



CCNA Cisco certified network associate

[سیسکو]

[Reza Khani]

[1390/06/19]

Active : server . switch . Router → دو دسته → IS & ES

IS → fire wall . Router . switch .

ES → End system → Server . pc .

Passive : cable . duct .

انواع شبکه :

MAN: بعنوان مثال اتصال سه شبکه در سه نقطه از شهر بهم توسط یک واسط (پارس آنلاین)

CAN: بسیار بزرگ و پیچیده و شامل همه ای LAN . WAN . MAN ها

PAN: مثل اینفرارد. بلوتوس

IANA ⇒ RIPE ⇒ Autonomous system ⇒ 2¹⁶ ⇒ 65535 ⇒ public 1-64512 ⇒ privet 64513-65535

به مجموعه ای از شبکه ها که تحت کنترل و نظارت یک مدیر واحد یا یک سازمان مدیریتی واحد باشند آتناموس سیستم می گویند.

به مجموعه آتناموس سیستم های پاپلیک اینترنت می گویند . ANP (network access point)

12 تا شرکت مالک اینترنت از جمله -AT & t DOP که با ارتباط پارشال مش و نیمه مش به هم متصل اند.

اولین بار شبکه ون بود که بین دانشگاه برکلی و وزارت دفاع امریکا راه اندازی شد.

دلیل به وجود آمدن OSI و TCP/IP « تمامی فروشنده ها و تولید کننده ها نرم افزار و سخت افزار به یک پارچه گی برسند . هر جا توانستید نرم افزار را به سخت افزار تبدیل کنید می توانید. تراول شوتینگ.

application لایه هفت « کارش ایجاد سوکت Socket . در ارتباط با سرویس های نرم افزار

presentation لایه شش « کدک و کمپرس . اضافه و باز کردن هدر

session لایه پنج « مسئول چک کردن بودن مقصد (حصول اطمینان از وجود مقصد)

Transport لایه چهار « TCP (user data gram) UDP زمان و حجم تاثیر گذار است .

S port	D port	SEG	ACK	Windows Size	Syn	ACK	push	Fin	RST	H len	option	Check SUN
--------	--------	-----	-----	--------------	-----	-----	------	-----	-----	-------	--------	-----------

Flag = 1 bite

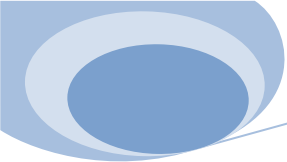
هدر تی سی پی که به ابتدا یک پکت می خورد و 400 بایت اول فایل فرمت فایل را مشخص می کند.

65535 پورت « یک تهاد D port و یک تعداد S port است D port پورت مقصد و تعدادشون 1024 عدد است همیشه یک Dissection را با یک source صدا می زنیم. از 1024 به بالا می شود Source port

SEG شماره گذاری

ACK رسید

Windows Size به تعداد پکت های که در یک لحظه ارسال می شود و رسیدش گرفته می شود می گویند. ویندوز سائز را نه فرستنده و نه گیرنده تعیین می کند بلکه کیفیت خط عامل تعیین کننده است.



در خواست کننده کلاینت Open active

جواب درخواست کننده Open passive
را می دهد مثلاً سرور

سه حالت ارتباط

1)connection negotiation

2) connection maintenance

3) connection termination

syn	ack	push	fin	Re send
1	0	0	0	0
1	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	1	0	1	1
0	0	0	0	1

H len یعنی طول هدر – در آی پی وژن چهار کلا 20 بایت می باشد.

Option بخشی از تنظیمات سکوریته مثل IPS VPN شماره پورت شان

Check sum کل هدر را چک می کند که درست عمل کرده باشد توسط الگوریتم CRC

Subneting: 217.218.196.0 /24 → پرفیکس

1)determine number of network and convert to binary

بین چندتا شبکه داری و عدد آن را تبدیل به باینری کن

تعداد شبکه 5 = باینری 101 = 3 بیت

2)reserve bits in subnet mask and find your network

ساب نت مسک را بنویسید 3 بیت را به ساب نت مسک اضافه کن و پیدا کن تعداد اضافه شونده را . همیشه عدد اضافه شونده ما بیت یک آخر بیت به دست آورنده است . بیت سوم اینجا می شود 32

255.255.255.0 11111111.11111111.11100000 255.255.255.224 /27

3)use Interment to create your network range

217.218.196.0 – 31 217.218.196.32 - 63

217.218.196.64 – 95 217.218.196.96 – 127

X= تعداد بیت اضافه شده $2^x=2^3=8$ تعداد شبکه

Y= تعداد صفرهای در اوکتد آخر $2^y=2^5=32-2=30$ تعداد هاست در هر شبکه

192.5.20.0 /24

تعداد شبکه 50 - تعداد بیت 6 بیت

255.255.255.252 /30

11111111.1111111.1111111.11111100

تعداد هاست $2^2=4-2=2$

192.5.20.0 - 4

تعداد شبکه $2^6=64$

192.5.20.8 - 12

255.255.0.0

150.5.0.0

/16

تقسیم شبکه به 100 شبکه

11111111.11111111.11111110.00000000

1100100

7 بیت

255.255.254.0 /23

$2^7=128$ no network

$$2^9 - 2 = 510 \text{ host}$$

150.5.0.0 150.5.1.255

150.5.2.0 150.5.3.255

150.5.4.0 150.5.5.255

150.5.6.0 150.5.7.255

150.5.8.0 150.5.9.255

8 / 10.0.0.0 تعداد 500 شبکه 9 بیت

11111111.11111111.10000000.00000000 /17 255.255.255.128

29=512 no network

10.0.0.0 10.0.127.255

1.0.128.0 10.1.255.255

10.1.0.0 10.1.127.255

10.1.128.0 10.1.255.255

10.2.0.0 10.2.127.255

10.2.128.0 10.2.255.255

[illegible]

همیشه از بزرگترین شبکه شروع می کنم : VLSM

1) determine number of **host** and convert to binary

2) reserve bits in subnet mask and find your network

3) use Interment to create your network range

60 را با 6 بیت می توان نوشت 217.218.196.0 /24 255.255.255.0

شبکه 64 تا 64 تا اضافه می شود. 11111111.11111111.11000000

255.255.255.192 217.218.196.0 – 63 /26 شبکه C

20 را با 5 بیت می توان نوشت.

217.218.196.64

255.255.255.0

1111111.1111111.1111111.11100000 /27 217.218.196.64 - 95 /27 network A

217.218.196.96 - 127 /27 network B

111111.111111.11111111.11111100 دو را با دو بیت می توان نوشت 255.255.255.252

217/.218.196.128 → 217.218.196.128 – 131 link A – c /30

217/.218.196.128 → 217.218.196.132 – 135 link B- c /30

لایه دو Data link

از لحاظ امنیتی و استاندارد ها لایه مهمی است و دو ساب لایر LLC & MAC در آن وجود دارد. پکت که به لایه دو می رسند تبدیل به فریم می شود توسط LLC و وظیفه CRC با آن است.

لایه دو حاوی استانداردهای لن و ون می باشد .

Ethernet 802.3 - FDDI - Token ring 802.5 - Wlan wireless 802.11

Ethernet>CSMA/CD شیوه دسترسی : مدت زمان هاب برای برخورد 60 ثانیه است

64 بایت اول پکت « نرمال کالیژن » دچار مشکل نمی شود « شامل دیتا نیست

بعداز 64 بایت اول «لایت کالیژن» عواملی مثل « کارت شبکه خراب . طول کابل . نویز زیاد

wireless 802.11 > CSMA/CA

اول از CSMA/CA استفاده می کند در صورت برخورد از CSMA/CD استفاده می کند.

محیط اترنت « دو محیط : شر بیس shared base دیکتد بیس dedicated base

shared base سیگنال بصورت شر مثل هاب

dedicated base اختصاصی مثل سویچ

هاب کالیژن فول وجود دارد همین طور برادکست اما در سویچ کالیژن به ازای هر پروت و برادکست یک بار

بسته های داده ای در لایه دو برادکست

Flood « پکت های که برای یک نفر خاص فرستاده می شود و همه گوش می کنند.

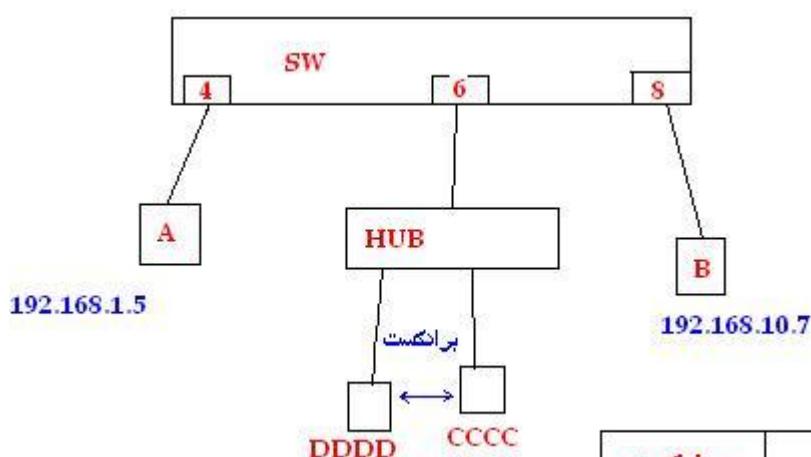
Multi cast برای یه گروه مشخص و یکسری از اعضا می توانند بگیرند پکت را

Uni cast برای یک نفر

Any cast پیغامی که فرستاده می شود اولین نفری که بتواند جواب بدهد . با آی پی ورژن 6 می آید

Unknown cast پکت های سرگردان در شبکه . یا پکت های مه یک هکر فرستاده . مبدا و مقصد شان را از دست دادن

سویچ در جهت ورودی هر بسته ای به دستش برسد مک را یاد می گیرد.



		S iD	D iD		
برادکست	AAAA	10.5	10.7	HL4	Hi
FFFFF					

D mac S mac

AAAA	BBBB	10.7	10.5	HL4	Hi
------	------	------	------	-----	----

مدت زمانی که مک آدرس بصورت پیش فرض در جدول می ماند.

بعد از جواب دادن b ارتباط فوروارد می شود دیگر مراحل جدول (برادکست)

انجام نمی شود.

Forward and filter decision making وظیفه سویچ در لایه دو

یک عدد مک آدرس هر سویچ دارد بنام Base Mac Address

Arp -A دستوری که کامپیوتر جدول آرپ خودش را نشان می دهد.

Arp -d دستور پاک کردن جدول آرپ سیستم

سویچ Switch لایه ای دو داریم لایه سه هم داریم و چند لایه هم داریم (malty layer switch) MLS که در لایه دو و سه و چهار کار می کند.

سری سویچ ها

2900 → 2960 – 2950

3500→3560 – 3550

3700→3750

4000→4006- 4003

4500→4510-4507-4506-4503

6500→6513-6509-6506-6503

سوییچ باید قابلیت کانفیک داشته باشد در غیر این صورت هاب می باشد . با پورت کنسول که در پشت سوییچ قرار دارد و با کابل کنسول که به کامپیوتر وصل می شود توسط کانکتور سریال و اسم کابل RS232 می شود و IOS را نصب کرد و از طریق IP آدرس هم می شود دسترسی داشت به سوییچ . برای دسترسی به کنسول باید از نرم افزارهای مختلف استفاده کرد که در ویندوز ایکس پی هایپرترمینال بصورت پیش فرض وجود دارد . secure CRT -tra terminal

Hyper terminal ⇒ name ⇒ com port 1 ⇒ 9600 bit ⇒ enter

در سوییچ سه مود اصلی برای وارد شدن داریم:

User Exec mode : >

یوزرها ب یوزر و پسوردسان وارد می شوند و کارهای محدودی می توانند انجام بدهند

Privilege mode : #

برای وارد شدن به این مود کامند Enable را می زنیم و پسورد را وارد می کنیم

Global config mode : (config)#

برای وارد شدن به این مود Conf terminal یا conf t

Host name دستور تغییر نام سوییچ

تغییرات اعمال شده را حتما باید ذخیره کرد در غیر اینصورت بعد از رفتن برق کل تنظیمات پاک می شود.

مثل رم کامپیوتر DRAM حافظه ای که آی او اس روش قرار دارد 16m-1G flash

NV ram حافظه غیر فرار (تنظیمات در اینجا ذخیره می شود) قسمت کوچکی از او اس ROM

در محیط پری ولیج مود برای ذخیره شدن تغییرات دستور زیر را می زنیم

WR* write* write memory* copy running- config startup-config

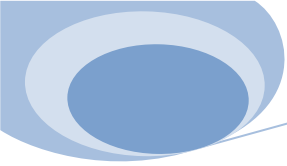
پاک کردن کل کانفیگ Erase startup –config enter

ری استارت شدن سوییچ Reload

اگر کانفیگ روش نباشد برای اولین بار می گوید می خواهی استپ به استپ ویزادو بریم جلو

Enable ⇒ conf t ⇒ host name ⇒ enable password ⇒ exit

بعضی از آی او اس ها پسورد ثانویه ندارند – قرار دادن پسورد ثانویه با دستور enable secret



Break Cisco password >>> web IFM

Conf t ⇒ service password –encryption ⇒ پسورد را با کارکتر نشان بده

قابل بازگشت Encryption - غیر قابل بازگشت hash

Google ⇒ break Cisco password ⇒ ifm ⇒ web sit for show pass encryption

16 Line VTY تا لاین وی تی وای تل نت

Conf t ⇒ line VTY 0 4 ⇒ enter ⇒ password ⇒ enter ⇒ login ⇒ exit

Interface VLAN 1 ⇒ ENTER ⇒ IP ADDRESS 192.168.10.100 255.255.255.0 ⇒

⇒ ENTER ⇒ NO SHUTDOWN از حالت خاموش در می آید

CMD ⇒ telnet 192.168.10.100 ⇒ enter ⇒ password login ⇒ enter ⇒ pass switch ⇒ shoe run

تل نت بسیار نا امن است . بهتر است از SSH استفاده شود.

SSH با استفاده از کلید امنیتی دیتا را اینکریپت می کند برای ساختن کلید « یورز نام . پسورد . دامین نام . اسم خود سویچ از ترکیب این چهار مورد کلید را می سازد.

Hay per terminal ⇒ conf t ⇒ user name ⇒ pass word ⇒ IP domain -name ⇒ crypto key geyte rsa ⇒ 1024 ⇒ enter ⇒ IP SSH Ver v2 ⇒ enter

Active SSH ⇒ line VTY 04 ⇒ transport input SSH ⇒ login local ⇒ exit ⇒ WR

SSH (پورت 22) پیش فرض در ویندوز نیست در نتیجه از برنامه ای دیگر استفاده می کنیم.

Putty ⇒ IP ⇒ user name ⇒ pass ⇒ EN ⇒ pass ⇒ show run

TFTP32 port 169 UDP

بک آپ گرفتن هم از او اس هم از کانفیگ در سویچ :«

در محیط پری ولیج از ای او اس و کانفیگش

Switch ⇒ copy startup-config tftp ⇒ enter ⇒ IP system ⇒ enter ⇒ name back up

Re store ⇒ En ⇒ conf t ⇒ show run INT valn 1 ⇒ conf t INT VLAN 1 ⇒ IP address 192.168.10.100 255.255.255.0 ⇒ no shutdown

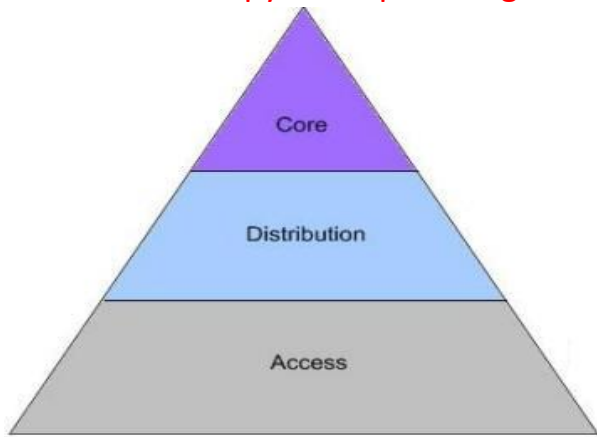
copy tftp: startup-config ⇒ IP system ⇒ file name ⇒ enter ⇒ copy startup-config ⇒ running - config ⇒ enter

SSH روی ای او اس های که سکيور باشد می شود زد

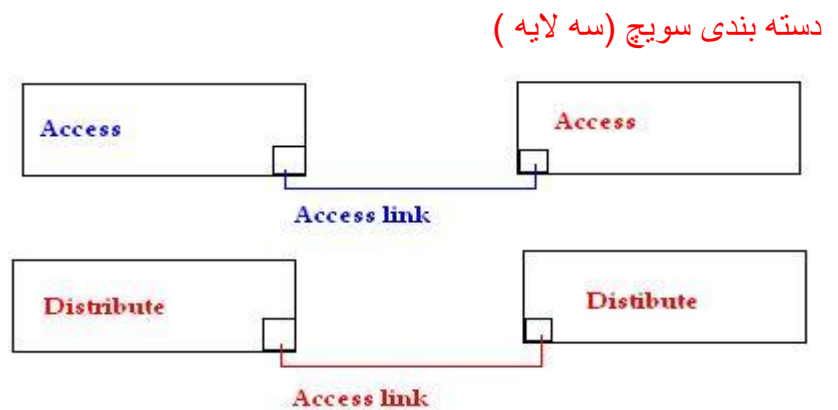
Backup => conf t>copy startup –config tftp:>IP system

Re store => conf t>copy startup –config tftp:>IP server

Active => copy startup –config running-config



Access:



دسته بندی سویچ (سه لایه)
سویچ های که کامپیوتر کلاینت بهش متصل اند می گویند اکسس شرایط

- 1-) L2 –SW
- 2-) low cost per port
- 3-)power full up link
- 4-) no firewall no filtering with policy(VLAN-STP-QOS)



نبايد در سویچ لایه اکسس فیلترنیگ و فایروال بنویسید هر چند که امکانش وجود دارد و پالیسی های فوق را باید ساپرت کند. مثل 2940-2950-2960

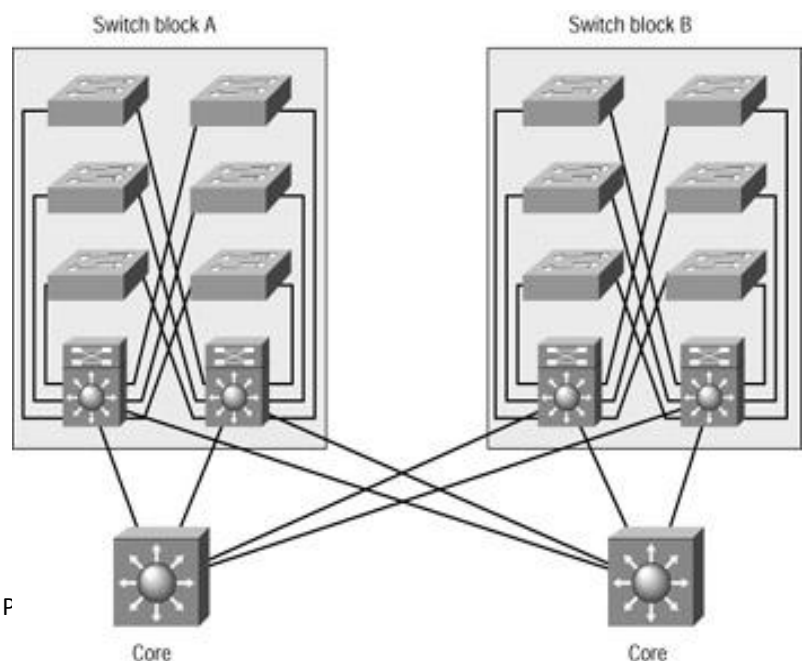
Distribute:

- 1-) L3 –SW
- 2-) full redundancy & full load balancing
- 3-) filtering & fire wall
- 4-)modular
- 5-) up link

Core:

- 1-) L3 –SW

down link



2-) modular

3-) down link

4-) redundancy

5-) no firewall no filtering with policy(VLAN-STP-QOS)

- مجموعه سویچ های اکسس و distortion را سویچ بلاک می گویند *
- اگر یک سویچ بلاک داشتیم احتیاج به Core نداریم .

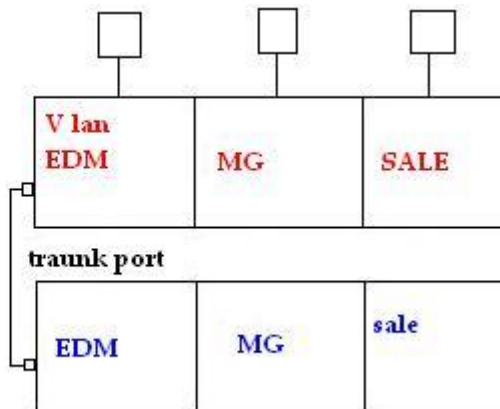
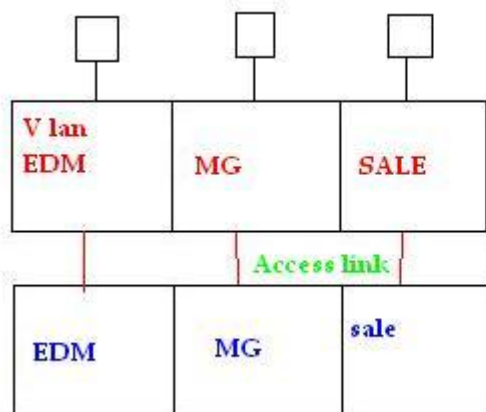
شبکه های در دیزان سه لایه ای «

زمانی که ما یک بلاک سویچ یک عدد داریم Collapse Core

زمانی که ما چند سویچ بلاک و دو سویچ کور داشتیم Dual Core

زمانی که ما چهار سویچ کور داریم Quad Core

دلیل ایجاد وی لن « بخش های مختلف سویچ با هم ارتباط داشته باشند اما با قوانین جدید . ایجاد می کنیم که برادکست دامین را خورد کنیم .



بجای اکسس
لینک از
پورت
ترانک
استفاده می
کنیم .

پورت ترانک پورتهای که عضو هیچ وی لنی نیست اما ترافیک همه وی لن ها را از خودش عبور می دهد. ترانک از دو روش استفاده می کنیم برای عبور ترافیک

منسوخ شده دیگر استفاده نمی شود ⇒ Cisco ⇒ Enter switch link ⇒ ISL

هر دو سویچ باید حتما سیسکو باشد – پکت را سنگین می کند چون 26 بایت به ابتدای پکت و 4 بایت به انتهای پکت اضافه می کند و پکت 1518 MTU بایت که جمعا 1548 بایت می شود.

IEEE 802.1Q « کلا 4 بایت به پکت اضافه می کند و از دوتا دو بایت تشکیل می شود .

توکن رینگ

TPID	3 BIT	1 BIT	12 BIT
------	-------	-------	--------

مشخص کننده نوع وی لن	802.1P cOS CLASS OF SERVICE	CFI CANONICAL	VLAN ID 4096 تعداد وی لن در سوییچ می توانیم داشته باشیم
----------------------	---	------------------	---

دو شیوه ساخت وی لن « VLAN.DAT فایلی که بعد از ساخت اولین وی لن ساخته می شود و وی لن بعد از Erse پاک نمی شود.

① Pre village mode > VLAN Data Base > VLAN 2 > name > exit خروج حتما باید زده شود برای ساخت

Show It

② Conf T V lan 4> enter > name در سوییچ های جدید

Show V lan دستور نمایش وی لن

Conf t > No V Lan 5 دستور پاک کردن وی لن

Conf t > V lan 5 > enter > name دستور تغییر نام وی لن

چطور پورت را عضو کنیم؟

Conf t> INT F 0/1 > switch port mode > Access dynamic trunk > switch port F access VLAN 2

Conf t > INT F 0/5 > switch port mode access

F : fast Ethernet trunk نمیدونم dynamic برای پی سی Access

در صورت ایجاد وی لن « افزایش سطح امنیت شبکه . منچینگ شبکه راحتتر می شود.

انتقال دیتا بین وی لن امکان پذیر نیست مگر پورت ترانک داشته باشیم (دیتا از پورت ترانک عبور می کند)

TPID بایت 2	3 BIT	1 BIT توپولوژی	1 BIT
----------------	-------	-------------------	-------

1 = توکن رینگ
0 = اترنت

اگر دو تاسویچ لایه دو داشته باشیم هر کدام با وی لن ها جدا باید بینشان روتر یا سویچ لایه سه باشد جهت عبور دیتا
 سویچ لایه دو فقط در وی لن یک می شود آی پی داد بصورت پیش فرض . وی لن یک همیشه بصورت دیفالت وجود دارد و همه پورت های سویچ عضو آن هستند.

ایجاد وی لن `EN>conf t>enter>VLAN4>enter>name it>enter>exit`

انتقال وی لن یک سویچ به سویچ دیگر « دو راه » 1- روی یک سویچ هر چی داریم در دومی بسازیم 2- در سویچ یک وی لن را که ساخته ام را کپی کنیم روی وی لن سویچ دو « تحت شرایط زیر

VTP VLAN trunk protocol پروتکل فوق وجود داشته باشد که سه وظیفه دارد (پیش فرض هست)

1- Create 2- delete 3- modify

3 mode VTP => server - client - trans parent

Server: Create . delete. modify

Client: هیچ کدام

trans parent: Create . delete. modify

پیش فرض تمام سویچ ها در مود سرور هستند . می شود به مود های دیگر بردشان . در مود سرور می شود وی لن های که درونشان ساخته شده به سویچ های که مودشان سرور یا کلاینت انتقال داد .

اگر یک سویچ مودش کلاینت باشد فقط می تواند تغییرات را دریافت کند از سویچ مود سرور

اگر یک سویچ ترنس پرنت باشد خودش کپی روی خودش انجام می دهد و تغییرات روی هیچ سویچی اعمال نمی کند و از هیچ سویچی تغییرات را نمی گیرد.

وی تی پی در یک محدوده می تواند تغییرات را انجام بدهد که به آن محدوده وی تی پی دامین می گویند بصورت پیش فرض وی تی پی دامین اسمی ندارد اگر اسمی بگذاریم هیچ تبدیلی با سویچ ها دیگر ندارد.

بررسی وضعیت وی تی پی:

`En > show VTP status > enter`

شامل سه ورژن که همه سویچ ها ورژن سه را ساپورت نمی کنند VTP

تعداد تغییراتی که در وی لن ایجاد شده `Conf T>revi > 0`

1005 تعداد وی لن ها که پشتیبانی میکند 5 تا برای سویچ

تعداد وی لن موجود در آن سویچ

`VTP option mode> server`

VTP domain

VTP pruning >disable

اسم گذاری دامین `VTP domain name >>> Conf T >enter> VTP domain>name>enter`

در سویچ های جدید با سویچ های قدیمی ترانک کردن فرق دارد.

مثلا 2950 و 2960 دات وان کیو کار میکند مابقی سویچ ها هم دات وان کیو و هم ISL

`INT 91/1 >Conf T>switch port trunk en Cass dot1q enter > switch port mode trunk enter`

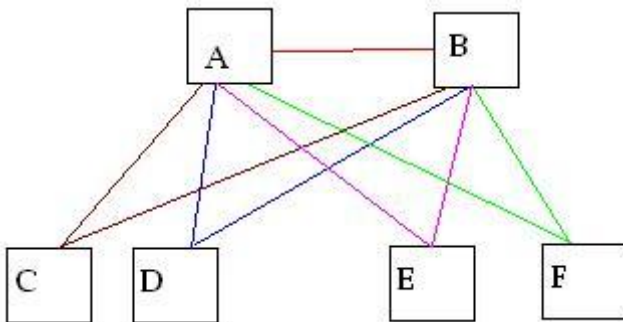
Revision number VTP > packet > summary – request – subset دارد 3

سویچ سرور تغییراتی در وی لن انجام شود عدد یک دونه اضافه می شود و به ازای هر تغییر پکت سامری می فرستد در کل شبکه می چرخد و به دست تمام سویچ ها می رسد . دو سویچ دیگر Revision number خودشان با پکت را مقایسه می کنند اگر تغییرات کمتر بود request می دهند که ما تغییرات را می خواهیم بر ایمان ارسال کن . سویچ سرور با پکت ساب ست تغییرات را ثبت می کند و سینک انجام می شود.

Revision number در دو حالت صفر می شود. 1) وقتی وی تی پی دامین را تغییر دهیم 2) وقتی مود وی تی پی از سرور به ترنس پرنت می بریم .

کجا لازمه Revision number را صفر کنیم « یک سویچ کارکرده را بخواهیم به شبکه خودمان اضافه کنیم باید وی تی پی دامین را تغییر نام بدهیم و مودش را عوض کنیم.

`Conf T>VTP mode transparent enter` `Conf T>VTP mode client enter` عوض کردن مود



سناریو : سویچ لایه دو + لایه سه

CDP > Cisco discoverer protocol پیش فرض در همه سویچ ها فعاله و سویچ می تواند همسایه شو شناسایی کند در سویچ A

دستور نمایش همسایه هایش `Show CDP neighbors`

`Switch a >>> Conf T enter >INT range F 0/20 -24 enter>switch port trunk encapsulation dot1q enter> switch port mode trunk`

از پورت 20 تا 24 ترانک می شود. Show run

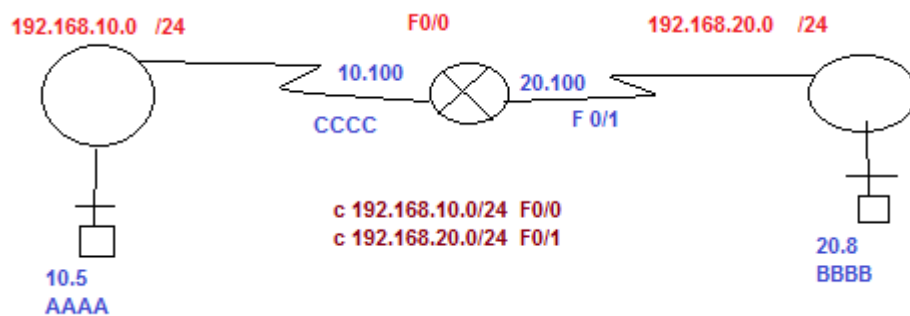
در سویچ B هم ترانک می کنیم پورت ها را در مابقی سویچ ها همین طور معرفی می کنیم .

برای عضو کردن پی سی ها»

INT range F0/1 -10 enter >switch port mode access enter> switch port access VLAN 10 enter

Conf T>INT range F0/11 -22 enter>switch port mode access enter> switch port access VLAN 20 enter>exit wr

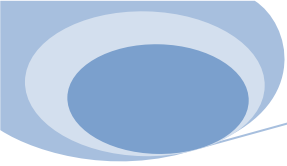
به کلاینت ها آی پی می دهیم.و تعریف گت وی 24 / 192.168.20.0



Mac	S Mac	HL3			
FFFFFF	AAAA	sip 10/5	D ip 20/8	HL4	Hi
		S iD	D iD		
cccc	AAAA	10.5	10.100	HL4	Hi

روتر خودش می تواند برادکست تولید کند و برادکست را از خودش عبور نمی دهد.

		S iD	D iD		
برادکست FFFFFF	AAAA	20.100	20.8	HL4	Hi



دادن آی پی به سویچ لایه سه « به اینترفیس وی لن ها » آی پی می شود و گت وی خاص اون وی لن استاندارد لایه دو 802.1x ایکس هر چه بود لایه دو می باشد.

- به ترانک نمی شود آی پی داد و اگر بدهیم از ترانک خارج می شود .
- فایل Vlan.dat حاوی وی تی پی دامین و وی لن ها می باشد.

دادن آی پی به وی لن :

Conf T>INT VLAN 10 enter>IP address 192.168.10.100 255.255.255.0 enter

روی اینترفیس فیزیکی وی لن می زنیم No shutdown > VLAN 1. روی اینترفیس مجازی نمی زنیم.

ساخت جدول روت برای سویچ

*****Conf T enter>IP routing enter *****

اگر سویچ لایه سه نداشتیم و از روتر استفاده کردیم > جایکه قیمت روتر از سویچ لایه سه ارزان تر است.

حالتی که روتر به سویچ لایه دو وصل است . Router on stick

تمرین :

1841 router int f0/0 enter ip address no show enter

2960 switch 2 vlan vlan 10 and vlan 20

ساب اینتر فیس تگ دات وان کیو می خورد . اینترفیس مجازی که زیر اینترفیس واقعی درست می شود.

Conf T>INT F0/0.10 enter>encapsulation DOT1Q 10 ENTER>IP ADDRESS ENTER>EXIT

Show VTP static -> VTP pruning mode

کارش: در تمام سویچ ها وی لن وجود دارد از طریق پورت ترانک در یک سویچ که کلاینت عضو گروه 30 و 50 باشد و اگر در سویچ دیگر کلاینت عضو گروه 10 باشد آیا برادکست آن در سویچ که حاوی کلاینت 30 و 560 است می آید ؟
بله

show Interface trance دستور نمایش پورت ترانک

در نتیجه این ترافیک در پورت ترانک رد می شود به سویچ دو می رسد در حالیکه هیچ کلاینتی عضو گروه 10 نداریم پس باید جلوگیری از این ترافیک بی خود کنیم برای جلوگیری VTP pruning در همه سویچ ها هم access هم designate port وقتی اینکار را کنیم سویچ اکسس با یک پکت به سویچ designate port اعلام می کند که من وی لن

های x و y را داریم برادکست این دو وی لن را برام بفرست و بقیه وی لن ها رو نفرست اگر وی لن جدید اضافه کنیم بصورت اتومات برادکست آن وی لن به دستش می رسد

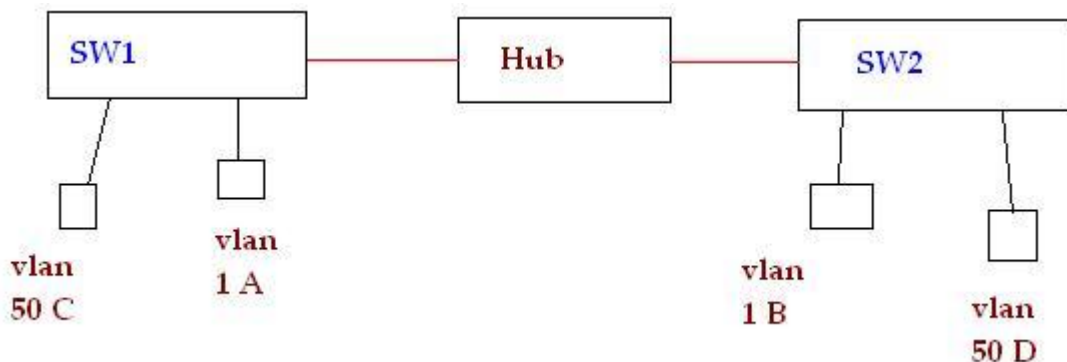
Conf t > VTP pruning غیر فعال no VTP pruning فعال

دستوری که برای وی تی پی پسورد می گذارد برای امنیت بیشتر اگر یک هکر توانست یک سویچ VTP password جدید در شبکه بگذارد تا پسورد را نزنند رپلیکت نمی شود با سویچ های دیگر

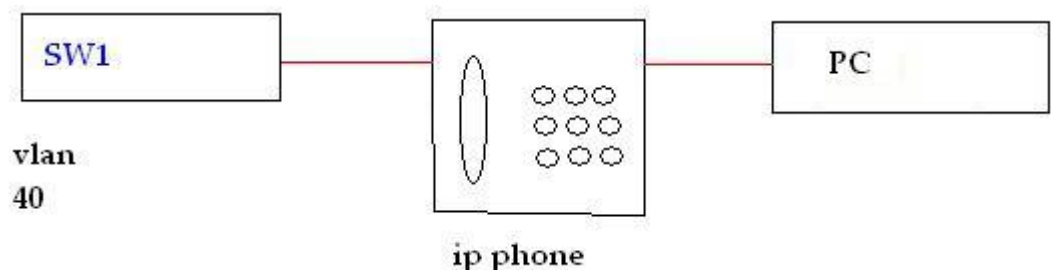
Show INT trunk > native VLAN

پیش فرض در همه سویچ ها وی لن یک native است می شود آنرا تغییر داد وی لن native تگ دات وان کیو نمی خورد.

در دو حالت استفاده می شود: کلاینت A با B راحت کار می کند در حالیکه کلاینت D و C نمی توانند. چون پورت ترانک نداریم که وی لن ها از خودش عبور دهد. بعلت نخوردن تگ دات وان کیو و پیغام DTP miss match می دهد چون ما نیاز داریم حتما وی لن 50 با هم کار کنند آنرا native می کنیم و native باعث می شود تگ دات وان کیو از روش برداشته شود تا ارتباط داشته باشیم.



حالت دوم: وقتی که یک ای پی فون داریم که با یک پورت به پی سی و با یک پورت به سویچ متصل است و ای پی فون دات وان کیو می فهمد در حالیکه پی سی نمی فهمد. وی لن 40 را native میکنیم که دیتا به دست یوزر برسد.

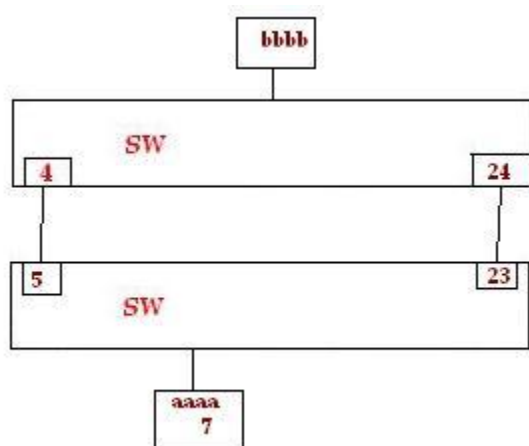


برای ساخت native

Conf t > enter > INT range F0/23 -24 > enter switch port trunk native VLAN 50 > enter

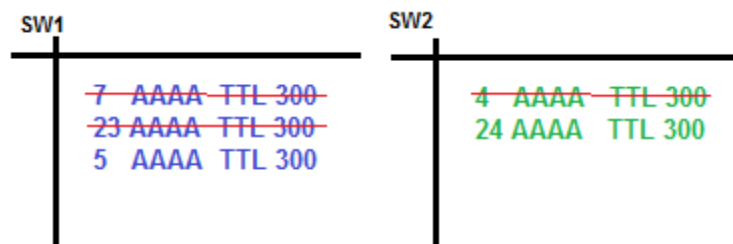
دستور نمایش Show INT trunk

برای خرید سویچ باید پارت نامبر داشته باشی نه مدل . پارت نامبر در دیتا شیت نوشته شده که شناسنامه ای آن سویچ است . اسم دیگر سویچ کاتالیست



STP >>> spanning tree protocol

اگر بین دو تا سویچ دوتا کابل برای بک آپ بکشیم در یک سناریو که اگر یک کابل قطع شد آن یکی کار کند .



دفعه اول دیتا به همه پورت ها ارسال می شود به غیر از پورت ورودی که به این کار اسلیت هوریزون می گویند مک آدرس فلونینگ از یک پورت سویچ منتقل می شود به پورت دیگر و بعد از مدتی مک تیبل اینکار را می کند و بعد لوپ اتفاق می افتد و بعد سویچ کرش می کند و از کار می افتد.

DEC NET شرکتی که روشی ارائه کرد که سویچ کرش نکند در صورتی که سویچ داشتیم دو کابل داشته باشد یکی برای بک آپ «یک پورتش را بلاک می کند و یکی را آزاد . وقتی که پورت آزاد به هر دلیلی قطع شد پورت بلاک را آزاد می کند و IEEE این استاندارد را نام گذاری کرد 802.1D or STP

انواع STP

CSTP 802.1d common

RSTP Rapid

PVST per vlan

PVST+ per vlan + dot 1 Q

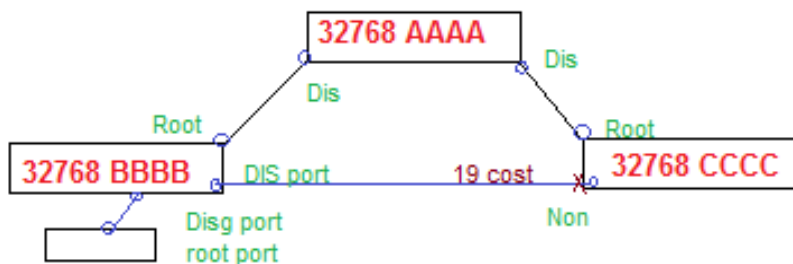
RPVST rapid per vlan

MST multi

MIST multi instant

پیش فرض در سویچ های سیسکو SPT فعال است ولی در هاب نیست

برای اینکه تشخیص بده کدام نقطه را ببندد نیاز به یک عددی داریم روی سویچ که آن را Bridge ID می گویند و از probity + Mack address تشکیل شده است



از 0 تا 61440 که عدد دیفالت سویچ 32768 است.

باید در این مجموعه یک رییس انتخاب شود و برای مشخص شدن رئیس انتخابات برگزار شود «اون سویچی رئیس می شود که بریدج آی دی پائین تری داشته باشد چون مک آدرس A از همه پائین تره رئیس می شود «چطور» توسط مکانزیمی «سویچ هر 2 ثانیه یک پکت را آزاد می کند بنام BPDU bridge protocol data unit

به رئیس ROOT Bridge می گویند

خودش Root bridge id
خودش Bridge id
0 Cost to root
2 ثانیه Hello time
20 ثانیه Max age
15 ثانیه Forward dilly

که حاوی

همه سویچهای که این پکت را می فرستند دفعه اول در روت بریج خودش را می نویسد چون فکر میکند خودش پائین ترین آی دی را دارد بریج آی دی هم خودش می نویسد .

Cost to root هزینه رسیدن به ریاست که صفر می گذارند.

هلو تایم 2 ثانیه . مکس ایج 200 ثانیه . فوراد دیلی 15 ثانیه

محاسبه کاست در اس تی پی توسط لینک

10m 100 - 100m 19 -1000m 4- 10000m 2

چند عامل دیگر برای بستن پورت : سه عامل

Root port - designate port – none designated port

هر سویچی غیر از سویچ پورت باید یک روت پورت داشته باشد فقط یک عدد . پورتهی که بسمت سویچ روت می رود . روت پورت هیچ وقت بلاک نمی شود.

designate port پورتهایی که همیشه جریان دارد و بلاک نمی شود. تمامی پورت های روی سویچ بریج از نوع designate port هستند و اگر به یک سویچ یک کلاینت وصل کنیم آن پورت designate port است. تمامی پورت های روی روتر پورت از نوع designate port هستند.

4 تا قانون: اگر جای سر دو راهی مانند برای انتخاب designate بین B و C

1-) lowest bridge ID

2-) lowest cost to root

3-) lowest sender bridge ID

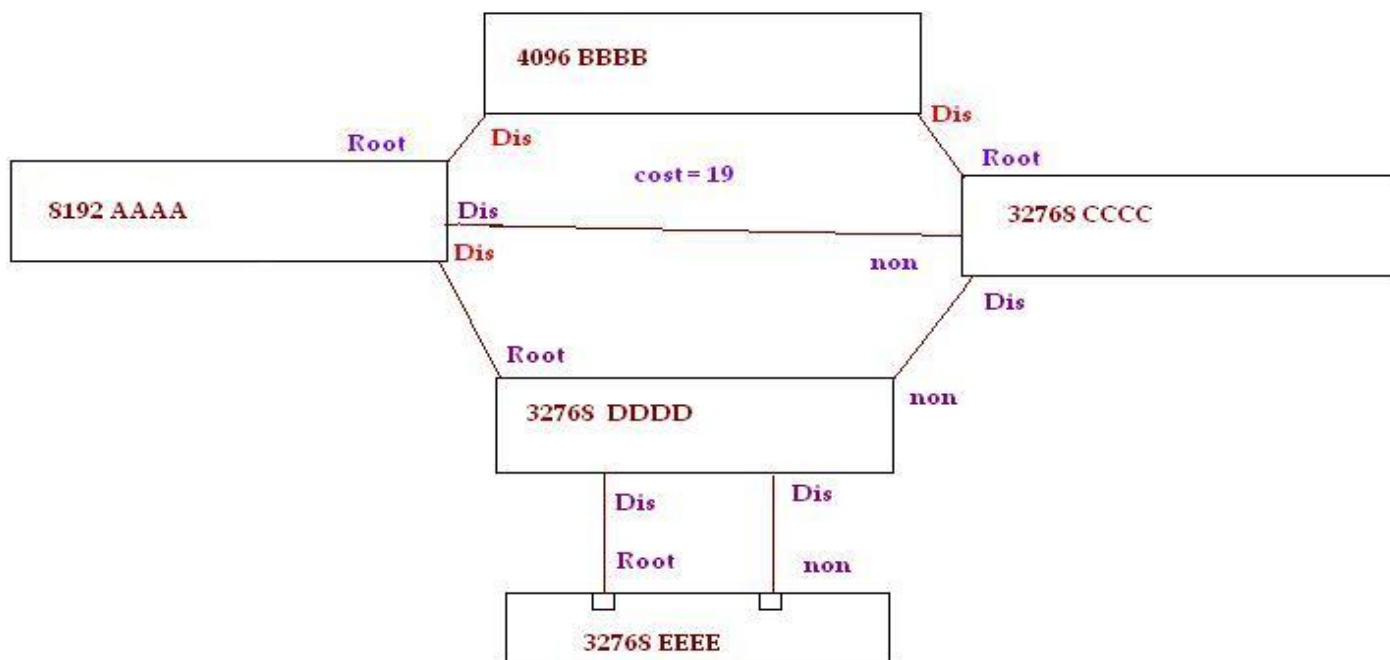
4-) lowest port ID

وضعیت STP

	BPDUs	DATA
	S & R	S & R
STP DISABLE	✗ ✗	✗ ✗
STP BLOCK	✗ ✓	✗ ✗
STP LISTEN	✓ ✓	✗ ✗
STP LEARN	✓ ✓	✗ ✓
STP FORWARD	✓ ✓	✓ ✓

15+15 = 30 ثانیه CSTP 20+ ثانیه مرجع = 50 ثانیه مدت زمانی که کابل به سویچ می زنیم

802.1D CSTP COMMON SPANNING TREE در سویچ های جدید کاهش پیدا کرده فوراد دیلی 15 ثانیه جمعا 35 ثانیه PVST



یک بار در جهت حرکت عقربه ساعت و یک بار عکس عقربه ساعت محاسبه شود . کاست تو روت . مشخص کنید روت پورت و دزینگت و نان دزینگت پورت را

[illegible]

RSTP → rapid spanning tree 802.1W

به تنهای در سیسکو سایورت نمی شود همراه با PVST سایورت می شود. → RPVST

تفاوت با -CSTP ← فازهای که لینک آپ بشود DISABLE.BLOCK. LOST بجای DISCARDING در pvst به هر فازهای می گویند.

pvst انواع لینک ها را دارد با اسمی . edge . POINT TO PONIT . shared

edge: زمانی یک پورت فست و مود اکسس باشد

زمانی که سویچ پورتش به یک سویچ دیگر وصل است لینک POINT TO PONIT می شود. (سویچ تو سویچ)

زمانی که سویچ به یک عدد دیواسی که سیکنال متودش هالف دوپلکس باشد shared می گوئیم. مثل هاب

برای بررسی وضعیت spanning tree

[Show spanning tree summary](#)

پیش فرض در سوییچ های جدید ران است. PVST mode

تازمانی بین دو سویچ کابلی وصل نباشد می شود spanning tree بگیریم . no spanning tree instance exists

بعد از وصل کردن کابل یک پورت را فوروارد و یک پورت را بلاک. **Priority** (اولویت) هر پورت پیش فرض 128 می باشد و قابل تغییر

پتانسیل این را دارد که جایگزین بلاک شود AlterNet block

در سویچ یک : یکی از پورت بلاک یکی روت

در سویچ دو : هر دو پورت DIS است .

پورت فست کردن « یعنی اگر یک کامپیوتر را به یک پورت سویچ زدیم زمان 35 ثانیه را صبر نکنیم که آپ شود و آنرا صفر می کنیم چون کامپیوتر پکت BPUD نمی فرستد برای پورت فست کردن .

Conf t> int f0/1 enter spanning tree mode access enter spanning tree port fast enter

بعد از اینتر زدن یک هشدار می دهد (اشکال) فقط می توانند پورتی که به هاست وصل باشد اگر به این پورت سویچ وصل باشد این دستور را ننیزد چون یک لحظه لوپ و کرش بوجود می آورد.

نمایش اینکه پورت چه وضعیتی دارد. Show run int f0/1

PVST 3 mode

***** spanning tree به ازای هر وی لن جدا ران می شود.*****

در PVST می شود گفت ترافیک یکسری وی لن ها از ی طرف و یکسری دیگر از طرف دیگر برود.

زمانی که دوتا روت بریج داشته باشیم تا زمانی که ما PVST را تیون نکردیم.

خودم می توانم عدد بدم **Priority**

4096 روت را از 32768 کم می کند اگر بخواهیم عدد دیگری کم کنیم.

باید از 0 تا 4096 عدد بزنیم برای هر بار . عدد بعدی می شود 8192

تبدیل روت بریج Root

Conf t enter spanning tree clan 1/10/30

وی لن روت بریج پورت های DIS هست

Conf t enter spanning tree clan 1/40/50 برای طرف دیگر تعریف می کنیم

لود بلانس لایه دو می باشد برای لود بلانس باید با لایه سه یکی باشد.

سه حالت مختلف دارد ROUT:

1)connected route و خودش روتر جدول روت را اتومات دارد. شبکه مستقیم به روتر وصل است

2)static route با لینک سریال

مثلا وقتی دو روتر از طرف مخابرات وصل اند با خط سریال

3)dynamic route

```
Int ser 0/1/0 ip address 10.1.1.1 255.255.255.0 enter encapsulation ppp enter clock rate
19200 enter
```

clock rate میزان ترانسفر دیتا روی این لینک بین ما و مخابرات تعیین می کنیم

No shut enter wr enter

در روتر بعدی

```
Conf t > int f0/0 enter ip address 192.168.2.10 255.255.255.0 enter no shut
```

```
Int ser 0/1/0 ip address 10.1.1.2
```

نوشتن استاتیک روت در روتر یک

```
Conf t enter ip address route 192.168.20.0 255.255.255.0 10.1.1.2 enter wr enter
```

همین کار برای روتر دو باید انجام شود.

نمایش روتین تیبل show ip route

```
Conf t > int f0/0 enter ip address 192.168.10.100 255.255.255.0 enter no shut enter wr
```

دادن ای پی به روتر

***** دیفالت روت *****

```
0.0.0.0 0.0.0.0 default rout همه دنیا بزرگترین روت
```

```
Ip route 0.0.0.0 0.0.0.0 10.1.2.2
```

**** هیچ وقت دوتا دیفالت روت را نمی شود روبه روی هم بنویسید. ****

```
Ip route 192.168.10.0 255.255.255.0 10.1.2.1 enter wr enter
```

اگر کلمه K9 در ادامه ورژن IOS بود یعنی IOS سیکور را ساپورت می کند.

بین دو تا روتر از دو تا لینک استفاده بکنیم « ترافیک حساس آگه داشتیم و بک آپ لازم داشتیم یا برای لود بلانس

طرف DTE دستور clock rite نمی خواهد.

Clock rite فقط در سمت DCE باید وارد شود . فاصله یک روتر تا روتر دیگر را هاب HOP می گویند و فاصله بینشان را next hop گویند .

دستور نمایش جدول روت show ip route

اگر روت استاتیک بدیم به روتر کنار آی پی کلمه S نوشته می شود.

اگر دو تا لینک وصل باشد در این حالت پکت ها هر کدام از یکی از لینک ها ارسال می شود و باعث دیلی یا ژیتزر می شود و ترافیک را خراب می کند و در یک حالت باید یک لینک را بک آپ اون یکی قرار بدهیم.

هر دو تا لینک را agree get کنیم (تبدیل به یک لینک) و راه دوم برای چک کردن

Conf t> do show run

اگر بخواهیم کامندی در محیط کانف تی نمایش دهیم مثل شو ران باید اول کامند DO بزنینم.

IP route 192.1268.10.0 255.255.255.0 10.1.2.2 10 distance

عدد 10 اولویت روتر است که بین 1 تا 255 می باشد و هر چقدر این عدد بالاتر باشد اولویت پائین تر است.

اینکار را باید در روتر دیگر هم باید انجام داد با الویت کمتر . در واقع روتر لینکی که الویت پائین تر است نگه می دارد برای بک آپ و از اونی که الویت بالا دارد استفاده می کند.

اگر استاتیک روت یک ستاره جلوش بود یعنی دیفالت روت S*

ضعف بزرگ استاتیک روت « منج یا مدیریت کردن آن : به ازای هر لینک یک روت می خواهد

راه حل: سیسکو :هرجا بیشتر از یک روتر داشتی از دیفالت روت استفاده کن

داینامیک روت (ارتباط بین روترها را خودش معرفی میکند)

پروتکل های معروف

RIP routing information protocol FDVI

RIP v2 routing information protocol version 2 LDVI

IGRP inerter gateway protocol FDVI

EIGRP Enhanced inerter ADV-BH L

IS-IS interment system L L S I

OSPF open short path first L L S I

EGP Exterior gateway protocol F P V E

BGP Border gateway protocol L P V E

سه دیدگاه

INTERIOR داخل یک آتناموس سیستم کار می کند

EXTERIOR بین دو سیستم آتناموس سیستم کار می کند

Rip V2 بر اساس مالتا کست کار می کند با آی پی 224.0.0.4

(2) کلاس فول هستند یا کلاس لس : پروتکل های کلاس فوا فقط با کلاس فول کار میکنند ولی کلاس هم با کلاس فول هم کلاس لس

(3) Link state یا Distance vector هستند

Balance hybrid و path vector بین دوتا آتناموس

Distance vector خواص

- پروتکل های هستند که معمولا بر اساس برادکست کار می کنند (غیر از Rip V2)

- معمولا آنتن تیکت ندارند (غیر از Rip V2)

- معمولا پهنای باند زیادی را اشغال می کنند.

- مستعد لوپ هستند

- کاست یا متیریک ضعیفی (تعداد هاب کانت ها مسیر . تا 15 روتر بعد از خودش را می بیند) RIP IGRP

- از الگوریتم ساده برای رسیدن به مقصد استفاده می کنند.

متودی که اگر دیتا از یک اینترفیس برود به هر جا Split horizon می تواند به همه جا برود بجز همان اینترفیس برگردد.

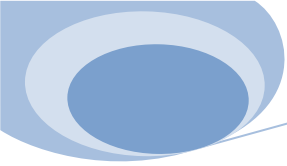
** در هر روتی که RIP به شما دسترسی داده با کاست 16 هرگز به آن مقصد دسترسی ندارد. **

EIGRP بهترین پروتکل دنیاست.

Distance Link state بر عکس خواص

Balance hybrid بهترین پروتکل Distance و Link state

Path vector بین دوتا آتناموس با BGP



```
Conf t>int f0/0 >ip address 192.168.10.1 255.255.255.0 > no shut > exit hostname >
```

```
Int ser 0/1/0 > ip address 10.1.1.1 255.255.255.0 >encapsulation ppp >clock rite 19200 > no shut >
```

```
Int ser 0/0/0 > ip address 10.1.2.1 255.255.255.0 >encapsulation ppp > no shut > wr
```

استفاده از RIP بجای استاتیک

ران کردن روتین پروتکل RIP v2 در روتر

```
Conf t>router rip > version 2 > معرفی کردن آی پی به روتر
```

کار یک روتین پروتکل داینامیک بصورت بیسک « نت ورک کانفیگ خودش را به همسایه هایش اعلام کند.

نمایش تمام اینترفیس ها و وضعیت آنها **Show ip int br**

```
Network 192.168.10.0 enter
```

```
Network 10.1.2.0 enter
```

```
Network 10.10.1.0 enter
```

برای همه روتر ها باید ست بشه

Distance برای RIP عدد 120 می باشد

** روت استاتیک با روت داینامیک کار نمی کند. ** برای کار کردن باید واسط بینشان باشد «حتی از هر دو داینامیک مختلف باشند» باید کامند redistribute استفاده کنیم.

```
Conf t>router rip > version 2 > redistribute static enter
```

Inter face loop back ایجاد اینترفیس مجازی لوک بک که هیچ وقت شات دان نمی شود برای تل نت . اس اس اچ و وی پی ان و تمرین و تست

ایجاد اینترفیس که نقش یک شبکه را بازی می کند در روتر»»

```
Conf t>int loop back 0 > ip address 192.168.30.1 >
```

در تمام روترها که RIP فعاله حالت Auto summery پیش فرض فعال است.

*****همیشه در روتین پروتکل RIP EIGRP باید دستور no Auto summery را زد*****

EIGRP : or Fast convergent

مزایای لینک استتیت و دیستنس وکتور را دارد و به آن بالانس هیبرید می گویند. و خالق آن سیسکو است و ضعف عمده آن فقط در روتر سیسکو کار می کند و در روترهای دیگر کار نمی کند و بر اساس مالنا کست کار می کند و انتتیکت کامل دارد و بر اساس MD5 می باشد و روتینگ تبیل را توسط هلو می فرستد و هلو را هر 5 ثانیه به 5 ثانیه ارسال می کند و 15 ثانیه دت تامیش است و از الگوریتم (Dual) Defused up date algorithm استفاده می کند.

آی پی مالنا کست 224.0.0.10

آپ دیت بین روترها را از طریق می فرستد (یعنی فقط تغییرات را ارسال می کند) و از سه تا تبیل استفاده می کند EIGRP یک روتین پروتکل میگویند.

1-Adjacency table همسایه هاشو شناسائی می کند

2-Topology table نسبت به توپولوژی شبکه آگاهی داشته باشد (اعلام لینک های کانکتد بهم دیگر) و مسیرهای بک 2-Topology table آپ را خودش نگه می دارد.

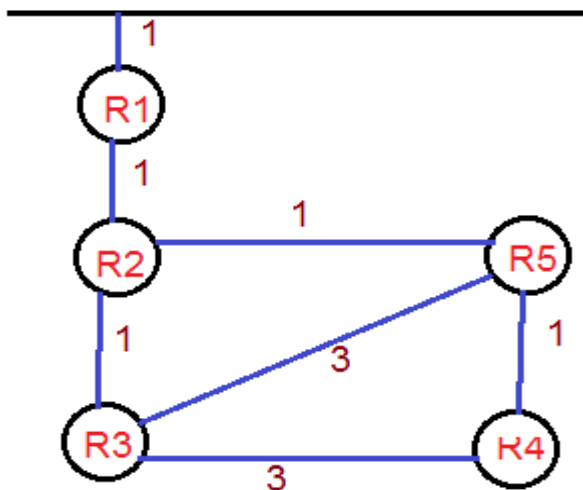
3-Routing table پیدا کردن بهترین و کوتاه ترین مسیر

اگر مسیر اصلی قطع بشود بدون از دست رفتن زمان (بیت 1 تا 2 ثانیه) مسیر جایگزین را از توپولوژی را در روتین تبیل می گذارد.

Advertise distance کاستی که همسایه اون روتر تا مقصد دارد می گویند.

FD=feasible فاصله ای که یک روتر خودش تا مقصد دارد می گویند.

در EIGRP به بهترین مسیر برای رسیدن به مقصد successor مسیر برنده می گویند. 10.1.1.0 /24



از طریق	Via	AD	FD	network
R2	2	3	10.1.1.0 /24	
R4	4	7		
R5	3	6		

AD مهم است اگر مسیر اصلی قطع شود برای مسیر جایگزین

مسیر بک آپ If $AD \leq FD$ of successor = Fs fusible successor

ساکسور است $AD R3 \geq AD$ چون

اگر AD باقی بیشتر FD خودش بشود دوباره الگوریتم دوال ران می شود برای ساکسور

EIGRP برای محاسبه متریک از چند پارامتر استفاده می کند.

می شود برای EIGRP ست کرد یا نه ولی 2 تاشون پیش فرض است k1 و k3 می شود دستی تغییر داد .

K 1 = bandwidth

K2 = load 0

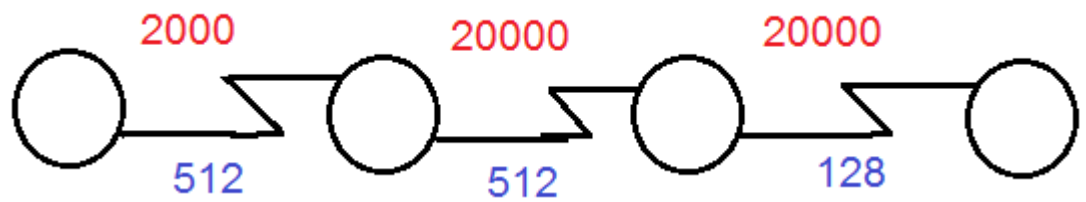
K3 = delay

K4 = MTU 0

K5 = Reliability 0

متریک EIGRP

$10^7 \rightarrow (256^*)$



EIGRP یک روتین پروتکل مستقل است و با همه روتین پروتکل ها کار می کند.

Conf t > bandwidth 256 enter

Conf t > Router EIGRP 1 enter network 10.1.34.0 enter or wall card mask

ولی بیت های بی ارزش تبدیل به بیت های با ارزش می شوند و برعکس در وال کارت مسک از لینک استت گرفته

اگر ندید تمام اینترفیس های که با ده شروع 0.0.0.255 enter wr

می شود روت کنند ولی اگر بدیم فقط این اینترفیس روت می کند.

نحوه محاسبه : ساب نت مسک کم می کنیم

255.255.255.192

-255.255.255.255

= 0.0.0.64

سامری چند شبکه در قالب یک ادورتایز مثل

172.30.7.0 /24 172.30.8.0 172.30.0.0

172.30.0.0 /24 255.255.248.0 در روتر

Conf t int ser 0/0 enter ip summery address EIGRP 1 172.30.0.0 255.255.248.0 enter

سامری برای اینکه روتین تیبل روت های دیگر را کوچک کنیم.

دستوری که در روتر چه پروتکلی ران است `show ip protocol`

AD EIGRP 90

AD OSPF 120

OSPF به همه مارک ها کار می کند و ضعف بزرگ آن ساخته شده برای TCP/ip و قدرتمند است و سه تا تیبل دارد.

همسایه هاشو پیدا می کند توسط هلو هر 10 ثانیه و دت تایم 40 ثانیه است هلو روی آی پی مالتا 1-neighbor table
کست 6 & 224.0.0.5

نمی تواند بک آپ انتخاب کند و بهترین مسیر را انتخاب و به روتین تیبل انتقال می دهد بعداز بین 2-topology table
رفتن مسیر دوباره الگورتیم را ران می کند برای پیدا کردن مسیر جایگزین

3-Routing table

در دو مود multi area و Single area اجرا می شود..

نهایت در یک اریا حداکثر 50 روتر باشد تا OSPF ران شود اگر اریا وجود نداشته باشد زمان ران شدن الگورتیم سونامی
بوجود می آید.

Designated Router (LAN or NBMA =none broadcast multiple access)

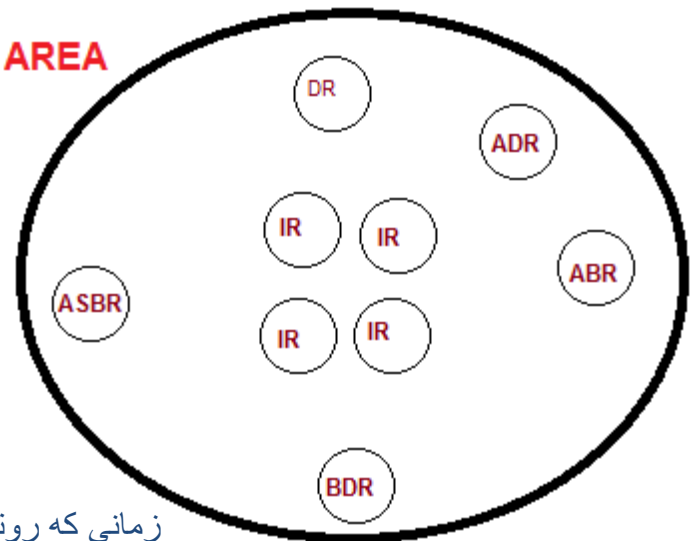
Backup designated router

Area border router

Autonomous system bound router

Internal Router

AREA



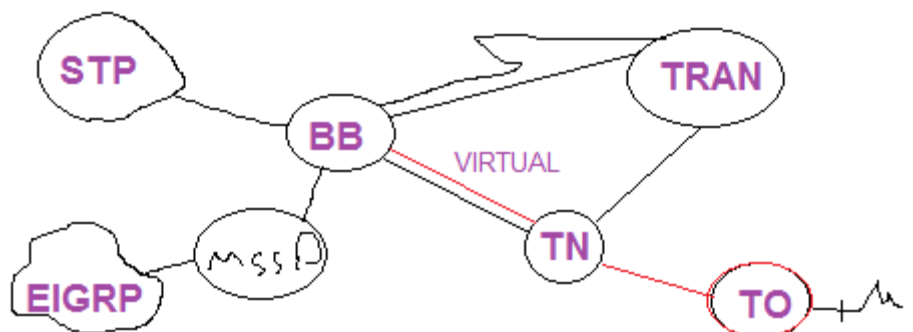
iR = روتر های داخلی یک اریا

زمانی که روتر به همسایه اش وصل است از این طریق متصل است . ABR

زمانی که ما از دنیای OSPF خارج می شویم مثل زمانی که EIGRP با یک نت ورک دیگر ASBR

در مالتی اریا یک اریا بک بون داریم بنام اریا صفر که تمام اریا ها از طریق اریا بک بون انجام می شود.

Transit area یک لینک یا دوتا لینک دارکتلی کانکند به بک بون داشته باشد می گویند.



Stub area فقط یک لینک مستقیم به بک بون دارند.

شبيه به استاب اريا هستند ولی از یک طرف به شبکه OSPF يا EIGRP يا RIPv1 متصل اند که به آنها NSSA می گویند.

یک سری از اريا هیچ لینکی مستقیمی به بک بون ندارند برای اینکه ارتباطش با بک بون برقرار شود باید یک پل زد از طریق اريا دیگر که به آن vacated link to tally stub area می گویند.



مراحل لود شدن OSPF بین دوتا روتر

فاز صفر فاز دان که هیچ اتفاقی نمی افتد . **فاز یک** init روترها برای هم هلو می فرستند همراه با هلو روتر id می فرستند و هم اريا id می فرستند و اگر انتتیکت بین شان باشد انتتیکت پسورد را می فرستند.

فاز دو محدود هلو مشخص می شود 2way

طی انتخابات DR و BDR انتخاب می شوند. برای مشخص شدن پارامترهای مثل priority که در این حالت در OSPF

یک است چون اولویت یکی است روتر آی دی (یک عدد مثل آی پی آدرس که باید دستی ست بکیم در روتر) چون پیش فرض ست نشده به سراغ فاکتور بعدی می رود که بزرگترین آی پی آدرس است (اینترفیسی که در OSPF معرفی شده) اگر اینترفیس لاک یک داشته باشیم آن اولویت دارد حتی اگر آی پی آن کم باشد

فاز سه Exchange بین روترهای پکتی به اسم DBD data base descriptor رد و بدل می شود. یا اسم دیگر این پکت DDP data base descriptor protocol

Agency table تشکیل می شود .

فاز 4 : لود : روتر ها پکت های ارسال می کند به اسم LSR و در جوابش پکت می خواهد به اسم LSU

LSR : link state request

LSU : link state up date

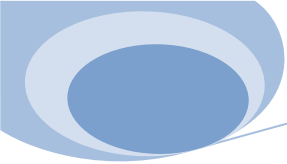
Full : فاز پنج : الگوریتم OSPF ران می شود Dijkstra و از روی توپولوژی تبیل به روتین تبیل می رسیم و تمام.

برای جلوگیری از سونامی Dijkstra در OSPF از چند تا پکت استفاده می کند . برای مثال ir تغییرات را به DR

DR به همه اعلام می کند.

این الگوریتم یکی از الگوریتم های پیمایش گراف است که مسئله کوتاه ترین مسیر از مبدأ واحد را برای گراف های وزن داری که یال با وزن منفی ندارند، حل می کند و در نهایت با ایجاد درخت کوتاه ترین مسیر، کوتاه ترین مسیر از مبدأ به همه رأس های گراف را به دست می دهد. همچنین می توان از این الگوریتم برای پیدا کردن کوتاه ترین مسیر از مبدأ تا رأس مقصد به این ترتیب بهره جست که در حین اجرای الگوریتم به محض پیدا شدن کوتاه ترین مسیر از مبدأ به مقصد، الگوریتم را متوقف کرد.

الگوریتم دایکسترا به نام کوتاه ترین مسیر تک منبع (single Source shortest path) نیز معروف است و مشابه الگوریتم پریم می باشد در صورتی که گراف یال با وزن منفی داشته باشد، این الگوریتم درست کار نمی کند و می بایست از الگوریتم های دیگر نظیر الگوریتم بلمن-فورد که پیچیدگی زمانی آنها بیشتر است استفاده کنیم



برای صحبت کردن روترها در OSPF از پکت های LSA = link state advertise استفاده می شود که شامل هفت تایپ هستند.

Type 1 برای صحبت کردن DR و BDR با ir

Type 2 برای صحبت کردن DR با بقیه

Type 3 برای صحبت کردن ABR با ABR همسایه

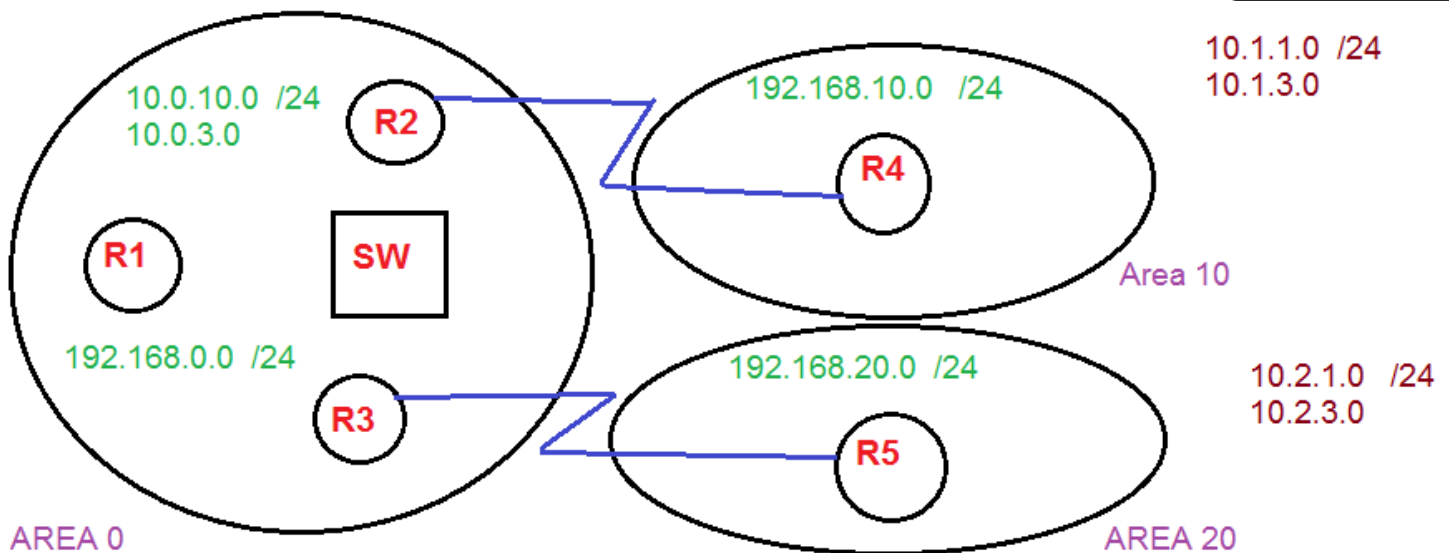
Type 4 لوکشین ABR را مشخص می کند

Type 5 ASBR با DR و BDR و همسایه (روت های اکسترنال) ASBR

Type 6 سائپورت نمی شود

Type 7 مربوط به ASBR ای است که درون یک NSSA قرار دارد.

پیاده سازی OSPF



R1 conf t int f0/0 ip address 192.168.0.1 255.255.255.0 enter no shut int loop 1 enter ip address 10.0.1.1 255.255.255.0 enter

R1 conf t Router ospf process ID enter

process ID کامندی که در روتر می زنیم

do show ip int br نمایش نت ورک های

برای اینکه بتوانیم انتخابات را خودمان برگزار کنیم باید روتر ای دی بدهیم هر روتری که بالاتر باشد DR

Router – id 1.1.1.1 enter

Network 192.168.0.0 0.0.0.255 area 0 enter wr

AD در OSPF 110 می باشد *

چون روتر یک را اول روشن کردیم DR میباشد.

دستور نمایش همسایه ها با آی دی شان show ip ospf neighbor

اگر بخواهیم یک روتر دیگر DR بشود باید ospf را ری استارت کنیم.

R1 clear ip ospf process enter yes enter

R1 show ip ospf brooder router دستور نمایش ABR ها

Access List : ACL

نحوه دسترسی یوزرها به شبکه یا شبکه به شبکه ها

فایروال یک آپرسین لایه هفت است ولی فیلترینگ در بر اساس سورس آی پی آدرس

ACL → standard * extended

مک آدرس لایه دو - آی پی آدرس لایه سه - پورت لایه چهار

Src – DST mac * SRC-DST-ip * SRC-DST-port

استاندارد : کلاینتی که قراره به روتر تا نت نکند کل ترافیک کلاینت به بیرون قطع می شود.

اکستندد : می شود تعریف کرد چه چیزی قطع یا بسته باشد مثلا پورت 23 که نتواند تل نت بزند.

اکسس لیست ها شماره دارد که در استاندارد از 1 تا 99 و اکسس اکستندد از 100 تا 199 می باشد و در کل دو وظیفه دارد . یا به یک ترافیک اجازه بدهد Permit یا جلوگیری کند از یک ترافیک Deny

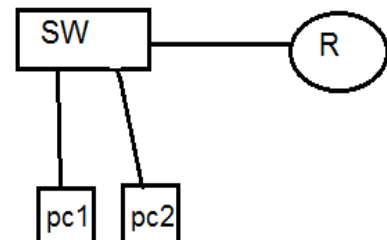
نوشتن اکسس لیست که پی سی یک نتواند تل نت کند .

REMARK توضیح برای اکسس لیست

IN ROUTER 192.168.10.10 CONF > ACCESS LIST 1 REMARK "FOR PC 1 " ENTER

ACCESS LIST DENY HOST 192.168.10.10 ENTER

192.168.10.10 اگر هاست نزنم



• نوشتن اکسس لیست چهارتا شرط دارد به شرط نوشتن اکسس کافی نیست *

1 - چه نوع اکسس لیستی بنویسم استاندارد یا اکستندد

2 - روی کدام روتر بنویسم یا سویچ

3 - روی کدام اینترفیس بنویسیم

4 - در چه جهتی بنویسیم ورودی یا خروجی

یک اکسس لیست را روی دو اینترفیس نمی نویسیم ****

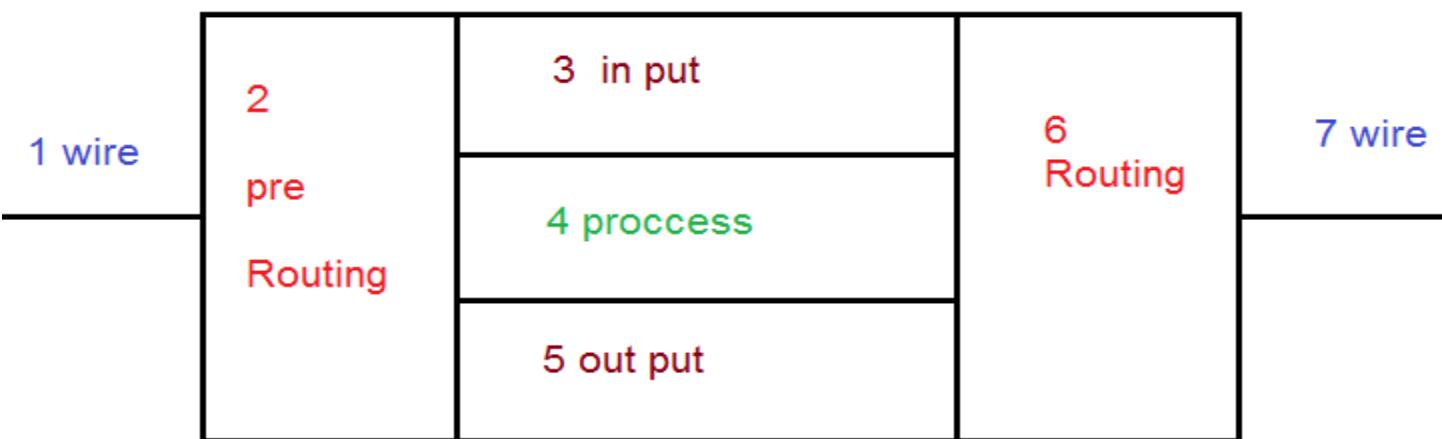
Conf t > int f0/0 enter ip access –group 1 in enter

الان برای پی سی 2 هم بسته است باید پی سی 1 را باز کرد همه پورت های بسته شد باید کارهای که می خواهیم را باز کنیم

آخرین خط از اکسس لیست که در روتر یا سویچ اعمال می شود Deny است باید این حالت رو تغییر داد « دو راه »
یا کلا شرط را Deny any یا Permit any کرد. تغییر شرط

دو تا اکسس لیست را با دو شماره مختلف به یک اینترفیس اختصاص داد. *****

Permit any حتما باید آخرین خط باشد.



طریقه نوشتن اکسس لیست: بجای شماره می توانیم از نام استفاده کنیم

Conf t> ip access-list extended deny-policy enter deny tcp host 192.168.10.10 host 192.168.20.10 eq 80 enter

Eq = برابر است با

Conf t > int f0/0 ip access-group deny-policy in enter

Conf t > access list extended deny-policy enter permit ip any any enter

برای بستن تل نت روتر یک که پی سی 2 نتواند تل نت کند . باید همان فیلترینگ قبلی را ادیت کنیم چون any و any دارد نمی شود.

Conf t

No ip access list extended deny-policy enter

Ip access list extended deny-policy enter

Deny tcp host 192.168.10.11 host 192.168.10.100 eg 23 enter permit ip any any enter

قسمت سوم : هیچی به روتر 3 تل نت نکند بجز w2

تل نت به لاین وی تی وای زده می شود پس بهتر است لاین وی تی وای را ببندیم و اکسس لیست استاندارد می نویسیم.

Conf>ip access list standard telnet enter permit host 192.168.30.10 enter line vty 04 enter access –class telnet in enter

DHCP

در روتر و سویچ لایه 3 می شود پیاده سازی کرد پیاده سازی در سیسکو استیبل تر است. چهار مرحله ای پی گرفتن

Discover

ای پی خودش - کلاینت Src ip 0.0.0.0

Src mac aaaa

Dst ip 0.0.0.0

Dst mac ffff

Offer

Src ip 192.168.10.100

Src mac bbbb

Dst ip 0.0.0.0

Dst mac aaaa

Request

Src ip 0.0.0.0

Src mac aaaa

Dst ip 192.168.10.100

Dst mac bbbb

ACK

192.168.10.100**Bbbb****192.168.10.10****Aaaa**

DHCP در پورت 67 و 68 یو دی پی کار میکند

کانفیگ DHCP

روی سویچی که وی لن مان را ساخته ایم

Conf> ip DHCP pool vli0 enter network 192.168.10.0 255.255.255.0

Pool تعریف نام ک رنج آی پی را مشخص کنیم

به ازای هر وی لن جدا آی پی بدهید

Default-router 192.168.10.100 enter

می توانید آی پی دیفالت گت وی بدید

DNS-server 192.168.10.99 enter آی پی دی ان سرور

Ip DHCP excluded-address 192.168.10.1 192.168.10.10 enter wr

NAT

ترجمه آدرس ها پراویت به پابلیک و یا بر عکس – فقط روی روتر پیاده سازی می شود. دستور سورس پورت و دسنیشن پورت را نشان می دهد net stat

سورس پورت با آی پی پراویت فرستاده می شود به روتر و روتر توسط نت سورس و آی پی را از پکت بر می دارد و آی پی پابلیک خودش را می گذارد روش و می فذستد و جواب که برگشت هدر آی پی پابلیک را برداشته و هدر آی پی پراویت را می گذارد.

نت یک جدول حاوی آدرس پابلیک و آی پی پراویت و سورس پورت و دسنیشن پورت ها موجود است ****

در دو حالت نت پیاده سازی می شود.

Static Nat اگر بخواهیم سرورها را پشت نت بزاریم

dynamic Nat اگر بخواهیم به یوزرها دسترسی اینترنتی بدهیم

Static Nat به ازای هر سرور یک آی پی ولید مپ می کنیم روی آی پی پراویت

اولین کار برای نوشتن نت : روی روتر اینترفیس داخلی و بیرونی مشخص می کنیم

```
CONF T> INT F0/0 ENTER IP NAT INSIDE ENTER INT F0/1/0 IP NAT OUT SIDE ENTER
```

```
CONF T > IP NAT INSIDE SOURCE STATIC 192.168.10.10 217.218.196.4 ENTER
```

dynamic Nat

```
CONF T> INT F0/0 ENTER IP NAT INSIDE ENTER IN ser 0/1/0 ENTER IP NAT ENETR ip nat + quit
```

```
CONF T> IP NAT POOL INTERCT NETWORK 255.255.255.0 ENTER
```

برای اینکه دسترسی داشته باشد به پول در نت داینامیک احتیاج به مجوز دارن : مجوز نوشتن اکسس لیست

```
Access –list permit 192.168.20.0 0.0.0.255 enter ip nat inside source list 1 pool internet over load enter
```

Sh ip nat translations دستور تیبیل نت

• اگر در نت همزمان درخواست پیش بیاد – نت نمی تواند به هر دو دسترسی بدهد.

```
Clint2 sp 2025 p1.94.1.3
```

```
Clint 1 sp 2025 p1.91.1.0
```

در این حالت path استفاده می کنیم که sp path کلاینت دو را عوض می کند.

Van : PPP VPN farm rely ون شامل سه پروتکل

اگر از لن خارج شویم به آن ون می گویند

PPP مثل دیال آپ : point to point protocol

لایه دوی که از یک ساب لایر LCP link control استفاده میکند که چهار کار را برای PPP انجام میدهد و هر HDLC است که مختص سیسکو است.

Authentication

مزایای : بین دوتا روتر اتنتیکت برقرار کند. 4 مورد

انواع اتنتیکت : pap. chap . ms chap. ms chap v2

فشرده سازی Compression

Call back اگر ماژول دیال آب در روتر باشد و از راه دور دیال کنیم برای اینکه هزینه کم شود تلفن قطع شده و تلفن قطع می کند نوشتن شماره شما را می گیرد و امنیت بیشتر می شود حتما باید روتر شماره شما را داشته باشد

Multi link یکی کردن پهنای باند چند خط تلفن برای استفاده همزمان مثلا در isp ها

در لایه دو و ن مک آدرس نداریم فقط در لن هست.

VPN

ارتباط دو یا چند شبکه بصورت ارزانتر در بستر اینترنت

به شرطی می تواند سکيور باشد از پروتکل های زیر استفاده کنیم

PPTP-L2Tp-Slip

L2Tp می تواند سکيور باشد به شرطی که از IPSEC در کنارش باشد رمزنگاری با کلید shared key

در سه مرحله کارش انجام میشود :نگوشین – اینترکشین – انتنتیکت (دفعی هلمن) هر دو طرف باید کلید را داشته باشند

(دفعی هلمن) public key- privet key

هش می شود « با سه متدود « DES – 3DES – AES

Frame Relay

NBMA: none broadcast multiple شبکه های (از نوادگان ATM * MPLS * x.25)

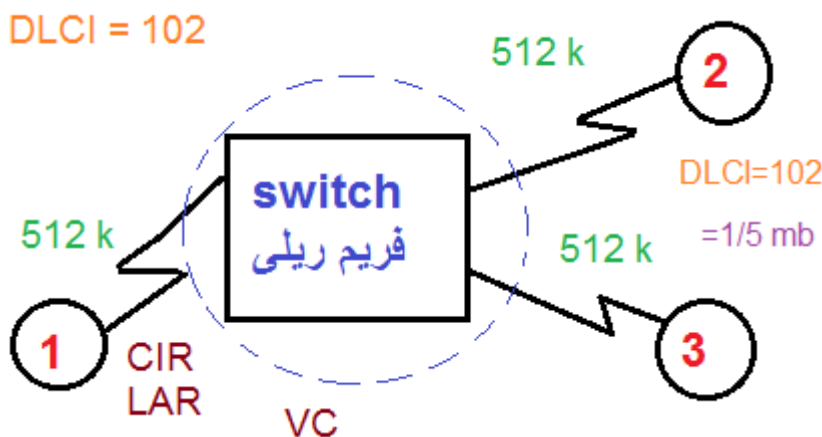
فریم ریلی یک استاکچر شر برای نقاط مختلف – یک تکنولوژی پکت سوچینگ

مثال پهنای باندی M/B 1.5 که بین سه شعبه شر شده.

اگر دوتا شعبه استفاده نکنند شعبه یک

می تواند کل 1.5 مگ را استفاده کند.

پهنای باند = commuted inter rite



Local access rite لینک فیزیکی تا پرووایدور

بجای مک آدرس از لایه دو DLCI استفاده میکنیم یک عدد که یونیک نیست که گیت ورودی و خروجی ما را در یک نقطه مشخص می کند شبکه فریم ریلی در چند ساختار می تواند پیاده سازی شوند.

اگر دو بخواهد با سه صحبت کند باید از طریق یک عبور کند Hub and spook

Parcel mesh

در دو مدل پیاده سازی می شود بین چند نقطه malty point یا بین دو نقطه point to point

تشکیل یک لن با سه شبکه در شهرهای مختلف با یک رنج آی پی : malty point

IP v6

در آی پی ورژن 6 مک آدرس برادکست نداریم.

از هشت پارت هگزا دسیمال تشکیل می شود (ترکیبی از اعداد و حروف)

شامل سه حالت : link local-site local-global

link local – به هر اینترفیسی بدیم یک آی پی تشکیل می شود که ارتباط در لن بر اساس لینک لوکال است

site local- دو کامپیوتر بخواهند از لن خارج بشوند از آی پی اصلی در لن

global-در لن لینک لوکال FE 80 و 2001 شروع می شود.

آی پی که خودمان به اینترفیس دادیم با FEC شروع می شود ولی با هرچیز دیگر می تواند شروع بشود.

از دو قسمت شصت و چهار بیت تشکیل شده است.

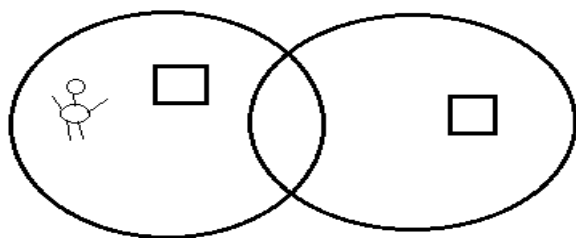
3/bit	13/bit	8/bit	24/bit	16/bit	Mac 64/bit
Format prefix	TLA : top level aggregator	Reserve	NLA: next level aggregator	SLA : site level aggregator	
	NAP 2 ¹³		Autonomous system	ISP	
	مالک اینترنت				

Ipsec پیش فرض در ای پی ورژن 6 موجود است.

Wire less

لایه دو – با استاندارد 802.11 – در لن . ون . پن و من قابل پیاده سازی است.

اکسس پوینت یک دیوایس لایه یکی که فیچرهای از لایه دو را پشتیبانی می کند و یک محیط shred base است و از متدود CSMA/CA (جلوگیری از برخورد) استفاده می کند .



SSID « باید یک نام داشته باشد و مشخص کننده

همپوشانی 10 تا 15 درصد %

سه نوع اکسس پوینت : Root – Bridge – Repeater

Root – اکسس روت : سرویس دهنده مرکزی که اکسس های دیگر از این سرویس می گیرند.

Bridge – اکسس بریج : 10 تا 15 % همپوشانی داشته باشند اگر دوتا باشند در دو کانال مختلف باید باشند.

Repeater – اکسس ریپیتر : همپوشانی 50% باشد

یک کلاینت بتواند جابه جا شود در شبکه : کلاینت رومینگ « دو نوع « لایه دو و لایه سه

لایه دو « شبکه لایه دو باشد « همه کلاینت ها در یک وی لن . پسورد و SSID همه باید یکی باشد و یک رنج ای پی داشته باشند.

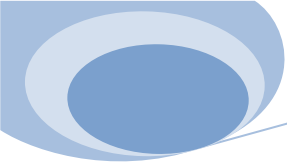
لایه سه « SSID و پسورد همه باید یکی باشد.

فرکانس وایرلس 2.4 GH 5.8 GH نیازی به مجوز ندارند فرکانس MH900 مجوز می خواهد

دوتا اکسس پوینت کنار هم : اگر یکی از کار بیافتد : چون فرکانس های

همه کلین کانال 23 → 802.11A

3 تا کلین کانال 11 → 802.11 G B



1 و 6 و 11 قطع نمی کنند بخاطر فاصله ای که دارند.

غیر قابل نفوذترین وایرلس ها 802.11x WEP WEP2

کانفیگ فریم ریلی « DLCA روی سویچ تعرف می شود.

کلیک راست ← پورت 2 ← 302/202 پورت 1 ← 103/102

Conft> int ser 0/0 enter encapsulation farm rely enter ip add 192.168.10.1 255.255.255.0 enter
no shut

Farm rely map ip 192.168.10.0 102 broadcast enter

غیر فعال کردن اسلپت هوریزون در روتر یک در EIGRP

Int ser 0/0 enter no ip spilt-horizon EIGRP enter

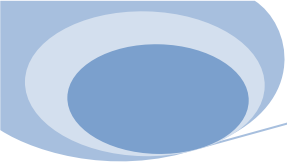
کانفیگ آی پی ورژن 6

Conft> int f 0/0 enter ipv6 address ifc0:1111:2222:0:1 /32 enter

در آی پی ورژن 6 باید روت داینامیک نوشت مثل مالتا کست را باید در آی پی ورژن 6 فعل کرد و پیش فرض نیست

Conft>ipv6 unicast-routing enter

Ipv6 router rip 1 enter exit



CCNA

(Cisco certified network associate)