted فيكون لها limit لعدد الpacket فى الثانية وهو 15 وفى حالة قام جهاز بارسال عدد اكثر سيقع الport فى حالة الerror disable
- لتغير الrate limit نستخدم امر **ip arp inspection limit rate 30** حيث 30 هو الrate limit

IP spoofing

- من هجمات الDOS التى تحصل :

1. Ping flood
2. SYN attack

- يقوم SYN attack على عمل الكثيرمن three way handshake بدون ارسال ACK فى النهاية من ما يتسبب فى ان الsession تظل مفتوحة على server
- يقوم الIP spoofing على تزوير الIP عند عمل attacks مثل SYN attack وبتالى لايمكن منع الattacker او وضعه فى blacklist واحينا ما يتم ذالك من خلال جعل الIP الموجود فى الpacket يكون ip الخاص بالجهاز الحاصل عليه الattack وبتالى لن يقوم بوضع نفسه فى blacklist
- للحماية من هذا الattack فاننا نستخدم Source guard وهو عبارة عن امر يستفيد من binding table الخاص بالDHCP snooping لكى يقارن معلومات الpacket بالموجودة فى الtable واذا لم تكن صحيحة فان الpacket لن تمر من الswitch
- الاداة المستخدمة فى تنفيز ping flood attack او SYN attack هى اداة **hping3** ولعمل ping flood نستخدم امر **hping3 -I --flood 192.168.1.1**
- لتزوير الip فاننا نقوم باضفة a- ثم الip كتالى **hping3 –I flood -a 192.168.1.20 192.168.1.1** ويمكن جعل الip الموزور هى نفس الip الذى نقوم بالattack عليه
- لعمل SYN attack نستخدم الامر الاتى **hping3 -V -c 1000 -d 100 -S -p 21 --flood -a 192.168.1.20 192.168.1.1** حيث :
  1. -V verbose mode
  2. -c count number
  3. -d packet size
  4. -S SYN attack
  5. -p port number
- يتم الحماية من هذا الattack من خلال الدخول على الinterfaces الخاصة بالPCs و كتابة امر **ip verify source** ويمكن رؤية الconfiguration التى تمت من خلال امر **show ip verify source**
- فى حالة كان هناك جهاز يحتوى على IP static فلن يكون موجود فى binding table وبتالى سيكون غير قادر على الاتصال
- يمكن حل المشكلة السابقة من خلال اضافتة فى الbinding table بشكل static من خلال الامر
  Ip source binding 000C.299D.4B09 vlan 1 192.168.1.5 int e0/2 حيث:
  1. 000C.299D.4B09 هو mac الخاص بالجهاز
  2. 1 هى الvlan
  3. 192.168.1.5 هو ip الجهاز
  4. e0/2 هى الinterface المتصل به ال الجهاز فى الswitch
- لكى نرى الsource binding نستخدم امر **show ip source binding**

LAN security feature

- وهم بعض الfeatures التى تعمل فى الLAN والتى تقوم بالحماية من بعض الattack ومنها :

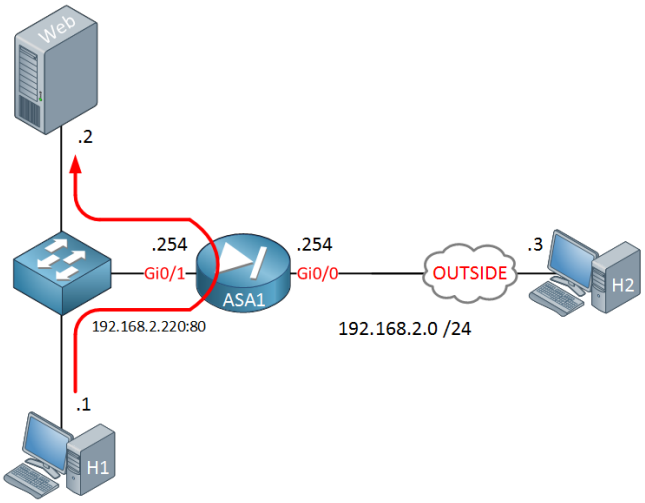
1. Protected ports

- وهى واحدة من الfeatures والتى تمنع مجموعة من الاجهازة من التواصل معا
- هذه الخاصية تتم من خلال تحويل الport الى protected
- يتم تحويل الport الى protected منم خلال امر **switchport protected** داخل الport
- جميع الdevices المتصلة بport protected لاتستطيع التواصل معا
- هذه الخاصية لا تعمل على switches مختلفة اى ان two devices فى protected ports يستطيعو التواصل معا اذا كانو فى switches مختلفة

2. Private VLAN

- هى طريقة افضل من الprotected ports فى منع اجهزة معينة من التواصل معا
- تقوم على تقسيم الvlan الواحدة الى اكثر من sub vlan وتسمى الvlan الاساسية بprimary VLAN
- يوجد نوعان من الsub VLAN وهم isolated و community ولاكن يجب الا يكون هناك اكثر من isolated vlan والباقى يكون community
- الاجهزة الموجودة فى الisolated vlan لن تسطيع التواصل معا وبالاضافة الى ذالك الاجهزة التى فى community vlan مختلفة لن تسطيع التواصل معا ولن تستطيع التواصل مع من فى الisolated
- عدم تمكن الاجهزة فى isolated vlan من التواصل معا يعد خاصية مهمة للsecurity لانها تقوم بعزل الاجهزة عن بعضها
- لكى نجعل port قادر على التعامل مع جميع الsub vlans فاننا نقوم بتحويله الى promiscuous وهذا يحدث مع الports المتصلة بالrouter
- تتميز الprivate vlan عن الprotected port فى انها تتعامل عبر الswitches عكس الprotected port والتى تعمل على نفس الswitch فقط

- لكى يتم تطبيق الvlan private وتكون على اكثر من switch فهناك طريقتان :
  1)ان يكون الswitches على transparent mode
  2) ان يتم تشغيل الVTP v3 على الswitches وهذا هو الحل الافضل
- من مزايا الVTP v3 هو انه سيقوم بنقل الconfiguration الخاصة بالvlans و sub vlans مما يسهل عملية الconfiguration
- الVTP v3 يعمل على الswitches من اول version 15 لذالك فى حالة كان الswitch اقدم من ذالك فانقوم بستعمال الطريقة الاولة وهى جعل الالswitch يعمل فى transparent mod ونقوم بعمل الconfiguration يدوى على جميع الswitches
- لكى يعمل الVTP v3 على الswitch الاخر يجب بطبع ان يكون ال link بينهم trunk وايضا يكونو لهم نفس الdomain
- يتم نقل الdomain من switch الى اخر تلقائيا اذا كان موجود بnull ولان اذا احتوى على قيمة فلن يتم تغيره الا يدويا
- يتم التحويل الى VTP v3 من خلال امر **vtp version 3** ويلزم تحويله على جميع الswitches
- لكى يتم نقل الالمعلومات من خلال VTP v3 يلزم تحويل واحد من الswitches الى primary server وذالك من خلال امر **vtp primary vlan**
- لكى نقوم بانشاء private vlan فاننا نستخدم امر vlan ثم رقم الvlan مثل الطبيعي ولاكن بعد الدخول على الconfiguration الخاصة بالvlan نقوم بكتابة امر **private-vlan isolated** لتحديدها كا isolated ويمكن تغير كلمة isolated الى community
- لتحديد الvlan primary فاننا نقوم باذالة isolated ونضع primary ليصبح الامر **private-vlan primary** وبعده نستخدم امر **private-vlan association 200,300,400** لكى نضع كلا من 200 و 300 و 400 كا sub vlans تحت الprimary
- يمكن استخدام امر **private-vlan add** او نستبدل add ب remove لكى نضيف او نزيل sub vlan ويتم اضافة رقم الvlan بعد الامر
- VTP v3 يقوم بنقل الvlans وال sub vlans ولاكنه لايقوم بنقل الports الموضوع عليها الvlans
- لكى نضع port فى sub vlan فاننا نقوم بتحويله الى private vlan host من خلال امر **switchport mode private-vlan host** ثم نقم باضافته من خلال امر **switchport private-vlan host-association 100 200** حيث ان 100 هى الvlan primary و 200 هى secondary
- الlinks بين الswitches يجب ان تكون trunk بينما فى الlink الخاص بالrouter (المسموح لاى جهاز بالاتصال عليه) يجب ان تكون promiscuous وذالك من خلال امر **switch port mode private-vlan promiscuous** وبعد ذالك يتم تحديد ما هى الvlans المسموح لها الاتصال عبره وذالك من خلال امر **switchport private-vlan mapping 100 200,300,400** حيث 100 هى الvlan primary بينما الvlan200 و 300 و 400 هم الvlans private المسموح لهم الاتصال عبره
- يوجد attack يمكن تنفيزه على الvlans private ويسمى hair pin routing وهو يقوم على عمل static routing بحيث يقوم بارسال الpacket الى الrouter ويقوم الrouter بارسالها الى الvictim وبتالى يمكنه الاتصال مع device اخر غير موجود معه على نفس الcommunity
- يمكن الحماية من هذا الattack من خلال تطبيق ACL فى الrouter تقوم فيها بمنع اتصال الشبكة بنفسها
- لايوجد routing بين الsub vlans



3. Storm control

- الCPU الخاص بالswitch هو من يقوم بتعامل مع ال mac addresses الخاصة بالbroadcast و الmulticast
- هناك ما يسمى بunknown cast وهى الunicast packet ولاكن الdestination mac غير معروف ويتم التعامل معاها ايضا من خلال الCPU
- Storm control هى خاصية تحدد limit لعدد الpacket التى يجب ان يتعامل معاها الswitch
- يتم استخدام الstorm control من خلال امر **storm-control broadcast level pps 2** حيث :

			نوع الsignal
• تستخدم بتحديد نسبة مئوية للlimit	level <0.00-100.00>	• يتم اختيارها لتحديد limit للbroadcast signal	**broadcast**
• تستخدم لتحديد الlimit بbit per second	bps	• تستخدم لتحديد الlimit للmulticast signal	**multicast**
• تستخدم لتحديد الlimit بpackets per sec.	pps	• تستخدم لتحديد limit الunknown cast signal	**unicast**

- عند تحديد الlimit بعدد packet معين فان باقى الpackets سيحدث لها drop
- لرؤية الconfiguration الخاصة بال control storm نستخدم امر **show storm-control**

- يمكن تحديد action معين يقوم به الswitch فى حالة حدث storm من خلال امر **storm-control action shutdown** وهنا سيقوم بعمل shutdown للport ويمكن اذالة shutdown و وضع trap وهى تقوم بارسال syslog بحدوث storm
- يتم تنفيذ امر storm داخل الconfiguration الخاصة بالinterface

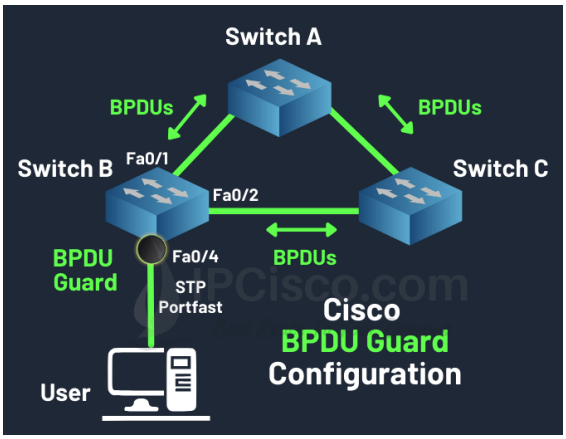
4. Port blocking
   - هى خاصية تقوم بعمل block لاى packet غير معروفة للswitch ويمكن ان تكون هذه الpacket من نوع unicast او من نوع multicast
   - يتم تطبيق الport blocking من خلال امر **switchport block unicast** او نستبدل unicast ب multicast
   - يتم تطبيق الامر السابق من داخل الinterface
   - لاينصح بتشغيل هذا الfeature لانه قد يتسبب فى كثير من المشاكل
5. Control plane rate limiting
   - وهى تقوم على تحديد limit لprotocol معين وتتيم كتالى **psp arp pps 2** حيث يمكن تحديد dhcp او igmp بدلا من الarp
   - لايفضل تشغيل هذه الخاصية بسبب وجود بدائل افضل مثل تفعيل DHCP snooping فى DHCP protocol
6. Resilient configuration and IOS
   - هو feature يقوم على حماية الIOS و الconfiguration من حدوث delete لهم
   - يتم هذا الfeature من خلال تنفيز امر وهو **secure boot-image** لحماية الIOS و **secure boot-config** للحماية الconfiguration

STP Optimization

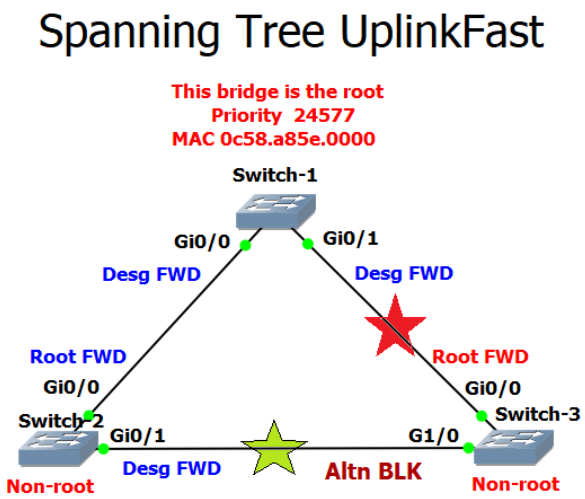
- STP هو protocol يستخدم لمنع حدوث loop عند انتقال الbacked فى الشبكة
- يوجد من STP عدة versions مثل :
  1. Common STP
  2. PVST وهو مثل common ولاكن يدعم الvlan ويعمل على vlan بشكل مستقل
  3. Rapid PVST+

STP convergence optimization

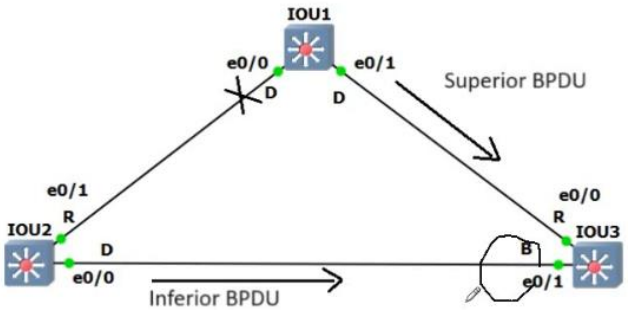
- هى مجموعة من الfeature التى تستخدم لتسريع بروتوكول STP
- بنسبة لحالة الport فى الSTP فيوجد حالتان :
  1. Block تعنى انه لا يعمل
  2. Forward تعنى انه يعمل ومتصل بdevice
- لكى ينتقل الport من block الى forward سيحتاج الى 30 ثانية
- يجب تحويل الport الى port fast فى الports المتصلة بالPCs وهذا يقلل من وقت تحول الport الى forward الى حدود ثانيتين
- رسالة BPDU لها نوعان وهم :
  1. Configuration BPDU وهى التى ترسل من الroot switch الى باقى الswitches
  2. TCN (topology change notification) ويتم عملها من اى switch عند حوث تغير فى الconnections
- TCN تقوم بجعل الswitches تقوم بحذف الmac address table عند جدوث اى تغير فى الاتصال
- تحويل الport الى fast port يمنع الswitch من ارسال TCN عند حدوث له تغيير ويكتفى بارسالها فقط عند حدوث تغيير فى باقى الports
- لتحويل port الى port fast فاننا ناتى على الport ونقوم بتحويله الى access ثم نستخدم امر **spanning-tree portfast**
- عند تطبيق الportfast على port ثم يعاد استخدام هذا الport مرة اخرى على switches فيؤدى ذالك الى loop ويمكن الحماية من هذا السيناريو من خلال استخدام **BPDU guard** مع الportfast
- BPDU guard هى خاصية يتم تطبيقها على الport وتقوم على ان هذا الport لايجب ان يستلم BPDU واذا حدث واستلم واحدة سيقع فى حالة error disable
- يتم تشغيل الBPDU guard من خلال امر **spanning-tree bpduguard enable**
- يمكن تحويل الrouter الى switch من خلال استخدام امر **bridge 1 protocol ieee** ثم نقوم بضم الinterfaces الى bridge 1 من خلال الدخول على الinterface واستخدام امر **bridge-group 1**
- يمكن تنفيذ الportfast بشكل global على مستوى الswitch من خلال امر **spanning-tree portfast edge default** وهو يقوم تلقائيا بجعل الport يتحول الى portfast عند تحوله الى access mode
- يمكن تفعيل الBPDU guard بشكل global من خلال امر **spanning-tree portfast edge bpduguard default** وهو يقوم بتشغيل ال BPDU guard فى حالة كان الaccess port
- لكى نمنع portfast او bpduguard فى interface معينة فاننا نقوم بدخول عليها واستخدام امر **spanning-tree bpduguard disable** ويمكن استبدال كلمة bpduguard بكلمة portfast
- فى حالة كان الlink يتصل بserver فان الlink يجب ان يكون trunk وبتالى سيصعب عمل له portfast ولاكن يمكن تخطى ذالك من خلال امر **spanning-tree portfast edge trunk**
- توجد خاصية تسمى بالuplink fast وهذه الخاصية تساعد الconnection التى بين الswitches على ان تقوم بشكل سريع بدلا من استغراقها 30 ثانية
- هذه الخاصية تكون مفعلة بشكل تلقائي فى rapid PVST
- يتم تفعيل الuplink على الswitch بشكل global وليس على ports معينة
- فى حالة حدث خلل فى اى من الports وتحول احدهم من الblock الى الforward سيحدث ذالك فى 2 او 3 كاكثر تقدير ولاكن فى حالة روجع هذا الport مرة اخرى للblock فانه سياخذ 35 ثانية



- يجب ان يتم تطبيق الuplink على access switch وليس distribution او core switch لان عند تطبيق uplink وتحول port من block الى forward سيقوم هذا الswitch بارسال الmac addresses عبر هذا الlink بمعدل 150pbs والذى يعتبر معدل كبير ولذالك كونه distribution او core يعنى انه يحمل الكثير من الmac address وبتالى هذا سيكون load كبير على الswitches التى تتلقى الmac addresses
- قامت CSICO بتجنب المشكلة السابقة من خلال انها تقوم بتغيير الpriory الخاصة بالswitch المطبق عليه الuplink وتزيدها بمقدار 49152 وايضا تقوم ذيادة الcost الخاص بالlinks الى 3000 لكى تتاكد من عدم تحول هذا الswitch الى core او distribution
- لتشغيل الuplink ناتى فى الconfiguration mode ونستخدم امر **spanning-tree uplinkfast**
- لرؤية معلومات عن الspanning tree نستخدم امر **show spanning-tree summary**
- لكى نقوم بتعديل الrate الخاص بارسال الmac address فاننا نستخدم هذا الامر **spanning-tree uplinkfast max-update-rate**



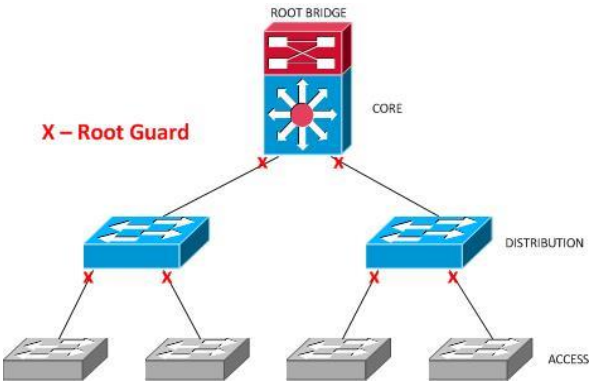
- الblock port لايقوم باستلام data او ارسال BPDU ولاكنه يقوم باستلام BPDU ويقوم بعمل لها process ولاكن لايقوم ايضا بتمريرها
- الBPDU التى ترسل من خلال الROOT تسمى superior BPDU
- فى الصورة المقابلة عند حوث مشكلة فى الLink الذى بين root و الdesignate switch فان الdesignate switch سيقوم باختيار root جديد وسيضع نفسه الroot وسيقوم بارسال رسالة الى باقى الswitches وتسمى inferior BPDU ليعلمهم بانه اصبح الroot
- المشكلة فى المثال السابق هو ان باقى الswitches متصلة بالroot الحقيقى ولاكن بسبب ان الport بين هاؤلاء الswitches وroot الجديد يكون block فهم لا يستطيعون اخباره بان الroot ماذال يعمل وانه لايجب ان يتحول الى root ولكى يقومو بتحويله من block الى forward فانه سيحتاج الى 50 ثانية



- توجد خاصية تقوم بحل مشكلة التاخير الموجودة فى المثال السابق وتسمى backbone fast وهى ايضا تكون مفعلة تلقائيا فى rapid PVST
- يقوم backbone fast بحل المشكلة السابقة من خلال انه عندما يستقبل الswitch رسالة inferior BDPU يقوم فورا بارسال رسالة تسمى RLQ او root link query الى الroot مما يجعل الroot يرد عليه برسالة RLR او root link replay وهذه العملية تختصر 20 ثانية على قيام الport من حالة الblock الى الforward
- يتم تفعيل الbackbone fast على جميع الswitches وليس فقط الaccess switch كما فى الuplink
- يتم تفعيل الbackbone fast من خلال امر **spanning-tree backbonefast**

STP filter

- عندما يكون من المفترض ان لا يستقبل الswitch ب BPDU من port معين ولاكن قام بستقبلها فان الSTP filter هى طرق التعامل مع هذه الحالة
- من امثلة الSTP filter هو BPDU guard
- يوجد حل اخر وهو BPDU filter وهو يختلف عن الBPDU guard فى انه لايجعل الport فى حالة error disable اذا استلم BPDU
- فى حالة تم تفعيل الBPDU filter على مستوى الinterface فان الinterface لن يقوم بارسال او استلام BPDU واذا قام باستلام واحدة سيقوم بعمل لها drop وهذه الطريقة لا يفضل استخدامها لانها قد تتسبب فى loop
- فى حالة تفعيل الBPDU filter على مستوى global فان جميع الinterfaces التى تكون portfast لن تتمكن من ارسال BPDU ولاكن ستستقبل BPDU وستقوم بعمل لها process
- لتفعيل BPDU filter على مستوى global فاننا نستخدم امر **spanning-tree portfast edge bpdufilter default**
- لرؤية الBPDU التى يتم ارسالها و استقبالها من port معين نستخدم امر **show spanning-tree int e0/0 detail | in BPDU** ولكى نقوم بعمل clear للعداد فاننا نستخدم امر **clear spanning-tree counters**
- بعد عمل clear سيقوم الinterface بارسال مجموعة من الBPDU حتى وان كان مفعل عليه portfast ثم سيقوم بثبات
- لتفعيل الBPDU على مستوى الport نستخدم امر **spanning-tree bpdufilter enable**



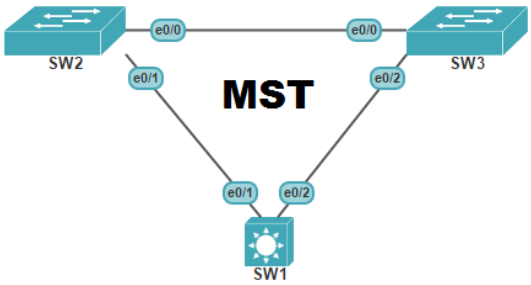
- واحد من اهم STP filter هو root guard وهو يقوم على سيناريو امكانية ارسال switch برسالة superior BPDU الى root switch عن طريق الخطاء او حتى وجود attacker قام بارسال superior BPDU افضل من التى لدى الroot switch
- السيناريو السابق يمكن ان يقوم به الattacker للحصول على man in the middle
- Root guard يقوم بمنع اى switch اخر غير الcore switch من ان يصبح هو الroot
- يتم تطبيق الroot guard على core switch وعلى distribution switch ويفضل تطبيقه ايضا على الaccess switch
- فى حالة قام واحد من الinterfaces الموجود عليها الroot guard باستلام superior BPDU سيقوم بايقاف الport فى حالة root inconsistence حتى يتوقف ارسال الsuperior BPDU
- لارجاع الport او الinterface الى الconfiguration الdefault فانه يمكننا :
  1. عمل **show run int e0/0** و رؤية الconfiguration ومن ثم وضع no قبل السطر الذى اريد ايقافه
  2. استخدام امر **default interface e0/0**
- لرؤية الports التى فى حالة inconsistency فاننا نستخدم امر **show spanning-tree inconsistentports**

Loop prevention

- عندما يكن من المفترض ان يستلم الswitch رسالة BPDU ولاكن لايجدها فهنا نقوم باستخدام loop prevention لمنع حدوث loop محتمل
- عندما يكون هناك port فى حالة الblock فانه يستلم BPDU يقوم بعمل لها process ولاكن لايقوم باستلام data ولاكن فى حالة لم يقم باستلام BPDU يقوم بعتبار ان الlink لم يعد موجود وبتالى سيقوم بالرجوع الى حالة الforward ويبدا العمل
- المشكلة فى السيناريو السابق ان ايقاف الlink ليس السبب الوحيد لعدم وجود BPDU ولاكن يمكن ان يكون الlink متصل بشكل جيد ولاكن مفعل عليه ما يمنع ارسال الBPDU وذالك يمكن ان يحدث على سبيل المثال من خلال تشغيل الBPDU filter على مستوى الport
- فى حالة لم يستلم الswitch الذى لديه port فى حالة الblock رسالة الBPDU فانه لن يقوم بتشغيل الport وانما سيقوم بوضع الport فى حالة loop inconsistent
- الخاصية التى تحمى من المثال السابق تسمى loop guard ويتم تشغيلها من خلال النزول على الport واستخدام امر **spanning-tree guard loop**
- يمكن تفعيل الloop guard بشكل global من خلال امر **spanning-tree loop guard**default
- فى بعض الحالات عندما يحتوى الlink بين الswitches على مسار للارسال ومسار للاستلام ويحدث خطاء فى مسار الارسال فان المشكلة السابقة يمكن ان تحدث حيث سيقوم الport الذى فى حالة الblock الى الforward متقدا بعدم وجود الlink مما يؤدى الى امكانية حدوث loop
- السيناريو السابق يمكن ان يحدث فى الfiber optics cable
- يمكن الحماية من هذا السيناريو من خلال استخدام UDLD وهى اختصار ل unidirectional link dedication
- عند تفعيل الUDLD فان له two mod وهما :
  1. Normal mode وهو يكتفى فقط باظهار syslog او حتى ارسالها الى SNMP server
  2. Aggressive mode سيجعل الinterface يقع فى حالة error disable
- يفضل تشغيل كلا من loop guard و UDLD معا بسبب ان كلا منهم مكمل للاخر حيث ان loop guard يستطيع معرفة مشكلة الSTP ولايمكنه معرفة المشكلة الphysical وعلى العكس تماما الUDLD
- يقوم UDLD بستعمال well known mac address وهو 01:00:0C:CC:CC:CC وهو يستخدم ايضا من قبل الكثير من الprotocols مثل vtp
- يتم تفعيل الUDLD على كلا الswitches اى طرفى الاتصال الخاص بالlink
- لكى يتحقق الUDLD من الlink فانه يرسل رسالة UDLD message كل 15 ثانية ويمكن تعديل هذه المدة من خلال امر **udld message time** ثم يتم اعطاء المدة
- لتفعيل الUDLD نستخدم امر **udld enable** ونقوم باستبدال كلمة enable بكلمة aggressive لتشغيله ولاكن فى وضع الaggressive
- لتفعيل الUDLD على الtwisted pair فاننا يجب ان نقوم بتفعيله من داخل port وليس global وذالك من خلال امر **udld port** ونقوم باضافة aggressive اذا كنا نريد تفعيل الaggressive
- فى حالة كان UDLD مفعل بشكل global وايضا داخل الport فما سيتم تطبيقه هو ما داخل الport
- لكى نرى الUDLD على الports نستخدم امر **show UDLD**

MST (multiple spanning protocol)

- ظهر PVST لكى يحل مشكلة common STP فى عدم دعمه للvlans وظهر MST لكى يحل مشكلة الPVST فى كثرة الprocessing الناتج من كون كل vlan لها spanning tree منفصل
- يقوم MST بحل المشكلة السابقة من خلال جعل مجموعة من الvlans فى group واحد ويقومو بالعمل معا ويطلق على هذا الgroup ب instance
- يعد MST مناسب جدا للorganization ذات الحجم الكبير والتى تحتوى على الكثير من الvlans
- فى الMST يتم تقسيم الشبكة الى عدة regions وكل واحدة يكون لها regional root خاص بها ويتم اختيار واحد من الregional roots لكى يصبح root لكامل الtopology
- فى كل region يعمل الRSTP بين الswitches الخاصة بالregion فقط بينما ما يربط كل regions معا هو common STP



- الswitches التى لديها نفس الinstances و نفس الname و نفس الrevision number تكون فى نفس الregion
- من الافضل ان لا تذيد عدد الinstance عن 3 او 4
- الdefault ان جميع الvlans تكون تحت instance 0
- يفضل تشغيل VTPv3 على الswitches لكى يقوم بنقل الvlans والconfiguration الخاصة بMST
- لتشغيل VTPv3 نستخدم امر **vtp version 3**
- يجب استخدام هذا الامر على جميع الswitches لجعلها second server فى الMST **vtp mode server mst** ولجعل هناك switch يكون ال primary sever ويقوم بتوزيع الconfiguration الخاصة بالmst فاننا نستخد امر **vtp primary mst** ولجعله يوزع الvlans نستخدم **vtp primary vlan**
- لرؤية معلومات عن الvtp فاننا نستخدم امر **show vtp st**
- يفضل فى الMST عمل الconfiguration اولا ثم نقوم بتشغيلها
- **Spanning-tree mst configuration** هو ما نستخدمه لدخول الى configuration الخاصة mst وهى تحتوى على مجموعة من الخيارات كتالى

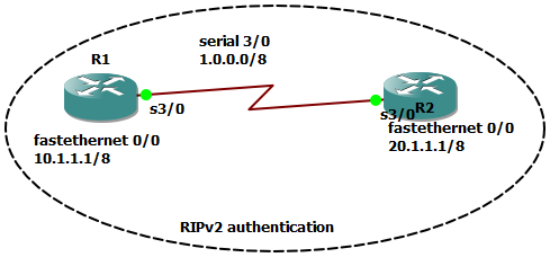
```
IOU1(config)#spanning-tree mst configuration
IOU1(config-mst)#?
  abort          Exit region configuration mode, aborting changes
  exit           Exit region configuration mode, applying changes
  instance       Map vlans to an MST instance
  name           Set configuration name
  no             Negate a command or set its defaults
  private-vlan   Set private-vlan synchronization
  revision       Set configuration revision number
  show           Display region configurations
```

- يجب الالتزام بنفس الinstance و بنفس الname و نفس revision number فى نفس الregion
- لوضع اسم للregion نستخدم امر **name MST** وهنا MST هو الاسم ويكون ايضا case sensitive
- لتحديد الrevision number نستخدم امر **revision 100** حيث ان 100 هى الrevision number
- لانشاء الinstance نستخدم امر **instance 1 vlan 10-19** حيث 1 هو رقم الinstance و 10-19 هى rang من الvlans التى ستوضع فى instance 1
- لرؤية الconfiguration الخاصة بالmst نستخدم امر **show spanning-tree mst configuration**
- لتشغيل الmst نستخدم امر **spanning-tree mode mst** ونقوم بهذا الامر على جميع الswitches
- لرؤية المعلومات حول mst معينة نستخدم امر **show spanning-tree mst 1** حيث 1 هو رقم الmst
- لجعل switch معين هو الprimary لinstance معينة نستخدم امر **spanning-tree mst 2 root primary** حيث 2 هنا هو رقم الinstance
- عند ارسال packet من region الى اخرى فان الpacket يجب ان تعبر من خلال topology root
- لكى نقوم بارجاع switch من VTPv3 الى VTP v3 فاننا نستخدم امر **vtp version 2** ولاكن قبلها يجب تحويله الى transparent بنسبة للmst وذالك من خلال امر **vtp mode transparent mst**
- لؤرية المعلومات عن الtopology كاملة نستخدم امر **show spanning-tree mst** ولاكن بدون استخدام رقم للmst

Routing protocols authentication

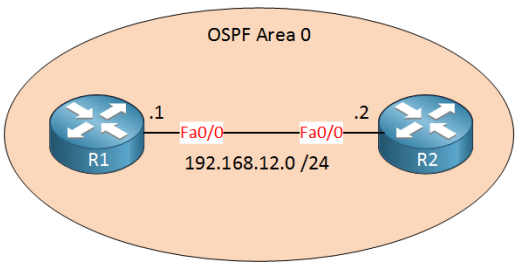
- تنقسم انواع الdata التى تتحرك فى الnetwork الى
  1. control plane هو الupdate الذى يرسل بين الswitches او بين الrouters مثل الذى يستخدم لبناء وتعديل ال routing table او mac address table
  2. data plane هو الdata الفعلية التى تنقل فى الnetwork
  3. management plane هو الtraffic الذى من خلاله اقوم بعمل management للdevice مثل الSSH و الSNMP
- يلزم وجود authentication عند تفعيل الrouting protocol بين الrouters
- عند عدم وجود authentication فيمكن للattacker القيام بالاتى :
  - يمكنه جعل الdevice الخاص به يعمل كا router ويقوم بتشغيل الrouting protocol ويستلم ويرسل الupdate بين الrouters
  - يمكنه عمل conflict بين شبكة موجودة بالفعل وشبكة وهمية من خلال جعلهم بنفس الnetwork id مما قد يؤدى الى وقع الشبكتان
- فكرة عمل الauthentication هو انشاء key بين الrouters وتكون جميع معاملتهم فيها هذا الkey لتاكد من صحة الauthentication ويسمى هذا الkey بالpre-shard key

RIPv2



- يدعم برتوكول rip v2 عملية الauthentication
- فى الrip نقوم بعمل سلسلة مفاتيح ويكون لها اسم و تحتوى على اكثر من مفتاح وكل مفتاح يكون لديه رقم وايضا كل مفتاح لديه password مختلف
- فكرة وجود عدة مفاتيح يمكن ان تكون ان كل مفتاح له مدة استخدام ويتم تغيره
- لايشترط ان يتشابه اسم سلسلة المفاتيح بين الrouters
- يمكن انشاء اكثر من سلسلة مفاتيح وعند استخدام السلسلة فاننا نقوم بدخول على الinterface وتطبيق هذه السلسة
- فكرة وجود اكثر من سلسلة يمكن ان توجد بسبب وجود اكثر من router متصلين معا وبين كل router والاخر توجد سلسلة مختلفة بمفاتيح مختلفة
- لعمل key chain (سلسلة مفاتيح) فاننا نستخدم امر **key chain CISCO** فى الconfiguration mode حيث ان CISCO هى اسم الchain
- بعد انشاء key chain نقوم بدخول على الconfiguration الخاصة بالchain تلقائيا وعندها يمكننا انشاء Key من خلال امر **key 1** حيث ان 1 هو رقم الkey
- بعد انشاء الkey اذا اردنا وضع له password فاننا نستخدم امر **key-string CCNP** حيث ان CCNP هى الpassword ويجب الانتباه الى ان الkey يجب ان يكون متشابه فى الrouter المقابل وان المسافات **تحسب من ضمن الpassword**
- Accept life time هو المدة التى سيقوم الrouter باستقبال الkey واعتباره key صحيح ويوجد ايضا send life time وهى المدة التى سيستخدم فيها الkey عند ارسال الpackets الخاصة بالrouting ويجب التاكد من كون الtime على الrouters متماثل
- يمكننا تحديد الaccept life time الخاص بال key من خلال امر **accept-lifetime 00:00:00 1 jan 2024 00:00:00 1 june 2024** حيث ان الوقت الاول هو الstart والوقت الاخير هو end ويمكن تغير الend الى كلمة Infinite لجعله يقبل الkey مدى الحياة
- لتحديد الsend life time فاننا نستخدم نفس الامر ولاكن نقوم بتغيير accept-lifetime ب send-lifetime
- فى حالة اردنا تطبيق key chain على interface معينة فاننا نقوم بدخول على الinterface وتطبيق امر **ip rip authentication key-chain CISCO** حيث ان هذا الامر يطبق عند استخدام الrip وايضا CISCO هو اسم الchain وبعد ذالك نقوم باستخدام امر **ip rip authentication mode text** وهو يستخدم لتعريف الmode او طريقة ارسال الKey فى الpacket وفى الrip يوجد طريقتان :
  1. Text يعنى انه سيرسل كا clear text وهو الdefault
  2. Md5 ويعنى انه سيرسل مشفر باستخدام الmd5
- لرؤية الkey chains الموجودة على الrouter فاننا نستخدم امر **show key chain**
- اذا كان الkey الmode الخاص به MD5 فيجب ان يتشابه رقم الkey فى كلا الطرفين واذا كان clear text فلا يهم

OSPF



- OSPF يدعم الauthentication باربع طرق :
  1. Null (type0)
  2. Clear text (type1)
  3. MD5 (type 2)
  4. SHA (type 2)

- جميع الطرق او الmodes ليست compatible معا اى انها يجب ان تكون سابتة فى الطرفين
- يمكن تشغيل الauthentication فى الOSPF باكثر من طريقة منها النزول تحت الinterface واستخدام امر **ip ospf authentication** وبعد ذالك نقوم بتحديد الmode كتالى :
  1. فى حالة قمت بكتابة الامر السابق فقط وضغط enter فاسيتم اعتباره clear text
  2. Null وهو يعنى انه لايوجد authentication
  3. message-digest تعنى الMD5
- بعد استخدام الامر السابق واختيار انه clear text يمكننا تحديد الkey من خلال امر **ip ospf authentication-key** وفى حالة كان clear text فانه يكون بحد اقصى 8 character وفى حالة قمنا بادخال اكثر من 8 سيقوم باخذ اول 8 جروف فقط وسيقوم باعلامنا بذالك من خلال alert فى الconsole (الalert يظهر فى الاصدرات 15 والاعلى)
- فى حالة قمنا باختيار الkey من نوع MD5 فاننا اذا اردنا وضع الkey فاننا نستخدم امر **ip ospf message-digest-key 1 md5 123** حيث ان 1 هو رقم الid ويجب ان يتشابه فى كلا الطرفين و 123 هو الkey وله حد اقصى 16 حرف
- يمكننا عمل authentication للarea كاملة بدلا من كل interface من خلال امر area 0 authentication وهذا الامر يستخدم داخل OSPF authenticatin ويمكننا استخدامه كما هو وهنا يعنى ان الkey يكون clear text ويمكننا اضافة كلمة message-digest الى الامر لاستخدامه بmd5
- الامر السابق يحدد فقط الmode اى ان لتحديد الkey فيجب النزول تحت كل interface واستخدام امر اضافة key
- فى حالة كان هناك authentication فى الarea واخر فى الinterface فالذى يعمل هو الذى يوجد فى الinterface
- فى بعض الversions من الrouters تدعم استخدام الkey chain مع OSPF protocol وايضا تدعم تشفير الkey بالSHA
- عند وضع تشفير للkey الموجود فى الkey chain فاننا ننشئ الchain وننشئ الkey وبعد الدخول على configuration الخاصة بالkey الموجودة داخل الconfiguration الخاصة بالchain فاننا ننستخدم امر **cryptographic-algorithm hmac-sha-512** لجعل الkey يتم تشفيره
- عند ملاحظة المثال السابق نجد ان طريقة التشفير هى hmac-sha-512 وهى طريقة تقوم بتشفير الkey بعد تشفريه بsha-512
- بعد انشاء الkey chain نقوم باضافته الى الospf من خلال امر ip ospf authentication key-chain CISCO حيث ان CISCO هو اسم الkey chain

EIGRP

- فى الauthentication الخاصة بال EIGRP يوجد نوعان هم :
  1. Classic EIGRP authentication
  2. Named EIGRP authentication
- النظام الافضل فى EIGRP authentication هو الnamed وهو مدعوم على الrouters من version 15 و اعلى
- فى الclassic نقوم بعمل key chain ونقوم بعمل key وبعد ذالك نقوم بدخول على الinterface ونستخدم امر **ip authentication key-chain eigrp 1 CISCO** حيث 1 هو رقم الautonoums system الموجود فيه الeigrp و CISCO هو اسم الkey chain
- لتحديد الmode الخاص بالkey فاننا نستخدم امر ip authentication mode eigrp 1 md5 حيث ال1 هو رقم الautonomous system ولا يوجد mode اخر غير الmd5 يستخدم
- مشكلة الclassic ان الامر الخاص به لايشبه باقى الprotocols ويجب حفظ الامر
- فى الnamed نستخدم امر **router eigrp EIG** حيث EIG هو اسم ولا يشترط تشابهه فى الrouter المقابل و بعد الامر نستخدم **address-family ipv4 autonomous-system 2** حيث 2 هو رقم الautonomous system
- بعد تنفيذ الامرين السابقين سنقوم بالدخول على address family configuration بشكل تلقائى وبعد ذالك يمكننا استخدام امر **af-interface f0/0** وهنا نقوم بتحديد الinterface الذى سيعمل عليها الauthentication و اذا اردنا تطبيقه على جميع الInterfaces فاننا نكتب default بدلا من f0/0 وعند ذالك سنقوم بدخول على configuration والتى يوجد بها اوامر كثيرة كتالى :

```
add-paths            Advertise add paths
authentication       authentication subcommands
bandwidth-percent    Set percentage of bandwidth percentage limit
bfd                  Enable Bidirectional Forwarding Detection
dampening-change     Percent interface metric must change to cause update
dampening-interval   Time in seconds to check interface metrics
default              Set a command to its defaults
exit-af-interface    Exit from Address Family Interface configuration mode
hello-interval       Configures hello interval
hold-time            Configures hold time
next-hop-self        Configures EIGRP next-hop-self
no                   Negate a command or set its defaults
passive-interface    Suppress address updates on an interface
shutdown             Disable Address-Family on interface
split-horizon        Perform split horizon
summary-address      Perform address summarization
```

- من الاوامر السابقة امر authentication وهو امر يستخدم لتطبيق او استخدام key chain على address family معينة كتالى **authentication key-chain CISCO** حيث CISCO هو اسم الchain ويمكننا تحديد الmode والpassword ايضا من خلال امر **authentication mode md5 123** وهو يدعم نوعان من الmode وهم :
  1. Hamc-sha-256
  2. Md5

Passive interfaces

- فى الrouter عندما يكون هناك Interface متصل LAN وهذه الLAN اتحتوى على routers فاننا يجب ان نعرف هذه الinterface على انها passive interface
- تقوم الpassive interface بعدم ارسال او استقبال اى hello message خاصة بالrouting protocol من هذه الinterface وبتالى عدم تفاعلها مع اى router يمكن ان يكون في هذه الLAN (يقصد بهذا عدم تفاعلها مع اى router من صنع الattacker)
- توجد حالة اخرى لتشغيل الpassive interface وهى ان يكون الLAN المقابلة بها router ولاكن يعمل بrouting مختلف وفى هذه الحالة اقوم باستخدام الpassive interface لتاكد من عدم تعامل هذه الinterface مع الrouter المقابل لها فى حالة انه قام بتغيير طريقة الrouting
- المثال السابق مناسب فى حالة شركات الISP لانها لاتريد من الrouters الخاصة بها التفاعل مع الrouter الموجود لدى الclient
- يختلف الpassive interface فى الRIP انه لايقوم بارسال hello message ولاكن يقوم باستقبالها
- عند تطبيق الpassive interface فى ospf او فى eigrp نستخدم امر **passive-interface f0/0** حيث ان f0/0 هى الinterface وفى حالة اننا نريد جعل جميع الinterfaces تكون passive نستخدم امر **passive-interface default**
- الامر السابق مفيد فى حالة اننا نريد جعل interface واحدة او اكثر التى ليست passive ونزيل الinterface من كونها passive من خلال وضع no قبل امر وضعها