پیکربندی امن تجهیزات شبکه و زیرساخت
با رویکرد دفاع در عمق
Defense in Depth best practices

ایمان مجتهدین یزدی mojtahedin@cert.um.ac.ir
کارشناس آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

سازمان فنآوری اطلاعات ایران – مرکز ماهر – تابستان ۱۳۹۵

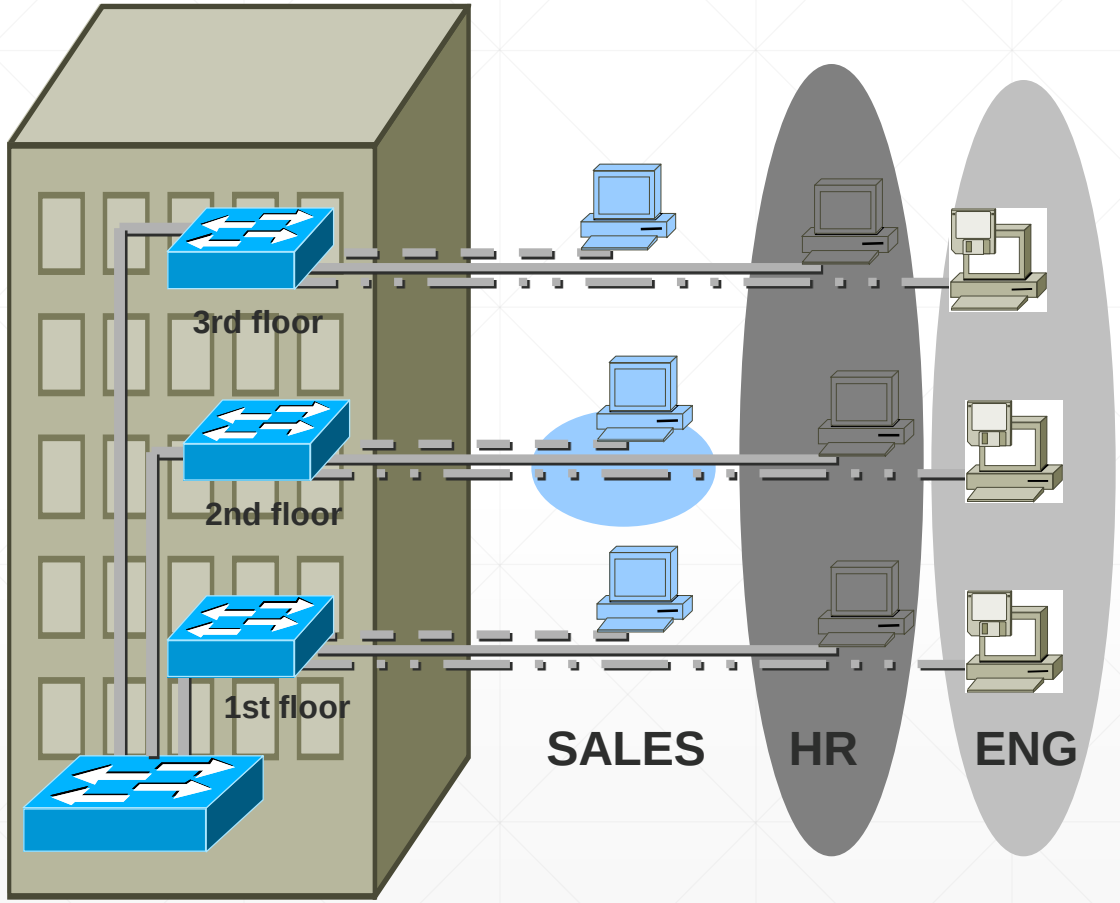
(کارگاه آموزشی مدیران و کارشناسان فنآوری اطلاعات – ارومیه – استان آذربایجان غربی)

Outline

Some Layer 2 & 3 security Best Practices

- Secure Management (Management Zone, https, ssh, …)
- Port-Security
- VACL
- DHCP Snooping
- DAI
- IP Source Guard
- VLAN hopping
- Root Guard & BPDU Guard
- SSH
- Layer 3 Security ...

VLAN Overview



- Segmentation
- Flexibility
- Security

A VLAN = A broadcast domain = Logical network (subnet)

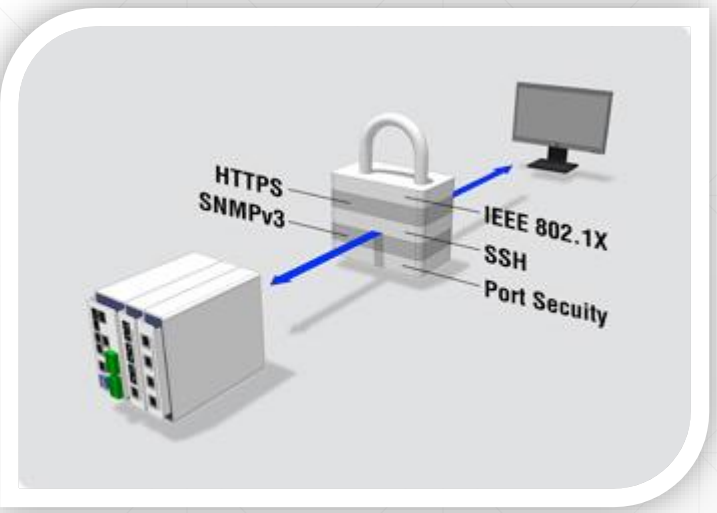
VLAN Configuration Steps

- Enable VTP (optional)
- Enable trunking
- Create VLANs
- Assign VLAN to ports

Some Layer 2 & 3 security Best Practices

- قبل از وارد شدن به موضوع امنیت در لایه 2، یادآوری مطالب زیر خالی از لطف نخواهد بود:

1. Physical Security
2. Passwords (Service Password-encryption)
3. Different privilege levels
4. Grant remote access only to those who absolutely need it
5. Preventing CAM overflow attacks with port security



- عملیات سوئیچینگ(Packet Forwarding)
- زمانی که حمله MAC flooding انجام می شود، در اثر پر شدن حافظه سوئیچ، تمامی بسته های دریافت شده توسط سوئیچ مانند بسته های Broadcast به تمام پورت های سوئیچ غیر از پورت دریافت کننده ارسال می شود(Flooding) .
- این حمله ضمن پایین آوردن ناگهانی و محسوس سرعت و بهره وری شبکه، باعث می شود امکان شنود (Sniff) اطلاعات بر روی پورت های سوئیچ فراهم باشد.

- نحوه پیکربندی Port Security :

```
Switch(if-config)# switchport mode access
Switch(if-config)# switchport port-security
Switch(if-config)# switchport port-security
```

- Aging
- Mac-address
- Maximum
- violation

- نحوه پیکربندی Port Security :

نکته 1 :

Switch(if-config)# switchport port-security mac-address
- H.H.H
- sticky

نکته 2 :

Switch(if-config)# switchport port-security violation
- Protect (Drops packet)
- Restrict (Drops packet / snmp trap)
- Shutdown (Error disable / snmp trap)

- Port Security Monitoring :

به منظور بررسی و مانیتورینگ وضعیت پورت های Secure می توان از دستور زیر استفاده کرد :

Switch# show port-security interface

نکته مهم :

پیکربندی Port-Security را در چهار حالت زیر نمی توان استفاده کرد :

1. Trunk Ports
2. Ports placed on etherchannel
3. Destination SPAN port
4. 802.1 x ports

- بر خلاف تصور، ACL ها همیشه برای اعمال دستورات Permit یا Deny به کار نمی روند بلکه می توان از آنها برای آشکار کردن (Mark) یک نوع ترافیک خاص و تصمیم گیری در خصوص نتیجه این تجزیه و تحلیل استفاده کرد.
- برای کنترل دسترسی و آنالیز ترافیک اطلاعات کلاینت های موجود در داخل یک VLAN باید از ابزاری به نام VLAN Access-List یا VACL استفاده کرد.

VACL Configuration

```
Switch ( config )# ip access-list extended No_123_contact
Switch ( config-ext-nacl )# permit ip 172.10.10.0 0.0.0.3 172.10.10.0 0.0.0.255
```

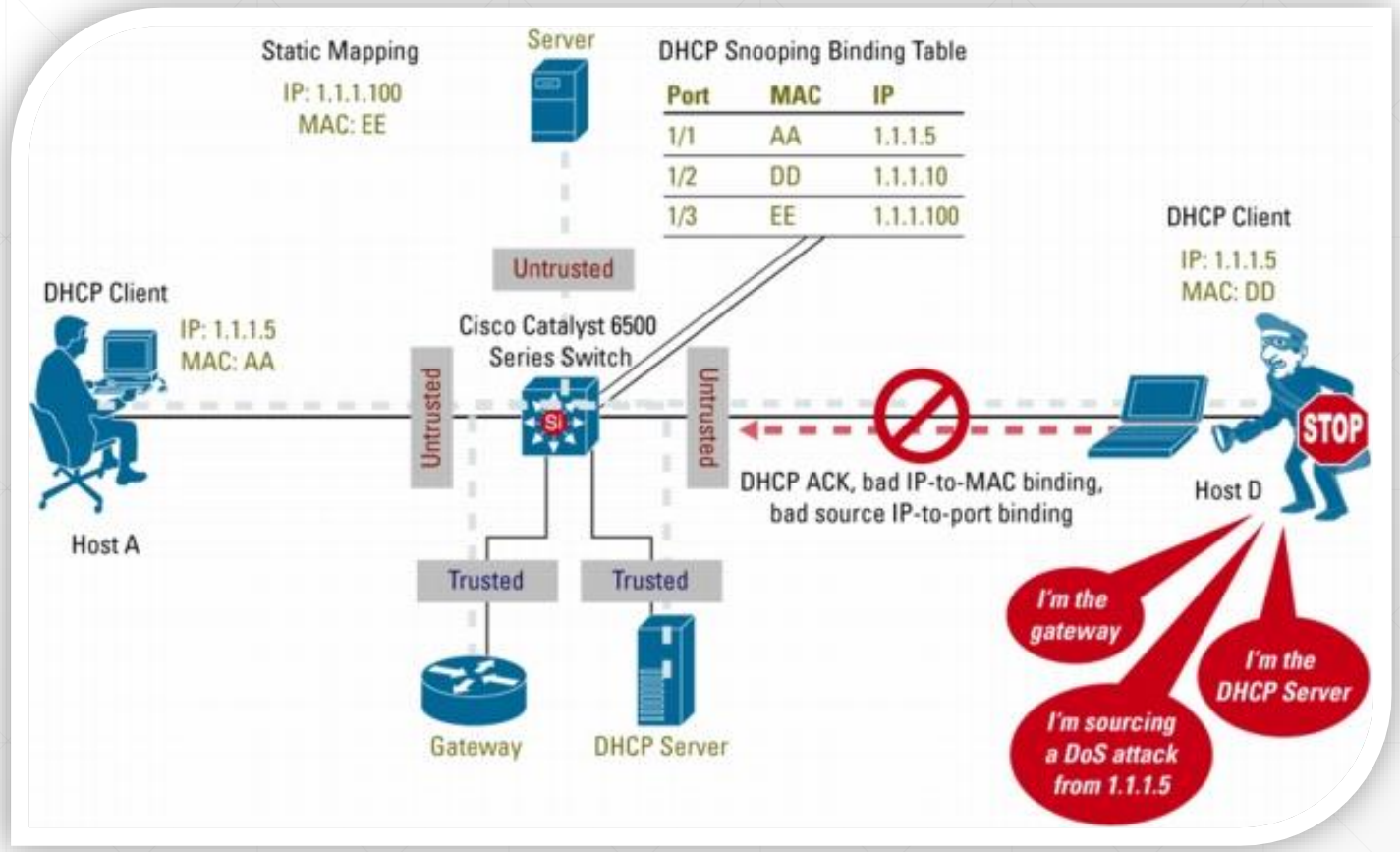
نکته : ACL فوق با وجود کلمه Permit در اینجا فقط نقش فیلتر کننده یا مشخص کننده ترافیک مورد نظر ما با هدف ممانعت از تبادل اطلاعات بین کلاینت های دارای آدرس شبکه 172.10.10.1-3 با بقیه کلاینت های موجود در شبکه با آدرس 172.10.10.0 / 24 را دارد که در ادامه و در قالب پیکربندی زیر به کمک خواهد آمد:

```
Switch ( config )# vlan access-map No_123 10
Switch ( config-access-map )#match ip address No_123_contact
Switch ( config-access-map )#action drop
Switch ( config-access-map )#vlan access-map No_123 20
Switch ( config-access-map )#action forward
Switch ( config )# vlan filter No_123 vlan-list 100
```

VACL notes :

- VACLs run from top to bottom.
- VACLs have an implicit deny at the end.
- Only one VACL can be applied to a VLAN.
- Use sequence number so you can edit the VACL.
- If there is an ACL and VACL on a L3 interface, at first the VACL will be processed then ACL.

DHCP SNOOPING



- آسیب پذیری از ناحیه عملکرد یک **DHCP** سرور جعلی بروز می کند.
- عملکرد **DHCP SNOOPING** مشابه عملکرد یک فایروال میان کلاینت ها و سرور های **DHCP** جعلی است.

DHCP SNOOPING configuration

- فعال سازی **DHCP Snooping** در Global Mode :

Sw1(config) # ip dhcp snooping vlan <vlan ID>

- مشخص نمودن Trust Port متصل به سرور **DHCP** معتبر در داخل شبکه.

Sw1(config-if) # ip dhcp snooping trust

- بررسی وضعیت

sw1 # show ip dhcp snooping

DHCP SNOOPING configuration …

- تعیین نرخ مجاز دریافت درخواست آدرس بر روی پورت شبکه متصل به سرور **DHCP** :

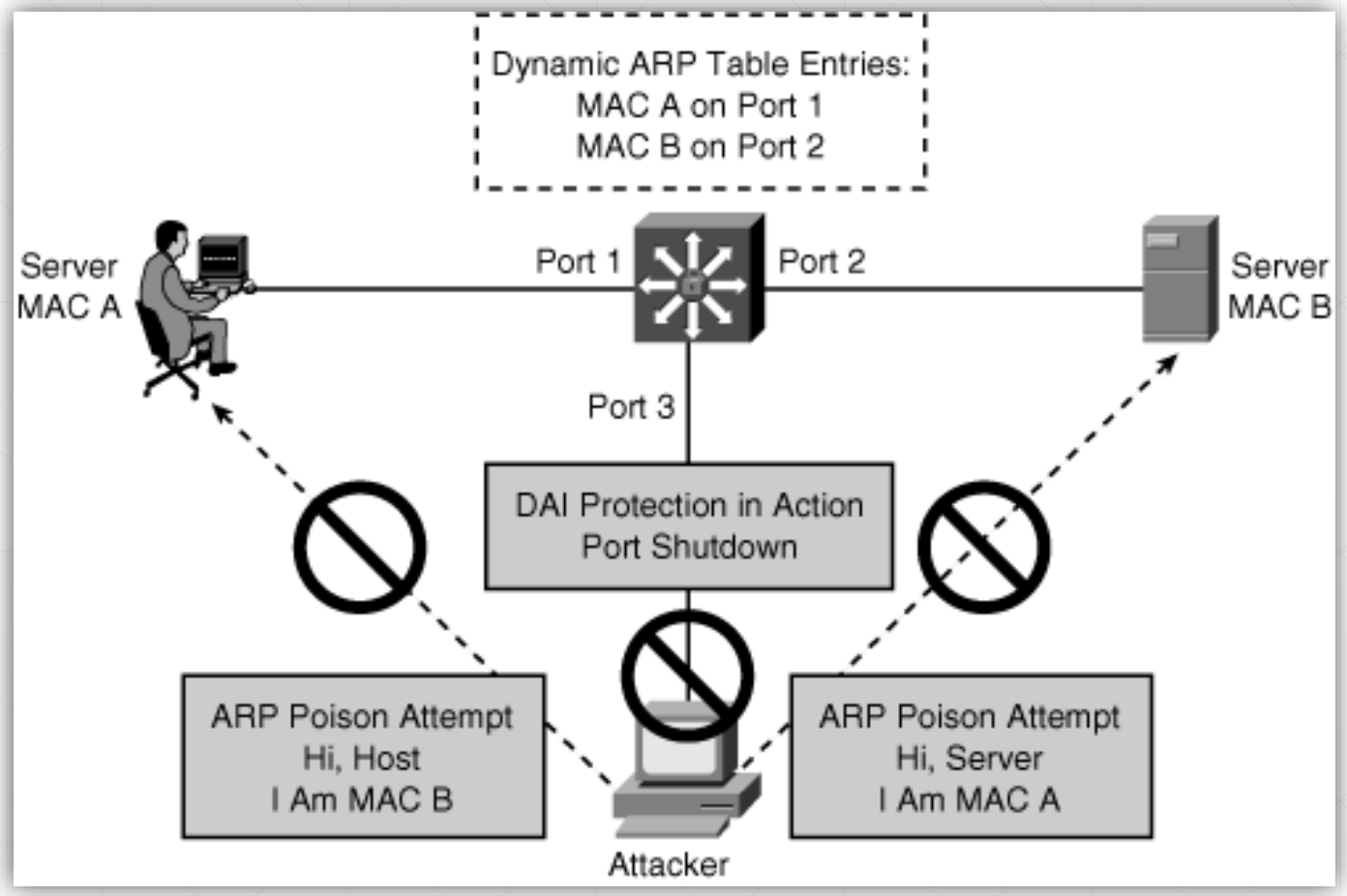
Sw1(config) # interface fa 0/10

Sw1(config-if) # ip dhcp snooping limit rate <1-2048>

Dynamic ARP Inspection (DAI)

- ابزاری جهت مقابله با حمله ARP cache poisoning یا ARP Spoofing که نهایتا منجر به اجرای حمله MAN in the middle میشود.
- از آنجا که DAI از جدول DHCP snooping برای عملکرد خود استفاده می نماید بنابراین لازم است تا قبل از پیکربندی DAI ، مکانیزم DHCP Snooping فعال شده باشد.
- مکانیزم DAI بر روی پورت هایی که بصورت Untrusted پیکربندی شوند نسبت به ارزیابی بسته ها در هنگام ورود (Ingress buffer) عمل خواهد کرد.

Some Layer 2 & 3 security Best Practices / DAI



DAI configuration

Switch (config) # ip arp inspection vlan < VLAN ID >

Switch (config) # interface fast 0/9

Switch (config-if) # ip arp inspection trust

- نکته 1) بصورت پیش فرض تمام پورت ها در مود Untrusted قرار دارند مگر اینکه ما بخواهیم پورتی را بصورت Trust مشخص کنیم.
- نکته 2) سیسکو توصیه میکند در پیکربندی DAI ، تمام پورت های متصل به کلاینت ها در مود Untrust و تمام پورت های متصل به سوئیچ های دیگر از جمله پورت های مربوط به Ether-Channel در مود Trust قرار گیرند.

Enable Password and password encryption.

- استفاده از Enable Secret بجای Enable password
- پسوورد تنظیم شده با Enable secret بر Enable password اولویت دارد.
- برای Encrypt نمودن سایر پسوورد های موجود در Running config می توان از دستور Service Password-encryption استفاده نمود.
- متد Encryption در دستور Enable Secret از Service password-encryption قوی تر است.

Enable secret -> MD5

Service password-encryption -> Vigener cipher

مرکز ماهر

Enable Password and password encryption.

- تعیین محدودیت در انتخاب حداقل تعداد کاراکتر های پسورد.

Router(config) # Security password min-length < 0 – 16 >

- پسورد باید مخلوطی از حروف و اعداد باشد.
- بهتر است اعداد انتخاب شده در وسط عبارت استفاده شوند نه در ابتدا و انتهای عبارت.
- MD5 یک الگوریتم رمزنگاری نیمه ایمن است که یک رشته کاراکتر را به یک مقدار ۱۲۸ بیتی تبدیل می کند.
- یکی از روش های کشف پسورد MD5 استفاده از Rainbow Table میباشد.
- استفاده از SALT و اضافه نمودن تعدادی بیت بصورت رندوم به ابتدای عبارت پسورد، باعث مقاوم تر شدن عبارت پسورد در مقابل روش های Dictionary و Brute Force می گردد.

NTP (Network Time Protocol)

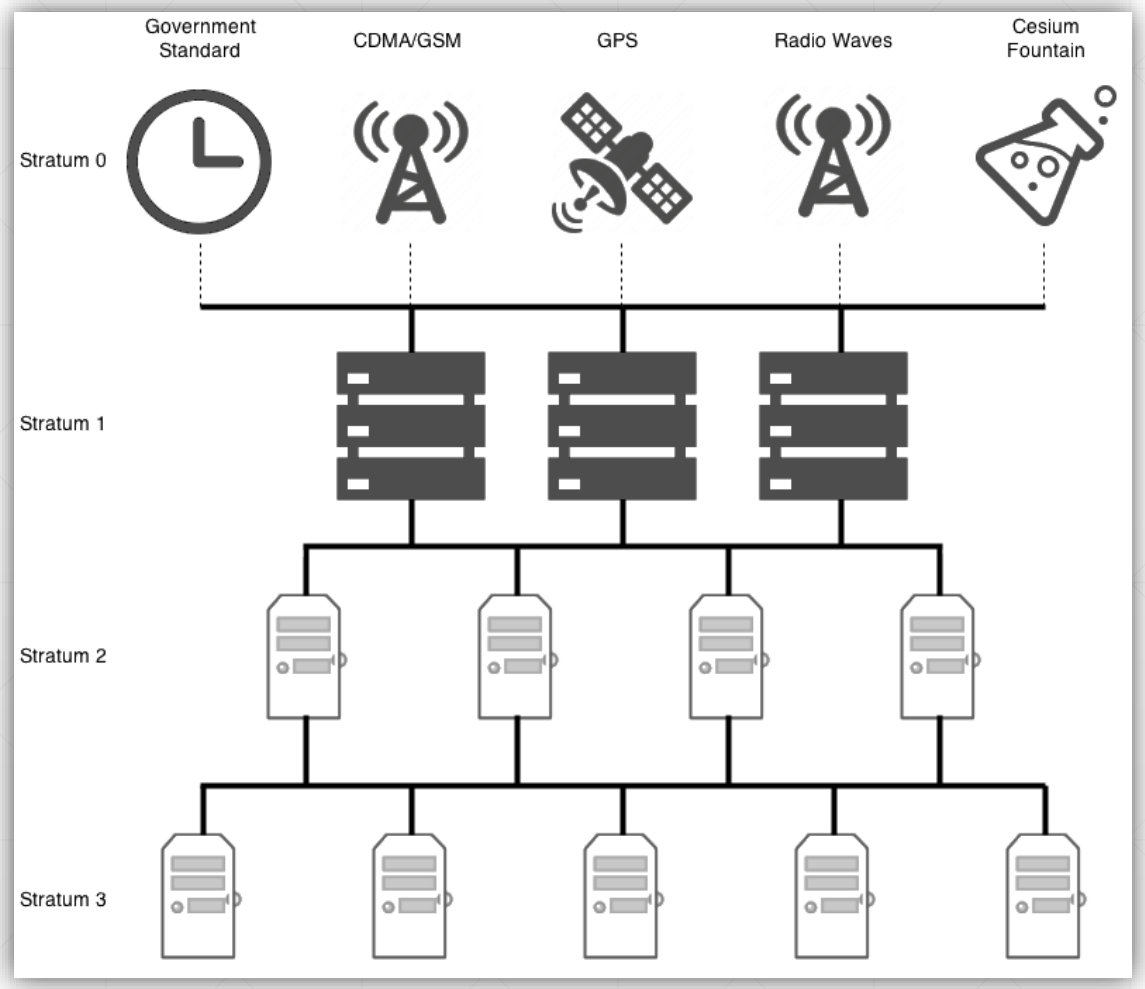
- استفاده از NTP و یکسان سازی زمان بر روی روتر ها و سوئیچ ها موجب افزایش اعتبار و دقت اطلاعات ثبت شده در سرور Syslog می شود.
- همچنین عملیات Replication بین سرور های Domain controller، بهره برداری از سرویس های Digital Certificate و صحت عملکرد سرویس های Accounting شدیدا به دقیق بودن و همسان بودن زمانی تجهیزات وابسته است.
- بسته های NTP مبتنی بر پورت شماره ۱۲۳ و از نوع UDP می باشند.

NTP (Network Time Protocol)

Stratum 0 : Atomic Clock

Stratum 1 : Master Time server

Cisco Router



NTP (Network Time Protocol)

- همیشه NTP Server با ارسال پیام بر روی پورت شماره ۱۲۳ UDP ، بصورت یک طرفه آخرین وضعیت اطلاعات زمان را به اطلاع کلاینت ها رسانده و کلاینت ها بر اساس این اطلاعات ساعت داخلی خود را تنظیم می نمایند.
- امنیت پروتکل NTP باید از طریق ACL و استفاده از نسخه ۳ این پروتکل که مکانیزم Authentication را پشتیبانی می نماید فراهم گردد.

NTP (Network Time Protocol)

- برخی دستورات مربوط به مشاهده و تنظیم زمان (Enable Mode) :

```
Router1 # show clock

Router1 # clock set 10:00:00 may 31 2016
```

- جهت تبدیل یک روتر به NTP master (فقط برای روتر) :

```
Router1(config) # clock timezone IRTS 3 30

Router1(config) # ntp master

Router1(config) # ntp authenticate

Router1(config) # ntp authentication-key 1 md5 XXXXXXXXX
```

NTP (Network Time Protocol)

- تنظیم NTP بر روی کلاینت :

```
ntp authenticate
ntp authentication-key 1 md5 XXXXXXXXXXXXXXXX 7
ntp trusted-key 1
ntp server 192.168.9.20 key 1 prefer
```

- بررسی عملکرد پروتکل NTP :

```
Router1 # debug ntp event
Router1 # show ntp status
Router1 # show ntp association
```

Telnet and SSH

- Telnet ی پروتکل ارتباطی جهت مدیریت از راه دور روتر ها و سوئیچ هاست که بزرگترین مشکل آن انتقال اطلاعات از جمله User name و Password بصورت Clear Text می باشد.
- Secure Shell یا همان پرتکل SSH ، روش ایمن تر از Telnet می باشد که در عمل، داده ها را بصورت رمز شده منتقل می کند.
- برای استفاده از SSH دو متد زیر را میتوان مورد استفاده قرار داد:

1. Local database on the router
2. Authentication via AAA

Telnet and SSH

پیکر بندی پروتکل SSH :

```
Router1 (config) # line vty 0 4

Router1 (config-line) # login local

Router1 (config-line) # transport input ssh

Router1 (config) # username apa privilege 15 secret ramz

Router1 (config) # ip domain-name cert.um.ac.ir

Router1 (config) # crypto key generate rsa
```

Telnet and SSH

پیکر بندی پروتکل SSH (ادامه) :

Router1 (config) # ip ssh ?

Authentication-retries	تعداد مرتبه سعی در ورود
Maxmaxstartups	تعداد کاربران همزمان

ایجاد محدودیت در ارتباط SSH :

Router1 (config) # line vty 0 4

Router1 (config-line) # access-class 1 in

BANNER (MOTD, EXEC, Login)

- طراحی و پیکربندی بنر نوعی اطلاع رسانی و اتمام حجت است.
- برخی مجرمان جرایم رایانه ای با استدلال در خصوص عدم اطلاع از مالکیت روتر توانسته اند از حکم صادره تبرئه شوند.
- انواع مختلف بنر (Banner) :

1. MOTD banner (Message of the day)
2. Login banner (after MOTD before Exec)
3. Exec Banner (After successful login)

BANNER (MOTD, EXEC, Login)

نکته : ^C به عنوان کاراکتر آغازین (Delimiting Character) هر کاراکتری میتواند باشد.

```
banner exec ^C
==============================
Ferdowsi Uni. APA lab.
(exec Banner)
==============================
hostname: $(hostname).$(domain)
VTY Line: $(line)
^C
```

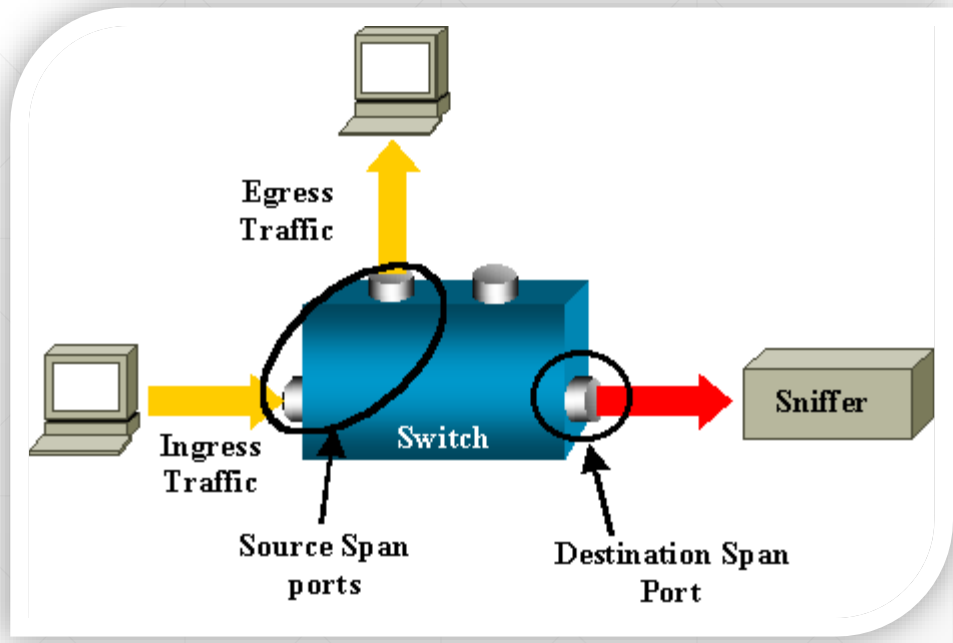
نکته: بعد از ورود نمایش داده می شود.

```
banner login ^C
---------------------------
+    Welcome back (login_B)+
---------------------------
^C
```

نکته: قبل از ورود نمایش داده می شود.

```
banner motd ^C
*********************************************
*      Message of the day                   *
*********************************************
^C
```

- به منظور فراهم نمودن امکان اتصال یک Network Analyser به شبکه، نیاز است تا بتوانیم ترافیک همه یا
تعدادی از پورت های یک یا چند سوئیچ را به سمت یک پورت مشخص هدایت کنیم. به پورتی که دارای چنین ویژگی و خاصیتی باشد اصطلاحا SPAN Port می گوییم.



Span Port Types :

- Local SPAN
- VLAN-Based SPAN (VSPAN) or Remote SPAN (RSPAN)

❑ تعداد Session های همزمان برای اجرای SPAN port به توان و مدل سوئیچ بستگی دارد که می توانند حتی به شصت و چهار Session همزمان هم برسد.

- **Local SPAN**

Switch (config)# monitor session 1 source interface fast 0/1 – 3

Switch (config)# monitor session 1 destination interface fast 0/4

❑ جهت مانیتورینگ وضعیت SPAN می توان از دستور زیر استفاده کرد:

Switch # show monitor

- **VLAN-based SPAN (VSPAN) or Remote SPAN (RSPAN)**

برای پیکربندی RSPAN ابتدا لازم است یک VLAN اختصاصی برای تبادل ترافیک پورت SPAN ایجاد نماییم:

Source Switch :

Switch (config)# vlan 30

Switch (config-vlan)# remote-span

Switch (config)# monitor session 1 source interface fast 0/1 – 3

Switch (config)# monitor session 1 destination remote vlan 30 reflector-port fast 0/24

Destination Switch :

Switch (config)# monitor session 1 source remote vlan 30

Switch (config)# monitor session 1 destination interface fast 0/10

مرکز ماهر

برخی ملاحضات مربوط به انتخاب پورت های Source و Destination :

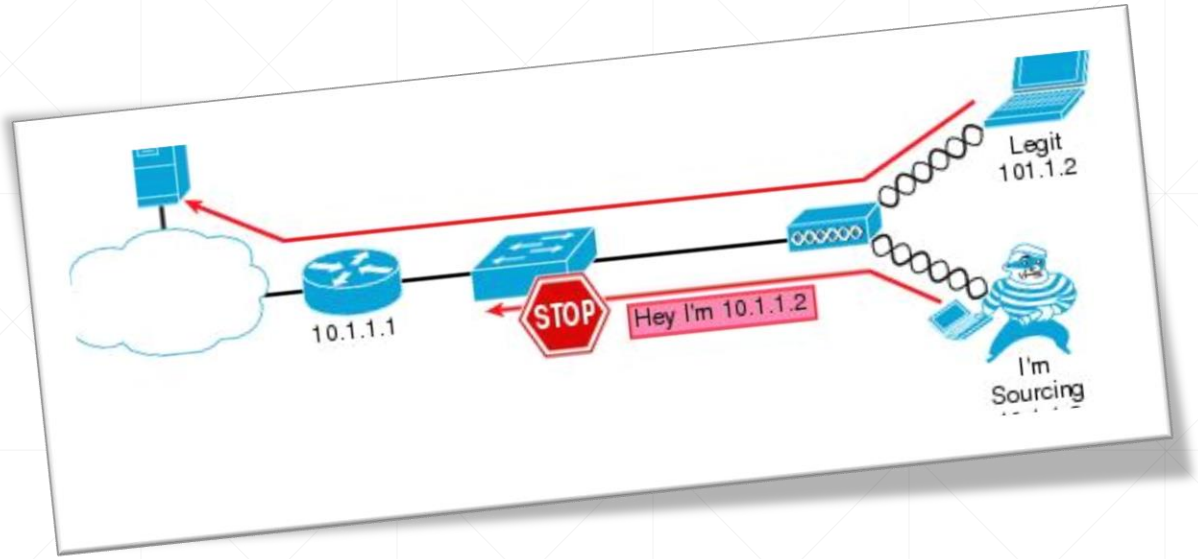
Source span ports

- A source port can be monitored in multiple , Simultaneous SPAN sessions.
- A source port can be part of an ether-channel.
- A source port can not be configured as a destination.
- A source port can be any port type-Ethernet, Fast Ethernet, Gigabyte Ethernet, …

Destination span port

- A destination port can be any port type-Ethernet.
- A destination port can participate in only one SPAN session.
- A destination port can not be configured as a source SPAN port.
- A destination port can not be part of an ether-channel.
- A destination port doesn’t participate in STP, CDP, VTP, PAGP, LACP or DTP.

IP Source Guard



- به منظور ممانعت از بهره برداری غیر مجاز یک کلاینت از آدرس IP کلاینت دیگر مورد استفاده قرار می گیرد.
- IP source guard هم همانند DAI از دیتابیس DHCP Snooping استفاده می نماید.
- به تعبیر دیگر با پیکربندی این ویژگی بر روی سوئیچ، کلاینت های شبکه تنها از طریق IP Address ارائه شده از سوی سرویس DHCP قادر به اتصال به شبکه خواهند بود و در صورت تنظیم آدرس شبکه بصورت دستی ، ارتباطشان از شبکه قطع خواهد شد.

IP Source Guard configuration:

Switch (config) # ip dhcp snooping vlan <vlan 10>

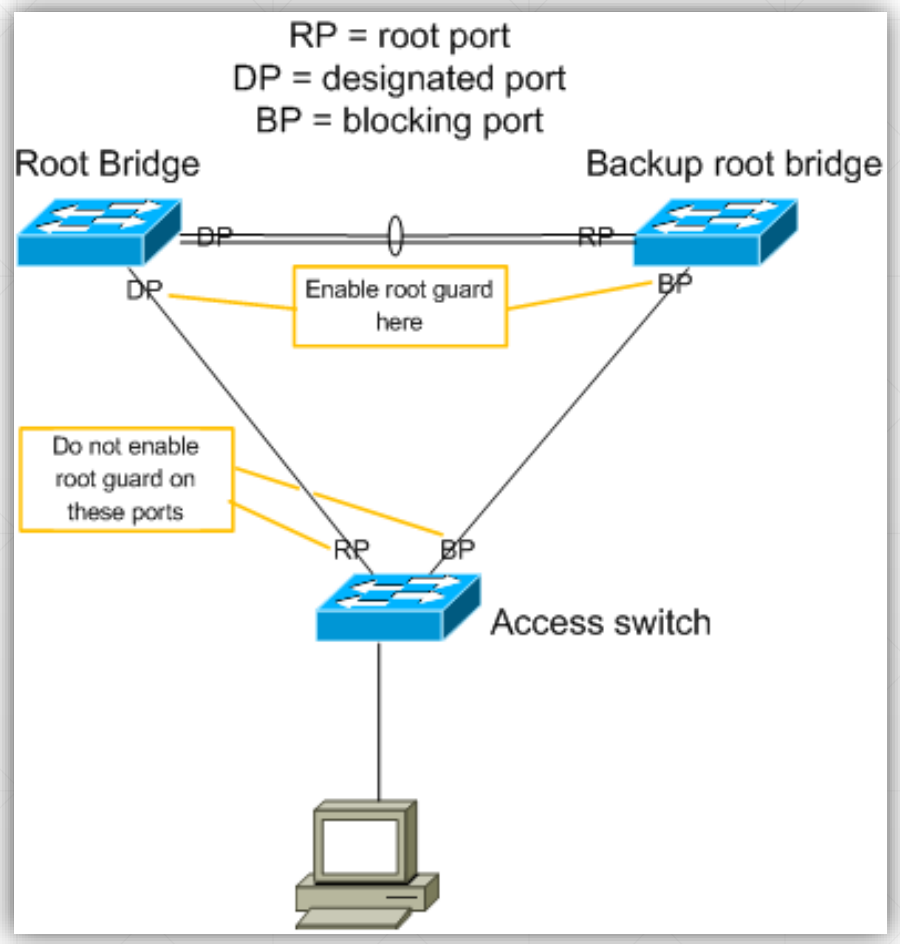
Switch (config) # ip dhcp snooping information option

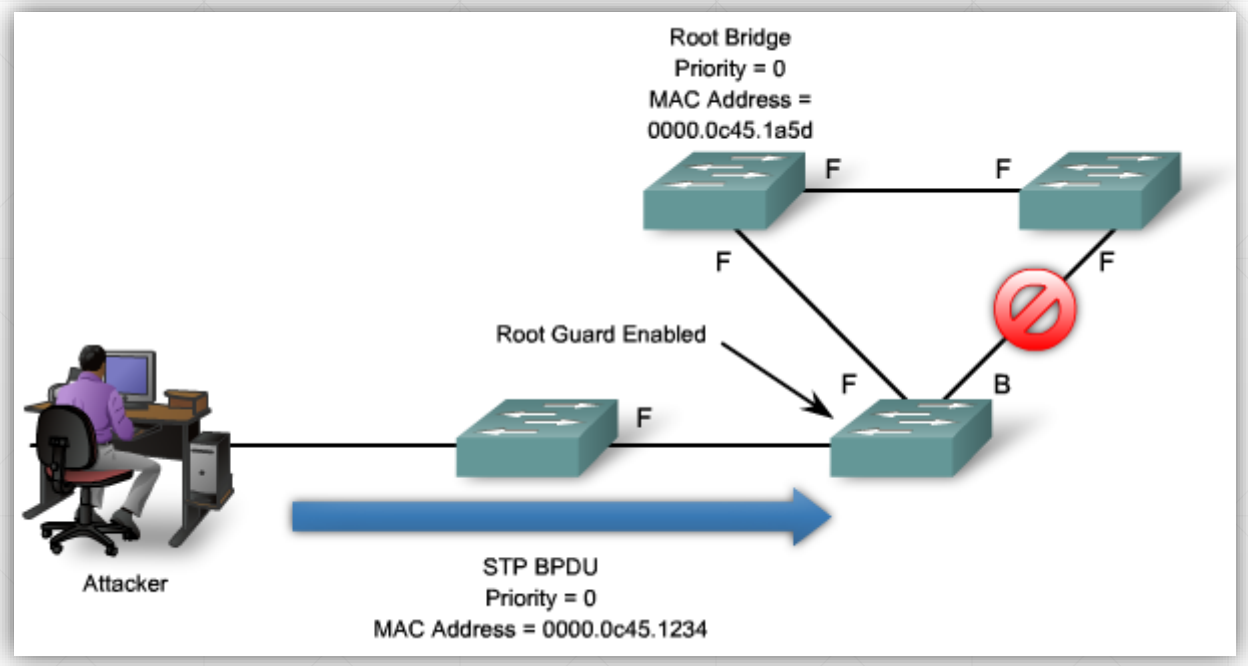
Switch (config) # interface gig 1/1

Switch (config-if) # ip verify source

ROOT Guard

- اجرای حمله از طریق ارسال بسته جعلی STP BPDU یا Superior BPDU به نحوی که محاسبات سوئیچ ها در انتخاب Root Port مختل شود.





ROOT Guard

- به منظور دفاع در مقابل این حمله از دو ابزار بسیار کارآمد و مفید استفاده می گردد:

1. Root Guard
2. BPDU Guard

- در پروسه مربوط به عملکرد STP ، سوئیچ با Bridge ID کوچکتر نقش Root Bridge را احراز خواهد کرد. در محاسبه Bridge ID مقادیر و پارامتر های مختلفی از جمله پهنای باند ارتباطی، Priority و MAC سوئیچ تاثیر گذار خواهند بود.
- مکانیزم Root Guard در سطح اینترفیس های سوئیچ فعال می گردد.

```
Switch(config)# interface fa 0/24
Switch(config-if)# spanning-tree guard root
```

ROOT Guard

- در صورتیکه بر روی پورت محافظت شده با مکانیز Root Guard یک بسته BPDU با Priority کوچکتر شنیده شود، در این حالت سوئیچ آن پورت شبکه را وارد حالت root-inconsistent برده و باعث جلوگیری از تحریک پروسه STP خواهد شد.
- در صورتیکه پورت های سوئیچ بصورت Port Fast پیکربندی شده باشند پیشنهاد می شود بجای Root Guard از مکانیزم دفاعی BPDU Guard استفاده شود. در این حالت اگر بسته BPDU بر روی پورت محافظت شده شنیده شود، پورت مذکور فورا توسط سوئیچ به وضعیت err-disable برده خواهد شد.

```
Switch(config-if)# spanning-tree bpduguard enable
```

- یک روش ساده تر برای فعال سازی bpduguard استفاده از دستور زیر در محیط Global config است:

```
Switch(config)# spanning-tree portfast bpduguard default
```

Questions ?

Thanks for your Attention