CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

توپولوژی امن سازی لایه 2 و 3 با استفاده از سوئیچ و روتر

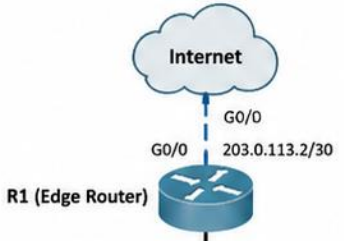
(برای پیاده سازی در Packet Tracer)

اهداف

- امن سازی لایه 2 با استفاده از قابلیت های سوئیچ
- امن سازی لایه 3 با استفاده از ACL روی روتر
- تفکیک شبکه با VLAN
- احراز هویت دسترسی به سوئیچ (SSH)
- جلوگیری از حملات رایج لایه 2

راهنما

- لینک اترنت
- لینک ترانک 802.1Q
- لینک سریال / WAN



امن سازی لایه 3 (روی روتر (R1)

- Extended ACL برای کنترل دسترسی بین VLAN ها
- فقط اجازه دسترسی به سرور از VLAN های مجاز
- مسدود کردن دسترسی بین VLAN های کاربری
- جلوگیری از دسترسی به شبکه مدیریت از بیرون
- NAT Overload برای دسترسی کاربران به اینترنت

شبکه ها و VLAN

VLAN 10 – USERS	192.168.10.0/24
VLAN 20 – SERVERS	192.168.20.0/24
VLAN 30 – GUESTS	192.168.30.0/24
VLAN 99 – MGMT	192.168.99.0/24

Gateway (SVI روی MLS1)

VLAN10:	192.168.10.1
VLAN20:	192.168.20.1
VLAN30:	192.168.30.1
VLAN99:	192.168.99.1

امن سازی لایه 2 (روی سوئیچ های دسترسی)

- خاموش کردن پورت های استفاده نشده
- Port Security (محدود کردن MAC Address
- BPDU Guard + Root Guard
- DHCP Snooping
- DAI (Dynamic ARP Inspection)
- جلوگیری از حمله CAM Table (Port Security + Shutdown)
- دسترسی امن به سوئیچ با SSH و غیرفعال کردن Telnet

VLAN 99 فقط برای مدیریت سوئیچ ها استفاده می شود
IP مدیریت سوئیچ ها در شبکه 192.168.99.0/24

مدیریت امن

- فقط از VLAN 99 و VLAN 9
- غیرفعال کردن HTTP و Telnet
- رمزنگاری رمزهای عبور
- Banner Login

سیاست‌های دسترسی (R1) روی (R1)

اجازه:

- فقط VLAN 10 به Server1 (192.168.20.10) و Server2 (192.168.20.20)
  VLAN 30 فقط به اینترنت

مسدود:

VLAN 30 به VLAN 10
VLAN 10 و VLAN 20 به VLAN

- هرگونه دسترسی به شبکه مدیریت (192.168.99.0/24) از بیرون
  سایر ترافیک های غیر مجاز

جلوگیری از حملات ARP Spoofing با استفاده از Dynamic ARP Inspection – DAI

- قابلیت DAI به ما کمک میکند تا با کمک قابلیت های DHCP از حملات ARP Spoofing جلوگیری کنیم. به همین دلیل DAI به صورت همزمان با قابلیت DHCP Snooping بکار می رود

- **ARP چیست؟**
- پروتکل ARP برای تبدیل آدرس IP به آدرس MAC مورد استفاده قرار می گیرد به طور مثال ، Host B می خواهد اطلاعاتی را برای Host A ارسال کند اما MAC آدرس Host A را ندارد به منظور پیدا کردن MAC آدرس Host A یک بسته Broadcast برای تمام دستگاه های آن broadcast domain ارسال می کند تا MAC آدرس مربوط به IP آدرس Host A را بدست آورد.

- تمام دستگاه های این broadcast domain این بسته را دریافت می کنند و Host A به آن پاسخ می دهد و MAC آدرس خود را اعلام می کند. احتمال حمله ARP spoofing و ARP cache poisoning وجود دارد و این امکان وجود دارد که به جای دستگاه مورد نظر مهاجم پاسخ ARP را با اطلاعات مورد نظر خود ارسال کند

- با استفاده از قابلیت DAI میتوان شبکه ها را در مقابل حملات جعل هویت ARP محافظت کرد.
- عملکرد این قابلیت شبیه به DHCP Snooping است. از پورت های قابل اعتماد و غیر قابل اعتماد استفاده می کند. پاسخ های ARP فقط در پورت های قابل اعتماد وارد پورت سوئیچ می شوند.
- اگر پاسخ **ARP** به سوئیچ از پورت غیر قابل اعتماد ویا untrusted port بیاید، محتویات بسته پاسخ ARP با جدول اتصال DHCP مقایسه می شود تا صحت آن بررسی شود.
- اگر پاسخ **ARP** معتبر نباشد و در جدول DHCP Snooping نباشد، پاسخ ARP داده نمی شود و همچنین آن پورت غیرفعال می شود.

- برای پیکربندی Dynamic ARP Inspection باید این کار را برای یک یا چند VLAN انجام دهیم. به عنوان مثال فعال کردن DAI برای VLAN 60:
- Switch1(config)# ip arp inspection vlan 60

- تنظیمات پیش فرض Dynamic ARP Inspection باعث می شود تمام پورت های سوئیچ غیر قابل اعتماد untrust شوند.
- بنابراین موارد مورد اعتماد باید مشخص شوند. این پورت قابل اعتماد پورت هایی هستند که انتظار می رود پاسخ های ARP از آنها دریافت شود.

- پیکربندی پورت به عنوان یک پورت قابل اعتماد DAI مانند زیر است:
- Switch1(config)# interface gigabitethernet 0/1
- Switch1(config-if)# ip arp inspection trust

بررسی حمله Double Tagging Attack

- زمانیکه روی Switchخود VLANها را پیکربندی میکنیم ارتباطی در حالت پیشفرض بین VLANها وجود ندارد و برای ایجاد ارتباط بین VLANها از Inter VLAN Routing بر اساس نیاز ها و سیاست های مورد نظرمان استفاده میکنیم.

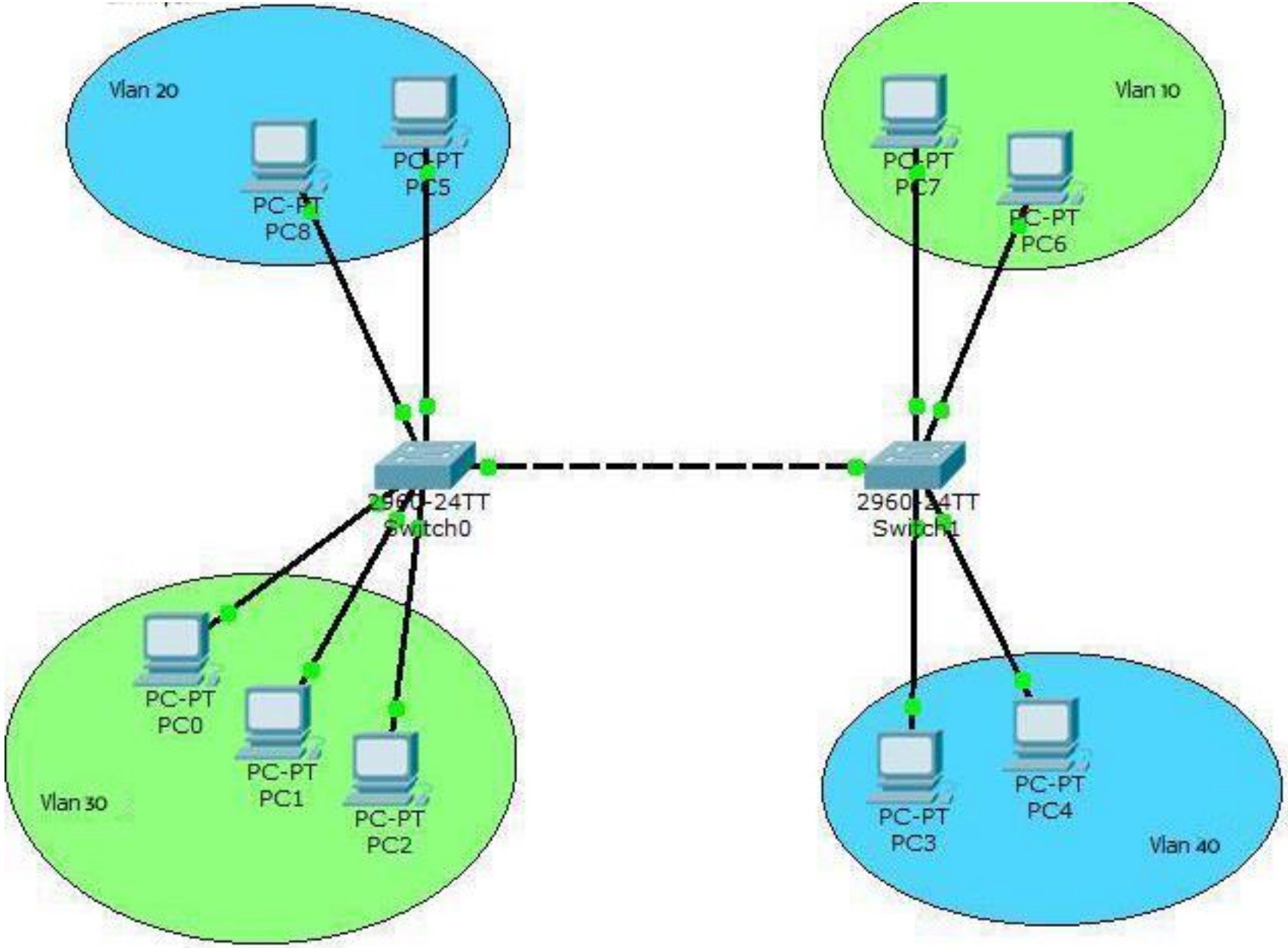
- اما روش هایی وجود دارد که مهاجم با استفاده از این روش ها به صورت غیر مجاز از یک VLAN به VLAN دیگر نفوذ می کند.

• تحقیق جلسه آینده : Double Tagging

• با Native VLAN آشنا شوید :

• تکنولوژی Trunking یک تکنولوژی لایه ۲ است. در پورت های Trunk، همه فریم ها با Vlan های مربوطه تگ گذاری می شوند و به پورت ترانک دیگر انتقال پیدا خواهند کرد. برای این منظور در سوئیچینگ شبکه ها، همه سوئیچ ها توسط پورت های Trunk متصل می شوند.

- به طور مثال VLAN 10 به عنوان Native-VLAN ما است، و نفوذگر که در Native-VLAN قرار دارد می خواهد به VLAN-20 نفوذ کند. پس بسته مورد نظر خود را با تگ ۲۰ ارسال می کند.
- سوییچ با دریافت Frameتگ ۱۰ را روی آن میزند که باعث می شود Frame ما دارای دو تا تگ بشود. این Frame هنگامیکه روی پورت ترانک ارسال می شود، Tag مربوط به Native-VLAN آن حذف میشود، اما همچنان تگ ۲۰ را دارد.
- در نتیجه، هنگام دریافت فریم توسط سوییچ مقابل با دیدن تگ ۲۰ روی فریم، آن را تحویل VLAN 20میکند. بدین صورت است که مهاجم از VLAN-10به VLAN-20نفوذ می کند.


Vlan 20
PC-PT
PC8
PC-PT
PC5
Vlan 10
PC-PT
PC7
PC-PT
PC6
2960-24TT
Switch0
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
Vlan 30
PC-PT
PC3
PC-PT
PC4
Vlan 40

- شرکتی را در نظر بگیریم که در یکی از VLANها کاربران زیادی داشته باشد عمل تگ برداشتن و تگ زدن پورت ترانک(trunk) باعث کندی شبکه خواهد شد.
- در کل سوئیچ میتوانیم فقط به یک VLAN اجازه تردد بدون تگ زدن بدهیم، که به این عمل Native VLAN میگویند.
- Vlan1در واقع همان Native VLAN در سوئیچ های سیسکو است. برای اهداف امنیتی توصیه می شود که vlan Native پیش فرض را به یک vlan دیگر تغییر دهید.
- switch(config-if)# switchport trunk native-vlan NUMBER

```
Core-switch# show interface trunk
```

```
core-switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1
```

```
core-switch(config)#interface range fa0/2-4

core-switch(config-if-range)#switchport trunk native vlan 100
```

```
core-switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      100
Fa0/3       on           802.1q         trunking      100
Fa0/4       on           802.1q         trunking      100
```

- به معنای دیگر در صورتی که Native Vlan بر روی یک پورت به صورت مثال ۱ تعریف شده باشد در صورتی که پکتی از آن پورت وارد سوییچ شود و دارای tag مربوط به Vlanها نباشد آن را جزو پکتهای مربوط به Vlan 1 در عملیات سوییچینگ به حساب میآورد.
- این vlan دارای یک مشکل بزرگ امنیتی است که میتوان ان را هک کرد و به ان vlan hopping میگویند

```
Core-switch# show interface trunk
```

```
core-switch#show interface trunk
Port        Mode        Encapsulation  Status        Native vlan
Fa0/2       on          802.1q         trunking      1
Fa0/3       on          802.1q         trunking      1
Fa0/4       on          802.1q         trunking      1
```

امن کردن SNMP سویچ و روتر سیسکو

- Simple Network Management Protocol یا همان SNMP پروتکل مشهور و پرکاربرد برای جمع آوری اطلاعات شبکه و مدیریت شبکه ست.
- از SNMP برای جمع آوری اطلاعات مربوط به کانفیگ ها و تجهیزات شبکه مثل سرورها، پرینترها، سوییچ ها و روترها، بر اساس یک IP، استفاده میشه، و یه نکته دیگه اینکه به ساختمان داده این پروتکل MIB یا Management Information Base

- SNMP بطور پیشفرض از پورتهای UDP 161 برای پیام های عمومی و از پورت UDP 162 برای پیام های trap استفاده می کنه
- اگر از سیستم های مانیتورینگ یا پروتکل SNMP استفاده نمی کنید می تونید با دستورات زیر این سرویس را غیر فعال کنید:

- Switch(config)# no snmp-server community
- Switch(config)# no snmp-server enable traps
- Switch(config)# no snmp-server system-shutdown
- Switch(config)# no snmp-server

- اگه سرویس SNMP را واسه سویچ ها و روترهای داخل شبکه نیاز دارید بهتره مستقیم برید سراغ SNMP ورژن ۳ این ورژن خیلی امن تر از ورژن ۱ است چرا که از یک رمزنگاری هش برای احراز هویت برای محافظت از community string استفاده می کنه.

- دستوراتی که در قسمت زیر آمده نشون میده که چطور یک مدل امنیتی برای snmp v3 ایجاد بشه ، در ابتدا اکسس لیست ۱۲ اجازه میده که فقط سیستم های خاصی سویچ را مدیریت کنند.

- Switch(config)# no access-list 12
- Switch(config)# access-list 12 permit 172.30.100.2
- Switch(config)# access-list 12 permit 172.30.100.3

- مرحله بعد تعریف یک گروه admin با با دسترسی خواندن و نوشتن MIB
- Switch(config)# snmp-server group admins v3 auth read adminview write adminview

- سپس یک کاربر بعنوان مثال root به این گروه با یک کلمه عبور تعریف میکنیم که می تونه قبل از ارسال هم با md5 رمز بشه و در انتهای دستور اکسس لیست ۱۲ به این کاربر اعمال میکنیم.

- Switch(config)# snmp-server user root admins v3 auth md5 MyP@ssw0rd access 12

Switch port Protected

- به زبان ساده Protected Port قابلیتی است که ازارتباط پورت های یک VLAN با یکدیگردر سوئیچ سیسکو جلوگیری مینماید .
- به بیان دیگر ، مثلا یک سوئیچ ۲۹۶۰ سیسکو را در نظر بگیرید که همه پورت های آن به صورت دیفالت در یک vlan قرار دارند ، پس همگی آنها میتوانند با هم در ارتباط باشند و مثلا از منابع و فایل های کامپیوتر هایی که به آن پورت ها متصل اند ، استفاده کنند ،، فرضا شما میخواهید پورت fast0/1 که متصل به کامپیوتر آقای X است ، با پورت fast0/12 که مربوط به کامپیوتر خانوم xxx است (که با هم فولدر آهنگ ها و .... را shareکرده اند) ، ارتباط نداشته باشند ولی به شبکه که به مابقی پورت های سوئیچ سیسکو ۲۹۶۰ متصل است دسترسی و امکان تبادل اطلاعات را داشته باشد ،، خب چه باید کرد ؟!
- راه حل استفاده از قابلیت Protected Portاست ، بدین ترتیب که ما پورت های fast0/1 و fast0/12 را Protected میکنیم ، بدین ترتیب ، این دو پورت با یکدیگر نمیتوانند تبادل اطلاعات نموده ،اما، به مابقی شبکه دسترسی دارند .

- Switch(config)#interface GigabitEthernet1/0/5
- Switch(config-if)#switchport protected
- Switch(config-if)#^Z

- Switch#sh int gi 1/0/5 switchport

تشخیص خرابی کابل شبکه با کمک TDRدر سیسکو

- TDR (Time-Domain Reflectometer) نحوه بررسی اتصال کابل‌های اترنت با استفاده از دستور TDR

- در صورتی که شما به هر دلیلی شک دارید که کابل اترنت Cat5/6 شما ممکن است خراب باشد، با استفاده از رابط خط فرمان CLI (Command-Line Interface) سوئیچ سیسکو و چند دستور می‌توانید از وضعیت زوج‌های مسی کابل‌های متصل به سوئیچ خود مطلع شوید.

- توجه داشته باشید که همه سوئیچ ها از این ویژگی پشتیبانی نمی کنند.

TDR Support	Model
Yes	2960
Yes	2960G
Yes	2960S
Unknown	2918
Unknown	2350
Unknown	2360
Unknown	2975
No	3560
Yes	3560G
Yes	3560E/3560X
No	3750
Yes	3750G

- ابتدا، با استفاده از SSH، Telnet یا رابط وب به سوئیچ مورد نظر خود متصل شوید.
- از دستور زیر برای نمایش لیست رابط‌ها در سوئیچ استفاده کنید:
- #show interfaces
- شما باید نام پورت مورد نظر خود را که می‌خواهید بررسی کنید، پیدا کنید. به عنوان مثال، فرض کنید می‌خواهید پورت GigabitEthernet1/0/1 را تست کنید.
- ۳- سپس از دستور زیر برای انجام تست بر روی رابط مورد نظر استفاده کنید:
- test cable tdr interface GigabitEthernet1/0/1

- ممکن است در بعضی سوئیچ ها به صورت زیر هم نوشته شود:

- test cable-diagnostics tdr interface GigabitEthernet1/0/1

- احتمالاً نتیجه‌ای مشابه زیر را دریافت خواهید کرد:

- TDR test started on interface Gi1/0/1
- A TDR test can take a few seconds to run on an interface
- Use 'show cable-diagnostics tdr' to read the TDR results.

- **۱۰ ثانیه صبر کنید** و سپس دستور زیر را وارد کنید تا نتایج تست TDRرا مشاهده کنید:
- show cable-diagnostics tdr interface GigabitEthernet1/0/1
- **خروجی نتایج TDR ممکن است مشابه زیر باشد:**

- TDR test last run on: December 05 18:50:53
- Interface Speed Local pair Pair length Remote pair Pair status

- Gi1/0/1 1000M Pair A 19 +/- 10 meters Pair B Normal
- Pair B 19 +/- 10 meters Pair A Normal
- Pair C 19 +/- 10 meters Pair D Normal
- Pair D 19 +/- 10 meters Pair C Normal

```
            '#show cable-diagnostics tdr int g7/36
Interface Speed  Local pair Cable length Remote channel Status
Gi7/36    100Mbps 1-2          0 m        Unknown       Terminated
                  3-6          0 m        Unknown       Terminated
                  4-5          0 m        Unknown       Short
                  7-8          0 m        Unknown       Short

            #show cable-diagnostics tdr int g7/37
Interface Speed  Local pair Cable length Remote channel Status
Gi7/37    10Mbps  1-2          5 +/-10m   Unknown       Open
                  3-6          4 +/-10m   Unknown       Short
                  4-5          0 m        Unknown       Short
                  7-8          0 m        Unknown       Short

            #show cable-diagnostics tdr int g7/38
Interface Speed  Local pair Cable length Remote channel Status
Gi7/38    10Mbps  1-2         19 +/-10m   Unknown       Short
                  3-6         19 +/-10m   Unknown       Short
                  4-5         17 +/-10m   Unknown       Short
                  7-8         16 +/-10m   Unknown       Short

            #show cable-diagnostics tdr int g7/41
Interface Speed  Local pair Cable length Remote channel Status
Gi7/41    10Mbps  1-2          3 +/-10m   Unknown       Short
                  3-6          4 +/-10m   Unknown       Short
                  4-5          0 m        Unknown       Short
                  7-8          0 m        Unknown       Short
```

- معمولاً نتایج TDR شامل اطلاعاتی مانند سرعت رابط، زوج محلی، طول زوج، زوج از راه دور، وضعیت زوج‌ها و ... است. این اطلاعات به کاربر این امکان را می‌دهد تا از وضعیت کابل‌ها مطلع شود.
- به عنوان مثال، در نتایج فوق، وضعیت زوج‌ها برای این رابط به صورت Normal نشان داده شده است که نشان می‌دهد کابل‌ها در وضعیت عادی و سالم قرار دارند. همچنین، طول زوج‌ها نیز به صورت "۱۹ +/- ۱۰ meters نشان داده شده است که نشان می‌دهد طول زوج‌ها در حدود ۱۹ متر است و با یک مرز انحراف ۱۰ متری قابل قبول است.

نتیجه	توضیح
Normal	وضعیت طبیعی و عادی کابل. همه‌ی زوج‌ها سالم و بدون مشکل هستند.
Open	اتصال بین دو پین در یک زوج مسی قطع شده است و کابل برای این زوج به درستی عمل نمی‌کند.
Short	اتصال بین دو پین در یک زوج مسی کوتاه شده است و کابل برای این زوج به درستی عمل نمی‌کند.
Impedance Mismatched	تطبیق هم‌راستایی امپدانس در یکی از زوج‌ها برای استفاده‌ی صحیح از کابل اترنت مورد نیاز نیست و کابل باید تعمیر شود.
No Cable	کابل در این رابط متصل نیست و تست TDR بر روی کابل انجام نمی‌شود.
Unknown	وضعیت کابل تشخیص داده نشده است و نتیجه‌ی دقیقی در مورد وضعیت کابل ارائه نمی‌شود.
Unsupported	رابط مورد نظر از نوعی کابل پشتیبانی نمی‌کند و امکان انجام تست TDR برروی این رابط وجود ندارد.
Disabled	رابط مورد نظر غیرفعال است و تست TDR برروی این رابط انجام نمی‌شود.
Error	خطا در اجرای تست TDR رخ داده است و نتیجه‌ی دقیقی برای وضعیت کابل ارائه نمی‌شود.

laptop

```
Labswitch1#test cable-diagnostics tdr int
Labswitch1#test cable-diagnostics tdr interface gi1/0/1
TDR test started on interface Gi1/0/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Labswitch1#show cabl
Labswitch1#show cable-diagnostics td
Labswitch1#show cable-diagnostics tdr int
Labswitch1#show cable-diagnostics tdr interface gi1/0/1
TDR test last run on: September 12 11:05:12

Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/1   1000M Pair A     0    +/- 10 meters Pair B      Normal
                Pair B     0    +/- 10 meters Pair A      Normal
                Pair C     0    +/- 10 meters Pair D      Normal
                Pair D     0    +/- 10 meters Pair C      Normal
Labswitch1#
```

در عکس فوق کابل شبکه را از سویچ جدا می کنیم و دوباره نتیجه را می بینیم

```
Labswitch1#test cable-diagnostics tdr interface gi1/0/1
TDR test started on interface Gi1/0/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Labswitch1#show cable-diagnostics tdr interface gi1/0/1
TDR test last run on: September 12 11:06:41

Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/1   auto  Pair A     N/A                N/A         Not Completed
                Pair B     N/A                N/A         Not Completed
                Pair C     N/A                N/A         Not Completed
                Pair D     N/A                N/A         Not Completed
Labswitch1#
```

```
TDR test started on interface Gi1/0/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Labswitch1#show cable-diagnostics tdr interface gi1/0/1
TDR test last run on: September 12 11:17:51

Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/1   100M  Pair A     0    +/- 1  meters Pair A      Normal
                Pair B     0    +/- 1  meters Pair B      Normal
                Pair C     1    +/- 1  meters N/A         Open
                Pair D     0    +/- 1  meters N/A         Normal
Labswitch1#
```

بک آپ گیری اتوماتیک از روتر و سویچ سیسکو

- بک آپ گیری اتوماتیک از روتر و سویچ سیسکو | احتمالا برایتان پیش امده که بدنبال راهی باشید تا از تنظیماتی که در طول زمان بر روی روتر خود انجام میدهید آرشیوی تهیه کنید تا احتمالا اگر مشکلی پیش آید یا به هر دلیل دیگر به آنها دسترسی داشته باشید، یکی از مهم‌ترین وظایف مدیر شبکه، گرفتن بک آپ از تنظیمات روترها و سویچ ها می‌باشد.

- جهت بک آپ گیری از تنظیمات روتر یا سویچ بر روی TFTP Server، از دستور زیر می‌توان استفاده کرد:

- R1(config)#copy startup-config tftp:

- با این همه در صورتی که تعداد تجهیزات شبکه زیاد باشد، بک آپ گرفتن یک به یک از دستگاه ها، روش درستی نیست، راهکار این مشکل استفاده از مکانیزیم بک آپ اتوماتیک بر روی روتر و سویچ است.
- دستور archive می‌تواند این کار را برای شما انجام داده و به طور اتوماتیک در زمان های تعیین شده، از تجهیزات شبکه بک آپ بگیرد.

- قابلیت Archive از IOS 12.3(4)T به بعد اضافه شد برای فعال سازی این قابلیت، از دستور زیر استفاده کنید:
- ابتدا با اجرای دستور archive، وارد مد پیکربندی archive می‌شویم. با استفاده از دستور path، محل ذخیره بک آپ ها را مشخص کنید.
- در مثال فوق، ۱۹۲.۱۶۸.۱.۱ آدرس FTP Server می‌باشد. FTP نیاز به احراز هویت دارد، بنابراین UserName و پسوردی که بر روی FTP Server تعیین کرده ایم را نیز مشخص می‌کنیم.

- R1(config)#archive
- R1(config-archive)#path ftp://UserName:Password@192.168.1.1/
- R1(config-archive)#write-memory
- R1(config-archive)#time-period 1440
- R1(config-archive)#notify syslog
- R1(config-archive)#maximum <1-14>

- دستور time-period باعث می‌شود هر ۱۴۴۰ ثانیه (معادل ۲۴ ساعت می‌باشد)، از تنظیمات روتر بک آپ گرفته شود.

- دستور notify syslog باعث می‌شود تا دستوراتی که در Global Mode اجرا می‌شوند به سمت Syslog Server ارسال شوند.

- با استفاده از دستور maximum می‌توان تعداد فایل های بک آپ را کاهش یا افزایش داد. به طور پیش فرض ۱۴ فایل بک آپ ذخیره می‌شوند.

- برای مشاهده بک آپ های گرفته شده، از دستور زیر استفاده کنید:

- **R1# show archive**
- The next archive file will be named ftp://192.168.1.1/R1-config-3
- Archive # Name
- 0
- 1 ftp://192.168.1.1/R1-config-1
- 2 ftp://192.168.1.1/R1-config-2 <- Most Recent

محافظت از اتصالات telnet http , ssh , در برابر حملات Dos Attack

- هکر می تواند از طریق برنامه های خاص اقدام به پیدا کردن مثلا پسورد telnet نماید و با ارسال تقاضاهای جعلی و برقراری جلسات مختلف حملات Dos Attackرا انجام دهد برای محافظت از telnet http , ssh , از روش فوق استفاده می کنیم

- #Config t
- #Login block-for 120 attempts 5 within 30
- در این مثال **اگر ۵ مرتبه** تلاش ناموفق برای دسترسی در مقطع **زمانی ۳۰ ثانیه و کمتر** اتفاق افتد – login برای **مدت ۱۲۰** ثانیه کلیه login request ها را بلوکه می کند
- برای غیر فعال کردن آن
- Config t
- No login block-for
- جهت مشاهد ه :
- Sh login

- فعال کردن لاگین های موفق

- #Config t
- #Login on-success log

- لاگین ناموفق

- #Login on-failure log

تعیین زمان Time out در SSH

- این مدت زمان به ثانیه است که بعد از اتصال sshدر این زمان باید حتما تشخیص هویت صورت گیرد . و اگر در این مدت زمان صورت نگیرد اتصال قطع می گردد
- #Config t
- #Ip ssh time-out 100
- زمان ssh time out به ثانیه و عددی بین 0 تا 120 ثانیه است

سناریوامنیتی سیسکو و زیرساخت

شماره یک : مرگ تدریجی یک سازمان

- در یک مجموعه سازمانی کاربرها صبح سرکار کندی شبکه را حس می‌کردن. تایم‌اوت می‌اومد. نِت پرش می‌زد. حتی طرف گفته بود VPN هم قطع شد" **و این یعنی مَرگ تدریجی یک سازمان!**

- **مرحله اول** بایستی هشدارهای syslog را بررسی کنید :

- %SW_MATM-4-MACFLAP_NOTIF: Host 00:de:ad:be:ef:fa flapping between port Gi1/0/2 and Gi1/0/3

ازاین هشدار syslog چه چیزی متوجه می شویم

- %SW_MATM-4-MACFLAP_NOTIF: Host 00:de:ad:be:ef:fa flapping between port Gi1/0/2 and Gi1/0/3

- **نکته قابل تامل** ؟! مگه یه **MAC** هم می‌تونه تو دو پورت باشه؟ پس قضیه از **این قراره:**
- یا یه نفر داره VMWare ESXi با vSwitch اشتباه پیکربندی کرده،
- یا یه کاربر عجیب داره کاری می‌کنه که نباید!

- کاری که باید انجام داد می ریم به سراغ ابزارهای زیر :

- - IP Device Tracking
- - DHCP Snooping
- - Source Guard
- - DAI

- **DHCP Snooping رو فعال کردم**

- conf t
- ip dhcp snooping
- ip dhcp snooping vlan 10,20,30
- interface GigabitEthernet1/0/1
- description --> Trusted uplink
- ip dhcp snooping trust
- Exit

- **هدف**: فقط پورت **uplink** به **DHCP** سرور رو اعتماد کنیم، بقیه نه! تا به کسی الکی DHCP نده.

IP Device Tracking

- IP Tracking را فعال می کنیم تا متوجه بشیم کی چه سیستمی IP گرفته
- حالا دیگه سویچ می‌دونه هر پورت، کدوم IPارو گرفته.
- ip device tracking

Source Guard

- هر کسی فقط با IPخودش ارتباط داشته باشد !

- **interface range** GigabitEthernet1/0/2 - 24
- **ip verify source**

- اگه یه کلاینت بخواد جعل یه IP دیگه رو انجام بده ، قشنگ بسته‌شو می‌ندازه تو سطل آشغال!

DAI (Dynamic ARP Inspection)

- **ip arp inspection** vlan 10,20,30

- و تمام! دیگه هیچکس نمی‌تونه با جعل ARP خودشو جای گیت‌وی یا سرور بزنه.
- اگر بسته‌ای از **ARP** بیاد که تو جدول **DHCP Snooping** نباشه، سویچ سریعا شناسایی می کند !

- توی سویچ‌های سری ۲۹۶۰، ۳۵۶۰، ۹۳۰۰ و کلی مدل دیگه به راحتی پیاده می‌شه.

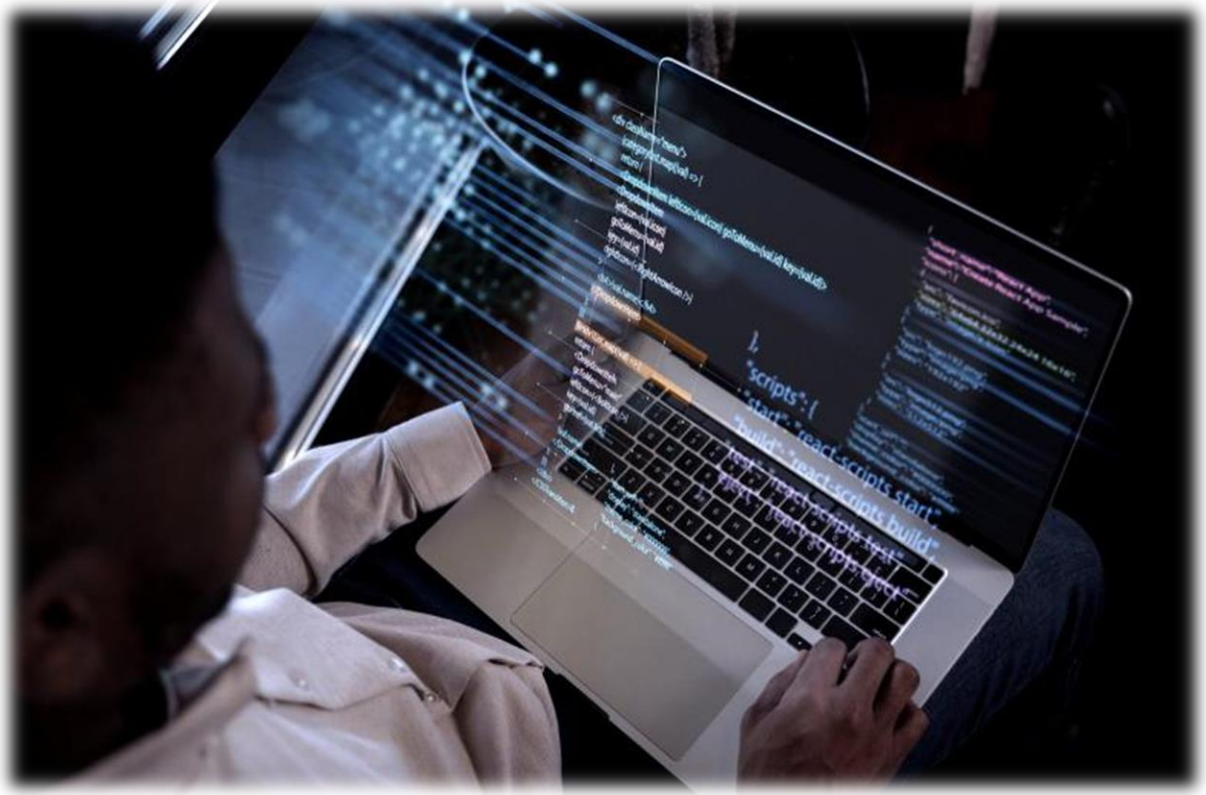
قاتل بی سروصدا CoPP Sniper

- یک اتفاق عجیب ترافیک CPU روتر تا ۹۵ درصد رفته بالا ولی هیچکس نفهمیده چی شده. یه نفر داره از تو لایه ۳ حمله می زنه و ارتباط با یکی از روترهای مرکزی قطع میشه

- همه نشانه ها به یک حمله ناشناس ختم می شود به نام :
- Control Plane Policing (CoPP) Bypass

- **درواقع هکردست گذاشته روی قلب روتر**
- **Control Plane!** جایی که پکت‌های پروتکلی مثل BGP ، OSPF ، SSH و حتی ICMP مستقیم می‌رن سمت **CPU!**
- یعنی انگار با دور زدن بقیه، رفته مستقیم مغز روتر رو هدف گرفته.

- **مرحله اول: شناخت قاتل**
- اول باید بدونی که CoPP وظیفه‌اش چیه. این فیلتر برای حفاظت از control plane هست. اگه درست کانفیگ نشه، حتی یه پینگِ خراب‌کار هم می‌تونه CPU روتر رو بزنه و نابود کنه !



- مرحله دوم: ایجاد ACL

- **ip access-list** extended PROTECT-CPU
- **permit** icmp any any echo
- **permit** tcp any any eq bgp
- **permit** ospf any any
- **deny** ip any any

- دراین دستور فقط پکت‌هایی که واقعا لازمه (پینگ، BGP، OSPF) حق دارن بیان سمت CPU بقیه؟ رد

- مرحله سوم: ساختن کلاس

- **class-map** match-all ALLOW-CPU
- **match access-group** name PROTECT-CPU

- مرحله چهارم: انداختن قاتل توی تله

- policy-map CPU-PROTECTION
- **class** ALLOW-CPU
- **police** 64000 8000 conform-action transmit exceed-action drop
- **class** class-default
- drop

- **نکته‌ی مخفی:**
- ما فقط ۶۴ kbps به پکت‌های مهم اجازه دادیم که CPU رو درگیر کنن. بقیه؟ پشت درِ موندن

- چسبوندن قانون به درب CPU

- control-plane
- service-policy input CPU-PROTECTION

- CPU از ۹۵ درصد شد ۱۵ درصد... آروم شد

- گاهی اوقات هکرها، نه از در اصلی، بلکه از در کنترل میان تو