Advance your IT career with hands-on learning

CCNA 200-301

WENDELL ODOM,
CCIE® NO. 1624 EMERITUS

ciscopress.com

سپاس خدایی را که به من این توفیق را عطا فرمود تا بتوانم قدمی در راه علم و دانش بردارم و به گردآوری اطلاعات مربوط به این دوره بپردازم .

بدینوسیله از زحمات و تلاش بی دریغ استاد محترم جناب آقای مهندس منتخبی و دوستانم که در تهیه این مجموعه با این جانب همکاری داشته اند ، تشکر و مراتب سپاس قلبی خود را اعلام نموده و موفقیت ایشان را ازخداوند متعال خواهانم.

مهدی خانلری _ تابستان 1402

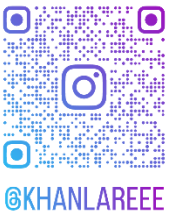
دوستان عزیز در این جزوه تمام تلاش خود را کرده ام تا بتوانم موضوعات این دوره را به صورت ساده برای شما عزیزان بیان کنم. اگر درباره قسمت های مختلف این جزوه سوال دارید، می توانید با من در تماس باشید.

Email : khanlareee@gmail.com

Telegram : https://t.me/khanlareee

LinkedIn : https://www.linkedin.com/in/mahdi-khanlari-a73037263

Instagram: @khanlareee



About CISCO Company

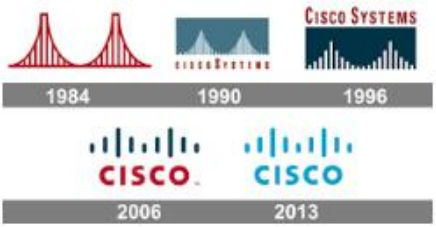
تاریخچه:

(لن بزاک و سندی لرنر) دارای مدرک لیسانس از دانشگاه ایالتی کالیفرنیا، فوق لیسانس اقتصاد سنجی از دانشگاه کلرمونت و فوق لیسانس علوم کامپیوتر از دانشگاه استنفورد، زوجی که در بخش کامپیوتر دانشگاه استنفورد کار می کردند، شرکت Cisco را در سال1984 تأسیس کردند. بزاک نرم افزار روترهای چند پروتکل را که توسط ویلیام یاگر (یک کارمند دیگر که کار خود را سال ها قبل از بزاک شروع کرده بود) نوشته شده بود، تکمیل کرد.

باوجوداینکه Cisco اولین شرکتی نبود که Router طراحی و تولید می کرد، اولین شرکتی بود که یک Router چند پروتکل موفق تولید می کرد که اجازه ارتباط بین پروتکل های مختلف شبکه را می دهد. از زمانی که پروتکل اینترنت(IP) به یک استاندارد تبدیل شد، اهمیت Router های چند پروتکل کاهش یافت. امروزه بزرگترین روترهایCisco طراحی شده اند تا بسته هایIP و فریم های MPLS را هدایت کنند. درسال1990، شرکت سیسکو به سهامی عام تبدیل شد و سهام آن در بازار بورس عرضه شد. بزاک و لرنر با 170 میلیون دلار از شرکت خارج شدند و بعد از مدتی جدا شدند. زمان انفجار اینترنت در1999، Cisco شرکت Cerent واقع در کالیفرنیا را با قیمت۷میلیارد دلار خریداری کرد. این شرکت گرانترین خرید Cisco در آن زمان بود. تنها خریدگران تر، مربوط به ساینتیفیک آتالنتا است.

در اواخر مارس2000، در اوج رشد دات کام، Cisco با ارزش مالی بالغ بر500 میلیارد دلار ارزشمندترین شرکت دنیا بود. در سال2007 نیز با ارزشی بالغ بر165 میلیارد دلار همچنان یکی از ارزشمندترین شرکتها بود .باخرید شرکت های دیگر، توسعه داخلی و همکاری با دیگر شرکت ها، Cisco به بازار بسیاری از قطعات دیگر شبکه (غیرازRouter)راه پیدا کرده است، مانند Ethernet Switching، دسترسی از راه دور،Routerهای شعبه ای، شبکه خودپردازهای بانک ها،امنیت ،fire wall ، تلفن اینترنتی و غیره. در2003، Cisco شرکت محبوب LinkSys تولیدکننده سخت افزار شبکه کامپیوتر را خریداری کرد و آن را در صدر تولید کننده های قطعات مربوط به کاربران عادی گذاشت.

ریشه نام سیسکو:



اسم «سیسکو» مخفف سانفرانسیسکو است. با توجه به اظهارات جان مرگریج، کارمند 34 ساله و مدیر پیشین شرکت، مؤسسان شرکت زمانی که داشتند به سمت ساکرامنتو رانندگی می کردند تا شرکت را به ثبت برسانند، با تصویر پل گلدن گیت در نور آفتاب مواجه می شوند و اسم و نماد شرکت را بر این اساس انتخاب می کنند. نماد شرکت منعکس کننده اصلیت سانفرانسیسکویی آن است که نشان دهنده پل گلدن گیت است که به سبک خاصی طراحی شده است. در اکتبر2006، سیسکو نماد جدید خود را که از نماد قبلی ساده تر بود، به نمایش گذاشت.

Switch And Switching

Implementing Ethernet LANs

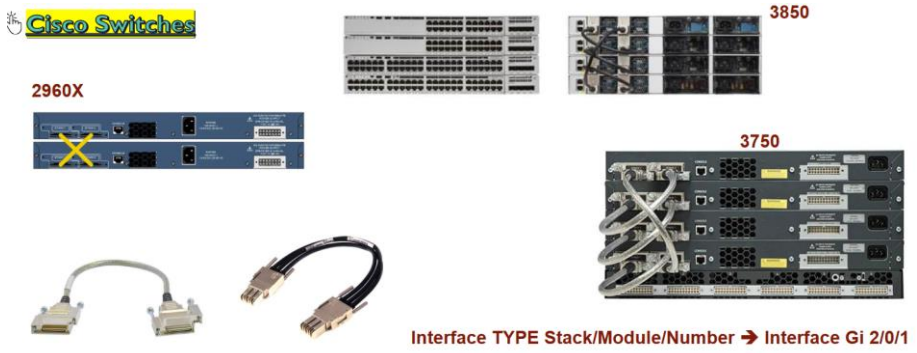
سوئیچ یکی از سخت افزارهای شبکه است که در عین شباهت به هاب (hub)، بسیار هوشمندتر از آن است. بر اساس مدل OSI سوئیچ ها در لایه 2 یا همان لایه Data Link کار می کنند و وظیفه این سخت افزارها، انتقال بسته های دیتا از یک دستگاه به جای دیگر از طریق شبکه و بر اساس آدرس سخت افزاری (Mac addresses) می باشد.

سوئیچ همانند بریج است با این تفاوت که تعداد پورت های بیشتری دارد. بریج ها دارای 2 الی 16پورت هستند اما سوئیچ ها شاید تا صدها پورت هم دارا باشند. (درسری های مختلف) ،تفاوت دیگر اینکه بریج ها اطاعات را ازطریق نرم افزارسوئیچ(هدایت)می کنند درحالی که سوئیچ این کار را ازطریق سخت افزاری به نامASIC انجام می دهد.ASIC ها نوعی ازپردازنده هستند که برای انجام اعمال خاص ومحدودی ساخته شده اند. برای همین هم قیمت آنها از انواع تخصصی تر، مثل پردازنده اصلی کامپیوتر می باشد.

Interface TYPE Module/Number ➔ Interface GigabitEthernet 0/1

STACK

با استفاده از Stack Switching میتوانیم در سوییچ هایی که قابلیت STACK دارند با متصل کردن چند عدد سوییچ که از یک برند، مدل و سری یکسان بهره می برند امکان Redundancy و Load Balancing را در آنها بوجود بیاوریم. طول کابل Stack نهایتا 5 متر است. هنگامی که تعدادی سوییچ را با کابل Stack به یکدیگر متصل می کنیم یکی از سوییچ ها بعنوان Stack Master شناخته می شود و سایر سوییچ های موجود در آن Stack بعنوان سوییچ های Slave شناخته می شوند.

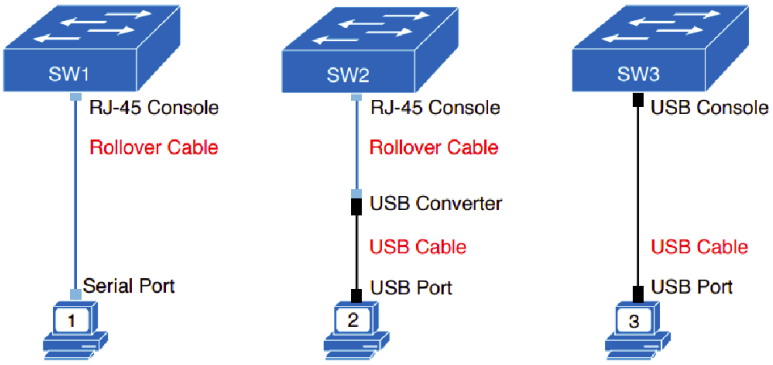


Device Access

Console Cable - DB-9 Female (RS232)

پشت دستگاه های سیسکو پورت کنسول قرار دارد. زمانی از این پورت استفاده می شود که برای اولین بار می خواهیم پیکربندی سوییچ یا روتر را انجام دهیم.

برای اینکه بتوانیم به کنسول دستگاه متصل شویم از این کابل بعنوان کابل کنسول یا Roll Over Cable معروف است استفاده می کنیم. یک سر این کابل سوکت RJ45 است که به پورت کنسول روتر یا سوییچ وصل می شود و سمت دیگر به پورت سریال COM کامپیوتر متصل میشود، که قرار است روتر یا سوییچ را پیکربندی کند. به این نوع ارتباط Local Access می گویند و در لحظه فقط یک نفر می تواند به دستگاه متصل شود و باید نزدیک دستگاه باشد بدلیل اینکه در ابتدا روتر یا سوییچ هیچگونه تنظیمات شبکه ای ندارد و به همین دلیل نمی تواند برای متصل شدن به آن از SSH یا Telnet ویا HTTPS استفاده کرد.

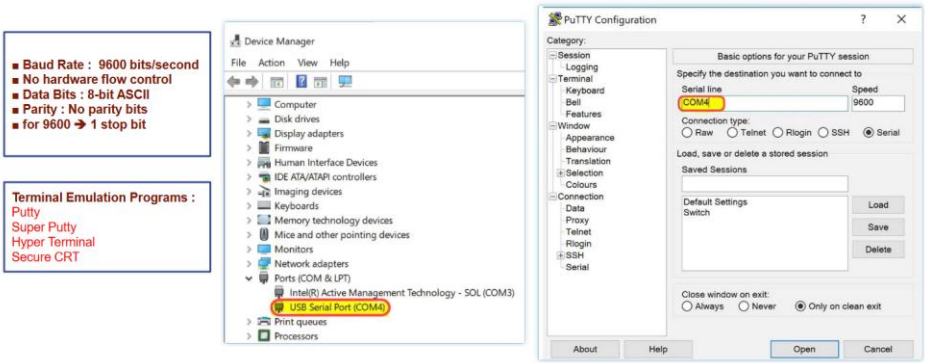


Software And Hardware

استفاده از PUTTY جهت پیکربندی و کانفیگ روتر یا سوییچ

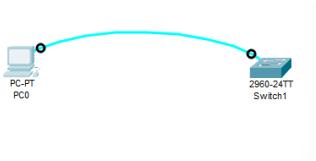
برای اینکه متوجه شویم سیستم ما کدام پورت COM را شناسایی کرده، وارد Device Manager می شویم.

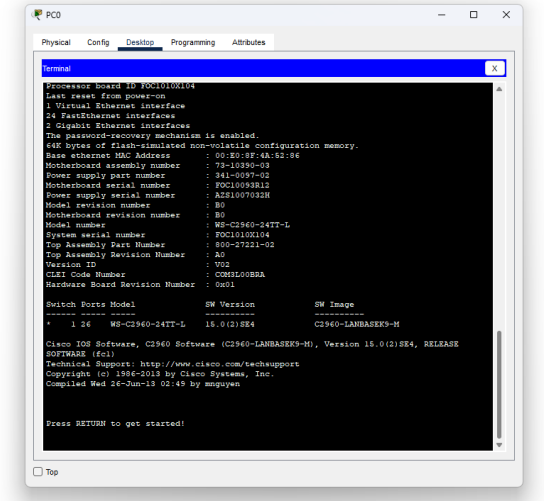
تنظیمات پیشفرض را تغییر نمی دهیم فقط: Serial line, Connection Type



اتصال کابل کنسول به PC در Cisco Packet Tracer

روی PC کلیک کرده، قسمت Desktop آیتم Terminal که نقش PUTTY را در شبیه ساز دارد، تنظیمات را تغییر نمی دهیم و فقط OK می کنیم سپس صفحه مشکلی رنگ سیستم عامل یا همان تنظیمات دستگاه برای ما نمایان می گردد.





دستورات HELP

برای گرفتن دستورات help از علامت سوال ؟ استفاده می کنیم، برای نمایش بیشتر Enter زده و دستورات خط به خط اضافه می شوند وبا کلید Space دستورات بصورت پاراگراف جدید نمایان می گردد و برای انتخاب زیر مجموعه ها می توان یک کلمه را بصورت روبرو Router>show ip ? استفاده کرد.

Using the Command-Line Interface

سطوح دسترسی به سوییچ : User Mode/Enable Mode/Global Mode

```
Switch>                    ← User Mode / User EXEC Mode        Limited Monitoring
switch> enable                                                 Limited Trouble shooting
Switch# disable            ← Enable Mode / Privilege Mode / Privilege EXEC Mode    Monitoring
Switch>                                                                           Trouble shooting
                                                                                  Limited Manage
```

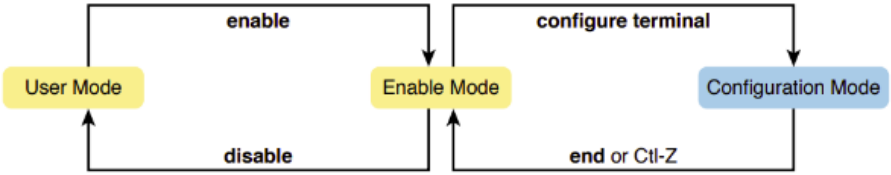
```
Switch>
switch> enable
Switch# Configure Terminal
Switch(config)# exit          ← Global Mode
Switch#
```

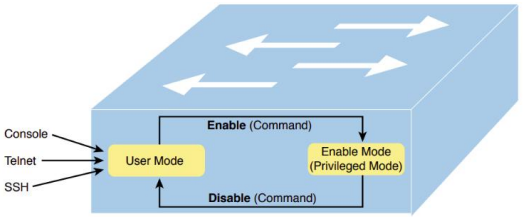
نکته: برای پریدن به ابتدا کلمه از کلید های ترکیبی Ctrl+A استفاده می کنیم.

نکته: برای پریدن به انتهای کلمه از کلید های ترکیبی Ctrl+E استفاده می کنیم

نکته: از Global Mode می توان با کلید های ترکیبی Ctrl+C یا Ctrl+Z می توان به User Mode به Enable Mode برگشت.

نکته: در Enable Mode می توان ابتدای هر کلمه را نوشت و برای تکمیل دستور از کلید TAB استفاده کرد.





User [1] ➔ Enable [2] ➔ Global [3] ➔ interface [4]

```
Switch#show history
Swtich#terminal history size <>
```

نمایش وضعیت interface های دستگاه

Switch>show interface status

```
SW1# show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          a-full  a-100 10/100BaseTX
Fa0/2                        connected    1          a-full  a-100 10/100BaseTX
Fa0/3                        connected    1          a-full  a-100 10/100BaseTX
Fa0/4                        connected    1          a-full  a-100 10/100BaseTX
Fa0/5                        notconnect   1            auto   auto 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        notconnect   1            auto   auto 10/100BaseTX
Fa0/9                        notconnect   1            auto   auto 10/100BaseTX
Fa0/10                       notconnect   1            auto   auto 10/100BaseTX
Fa0/11                       notconnect   1            auto   auto 10/100BaseTX
```

Translating Mode

وقتی اسمی را دستور بدهیم سیستم فکر میکند اسمی تعریف کردیم و برای آن روی DNS آی پی تعریف شده و آن را روی DNS سروری که نمی داند کجاست جست و جو می کند برای همین آن را broadcast می کند. برای پایان دادن به Translating Mode از کلیدی های ترکیبی: Ctrl+shift+6 استفاده می کنیم.

غیرفعال کردن Translating Mode

Switch(config)#no ip domain-lookup

نکته: انتخاب اسم ها همیشه با حرف بزرگ نوشته می شوند که مشخص شود دستور یا Command نیست.

نوشتن توضیحات برای interface

Switch(config)#interface fastethernet 0/1

Sitch(config-if)#description ccna-class

نکته: نوشتنdescription برای اینکه بدانیم کدام پورت به کدام Device متصل شده.

نام گذاری دستگاه:

Switch(config)#hostname SWH-1

Configuration Basic Switch management

انتخاب رمز جهت ورود به Enable Mode

```
Switch(config)#enable password 123456
```

انتخاب رمز برای اتصال کابل کنسول و ورود به User Mode

```
Swh-1(config)#line console 0
Swh-1(config-line)#password 999
Swh-1(config-line)#login
```

فعال کردن دستور رمز

انتخاب نام کاربری و رمز عبور:

```
Swh-1(config)#username farshad password farshad
```

حذف نام کاربری:

```
Swh-1(config)#no username farshad
```

نمایش نام های کاربری:

```
Swh-1(config)#show users
```

فعال کردن دستور رمز های ایجاد شده روی نام کاربری (local password checking)

```
Swh-1(config)#line console 0
Swh-1(config)#login local
```

تعیین زمان بیکاری که منجر به بستن Session می شود:

```
Swh-1#conf t
Swh-1(config)#line console 0
Swh-1(config-line)#exec-timeout 1
```

زمان انتخاب شده یک دقیقه است.

Local Device Access Configuration:

Method 1:

```
switch#configure terminal
switch(config)#line console <>
switch(config-line)#password <>
switch(config-line)#login
switch(config-line)#exit
switch(config)#
```

Method 2:

```
switch#configure terminal
switch(config)#username <> password <>
switch(config)#line console <>
switch(config-line)#login local
switch(config-line)#exit
switch(config)#
```

```
switch#show history
switch(config)#line console <>
swtich (config-line)# terminal history size <>
swtich (config-line)# logging synchronous
swtich (config-line)# exec-timeout <>
```

Command	Type	Algorithm
username *name* [algorithm-type md5] secret *password*	5	MD5
username *name* algorithm-type sha256 secret *password*	8	SHA-256
username *name* algorithm-type scrypt secret *password*	9	SHA-256

اگر تجهیزات شبکه بیشتر شود نمی توان روی هر سوییچ User/Pass بصورت دستی تعریف کنیم بلکه یک Server استفاده می کنیم و روی آن یک نرم افزار مثل cisco ice که از پروتکل Tac Acs استفاده می کند یا Tac Acs+ (Terminal Access Configuration) پس از قرار دادن سرور یک نرم افزار روی آن پیاده سازی می کنیم و نرم افزار از طریق یک پروتکل بین سرور و دستگاه های سیسکویی می تواند صحبت کند که آن پروتکل Tac Acs یا Radius است.

تعیین سطح دسترسی

Swh-1(config)#username Zahra privilege 0

Password Zahra

ایجاد سطح دسترسی جدید

Swh-1(config)#privilege configure level 2

برای اینکه دستورات بین لاگ ها گم نشوند از این دستور استفاده می کنیم تا بعد از هر لاگ ادامه دستور نوشته شده نمایان شود:

Swh-1(config)#line console 0

Swh-1(config-line)#logging synchronous

نمایش کانفیک دستگاه

Swh-1#show running-config

رمزگذاری سوئیچ سیسکو

Swh-1(config)#service password-encryption	type7
Swh-1(config)#username Ali Secret Ali	secret=type5(MDF)
Swh-1(config)#username Ahmad password 8 ahmad	8=type8

رمز Type 5

این روش پسورد و رمزگذاری سوئیچ سیسکو در حدود سال 1992 معرفی شد. این روش از یک الگوریتم هش بسیار ساده خلاصه پیام MD5 (Message-Digest 5) استفاده می‌کند که قابلیت تکرار MD5 1000 تا 32 بیت را دارد. با این‌حال الگوریتم MD5 مورد تایید موسسه ملی فناوری و استانداردها آمریکا (NIST) نیست. با این‌حال استفاده از رمز Type 5 زمانی توصیه می‌شود که سخت‌افزار سیستم از نرم‌افزارها و قابلیت رمزگذاری 6، 8 و یا 9 پشتیبانی نمی‌کند.

رمز Type 7

این روش از یک جانشین الفبایی ساده رمز Vigenere با یک کلید سخت کد و شناخته شده عمومی استفاده می‌کند. این روش را می‌توان با استفاده از ابزارهای موجود در اینترنت بلافاصله تبدیل به یک متن ساده کرد. همچنین رمزهای عبور در این مدل به صورت رشته‌های رمزگذاری شده در فایل پیکربندی ذخیره می‌شوند. NSA اکیدا توصیه می‌کند از نوع 7 استفاده نکنید.

رمز Type 8

با توسعه سیستم‌عامل‌های سیسکو پس از سال 2013، مدل Type 8 را می‌توان نسخه‌ی ارتقا یافته ی Type 4 دانست. گذرواژه‌های نوع 8 با تابع استخراج کلید مبتنی بر رمز عبور نسخه PBKDF2), SHA-256, an 80-bit salt 2) و 20,000 تکرار هش عمل می‌کنند که در مقایسه با انواع رمزهای قبلی، ایمن‌تر هستند. و همچنین پسوردها به صورت هش در فایل پیکربندی ذخیره می‌شوند.

Password type	Ability to crack	Vulnerability severity	NSA recommendation
Type 0	Immediate	Critical	Do not use
Type 4	Easy	Critical	Do not use
Type 5	Medium	Medium	Not NIST approved, use only when Types 6, 8, and 9 are not available
Type 6	Difficult	Low	Use only when reversible encryption is needed, or when Type 8 is not available
Type 7	Immediate	Critical	Do not use
Type 8	Difficult	Low	Recommended
Type 9	Difficult	Low	Not NIST approved

National Security Agency: Cisco Password Types and Recommendations

پاک کردن حافظه

Write erase/erase startup config

کپی کردن در حافظه

Swh-1#copy running-config Startup-config

یا دستور

Swh-1#write

نمایش مشخصات ios

Swh-1#show flash

نمایش اطلاعات سخت افزاری یا Up Time

Swh-1#show version

برای مثال در شبکه ای برق قطع و وصل شده از زمان up time متوجه می شویم سوییچ قطع بوده یا روتر .

Remote Device Access Configuration

در اکثر مواقع بعد از پیکربندی Router یا Switch نیاز داریم که از راه دور به دستگاه دسترسی داشته باشیم تا در صورت نیاز جهت پیکربندی یا رفع عیب به دستگاه متصل شویم، مثلا در نظر بگیرید شما یک یا چند Device را در سطح یک شهر یا کشور پیکربندی کرده اید و پس از این کار باید به مشترکین خود خدمات پشتیبانی ارائه دهید. در صورتی که از راه دور دسترسی به این دستگاه را نداشته باشید، هنگامی که نیاز به ایجاد تغییر در پیکربندی دستگاه یا رفع عیب باشید باید جهت دسترسی به دستگاه مسیر زیادی را طی کنید که مستلزم وقت و هزینه زیادی خواهد بود. جهت حل این مشکل سیسکو از پروتکل هایی مانند: Telnet,SSH استفاده می کندکه SSH در مقابل Telnet امنیت بیشتری دارد.

SSH هتگام انتقال ترافیک ابتدا آن را رمزنگاری می کند سپس ترافیک را ارسال می کند، اما Telnet ترافیک را به همان شکل اصلی خود یا Plane Text ارسال می کند.

برای اینکه بصورت Remote به دستگاه وصل شویم به یک شناسه (IP) نیاز داریم. برای اینکه بتوانیم به یک interface آی پی دهیم و از طریق آی پی به دستگاه متصل شویم interface vlan را انتخاب می کنیم، بدلیل اینکه تمامی پورت های سوییچ بصورت پیشفرض روشن (no shutdown) هستند و سوییچ دستگاهی است که ترافیک رادر لایه 2 انتقال می دهد، در نتیجه نمی توانیم به پورت های فیزیکال سوییچ ip دهیم چون روی interface های فیزیکال نمی توانیم ip تنظیم کنیم و باید از یک interface لاجیکال یه نامinterface vlan استفاده کنیم و به آن ip دهیم. بصورت پیشفرض روی سوییچ interface vlan 1 ساخته شده و خاموش (shut down) می باشد و هیچ تنظیماتی ندارد.

Switch>en

Switch#conf t

Switch (config)#interface vlan 1

Switch (config-if)#no shutdown

%LINK -5- CHANGED: interface vlan 1 , change state to up

Switch (config-if)#ip address 192.168.1.100 255.255.255.0

پورت هایی که برای مدیریت دستگاه بصورت local یا remote استفاده می کنیم را Line می گویند.

Switch (config)#line vty 0 15

Switch (config-if)#exit

Line console از طریق کابل کنسول local access

Vty برای virtual terminal SSH,telnet

Telnet Configuration :

1 – IP address Assignment

```
switch(config)#interface vlan <>
switch(config-if)#ip address <IP> <Subnet Mask>
switch(config-if)#no shutdown
switch(config-if)#exit
```

2 – User Mode Security ➔ Line VTY

```
switch(config)#line VTY <>
switch(config-line)# {password | secret } <>
switch(config-line)#login
switch(config-line)#exit
```

OR

```
switch(config)#username <> {password | secret } <>
switch(config)#line VTY <>
switch(config-line)#login local
switch(config-line)#exit
```

3 – Privilege Mode Security

```
switch(config)#enable {password | secret }  <>
```

برای telnet و SSH روی محیط enable حتما باید pass داشته باشیم.

```
Switch(config)#enable secret 123456
Switch(config)#username ali secret ali
Switch(config)#line vty 0 15
Switch(config)#login local
```

جهت استفاده از user ,pass

پروتکل های Remote Access

```
Switch(config-line)#transport input ?
All         all protocols
None        no protocols
SSH         TCP/IP  SSH protocol
Telnet      TCP/IP  Telnet protocol
```

دستور write را در محیط enable باید بدهیم اما با نوشتنdo قبل دستور می تواند ios را force کند دستوری که می خواهیم را در Global Mode اجرا کند. اما در این حالتAuto Complete یا help نداریم.

```
Switch(config)#hostname SWH-TBRZ
Switch(config-if)#do write
```

در SSH حتما باید برای درستگاه یک host name و doamin name استفاده کنیم، بدلیل اینکه برای ورود از الگوریتم RSA استفاده می کند.

```
Switch(config)#ip domain-name ccna.com
Switch(config)#exit
Switch(config)#crypto key generate rsa
%SSH -5- ENABLED
Switch(config)#do write
```

SSH Configuration :

1 – IP address Assignment

```
switch(config)#interface vlan <>
switch(config-if)#ip address <IP> <Subnet Mask>
switch(config-if)#no shutdown
switch(config-if)#exit
```

2 – User Mode Security ➔ Line VTY

```
switch(config)#username <> {password | secret } <>
switch(config)#line VTY <>
switch(config-line)#login local
switch(config-line)#exit
```

3 – Privilege Mode Security

```
switch(config)#enable {password | secret }  <>
```

4 – Hostname Configuration

```
switch(config)#hostname <>
```

5 – Domain name Configuration

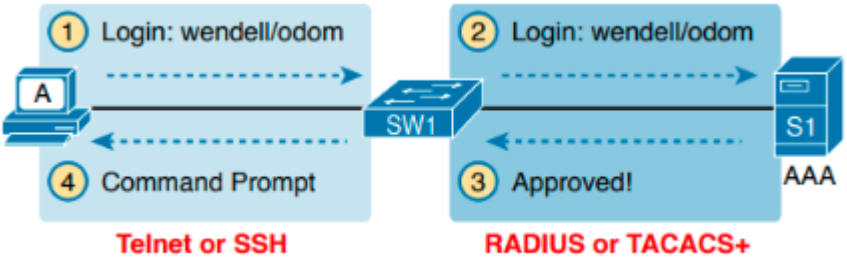
```
switch(config)#ip domain-name <>
```

6 – RSA Key generation Configuration

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

Show user
Show ip ssh
Show ssh

Device Access



login is used on Line and console and means that the password that is user for its authentication, is configured under vty and console as well.

Login local, means that authentication uses locally configured credentials using the username <> privilege <0-15> secret <> command in global configuration mode

روی هر interface می توان speed,Duplex را تنظیم کنیم.

```
Switch(config)#int fas 0/1
Switch(config-if)#description MR.ahmadi
Switch(config)#speed 10
Switch(config)#duplex half
```

بررسی وضعیت پورت های فیزیکال

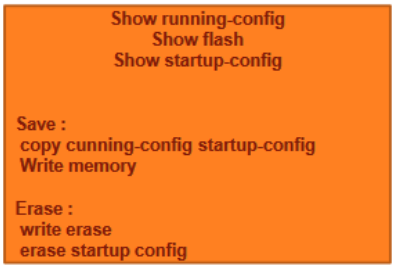
این دستور روی سوییچ استفاده می شود و روی روتر امکان پذیر نیست.

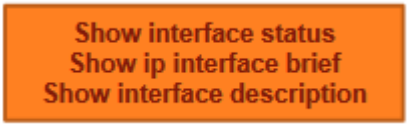
```
#show interface status
```

نمایش وضعیت interface های فیزیکال و interface های لاجیکال مثل vlan را نمایش نمی دهد.

LAN Switch Interface Status Codes

Line Status	Protocol Status	Interface Status	Typical Root Cause
administratively down	down	disabled	The **shutdown** command is configured on the interface.
down	down	notconnect	No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off, (b) **shutdown**, or (c) error disabled.
up	down	notconnect	Not expected on LAN switch physical interfaces.
down	down (err-disabled)	err-disabled	Port security has disabled the interface.
up	up	connected	The interface is working.





Connected

روشن بوده و ارتباط لایه 2 برقرار است.

Not connected

Interface فیزیکالی روشن بوده اما چیزی به آن متصل نیست، ارتباط لایه 2 بین ما و طرف مقابل به هر دلیل برقرار نیست.

Disable

ادمین با دستور shutdown خاموش کرده.

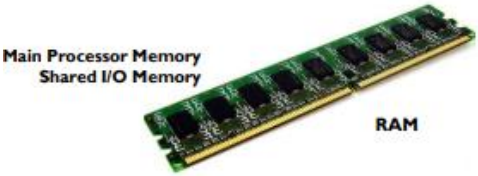
Cisco Memory Types

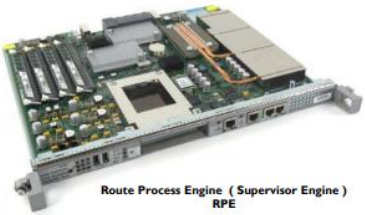
سیستم عامل دستگاه های سیسکو روی فلش قرار دارند و حجم کمی دارند و نسبت به مدل سوییچ ممکن است یک یا دو فلش داشته باشند.

بعد از اینکه دستگاه روشن شد POST(power on self test) انجام می شود، ROM سیستم عامل را از روی فلش ios برداشته و دستگاه بوت می شود.

بعضی از تنظیمات بصورت پیشفرض روی دستگاه قرار دارد، مثلا تمام پورت ها no shut,speed auto, duplex auto host name switch نامگذاری شده که روی حافظه غیر فرار فلش قرار دارد، که NVRAM نام دارد و startup config ما هست، یعنی بعد از اینکه دستگاه روشن شود تنظیماتی که در فضای NVRAM ذخیره شده باید این تنظیمات را بردارد و روی RAM قرا دهد یا همان Running Config.

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	• Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
ROM	Non-Volatile	• Bootup instructions • Basic diagnostic software • Limited IOS
NVRAM	Non-Volatile	• Startup configuration file
Flash	Non-Volatile	• IOS • Other system files

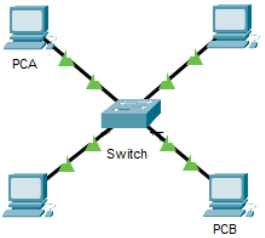




Address Resolution Protocol (ARP)

ARP پروتکلی است برای یافتن Mac Address از طریق ip مورد استفاده قرار می گیرد. Mac Address همان آدرس فیزیکی دستگاه می باشد که یک شماره منحصر به فرد جهانی است، که به هر کارت شبکه اختصاص می یابد. زمانی که یک دستگاه با دستگاه دیگر در شبکه LAN ارتباط برقرار می کند، برای آن دستگاه نیاز به Mac Address دارد و دستگاه از پروتکل ARP جهت دستیابی به Mac Address مربوط به آن دستگاه استفاده می کند.

مثال: فرض کنید PCA میخواهد با PCB ارتباط برقرار کند.



PCA آدرس ای پی PCB را می داند، با این وجود هنوز هم برای برقراری ارتباط با PCB به Mac Address آن نیاز داریم. بنابراین از IP به منظور قرار دادن یک دستگاه در شبکه مورد استفاده قرار می گیرد و Mac Address همان چیزی است که دستگاه مورد نظر را شناسایی می کند، بنابر این PCA به منظور یافتن mac Address ابتدا به لیست داخلی خودنگاهی می اندازد، به این لیست ARP Cache گفته می شود و بررس می کندکه آیا آی پی PCB دارای

MAC Add سازگار هست یا خیر. ARP Cache خالی است، حال PCA پیامی را در شبکه broadcast می کند تا بداند کدام PC دارای آن آی پی خاصی می باشددر ضمن به دنبال MAC Add نیز می باشد سپس PC که دارای آی پی سازگار باشد پاسخ داده و MAC خود را به PCA اعلام می کند. برای اینکه یک بسته به دست همه اعضای شبکه در broadcast که دادیم به همه برسد باید تمام بیت های host را یک قرار دهیم. مک آدرس 48 بیت می باشد که در مبنای 16 نماش داده می شود یا HEX یعنی هر 4 کاراکتر را یک کاراکتر HEX در نظر می گیرد. اینجا چهارتا 1 رو کنار هم قرار دهیم و تبدیل کنیم به HEX ، عددی که به HEX بدست می آید15 می شودکه اینجا 12 تا F خواهیم داشت.

BIN 1111 => HEX=F

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

F F F F F F F F F F F F

نتیجه: FFFF.FFFF.FFFF.FFFF 48bit

پس از اینکه broadcast انجام شد وهمهpc ها بسته را دریافت کردند pc ای که آن مطابق با ip درخواست شده باشد پاسخ می دهد و Mac خود را به PCA اعلام می کند، بنابراین با دریافت MAC ارتباط بین دو pc برقرار می شود. حال PCAکه دارای mac می باشد این اطلاعات را در ARP Chache ذخیره می کند.

از ARP Cache برای کارایی بیشتر شبکه استفاده می شود. Ip مرتبط با Mac را ذخیره کرده که اگر نیاز به برقراری ارتباط مجدد با آن دستگاه در شبکه را داشته باشد نیاز نباشد مجدد پیام را در کل شبکه broadcast کند بلکه تنها کاری که انجام دهد این است که از ARP Cache خود آن را بازیابی می کند.

دو نوع مختلف ورودی ARP وجود دارد: dynamic,static

زمانی که یک دستگاه پیامی را در شبکه توزیع می کند و درخواست MAC Add دارد بطور خودکار یک ورودی dynamic ایجاد می شود. ورودی های dynamic دائمی نیستند و بطور دوره ای حذف می شوند تا حافظه Cache پر نشود و ورودی های static زمانی بوجود می آیند که شخصی مرتبط با Mac را بصورت دستی و با استفاده از Command Line وارد نماید. مدیران شبکه جهت کاهش ترافیک غیر ضروری ARP از این روش استفاده می کنند برای مثال زمانی که می دانیم دو دستگاه به طور مداوم با یکدیگر ارتباط برقرار می کنند.

Arp -a		show arp table	
Arp -t		remove arp table	
Arp -s	10.0.0.3	90-02-7b-c	اضافه کردن مک بصورت دستی

نکته: عمر ARP Table ، 4 ساعت است.

نکته: هر interface در شبکه چه فیزیکال یا لاجیکال یک Mac یونیک دارد.

نکته: سوئیچ بر اساس Mac مبدا Learning انجام می دهد و ترافیک را بر اساس Mac مقصد فوروارد می کند و در جدول Mac address table آن را ذخیره می کند.

مشاهده Mac table Switch # show mac address-table

پاک کردن Mac table Switch # clear mac address-table

سوئیچ بر اساس destination mac که قبلا در جدول mac table ذخیره شده ، forwarding انجام می دهد.

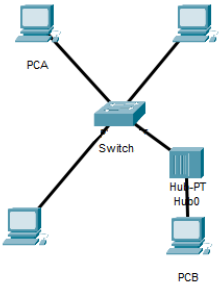
نکته: عمر mac table ، 5 دقیقه می باشد.

Mac-age-time = 300 sec

Application specific integrated circuit (Asic)

سیسکو جدول های Mac را تشکیل می دهد تا بتواند Traffic forwardingرا انجام دهد که این جدول ها در RAM ذخیره می شوند که باید پردازش شوند و بعد بسته فوروارد شود. در دستگاه های دیگر CPU این وظیفه رادارد اما سیسکو به ازای هر پورت یک CPU سخت افزاری جداگانه به نام Asic در نظر گرفته ، به همین علت سرعت forwarding تجهیزات سیسکو بالاست و به اصطلاح Wire speedعمل می کنند.

سیستم عامل سیسکو کل لایه های TCP /IP را درک می کند اما به صورت پیش قرض traffic forwarding سوئیچ تا لایه دو می باشد ، به همین دلیل می گویند سوئیچ یک دستگاه لایه دویی است.



اگر اتصال Pc3 به صورت Directory Connected باشد اگر پورت سوئیچ Not connected شود یا ادمین shut down کند ، Mac table که روی این اینترفیس یاد گرفته را پاک می کند اما ممکن است بین Pc3 و سوئیچ ، یک هاب قرار گرفته باشد که در ارتباط Pc3 با سوئیچ غیر مستقیم باشد ، حال اگر ارتباط بین Pc3 , Hub قطع شود ، سوئیچ هیچ LOG نمی دهد و جدول Mac هنوز مک این interface را نگه داشته و اگر بسته ارسال شود ، سوئیچ آن را فوروارد می کند و روی هاب Drop می شود و تا زمان Mac age time یا همان 5 دقیقه و Mac Pc را نگه می دارد.

مشاهده وضعیت فیزیکال Interface

Switch # show interface status

اما Interface vlan 1 لاجیکال هست و برای مشاهده وضعیت آن از این دستور استفاده می شود.

Switch # show ip interface brief

مشاهده اطلاعات بیشتر از interface که عمدتا لایه 3 هستند:

Switch # show ip interface vlan 1

بررسی اطلاعات روی interface جهت troubleshoot

مشاهده اطلاعات بیشتر از interface که عمدتا لایه 2 هستند.

Switch # show interface vlan 1

Mac address-Dly -Arp time out-tx load -reliability -Bw-Mtu

Interface Counters for Layer 1 Problems

CRC : ممکن است ارتباطی داشته باشیم که Pocket loss داشته باشیم یا کند باشد یا Gitter یا Delay ، که CRC آن را نمایش می دهد. عمدتا مشکل فیزیکی است مثل خرابی Patch cord, Patch panel ، ماژول ، کانکتور ، کابل یا نویز مثل رد شدن سیم برق از کنار کابل شبکه.

در شبکه اترنت ماکزیمم سایز Packet ، 1500 می باشد که همان MTU(maximum transfer unit) هست .

MTU=H4+H3+data

MSS (maximum segment size)=MTU – H4 –H3

ماکزیمم سایزی که می تواند داشته باشد.

MSS = 1500-20-20=1460 (MSS=MTU-H4-H3)

ممکن است پروتکلی استفاده شودکه هدراضافه کند ، حال باید بسته ها را کوچکتر(segmet) کنیم ، چون سایز بسته ای که می تواند در شبکه اینترنت جابجا شود 1500B است. اگر هدری اضافه کردیم پروتکل (ip sec- tunnel) از سایز دیتا باید کم کنیم.

Minimum size =64B => 20-10-18=68 (H4-H3-H2=packet size)

کمترین سایز بسته که می توان جابجا کرد 64 B است اگر کمتر از این حجم باشد padding انجام میدهد و خودش به آن اضافه می کند که حجم آن به 6 B برسد.

Runts : اگر تعداد بسته های دریافت شده کمتر از 64 B باشد.

Giant : در صورتیکه حجم بسته ها از 1500 B بیشتر باشد و فریم هایی که حجم آن از 1500 B بیشتر باشد را jumbo frame میگویند.

Input errors : مجموع خطاها.

Over run : بسته هایی که مجدد ارسال شده اند.

محاسبه مسیر MTU

C:\user\mahdi:>ping yahoo.com

بسته های 32 بایتی می فرستد و یاهو بسته را دریافت کرده و پاسخ می دهد این رفت و برگشت 32 ms طول می کشد.

Pinging yahoo [74.6.143.26] with 32 bytes of data:

Reply from 74.6.143.26:bytes=32 time=202 ms ttl=45

دستورات ping:

Ping -t -T بدون توقف بسته ارسال می کند تا زمانیکه CTRL+C رابزنیم.

Ping -l -L به صورت دستی سایز بسته را انتخاب می کنیم.

Ping yahoo.com -l 1700

Reply from 74.6.143.26 : bytes =1700 time = 226 ms ttl=44

Ping –f => set don't fragment flag in pacliet (ip v4-only)

Ping yahoo.com -l 1700 -f

Packet need to be fragmented but DF set

بسته را نمی تواند ارسال کند ، چون حجم بالای آن 1500 B بوده و flag Df را فعال کردیم و اجازه نمی دهد قطعه قطعه شود.

Ping yahoo.com -1 1400 -f

Reply from 74.6.143.26 : byte=1400 time=184ms ttl=43

چون نیاز نبود بسته را fragment کند آن را ارسال کرد.

مرز بین جایی که باید segmentation انجام شود و جایی که ping بدهیم و reply دهد و جایی که اگر یک بایت به آن اضافه کنیم و دیگر reply نمی دهد و پیام DF set میدهد ، MTU مسیر مشخص میشود.

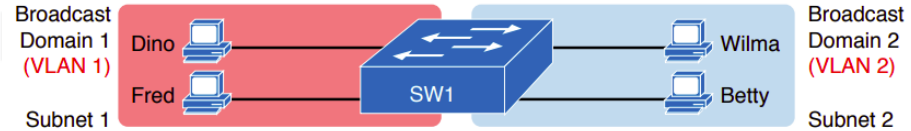
Virtual Lan

Virtual Local Area Network (Vlan)

تمام پورت های سوییچ در یک broadcast domain قرار دارند. سیسکو قابلیتی به نام vlan ارائه کرد که در سطح لایه دو میتوان broadcast domain ها را با vlan بندی جدا کنیم.(روی یک سوییچ فیزیکال اما پورت های سوییچ را لاجیکالی از هم جدا می کنیم ، مثل اینکه چند سوییچ مجزا داریم).

Implementing Ethernet Virtual LANs

Creating Two Broadcast Domains with Two Physical Switches and No VLANs



Creating Two Broadcast Domains Using One Switch and VLANs

در لایه 3 با جدا کردن network ها میتوان broadcast domain هارا جدا کرد اما سوییچ درکی از لایه 3 ندارد و به همین دلیل از vlan استفاده می کنیم.

12 بیت برای vlan در نظر گرفته شده است $4096= 2^{12}$

از صفر تا 4095 می توان vlan ساخت.

Vlan های رزرو شده:

0-4095

1002	fddi- default
1003	token-ring- default
1004	fddi net-default
1005	trnet-default

ISL: سیسکو اولین بار این پروتکل را معرفی کرد که بسیار سنگین و مجموعا 30 B هدر به بسته اضافه می کند، Isl مخفف inter switch link است که یکی از پروتکل های Vlan است .ISL اختصاصی سیسکو است.

820 .1Q : توسط موسسه مهندسان برق و الکترونیک (IEEE) این استاندارد ایجاد شده است مجموعا 4 بایت دارد که 12 بیت را به VLAN تخصیص داده. 2^{12} =4096

Switch (config)#vlan 20

Switch (config-vlan)#name class 302

exit

مشاهده vlan هایی که ساخته ایم:

Switch(config)# do show vlan brief

Switch(config)# do show interface status

```
SW1# show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

عضو کردن پورتها در vlan

Switch(config)# interface fast 0/1

Switch(config)# switchport mode access

با این دستور به پورت اعلام می کنیم که به یک end device متصل شده و باید ترافیک یک vlan را از خود عبور دهد.

Switch(config-if)#switch port access vlan 10

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 2
SW1(config-vlan)# name Freds-vlan
SW1(config-vlan)# exit
SW1(config)# interface range fastethernet 0/13 - 14
SW1(config-if)# switchport access vlan 2
SW1(config-if)# switchport mode access
SW1(config-if)# end

SW1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
2    Freds-vlan                       active    Fa0/13, Fa0/14
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

برای اینکه پورتها را تک به تک access یک vlan کنیم زمان بر بوده و به همین دلیل می توان از دستور range استفاده کنیم.

Switch(config)#int range fastethernet 0/2 – 3

Switch(config-if)#switchport mode access

#switchport access vlan 10

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface range Fastethernet 0/15 - 16
SW1(config-if-range)# switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SW1(config-if-range)# ^Z

SW1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1 default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
2 Freds-vlan                          active    Fa0/13, Fa0/14
3 VLAN0003                            active    Fa0/15, Fa0/16
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Vlan 1 به صورت پیش فرض روی همه پورتها ساخته شده است و می تواند ترافیک راعبور دهد.

پورت هایی که لازم نداریم را shut down می کنیم.

#int range fast 0/7 – 24, gig 0/1 – 2 shut down

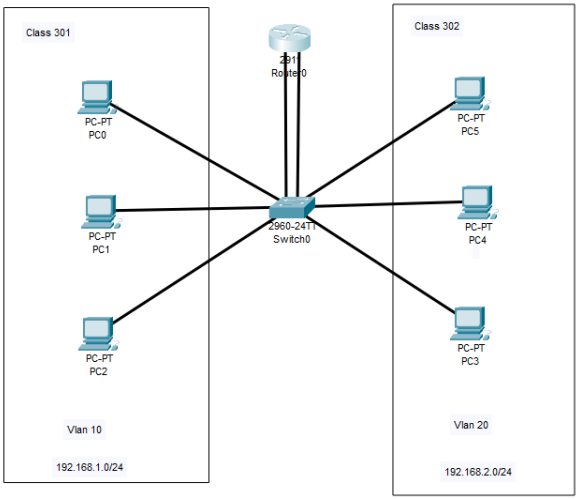
حال باید از یک دستگاه لایه 3 استفاده کنیم که بتواند ارتباط بین network ها و vlan های مختلف را برقرار کند. یک inter vlan routing نیاز هست داشته باشیم که از یک router استفاده می کنیم.

Inter-Vlan Routing

همانطور که قبلاً گفته شد Vlanها شبکه را به Broadcast Domain های کوچکتر تقسیم می کنند و همچنین باعث میشوند که بین این شبکه ها ارتباطی وجود نداشته باشد.

برای برقراری ارتباط بین این گروه از شبکه ها برای عبور ترافیک broadcast از Inter vlan routing استفاده میشود.

اگر سوئیچ لایه سه نباشد برای روتینگ و ارتباط بین vlanها نیاز به یک روتر داریم، باید به تعداد vlanها روی روتر Subinterface تعریف کنیم و در روتر مشخص کنیم هر subinterface مربوط به کدام vlan میباشد.



```
# int range 0/1-2
(config-if-range)#no shutdown
#exit

#int gig 0/1 switchport mode access
Switchport access vlan 10
# exit

#int gig 0/2 switch port mode access
Switchport access vlan20
#exit

Router >en
Router #conf t
Router(config)#int gig 0/1
(config-if)#no sh
```

Switchport کامند لایه دو بوده و روتر درکی از آن ندارد.

بعنوان gateway یک آی پی به روتر می دهیم.

```
Router(config-if)#ip address 192.168.1.1  255.255.255.0
#exit
(config)#int gig 0/2
(config-if)#no sh
# ip address 192.168.2.1  255.255.255.0
#exit
```

معمولاً اولین ip از network یا آخرین ip را برای geteway در نظر میگیرند.

روی روتر دستور show interface status نداریم، به جای آن :

Router#sh ip int brief

و بعد روی همه PC ها gateway را تعریف میکنیم.

روی سوئیچ هر پورت را اکسس یک vlan کردیم ، به این ترتیب ترافیک یک vlan از روی آن عبور میکند.

Trunk همزمان ترافیک چندین vlan را از پورت عبور میدهد.

پورت های سوئیچ روی حالت dynamic هستند، بدلیل اینکه هم قابلیت Access mode را دارند و میتوانند ترافیک vlan1 را عبور دهند و هم قابلیت اینکه اگر درخواستی رسید Trunk شود و ترافیک چندین vlan را عبور دهد.

Trunk به دو صورت static و dynamic که دو حالت auto و desirable دارد می باشد.

پورت در حالت Access : ترافیک یک vlanرا از خود عبور میدهد و Trunk هم نمیشود.

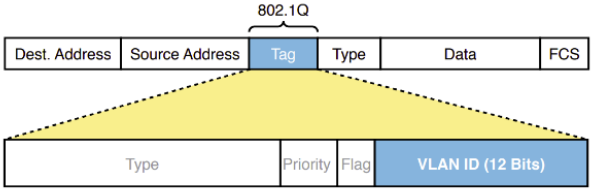
پورت در حالت Trunk: می شود به آن دستور دهیم هر ترافیکی که داریم Tag زده شود و عبور کند و اما Dynamic Auto درخواستی برای Trunk شدن به طرف مقابل نمی دهد اما اگر درخواستی دریافت کند که trunk شود، می پذیرد و حالت desireable هم درخواست میدهد برای trunk شدن و هم اگر درخواستی دریافت کند می پذیرد که Trunk شود.

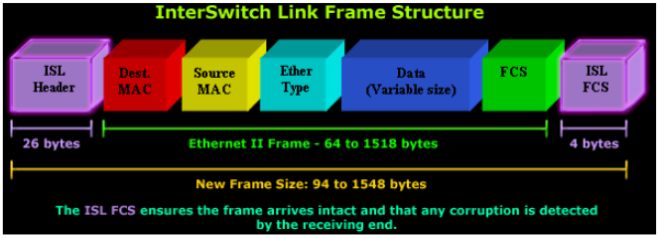
Administrative Mode: Access, dynamic Auto, trunk, dynamic desireable

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

Access :	Not send	Not Accept
Dynamic Auto :	Not sent	Accept
Dynamic Desireable :	Send	Accept
Trunk :	Send	_____

```
Switch(config-if)# switchport trunk encapsulation { ISL | dot1q | negotiate }
Switch(config-if)# switchport mode { access | trunk | dynamic auto | dynamic desirable }
Switch# show interface <> switchport
Switch# show interface trunk
```





Trunk mode : همان mode ON یعنی negotiate نمی کند، طرف مقابل را force میکند Trunk شود.

اینکه از چه مودی استفاده کنیم بستگی دارد پورت را برای چه Device ای استفاده می کنیم، به user تحویل میدهیم یا Device خودمان وصل می شود.

نکته: پورتی که تحویل user میدهیم حتماً باید Trunk باشد.

زمانی که میخواهیم با طرف مقابل negotiate کنیم که یا trunk باشد و یا Access از dtp استفاده میکنیم و force نمی کند که حتماً trunk باشد، ممکن است دستگاه طرف مقابل cisco نباشد و نتواند در حالت Auto کار کند مثلاً سرور قرار دارد و از مود ON یا desireable استفاده می کنیم.

زمانی که پورت را Access می کنیم، بدلیل اینکه پورت سوئیچ وارد negotiate ناخواسته ای نشود، قابلیت negotiate را می توان از آن گرفت.

Switch(config)# int fa 0/1

Switch(config)#switch port mode access

Switch(config)#switch port nonegotiate

زمانی که دستگاه را write erase کنیم تمام تنظیمات پاک میشود، اما فایل vlan.dat که فایل vlan database هست پاک نمی شود.

حذف Vlan database :

Switch#delete flash :vlan.dat

Vlan Trunking Protocol (VTP)

یک سوئیچ VTP سرور میشود و باقی سوئیچ ها VTP Client .

به ازای هر vlan که می سازیم یک Vlan روی کلاینت ها می سازد.

Switch#show vtp status

VTP oprating mode:server

اگر VTP استفاده نمی کنیم (در سطح CCNA یاد نمی گیریم) با دستور VTP Mode حالتoff یاTransparent انتخاب میکنیم چون فعلاً Vlan ها را دستی میسازیم.

مدیریت ترافیک عبوری Vlan ها :

(config)#int fas 0/1

(config-if)#switchport trunk allowed vlan 10

WORD	VLAN IDs of the allowed VLANs when this port is in trunking mode
add	add VLANs to the current list
all	all VLANs
except	all VLANs except the following
none	no VLANs
remove	remove VLANs from the current list

برای مشاهده Allowded Vlan :

Switch # show int trunk

برای اضافه کردن vlan جدید به vlan هایی که allowed کردیم حتماً در انتها کلمه add را بزنید در غیر این صورت Rewrite میشود و دستورات قبلی حذف میشود و این دستور جایگزین می شود و باعث می شود User قطع شود.

(config)#int fas 0/1

(config-if)#switchport trunk allowed vlan add 400

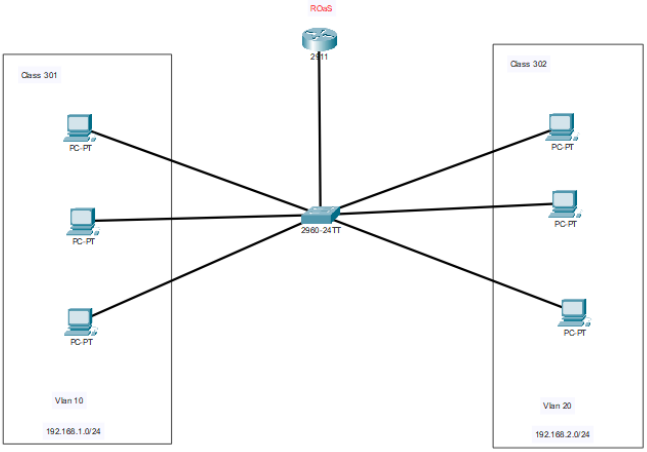
The Supported VLAN List on Trunks

```
SW1# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Gi0/1       desirable    802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/1       1-60

Port        Vlans allowed and active in management domain
Gi0/1       1-59

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1-58
```

switch(config-if)# switchport trunk allowed vlan VLAN_LIST

ROAS Solution

Roas روشی منطقی و به صرفه در شبکه های کوچک



برگرداندن تنظیمات به حالت پیش فرض

(config)#default int gig 0/1

Vlan هایی که قبلا ساختیم دیگرنیاز به تعریف نیست زیرا بصورت پیشفرض روی پورت Allowed شده.

Router#

Router(config)#int g 0/0 no shut

روی سوئیچ با دستور show int trunk میتوان وضعیت پورت ها و trunk را بررسی کرد.

Mode : On → static

Encapsulation : 802.1q

Status : Trunking

Port Gig 0/1 Vlan allowed and active in management domain 1,10,20

روتر یک اینترفیس لاجیکال دارد که وابستگی زیادی به اینترفیس فیزیکال دارد، روی روتر به اینترفیسی نیاز داریم که vlan را متوجه شود که به آن Sub interface می گویند.

Router(config)#int gig 0/0.100

نکته: عدد بعد از نقطه ارتباطی به شماره vlan ندارد و دلخواه میباشد.

وضعیت subinterface وابسته به اینترفیس لاجیکال می باشد یعنی اگر اینترفیس فیزیکال قطع شود تمام subinterface هایی که روی آن فیزیکال اینترفیس ساختیم down خواهد شد، اما بالعکس میتوان یکی از subinterfaceها را shut down کنیم.

Subinterface هم مثل فیزیکال اینترفیس هست که به آن ip می دهیم، با این تفاوت که Tagرا به آن میدهیم که بسته هایی که قرار است دریافت شود با Tag vlan هایی که دستور بدهیم دریافت میشود.

تعداد Subinterface هایی که میتوان ساخت بی نهایت است.

قبل از ip دادن باید مشخص کنیم که از چه پروتکلی استفاده میکنیم (ISL و یا dot1q) و بعد vlan را تعریف کنیم.

Router(config-subif)#encapsulaition dot1q 10 — 10 شماره vlan می باشد

Router(config-subif)#ip address 192.168.1.1 255.255.255.0

exit

Router(config)#gig 0/0.200 — 200 شماره Subinterface می باشد

Router(config-sub-if)#encapsulaition dot1q 20 20 شماره vlan می باشد

#ip add 192.168.2.1 255.255.255.0

exit

نکته: به ازای هر یک Vlan یک sub int باید ایجاد کنیم.

وضعیت interface و ip

Router(config)#do sh ip int brief

MLS Solution

Multilayer Switch(MLS)

سوئیچ های MLS بصورت پیش فرض لایه دویی هستند ولی با اعمال دستوراتی می توان فعالیت این سوئیچ ها را علاوه بر لایه دو به لایه سه هم برسانید. روی MLS وقتی پورتی را لایه 3 می کنیم با دستور ip routing به سوئیچ دستور می دهیم پورت هایی که در لایه 3 قرار دارند، ارتباط لایه 3 هم بین آنها برقرار شود.

وقتی پورتی را لایه 3 کنیم ترافیک broadcast از آن عبور نمی کند. برای اینکه interface vlan داشته باشیم حتما باید vlan آن را بسازیم اما بالعکس نیاز نیست.

نکته: روی MLS نمیتوانیم sub int بسازیم بدلیل اینکه vlan, Tag را می شناسد.

Access : ترافیک Vlan1 را عبور میدهد.

Trunk : اجازه عبور ترافیک چندین vlan به صورت همزمان با اضافه کردن Tag ترافیک را از هم مجزا میکند.

زمانی که ارتباط بین network ها برقرار کنیم باید به دستگاه علاوه بر ip وsubnet mask نیز ip gateway بدهیم.

: Native Vlan

وقتی در سوئیچ ها اقدام به ساخت Vlan میکنیم و پروتکل 802.1q را فعال میکنیم به فریم های داده یک هدر اضافه میشود که دارای یک tag مربوط به vlan خاص خود می باشد، اما اگر در این شبکه فریمی وجود داشته باشد که دارای این هدر نیست باید به vlan ای منتصب شود که این فریم ها متعلق به آن است که به این native vlan گفته میشود.

این اتفاق زمانی رخ میدهد که پورت در حالت ترانک باشد و از پروتکل 802.1q استفاده کند، معمولاً native vlan ها همان vlan های شماره یک هستند که بصورت پیش فرض بر روی سوئیچ ها وجود دارد.

در صورتی که native vlan بر روی یک پورت 1 تعریف شده باشد، در صورتی که پکتی از آن پورت وارد سوئیچ شود و دارای tag مربوط به vlan ها نباشد آن را جزو پکت های مربوط به vlan1 به حساب می آورد.

این vlan ها دارای یک مشکل بزرگ امنیتی است که میتوان آن را هک کرد که به آن vlan hopping میگویند.

: Switch spoofing

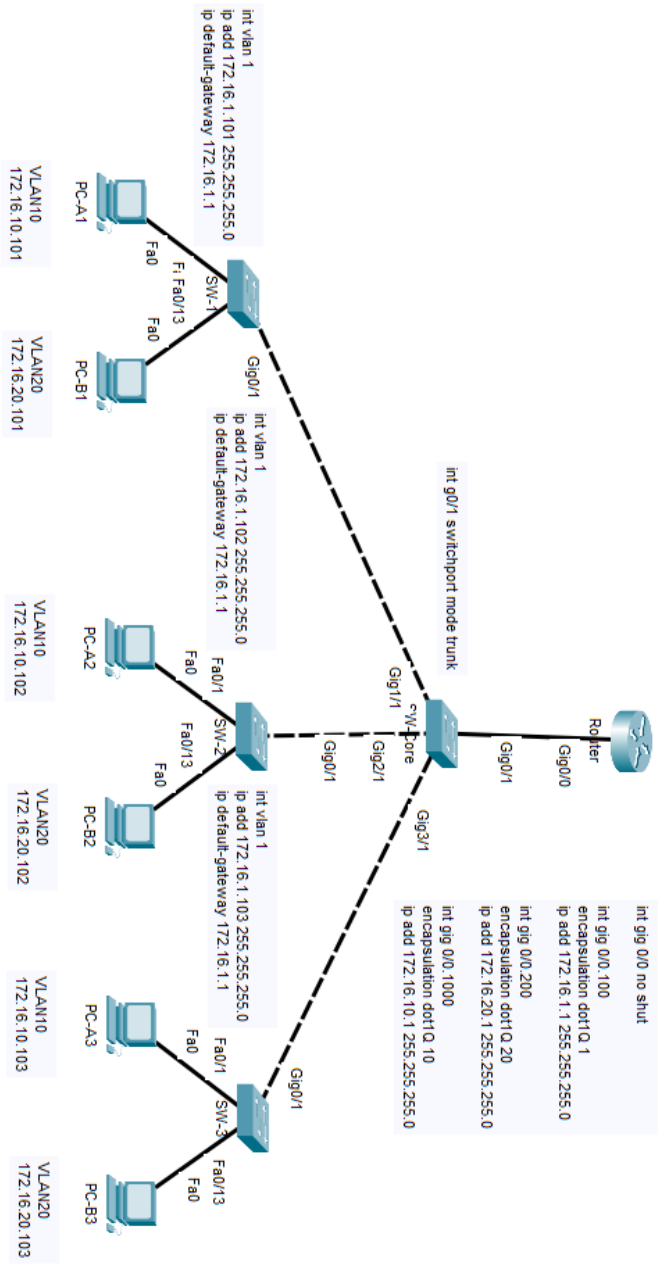
پورت های سوئیچ در حالت پیش فرض داینامیک هستند و امکان ترانک شدن در آن فعال است، اگر روی سوئیچ allowed vlan all فعال باشد (که پیش فرض روی این حالت است) سیستم را عضو Vlanای که مد نظرمان است می کنیم، حالا همه بسته ها به آن می رسد می توان در حالت ترانک جهت جلوگیری از no negotiation می توانیم استفاده کنیم.

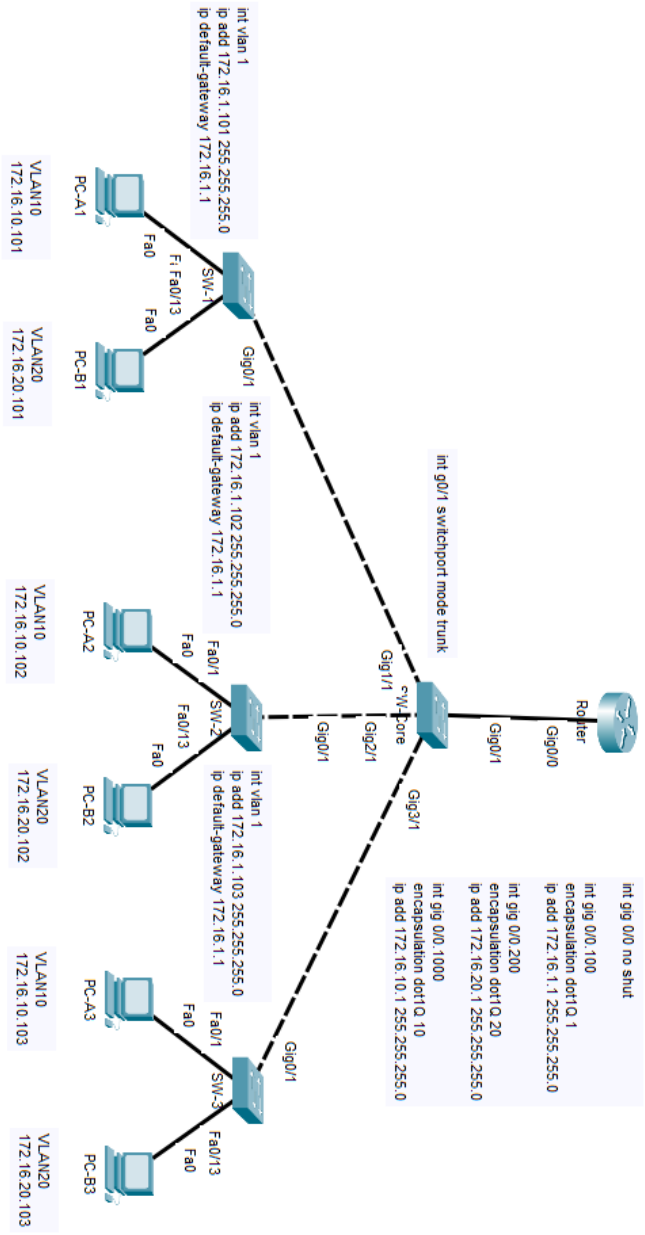
: Double tagging

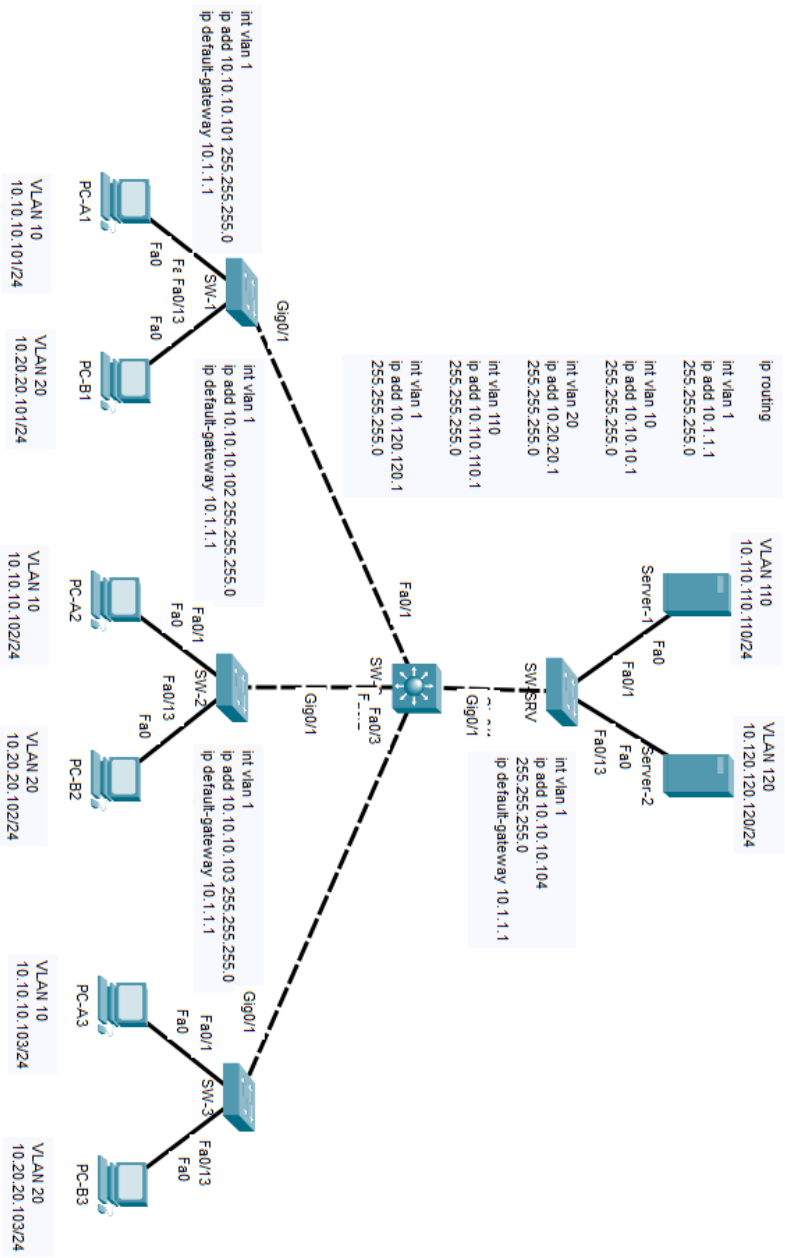
Native vlan پیش فرض vlan1 هستند که بسته ها بدون tag ارسال می شوند، در اینجا هکر به vlan1 رفته و کنار تگ 1 یک تگ 10 می چسباند ، سوئیچ هنگام پروسس به تگ 10 نگاه میکند و آن را به سمت vlan10 هدایت می کند.

برای جلوگیری از این کار میتوان native vlan را از vlan1 تغییر داد و یا native vlan را با تگ ارسال کنیم با دستور:

Switch(config-if)#switchport trunk native vlan tag


int gig 0/0 no shut
int gig 0/0.100
encapsulation dot1Q 1
ip add 172.16.1.1 255.255.255.0
int gig 0/0.200
encapsulation dot1Q 20
ip add 172.16.20.1 255.255.255.0
int gig 0/0.1000
encapsulation dot1Q 10
ip add 172.16.10.1 255.255.255.0
Router
Gig0/0
Gig0/1
SW-Core
Gig1/1
Gig2/1
Gig3/1
int g0/1 switchport mode trunk
Gig0/1
Gig0/1
Gig0/1
int vlan 1
ip add 172.16.1.101 255.255.255.0
ip default-gateway 172.16.1.1
SW-1
Fa0/1
Fa0/13
Fa0
Fa0
PC-A1
PC-B1
VLAN10
172.16.10.101
VLAN20
172.16.20.101
int vlan 1
ip add 172.16.1.102 255.255.255.0
ip default-gateway 172.16.1.1
SW-2
Fa0/1
Fa0/13
Fa0
Fa0
PC-A2
PC-B2
VLAN10
172.16.10.102
VLAN20
172.16.20.102
int vlan 1
ip add 172.16.1.103 255.255.255.0
ip default-gateway 172.16.1.1
SW-3
Fa0/1
Fa0/13
Fa0
Fa0
PC-A3
PC-B3
VLAN10
172.16.10.103
VLAN20
172.16.20.103


int gig 0/0 no shut
int gig 0/0.100
encapsulation dot1Q 1
ip add 172.16.1.1 255.255.255.0
int gig 0/0.200
encapsulation dot1Q 20
ip add 172.16.20.1 255.255.255.0
int gig 0/0.1000
encapsulation dot1Q 10
ip add 172.16.10.1 255.255.255.0
Router
Gig0/0
Gig0/1
SW-Core
Gig1/1
Gig2/1
Gig3/1
Gig0/1
int g0/1 switchport mode trunk
int vlan 1
ip add 172.16.1.101 255.255.255.0
ip default-gateway 172.16.1.1
SW-1
Gig0/1
Fa0
Fa0/13
Fa0
PC-A1
PC-B1
VLAN10
172.16.10.101
VLAN20
172.16.20.101
int vlan 1
ip add 172.16.1.102 255.255.255.0
ip default-gateway 172.16.1.1
SW-2
Fa0/1
Fa0
Fa0/13
Fa0
PC-A2
PC-B2
VLAN10
172.16.10.102
VLAN20
172.16.20.102
int vlan 1
ip add 172.16.1.103 255.255.255.0
ip default-gateway 172.16.1.1
SW-3
Gig0/1
Fa0/1
Fa0
Fa0/13
Fa0
PC-A3
PC-B3
VLAN10
172.16.10.103
VLAN20
172.16.20.103


ip routing
int vlan 1
ip add 10.1.1.1
255.255.255.0
int vlan 10
ip add 10.10.10.1
255.255.255.0
int vlan 20
ip add 10.20.20.1
255.255.255.0
int vlan 110
ip add 10.110.110.1
255.255.255.0
int vlan 1
ip add 10.120.120.1
255.255.255.0
VLAN 110
10.110.110.110/24
VLAN 120
10.120.120.120/24
Server-1
Server-2
Fa0
Fa0/1
Fa0/13
SW-SRV
Gig0/1
int vlan 1
ip add 10.10.10.104
255.255.255.0
ip default-gateway 10.1.1.1
Fa0/1
Fa0/3
Gig0/1
int vlan 1
ip add 10.10.10.101 255.255.255.0
ip default-gateway 10.1.1.1
SW-1
Gig0/1
Fa0/1
Fa0/13
Fa0
PC-A1
PC-B1
VLAN 10
10.10.10.101/24
VLAN 20
10.20.20.101/24
int vlan 1
ip add 10.10.10.102 255.255.255.0
ip default-gateway 10.1.1.1
SW-2
Gig0/1
Fa0/1
Fa0/13
Fa0
PC-A2
PC-B2
VLAN 10
10.10.10.102/24
VLAN 20
10.20.20.102/24
int vlan 1
ip add 10.10.10.103 255.255.255.0
ip default-gateway 10.1.1.1
SW-3
Gig0/1
Fa0/1
Fa0/13
Fa0
PC-A3
PC-B3
VLAN 10
10.10.10.103/24
VLAN 20
10.20.20.103/24

VLAN Trunking Protocol(vtp)

VTP پروتکل اختصاصی سیسکو است (Cisco Proprietary) که از آن برای تبادل اطلاعات دیتابیس VLAN بین سوئیچ های یک VTP دامین استفاده می شود و با کمک این پروتکل برای ایجاد یا حذف یک VLAN نیاز نیست که اینکار را روی تمام سوئیچ ها انجام دهید فقط کافیست روی یکی از سوئیچ ها (سرور) اینکار را انجام دهید این پروتکل روی باقی سوئیچ ها تغییرات شما را اعمال می کند.

VTP دامین یک گروه مدیریتی است که تمام سوئیچ های عضو این گروه باید دارای نام دامین و تنظیمات یکسان باشند در غیر اینصورت اطلاعات دیتابیس VLAN بین آنها تبادل نمی شود. پروتکل VTP برای تبادل اطلاعات از یک عدد تحت عنوان Revision Number استفاده می کند و بسته های خود را به عنوان VTP Advertisement روی پورت های Trunk خود ارسال می کند.

هر سوئیچ هر 5 دقیقه یکبار و یا در هنگام تغییر در دیتابیس خود اقدام به ارسال Advertisement می کند. همانطور که گفتیم در هر Advertisement یک عدد تحت عنوان Revision Number وجود دارد که به ازای هر تغییر در دیتابیس یک واحد به ان اضافه می شود.

VTP Advertisements:

Summary : بسته ای که حاوی اطلاعاتی مانند نام دامین و Revision Number است.

Subset :بسته حاوی اطلاعات(update)

Request :زمانی که یک کلاینت یک بسته Summary دریافت می کند بعد از چک کردن محتویات ان با تنظیمات خود اگر مقدار Revision Number بسته از مقدار خود بیشتر بود یک Request ارسال می کند و درخواست یک Subset می کند. همچنین در صورت ریست کردن یا تغییر نام دامین این بسته ارسال می شود.

عملکرد پروتکل VTP

زمانی که یک سوئیچ یک Summary دریافت کند مقدار Revision Number ان را با مقدار خود مقایسه می کند. اگر مقدار Revision Number بزرگتر از مقدار خود بود یک Request ارسال می کند و درخواست Subset می کند و دیتابیس خود را با Subset دریافتی بروز می کند. اگر مقدار برابر بود از Summary صرف نظر می کند و اگر مقدارRevision Number کوچکتر از مقدار خود بود یک Subset حاوی اطلاعات دیتابیس خود که جدیدتر است را برای سوئیچ همسایه خود ارسال می کند.

vtp versions

VTPv1 : نسخه پیش فرض سوئیچ می باشد. زمانی که در حالت Transparent است در صورت دریافت Advertisement، نسخه و نام دامین را چک می کند در صورت مطابقت با مشخصات خود Advertisement ها را ارسال می کند.

VTPv2: از شبکه های Token Ring پشتیبانی می کند. زمانی که در حالت Transparent است بدون در نظر گرفتن نسخه و نام دامین ، Advertisementها را ارسال می کند.

Consistency check زمانی که اطلاعات جدیدی از طریق CLI یا SNMP ایجاد شود مواردی مانند نام VLAN چک می شود. در صورت استفاده از نسخه دو تمامی سوئیچ های VTP دامین باید بتوانند از این نسخه پشتیبانی کنند. در نسخه دوم تنها یک سوئیچ نقش سرور را ایفا می کند و مابقی در نقش کلاینت عمل می کنند.

VTPv3 : بهبود مکانیزم احراز هویت، از VLAN رنج Extended (1006 تا 4094) پشتیبانی می کند. پشتیبانی از Private VLAN ،ایجاد مکانیزم Primary Server و Secondary Server ، امکان غیر فعال کردن VTP روی پورت ترانک.

نکته : نسخه سوم در Cisco IOS Release 12.2(52) و بعد از ان قابل دسترس است.

vtp roles

Server : نقش پیش فرض سوئیچ ها است. سوئیچی که دارای این نقش است دارای تمام امکانات است می تواند Vlanبسازد ، پاک کند و یا تغییر نام دهد. هر 5 دقیقه یکبار و یا در هنگام تغییر در دیتابیس VLAN خود Advertisement ارسال می کند. در هر VTP دامین حداقل باید یک سوئیچ دارای نقش سرور باشد.

Client : صاحب این نقش نمی تواند VLAN ایجاد یا حذف کند اما می تواند تنظیمات VTP خود را تغییر دهد. در این حالت هر 5 دقیقه یکبار Advertisement ارسال می کند.

Transparent :صاحب این نقش می تواند VLAN بسازد یا پاک کند اما تنها به صورت Localy (فقط روی این سوئیچ اعمال می شود). در این حالت بروز رسانی اطلاعات دیتابیس با دیگر سوئیچ ها انجام نمی شود و همچنین Advertisement ارسال نمی کند اما در صورت دریافت Advertisement اگر از نسخه یک VTP استفاده کند نام دامین و نسخه Advertisement را چک می کند در صورت مطابقت با مشخصات خود آن را ارسال می کند اما در نسخه دوم محتویات Advertisement را چک نمی کند و آن را ارسال می کند.

Off : همانند Transparent می باشد با این تفاوت که Advertisement ها را ارسال نمی کند.

شرایط عضویت در VTP دامین

عضویت در یک دامین هم نام

وجود لینک از نوع Trunk بین سوئیچ ها

وجود حداقل یک سوئیچ در حالتServer

VTP Pruning

قابلیتی است که می توان به وسیله آن ترافیک اضافه مثل Broadcast را کاهش داد. به این صورت که سوئیچ تمام پورت های Trunk خود را چک می کند و مشخص می کند که از هر پورت به چه VLAN هایی می رسد.به طور پیش فرض این ویژگی غیر فعال است.در صورت فعال کردن این ویژگی روی یک سوئیچ این ویژگی رو تمام سوئیچ های دامین فعال خواهد شد. در حالت معمول که در شکل زیر می بینید بسته ارسالی از PC متصل به سوئیچ یک روی کل شبکه ارسال می شود.

سانترال :

در شرکت های تجاری مختلف به علت وجود بخش های زیاد، نیاز به استفاده از چندین خط تلفن می باشد. درصورتی که از تلفن های معمولی استفاده شود نیاز هست تا هر خط تلفن به یک دستگاه تلفن جداگانه وصل شود که در این صورت تعداد تلفن های مورد نیاز بسیار زیاد شده و منجر به شلوغی بیش از حد میشود و مدیریت تعداد زیادی خطوط دشوار است.

در صورتی که فردی به یک خط تلفن در یک بخش تماس گرفته و با شخص دیگر در بخشی متفاوت کار داشته باشد، امکان وصل کردن آن شخص وجود ندارد که سیستم تلفن سانترال به حل این مشکل کمک کرده و میتوان تماس را به خط مورد نظر وصل کرد، اما اگر شبکه ما بزرگتر شود ظرفیت سانترال پاسخگو نیازهای ما نیست.

خطوط دیجیتال :

خط E1 : این خط معادل اروپایی خط T1 آمریکایی است . نرخ انتقال داده آن 2/048 mbps است. دارای 32 کانال 64kbps است که 30 عدد از کانال ها برای انتقال صوت و دو عدد دیگر برای همگام سازی و سیگنال دهی استفاده میشود.

خط T1 : در ژاپن و آمریکا استفاده میشود، نرخ انتقال داده آن 1/544 mbps بوده و 24 کانال صوتی دارد.

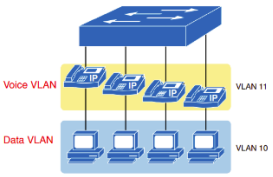
VOICE VLAN

اگر پورت سوئیچ را access کنیم فقط ترافیک یک vlan را عبور میدهد و اگر trunk کنیم pc درکی از tag زدن ندارد.

با استفاده از voice vlan میتوان voice را در کنار دیتایی که عبور میدهیم ترافیک voiceرا همزمان روی همان پورت عبور دهیم، در این حالت خاص یک پورت را میتوان Access دو تا vlan کنیم.

Pc دیتا را بدون tag به ip phone ارسال میکند و ip phone هم بدون تگ به سوئیچ ارسال میکند، سوئیچ دیتایی که بدون تگ دریافت کند متوجه میشود مربوط به PVID (port vlan id) است، اما ip phone دیتایی که برای سوئیچ ارسال میکند تگ میزند و با voice vlan tag ارسال میکند و سوئیچ متوجه میشود این دیتا مربوط به ip phone است.

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 10
SW1(config-vlan)# vlan 11
SW1(config-vlan)# interface range FastEthernet0/1 - 4
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# switchport voice vlan 11
SW1(config-if)#^Z
SW1#
```

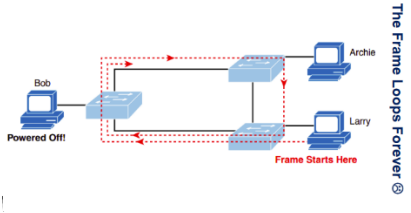



```
SW1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 11 (VLAN0011)
! The rest of the output is omitted for brevity
```

Spanning Tree Protocol (STP)

پروتکل جلوگیری از Loop در لایه دو

در طراحی شبکه داشتن یک جایگزین (Redundant) یک ویژگی محسوب می شود که در صورت از کار افتادن یک لینک اصلی از لینک جایگزین جهت جلوگیری از وقفه در جریان ترافیک استفاده شود.



ما Ethernet قابلیت تشخیص لینک جایگزین و غیرفعال کردن آن تا زمان مورد نیاز را ندارد در نتیجه باعث ایجاد Loop می شود و ترافیک Broadcast دائم در این مسیر در حال چرخش است و به مقدار آن اضافه می شود و در نهایت با پر شدن پهنای باند و درگیر شدن تجهیزات شبکه از کار می افتد که به آن Broadcast Storm گفته می شود.

مکانیزم STP:

Spanning Tree پروتکلی است که با تشخیص مسیر جایگزین یا مسیر دوم آن را تا زمانی که مورد نیاز نیست مسدود می کند.

Spanning Tree Algorithm:

1- Elect Root Bridge [RB]
2- Select Root Port Per SWH [RP]
3- Select Designated Port Per Link [DP]
4- Select Blocked Port Based on STP

الگوریتم STP:

1- [RB] نقطه شروع درخت که به آن سوئیچ ریشه گفته می شود و بقیه سوئیچ های غیر ریشه را [Non RB] می گویند.

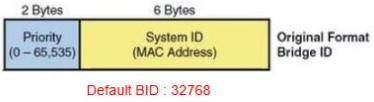
2- [RP] انتخاب یک پورت به ازای هر سوئیچ که نزدیک به RB باشد.

3- [DP] به ازای هر لینک یک ارتباطی انتخاب شود که ما را سریعتر به سوئیچ RB برساند.

4- بعد از انتخاب RB، RP و DP هر پورتی که باقی مانده باشد Block می کنیم.

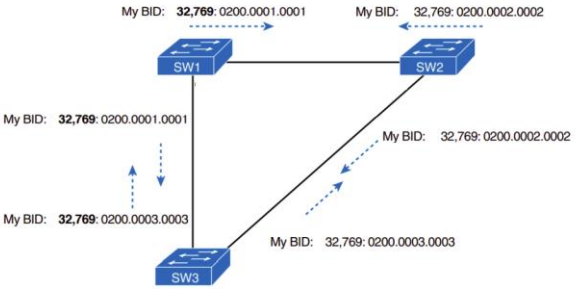
Bridge Protocol Data Units (BPDU)

سوئیچ ها زمانی که در شبکه فعال می شوند یک فریم با عنوان BPDU با بک آدرس MAC منحصر بفرد که متعلق به پورت مبدا خودشان است و یک آدرس Multicast که به عنوان MAC Address مقصد در نظر گرفته شده است در شبکه ارسال می کند.



1- Lowest BID <= Elect Root Bridge [RB]

هر سوئیچ یک شناسه دارد که بر اساس این شناسه مقایسه می شوند و سوئیچ روت انتخاب می شود. یک شناسه که اندازه آن 8 Byte = 64 bit است. هر سوئیچی که BID کمتری داشته باشد RB می شود.



نکته: با دستور show spanning-tree می توان متوجه شد کدام سوئیچ RB است.

نکته: بسته های BPDU هر 2 ثانیه یکبار ارسال می شوند و اگر بعد از 10 بار سوئیچ جواب ندهد آن سوئیچ از توپولوژی حذف می شود.

نکته: در STP بعد از انتخاب سوئیچ روت فقط RB می تواند بسته های BPDU تولید و ارسال کند، بقیه سوئیچ ها فقط امکان اصلاح و Forward به سوئیچ های دیگر را دارند.

ترافیکی که بین ارتباطات شبکه ارسال می شود	**Data Plane**
بسته های کنترلی مثل BPDU	**Control Plane**
بسته هایی مثل Telnet یا SSH	**Management Plane**

به دلیل اینکه MAC Address ثابت است و نمی توان آن را تغییر داد، با تغییر Priority به صورت دستی می توان RB را تغییر دارد:

switch (config)# spanning-tree vlan 1 priority 100

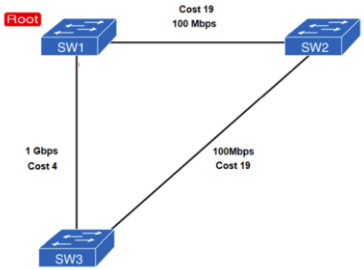
عدد 100 را اشتباه وارد کردیم و ios سیسکو مقادیر مجاز که قابل استفاده هستند را به ما نشان می دهد.

% Allowed values are: 0 4096 8192 12288 …….

2- Select Root Port per SWH [RP] <= Lowest Cost to RB

انتخاب روت پورت به ازای هر سوئیچ، هر سوئیچ باید یک پورت اصلی داشته باشد که با cost کمتر به RB برسد.

داخل BPDU که RB ارسال می کند، علاوه بر اطلاعات خودش قسمتی به نام Sender's Root Cost وجود دارد. Cost که BPDU را تولید و ارسال می کند را به بقیه اعلام می کند. زمانی که BPDU تولید و از دستگاه خارج می شود Cost محاسبه نمی شود، در واقع زمانی محاسبه می شود که وارد پورت می شود در نتیجه زمانی که RB بسته BPDU را ارسال می کند Cost آن صفر می باشدو به دست طرف مقابل که می رسد Operational Speed که دارد (سرعتی که با دستور Speed ادمین ست کرده) Cost را محاسبه می کند.



نکته: پورتی RP می شود که BPDU با Cost کمتری دریافت کند.

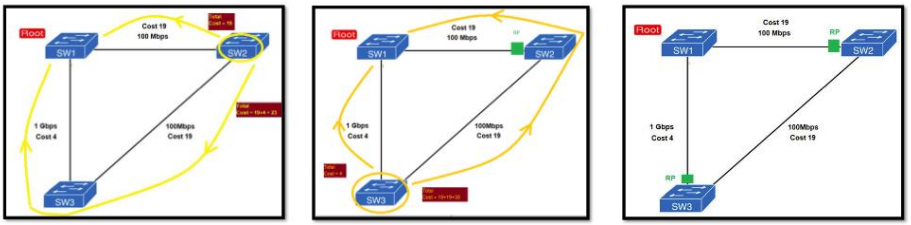
Path Cost Method

Ethernet Speed	IEEE Cost: 1998 (and Before)	IEEE Cost: 2004 (and After)
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	N/A	200
1 Tbps	N/A	20

STP/RSTP Short **MST Long**

Table 9-4 Fields in the STP Hello BPDU

Field	Description
Root bridge ID	The bridge ID of the switch the sender of this Hello currently believes to be the root switch
Sender's bridge ID	The bridge ID of the switch sending this Hello BPDU
Sender's root cost	The STP/RSTP cost between this switch and the current root
Timer values on the root switch	Includes the Hello timer, MaxAge timer, and forward delay timer

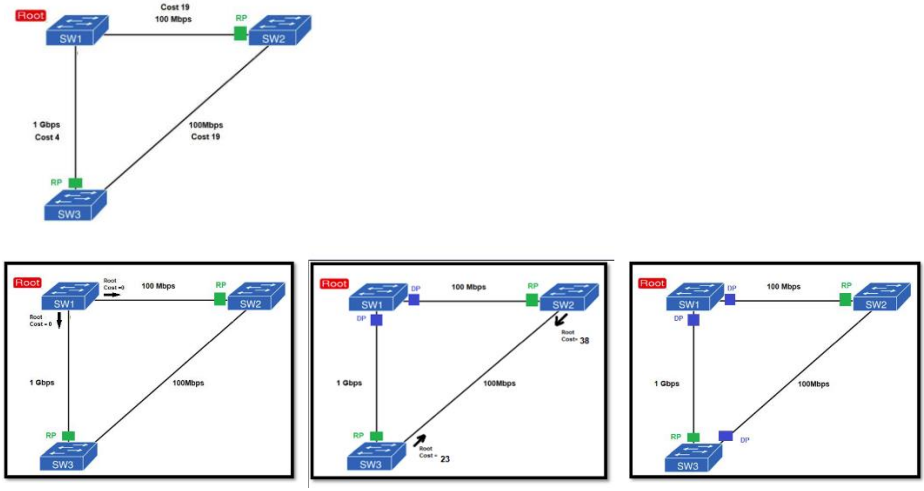


Select Designated Port per Link [DP] -3

DP پورتی است که BPDU با Cost کمتری ارسال کند.

چون RB همیشه BPDU ها را با cost صفر ارسال می کند پورت های آن DP است.

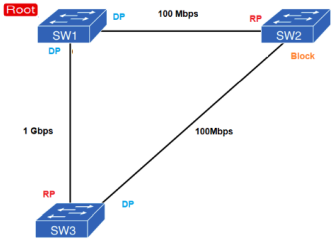
هرجا RP داشتیم روبروی آن DP است.



Select Blocked Port per based on STP -4

هر پورتی که باقی مانند BP می شود.

پورت هایی که به End Device وصل می شوند DP هستند.



پورت ها یک نقش (Role) و یک وضعیت (State) دارند که بر اساس نقشی که دارند وضعیت آنها مشخص می شود.

State: BLK نه ترافیک را عبور می دهد و نه از آن پورت MAC Learning می کند.

PORT State	
Role: RP / DP	State: FWD
Role: Block (Alternative)	State: BLK

STP Version

Traditional STP = IEEE 802.1d ieee
Rapid STP = IEEE 802.1w rstp
Multiple STP = IEEE 802.1s mst

انتخاب RB بدون وارد کردن Priority روی سوئیچ ها:

switch (config) # spanning-tree vlan 1 root secondary

تغییر DP و RP به صورت دستی: Change Cost

- Indirect: change speed under interface
- Direct: interface <> spanning-tree cost <>

STP Tie Breaker

Root Port Selection

1- Lowest cost to RB

2- Lowest sender BID -> BID = 2 Byte Priority + 6 Byte MAC (Def priority = 32768)

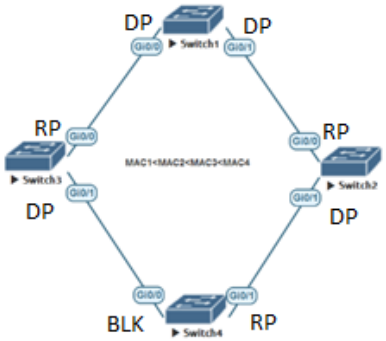
3- Lowest sender port-ID = 1 Byte Priority + 1 Byte port NUM (Def priority = 128)

4- Lowest Local port-ID

اگر جایی RP را نتوانستیم با شرط اول (دریافت BPDU با cost کمتر) انتخاب کنیم شرط دوم را بررسی می کنیم.

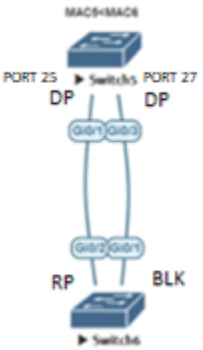
2- Lowest sender BID -> BID = Priority: MAC (def prio = 32768)

شرط دوم: پورتی RP می شود که Sender BID کمتری داشته باشد.



3- Lowest Sender port-ID-> PID: priority (1 Byte). Port NUM (Def prio = 128)

شرط سوم: پورتی RP می شود که PID (priority.port NUM) سوئیچی که BPDU را ارسال کرده کمتر باشد.



4- Lowest Local Port-ID

شرط چهارم: Local PID را مدنظر قرار می دهیم، کمترین آن RP می شود.

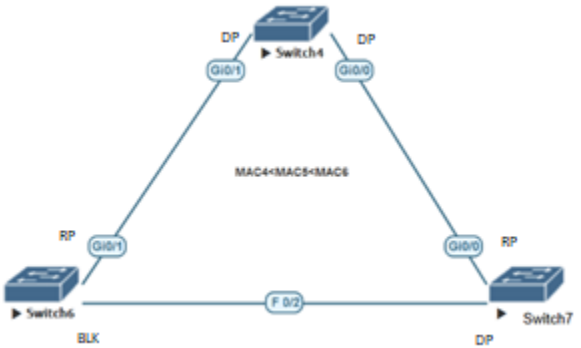
Designated Port Selection

1- Lowest Cost to RB

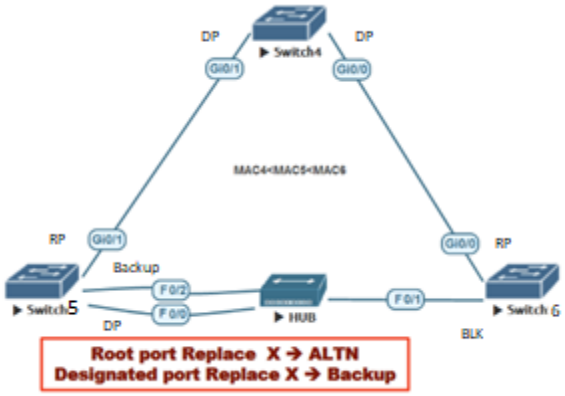
2- Lowest Sender BID-> BID = 2 Byte Priority : 6 Byte MAC (def priority = 32768)

3- Lowest Local port-ID

2-Lowest Sender BID



3-Lowest Local Port-ID



انواع پروتکل spanning tree

CST 802.1D

پیش تر در سوئیچ ها، روش پیش فرض CST یا Common Spanning Tree بوده است. در حال حاضر این ورژن مورد استفاده نیست. در این روش که استفاده از آن بیش از یک دهه کنار گذاشته شده است، یک root bridge برای تمامVLAN ها می‌شود. پس از استفاده از این روش، به سرعت مشخص گردید این روش بایستی ارتقاع داده شود و به ازای هر VLAN یک root bridge نیاز است.

PVST 802.1Q و+PVST

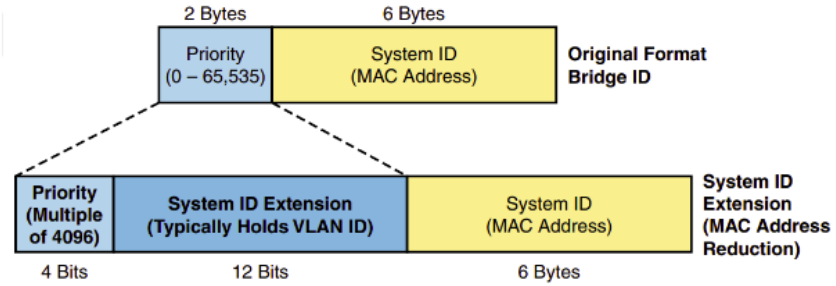
اگر به ازای هر VLAN یکبار spanning-tree را راه‌اندازی کنیم به آن PVST می‌گوییم. اگر در لینکی که encapsulation اش براساس ISL باشد، امکان اجرای CST و PVST با یکدیگر وجود ندارد. اما، +PVST بین سوئیچ‌هایی که CST را اجرا کرده و گروهی دیگر که PVST را اجرا کرده اند، امکان فهم اطلاعات بین طرفین را ایجاد می‌کند.

MST 802.1S

در روشMST ، به جای مفهوم VLAN از instance استفاده می‌کنیم و root bridge به ازای آن مشخص می‌شود. به مجموعه‌ای ازVLAN ها یک instance گفته می‌شود. علت استفاده از این روش زیاد شدن تعداد VLAN هاست که بار محاسباتی سوئیچ را بسیار زیاد خواهد کرد. به طور معمول، در شبکه‌ها، تعداد VLANها به عدد 100 نزدیک هم نمی‌شود. اما، این تعداد در شبکه هایی مانند دیتاسنترهای بزرگ، شبکه‌های زیرساختی ارائه دهنده سرویس مانند مخابرات و ...، کاملا متداول است.

Per VLAN Spanning Tree (PVST)

pvst برای هر vlan یک stp اجرا می کند و برای هر vlan یک درخت ایجاد می کندو انتخابات را برای هر vlan به صورت جداگانه انجام می دهدو به این شکل جریان ترافیک بهبود پیدا می کند. یعنی یک سوئیچ در یک vlan به عنوان RB نقش ایفا می کند و همان سوئیچ می تواند نقش یک سوئیچ معمولی را برای یک vlan دیگر ایفا کند.



Decimal Value	16-Bit Binary	Decimal Value	16-Bit Binary
0	0000.0000.0000.0000	32768	1000.0000.0000.0000
4096	0001.0000.0000.0000	36864	1001.0000.0000.0000
8192	0010.0000.0000.0000	40960	1010.0000.0000.0000
12288	0011.0000.0000.0000	45056	1011.0000.0000.0000
16384	0100.0000.0000.0000	49152	1100.0000.0000.0000
20480	0101.0000.0000.0000	53248	1101.0000.0000.0000
24576	0110.0000.0000.0000	57344	1110.0000.0000.0000
28672	0111.0000.0000.0000	61440	1111.0000.0000.0000

بعد از اینکه vlan ها را ساختیم، با این دستور vlan های ساخته شده را بررسی می کنیم:

switch# show vlan brief

بعد از اینکه پورت ها را Access آن vlan کردیم بررسی کنیم که پورت ها به درستی Access آن vlan مربوطه شده اند.

switch# show interface status

اگر interface را trunk کرده باشیم، به شرطی که طرف مقابل DTP داشته باشد و trunk شده باشد ارتباطات trunk و Allow vlan ها را به ما نشان می دهد.

switch# show interface trunk

stp که به ازای تمام vlan ها اجرا شده را نمایش می دهد:

switch# show spanning-tree

stp که به ازای vlan اجرا شده را نمایش می دهد:

switch# show spanning-tree vlan 10

switch# show spanning-tree sumary

STP topology changes : Insignificant, direct, indirec

Direct Topology Change: پورت بلاک اگر یک تغییری نسبت به سوییچی که پورت بلاک در شبکه دارد اتفاق بیوفتد (یک RP یا DP است قطع شود و پورت BLK بخواهد جایگزین آن شود) دو فاز 15 ثانیه ای را طی می کند که به آن Forward Delay phase می گویند.

نکته: در STP پورتی که FWD هست اگر نیاز باشد به پورت BLK تبدیل شود بدون تعلل انجام می گیرد چوت در غیر این صورت در شبکه Loop ایجاد می شود.

مراحل تغییر وضعیت پورت BLK به FWD (Forward Delay phase)

دو مرحله دارد (30ثانیه): مرحله اول LSN ، عمرکورد های جدول MAC Add Table 15ثانیه می گذرد و بعد از 15 ثانیه جدول MAC پاک می شود. بعد از 15ثانیه LSN وارد مرحله Learning می شود15 ثانیه صبر می کند تا MAC Address های جدید را از پورت های جدید یاد بگیرد و ترافیک FWD شود.

Indirect Topology Change: در صورتی که تغییراتی روی سوییچی که پورت بلاک ندارد اتفاق بیوفتد. در indirect علاوه بر مدت زمان 30 ثانیه مدت زمان دیگری هم صرف می شود و بیش از 30 ثانیه قطعی خواهیم داشت.

Max Age Time به اندازه 20 ثانیه صبر می کندکه مطمئن شود قطعی که در شبکه اتفاق افتاده و قطعی لحظه ای نباشد.

Max Age Time+Listening+ Learning+BPDU=52Sec

STP State \ Action	RCV BPDU	SND BPDU	LRN MAC	FWD MAC
Disable	N	N	N	N
Block	Y	N	N	N
Listening	Y	Y	N	N
Learning	Y	Y	Y	N
Forward	Y	Y	Y	Y

Disable: BPDU دریافت و ارسال نمی کند، MAC Learn نمی کند و ترافیک فوروارد نمی کند.

Block: BPDU دریافت می کند، چون باید متوجه تغییرات شبکه باشد اما BPDU ارسال نمی کند، MAC Learn نمی کند و ترافیک فوروارد نمی کند.

Listening: BPDU دریافت و ارسال می کند اما MAC Learn نمی کند و ترافیک فوروارد نمی کند.

Leraning: BPDU دریافت و ارسال می کند، MAC Learn می کند اما ترافیک فوروارد نمی کند چون درحال یادگیری مک آدرس هست.

Forward: BPDU دریافت و ارسال می کند، MAC Learn می کند و ترافیک را ارسال می کند.

Insignificant Topology Change

تشخیص تغییرات بی اهمیت در توپولوژی شبکه .هر کامپیوتری که در شبکه روشن و یا خاموش می شود و یا هر لینکی که از هر کامپیوتر قطع و یا وصل می شود منجر به UP و DOWN شدن یکی از پورتهای سوئیچ می شود. سوئیچ تغییر مورد نظر را از نوع DIRECT تشخیص می دهد و وارد پروسه همگرایی STP می شود. این در حالی است که End user ها در ایجاد LOOP نقشی ندارند زیرا لینک های REDUNDANT بین سوئیچ ها وجود دارند و همان ها سبب ایجاد LOOP خواهند شد که باید در پروتکل STP لحاظ شوند. پروتکل STP تغییرات پورتهای ACCESS (متصل به End user ها) را نادیده می گیرد و وارد پروسه همگرایی نمی شود البته باید توجه کرد که با فعال کردن ویژگی PORTFAST روی پورت های ACCESS ، پروتکل STP ، تغییرات ایجاد شده روی پورتهای PORTFAST را از دسته بندی بی اهمیت خارج می کند و آنجا تغییرات این پورت بسیار مهم می شود چرا که اگر BPDU ای روی آن پورت ها دریافت شود باعث ایجاد LOOP خواهد شد.

ممکن است اتفاقی یکی از پورت های سوییچ قطع شود (دستمان اتفاقی به Patch cord خورد و کانکتور آن شل بوده) و بعد بلافاصله آن را وصل کنیم. روی سوییچ پورت بلاک برای اینکه به فوروارد تغییر وضعیت پیدا کند حداقل 30 ثانیه طول می کشد. همه پورت های در مرحله اول پس از روشن شدن بلاک هستند که بعد از آن DP می شوند و یا بلاک باقی می مانند. بعد از هرقطعی و وصل شدن الگوریتم STP در کل شبکه مجدد اجرا می شود و این شرایط ایده آل نیست زیرا پهنای باند و دستگاه را درگیر می کند.

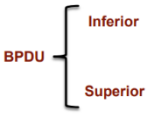
PortFast

ویژگی اختصاصی سیسکو برای بهبود سرعت تبادل اطلاعات در STP می باشد که باعث می شود Forward Delay phase را روی پورتی که به End Device متصل شده را حذف کنیم. پورت بدون گذشتن از وضعیت های مختلف به طور مستقیم در حالت Forwarding قرار می گیرد.

```
Switch(config)# int fa 0/3
Switch(config)# spanning-tree portfast
```

این قابلیت را فقط می توان روی اینترفیس های Non Trunk فعال کنیم و پورت اگر به دستگاه لایه 2 مثل سوییچ یا بریج وصل باشد و BPDU ارسال کند و BPDU که ارسال می کند شرایط بهتری داشته باشد اصطلاحا BPDU Superior ارسال کند و آن سوییچ RB شود (Mac یا priority پایین تری داشته باشد) خطرناک هست چون توپولوژی کل شبکه را تغییر می دهد و تمام ترافیک سمت آن ارسال می شود و کل شبکه قطع می شود.

به همین راحتی به همین سادگی شبکه یک Provider قطع میشه 😊



BPDU Guard

زمانی که BPDU Guard را فعال می کنیم اگر روی پورت سوئیچ BPDU دریافت شود ارسال روی این پورت متوقف می شود و پورت غیرفعال می شود. کاربرهای نهایی که به پورت های سوئیچ متصل هستند نباید روی این پورت BPDU ارسال کنند. این تنظیمات باید روی پورت های access که به دستگاه های نهایی متصل هستند اعمال شود و از اتصال سوئیچ غیر مجاز به شبکه جلوگیری می کند. با اینکار می توان جلوی تغییر در توپولوژی STP را گرفت.

مثال زیر نحوه اعمال BPDU Guard را نمایش می دهد.

SW(config)#interface fastethernet 0/2

SW(config-if)#spanning-tree bpduguard enable

درمحیط گلوبال با اجرای این دستور بجای اینکه روی هر پورت جداگانه بزنیم بصورت پیشفرض روی همه پورت های فعال می شود وبعد روی پورت هایی که نمی خواهیم BPDU Guard فعال باشد بجای enable باید disable بنویسیم.

SW(config)#spanning-tree portfast bpduguard default

نکته: چرا پروتکل STP خاص SWITCHING است و چرا از بین 3 لینک سوئیچ ، یکی از پورت ها در یکی از لینک ها باید بلاک شود در حالی که در روتینگ ما مشکل LOOP را نداریم و می توانیم بین روتر هایمان مسیرهای متفاوتی داشته باشیم ؟ روتر ها مانع از عبور بسته های broadcast می شوند در حالی که ماهیت سوئیچ ها متفاوت از روتر است و اصلا" آن ها از طریق همین بسته های broadcast مانند ARP جدول مک خود را کامل می کنند.

نمایش پورتی که err-disable شده و علت آن را به ما نمایش می دهد (روی packet tracer نمایش نمی دهد.)

Switch# show interface status err-disable

برای اینکه از وضعیت err-disable خارج شود یکبار باید پورت را خاموش و روشن کنیم. یک مکانیزم دیگر هست که سوییچ بررسی می کند که اگر مشکل حل شده باشد پورت را روشن کند که به آن err-recovery می گویند که بصورت پیشفرض فعال نیست، اما err-disable فعال هست.

Bridge Protocol Data Units(BPDU)

این Frame اظهار وجود یک سویچ در شبکه است که خودش را به سویچ های دیگر شبکه معرفی می کند و اطلاعاتی در خصوص پورت ها ، آدرس ها و ... ای که در اختیار دارد را در اختیار سایر سویچ ها قرار می دهد. اگر هر تغییری در شبکه در لایه دو انجام شود ، مثلا زمانیکه یکی از لینک ها down می شود و یا یک لینک جدید اضافه می شود یا یک سویچ جدید اضافه می شود و در نهایت یکی از سویچ های شبکه fail می شود ، سویچ های لایه دو با استفاده از Frame های BPDU همدیگر را از به وجود آمدن چنین شرایطی آگاه می کنند ، با استفاده از این اطلاعات جدید الگوریتم STP مجددا شروع به کار و اجرا می کند و توپولوژی جدید بدون Loop را ایجاد می کند. STP و BPDU به سریعتر شدن فرآیند Convergence در مسیریابی بین شبکه ای بسیار کمک می کنند.

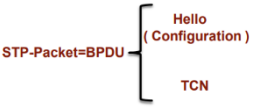
Convergence در واقع مدت زمانی است که شبکه باید تغییرات جدید را تجزیه و تحلیل و تغییرات جدید را اعمال و اجرایی کند. Frame های BPDU در شبکه بصورت پیشفرض هر 2 ثانیه یکبار در شبکه پخش می شوند و این موضوع باعث می شود که سرعت پیدا کردن مشکلات شبکه و Loop ها به حداقل برسد. به فرآیند ایجاد و ارسال کردن Frame های BPDU در اصطلاح فنی BPDU Advertisement گفته می شود ، بصورت کلی سه نوع BPDU در سویچ ها ایجاد می شود که به شکل زیر هستند :

Configuration BPDU :در پروتکل STP برای اطلاع رسانی به سویچ های شبکه استفاده می شود.

TCN BPDU (Topology Change Notification) :در خصوص تغییرات توپولوژی شبکه اطلاع رسانی می کند.

TCA BPDU (Topology Change Acknowledgement): تایید دریافت TCN BPDU است.

در پیام ها یا Frame های BPDU ارسال توسط سویچ ها اطلاعاتی از قبیل پورت ها ، آدرس ها ، اولویت ها و Cost های هر سویچ ارسال می شود. دقت کنید که همیشه هم فعال بودن BPDU در شبکه خوب نیست ، اما ما باید تمهیدات امنیتی مربوط به BPDU را نیز در نظر نداشته باشیم ، یکی از تمهیدات امنیتی که برای امن کردن BPDU و همچنین جلوگیری از اضافه شده سویچ های غیر مجاز در شبکه استفاده می شود مکانیزمی به نام BPDU Guard است.



Spanning Tree Protocols						
	Legacy STP	**PVST**	**PVST+**	**RSTP**	**RPVST+**	**MST**
Algorithm	Legacy ST	Legacy ST	Legacy ST	Rapid ST	Rapid ST	Rapid ST
Defined By	802.1D-1998	Cisco	Cisco	802.1w, 802.1D-2004	Cisco	802.1s, 802.1Q-2003
Instances	1	Per VLAN	Per VLAN	1	Per VLAN	Configurable
Trunking	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL	802.1Q, ISL

Name	Based on STP or RSTP?	# Trees	Original IEEE Standard	Config Parameter
STP	STP	1 (CST)	802.1D	N/A
PVST+	STP	1/VLAN	802.1D	pvst
RSTP	RSTP	1 (CST)	802.1w	N/A
Rapid PVST+	RSTP	1/VLAN	802.1w	rapid-pvst
MSTP	RSTP	1 or more*	802.1s	mst

To manage insignificant network changes

==========

Switch(config-if)# spanning-tree portfast
OR
Switch(config)#spanning-tree portfast default

Switch(config-if)#spanning-tree bpdugaurd enable
OR
Switch(config)#spanning-tree portfast bpdugaurd default

An easier way to select a RB Primary and secondary

==========

Switch(config)#spanning-tree vlan <> root primary ➔ Pri=24576
Switch(config)#spanning-tree vlan <> root secondary ➔ Pri=286702
Recommended for Networks that other switchs have default Pri.

To change STP Cost manually per VLAN

==========

Switch(config-if)#spanning-tree vlan <> cost <>
Switch(config-if)#spanning-tree path-cost <short-long>

To change STP Priority manually

==========

Switch(config-if)#spanning-tree vlan <> port-priority <>

To change STP mode

==========

Switch(config)#spanning-tree mode [pvst I rapid-pvst I mst]

Show STP Command

==========

Switch#show spanning-tree
Switch#show spanning-tree summary
Switch#show spanning-tree interface <> [detail I cost I priority]
Switch#show spanning-tree

Rapid Spanning Tree Protocol(RSTP)

همانطور که گفته شد به صورت کلی در پروتکل Spanning Tree زمانی بین 30 تا 50 ثانیه طول میکشد تا convergence در شبکه صورت گیرد، مخصوصا زمانی که تغییر کوچکی در ساختار شبکه رخ میدهد می بایست این زمان سپری شود تا مجددا کل شبکه با پروتکل stp همگرا شود.

این زمان زمان بسیار زیادی است و جهت برطرف کردن این مشکل Rapid stp بر اساس استاندارد IEEE 802.1W بوجود آمد تا زمان convergence را به 6 ثانیه برساند!

انواع وضیعت RSTP تا رسیدن به وضعیت مطلوب پورت

در STP پنج وضعیت disabled , blocking , listening , learning و forwarding داشتیم ولی در RSTP سه وضعیت زیر را داریم:

Discarding : فقط BPDU دریافت می کند

این وضعیت در RSTP در واقع ترکیبی است از سه وضعیت disabled , blocking , listening در STP ، در این وضعیت frame ها Drop می شوند و هیچ Mac address ای Learn نمی شود و به دلیل سرعت بالای پروتکل RSTP وضعیت listening احساس نیاز نشده و پورت سریعا به حالت negotiate در میاید.

Learning: علاوه بر دریافت BPDU ، ارسال BPDU را انجام می دهد و جدول MAC را نیز بروز می کند.

در این وضعیت frame ها drop میشوند ولی mac address ها را در سوئیچ نگهداری میکند یا به اصطلاح learn میشوند.

Forwarding: در این حالت سوئیچ فعالیت طبیعی خودش را انجام میدهد و frame های ورودی بر اساس mac address هایی که در سوئیچ learn شده اند ، فرستاده می شوند.

در جدول زیر وضعیت RSTP با CST مقایسه شده است:

Classic Spanning-Tree	Rapid Spanning-Tree	Port active in topology?	Learns MAC addresses?
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

نقش های پورت در RSTP

Root port :پورتی که از طریق آن با کمترین Cost به Root Bridge می رسیم.

Designated port :پورتی که می تواند یک سوییچ دیگر را با کمترین Cost به Root Bridge برساند.

Alternate port :پورت Backup برایRoot port

Backup port :پورت Backup برایDesignated port

Disabled port : پورت غیرفعال که در Spanning Tree استفاده نمی شود

Edge port : پورتی که به End User متصل است

عملکرد BPDU ها در RSTP

برای سازگاری بیشتر پروتکل RSTP با STP همچنان BPDU ها بر اساس استاندارد D802.1 فرستاده می شوند. BPDU ها هر 2 ثانیه یکبار برای همسایه ها از طریق تمام پورت ها ارسال میشود و زمانی که به اندازه 3 پکت BPDU جوابی از همسایه مورد نظر دریافت نگردد پورت در نظر میگیرد که همسایه ای وجود ندارد و پورت به وضعیت learning میرود.

RSTP Convergence

Convergence به مرحله ای گفته میشود که در لحظه اول تمامی سوئیچ ها خودشان را root switch در نظر میگیرند و شروع به ارسال BPDU می کنند، پس از ارسال و دریافت BPDU ها از سوئیچ های دیگر root switch در شبکه انتخاب می شود و دیگر هیچ سوییچی BPDU ارسال نمی کند مگر سوییچ root.

در واقع Convergence دو مرحله دارد:

انتخاب سوئیچ root یا همانRoot Bridge

انتخاب وضعیت پورت یعنی همان Backup port , Alternate port , Designated port , root port

Port Types (انواع پورتها)

Edge port :همان طور که از نام پورت پیداست، منظور پورتهایی هستند که به هاست ها یا PC ها در شبکه متصل هستند و در واقع لبه شبکه را تشکیل می دهند. برای جلوگیری از ارسال BPDU ها Port fast را فعال می کنیم ، BPDU Gaurdو Loop Guard را نیز انتخاب می کنیم.

Root port :پورتی از یک سوئیچ سیسکو که جهت برقراری ارتباط با root bridge مورد استفاده قرار میگیرد را root port می نامند. درواقع برای برقراری ارتباط با root bridge تنها از یک مسیر استفاده میشود و انتخاب root port مناسب به cost مسیرهای موجود برای دستیابی به root bridge بستگی دارد.

Point-to-point port: برای اتصال دو سوئیچ به یکدیگر استفاده میشود، زمانی که دو سوئیچ به صورت مستقیم به یکدیگر متصل هستند در نظر گرفته میشود که پورت ها به صورت Full duplex با یکدیگر negotiate کنند ، اگر وضعیت Half duplex باشد بدین معنی است که بیت دو سوییچ device های دیگری هم وجود دارد (در حالت half duplex دیگر پورتها را Point to point نمی نامیم)

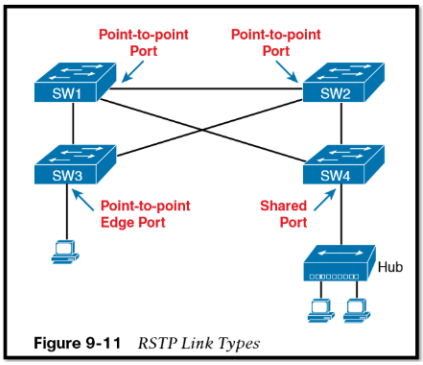


Figure 9-11 *RSTP Link Types*

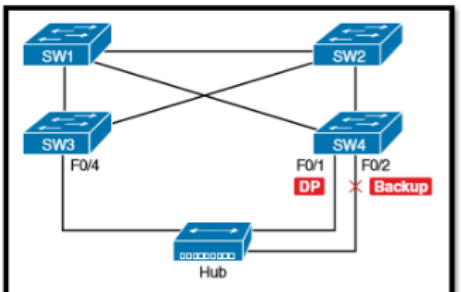


Figure 9-10 *RSTP Backup Port Example*

تنظیمات RSTP

برای فعال کردن RSTP بر روی یک پورت که نقش Edge Port را در شبکه ایفا می کند می بایست از دستور زیر استفاده کنید:

Switch(config-if)# spanning-tree portfast

برای فعال کردن RSTP بر روی یک پورت که نقش Point to Point را دارد و قرار است با سوئیچ مجاور به صورت Full Duplexکار کند ، از دستور زیر استفاده میکنیم:

Switch(config-if)# spanning-tree link-type point-to-point

تنظیمات Rapid Per-Valan spanning tree protocol یا RP+

برای فعال کردن RPVST بر روی کل سوییچ سیسکو از دستور زیر استفاده کنید:

Switch(config)#spanning-tree mode rapid-pvst

برای برگشتن به حالت پیش فرض PVST از دستور زیر استفاده میکنیم:

Switch(config)# spanning-tree mode pvst

در حالتی که RPVST سوئیچ شما PVST را هم ساپورت میکند، در واقع شما هم stp که بر مبنای IEEE 802.1D است را ساپورت میکنید و هم RSTP را که به صورت ایده آل برای سوییچ فعال میباشد.

عیب یابی پروتکل RSTP

برای عیب یابی و بررسی وضعیت rstp از دستور زیر استفاده میکنیم:

Switch# show spanningtree vlan vlan-id

MST- Multiple Spanning Tree

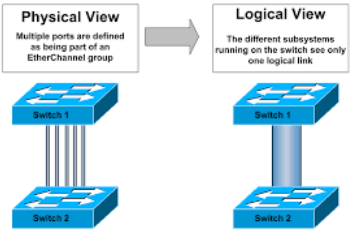
زمانی تعداد VLAN خیلی زیاد باشند و ما از PVST یا Per-VLAN RSTP استفاده کرده باشیم برای هر VLAN نیاز به محاسبه جداگانه دارد که باعث مصرف زیاد CPU و RAM می شود. برای برطرف کردن این مشکل ما از MST استفاده می کنیم به این صورت که VLAN های که قرار است Root Bridge یکسانی داشته باشند را در یک instance قرار می دهیم به طور مثال vlan های 11 تا 20 را در 1 instance و 21 تا 30 را در 2 instance قرار می دهیم.

نکته : امکان ساخت حداکثر 16 تا instance وجود دارد.

نکته: MST که فعال شود 0 instance ایجاد می شود و تمام vlan ها به صورت پیش فرض عضو این instance می شوند.

نکته : به کلیه سوئیچ هایی که MST را اجرا کنند و در یک ناحیه قرار بگیرند به اصطلاح MST Region گفته می شود.

Ether Channel



به وسیله EtherChannels می توانیم چندین خط فیزیکی را با هم ادغام و به یک خط منطقی تبدیل کنیم. به طور معمول Spanning Tree لینک های جایگزین را مسدود می کند اما EtherChannels قابلیت Load Balancing را بدون مسدود کردن پورت ها برای ما ایجاد می کند.

یک نمونه از کاربردEtherChannel

فرض کنید یک شرکت دارای دو سوییچ است که از طریق یک پورت Fast Ethernet به یکدیگر متصل شده اند بعد از مدتی این شرکت گسترش پیدا می کند و دیگر لینک Fast Ethernet جوابگوی نیاز انها نخواهد بود اگر یک پورت Fast Ethernet دیگر را بین این دو سوییچ متصل کنیم پروتکل Spanning Tree برای جلوگیری از ایجاد Loop در شبکه یکی از این دو پورت را Block می کند یکی از راه حل ها ، خرید یک سوییچ دارای پورت Gigabit Ethernet است که اینکار مقرون به صرفه نیست راه حل منطقی استفاده از EtherChannel است تنها موردی که در استفاده از این تکنولوژی باید در نظر گرفت داشتن پورت های آزاد است. ترافیک براساس MAC Address یا IP Address یا Port Address مبدا یا مقصد بین لینک ها تقسیم می شود. و از طریق Config Mode قابل تنظیم است.

Switch(config)#port-channel load-balance {dst-ip|Srt-ip|dst-mac|srt-mac| src-dst-ip| dst-dst-ip}

ایجاد EtherChannel

حداکثر تعداد پورت هایی که می توان به EtherChannel اضافه کرد 8 تا می باشد. یعنی حداکثر پهنای باندی که ما می توانیم به ان دست پیدا کنیم در Fast Ethernet پهنای باند 800 Mbps، در Gigabit Ethernet پهنای باند 8 Gbpsو در Ten Gigabit Ethernet پهنای باند 80 Gbpsخواهد بود.

همه پورت ها باید دارای سرعت و Duplex یکسان باشند.

همه پورت ها انتخابی باید فعال باشند.

در صورت استفاده از EtherChannel در لایه سوم ، IP را تنها به پورت منطقی اختصاص دهید نه به پورت های فیزیکی به صورت تک.

همه پورت های EtherChannel را در یک VLAN قرار دهید، یا همه را در حالت Trunk قرار دهید. اگر حالت Trunkرا انتخاب کردید باید توانایی حملVLAN های یکسان را داشته باشند و از یک حالت ترانک استفاده شود.

تنظیماتی که روی Prot Channel اعمال می کنیم روی تمام پورت ها مربوطه تاثیر می گذارد ولی تنظیماتی که شما به یک اینترفیس فیزیکی اعمال می کنید تنها روی همان اینترفیس تاثیر می گذارد.

پروتکل مورد استفاده در دو سمت لینک باید یکی باشد.

نکته : نحوه تقسیم ترافیک بین پورت ها در EtherChannel به تعداد پورت ها بستگی دارد و قابل تغییر نیست برای تقسیم مساوی ترافیک بهتر است تعداد لینک 2 ، 4 یا 8 تا باشد در جدول زیر این مقادیر نشان داده شده است.

Number of Ports in the EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

پروتکل های قابل استفاده برای EtherChannel

PAgP-Port Aggregation Protocol : پروتکل اختصاصی سیسکو است که به صورت dynamic با سمت مقابل برای ایجاد Channel مذاکره می کند و دارای سه حالت زیر است:

On : در این حالت برای ایجاد Channel مذاکره نمی کند و برای ایجاد Channel باید طرف مقابل نیز در حالت onباشد.

Auto : مذاکره برای ایجاد Channel را با طرف مقابل شروع نمی کند ولی در صورت دریافت پیام PAgP به آن پاسخ می دهد. در صورتی Channel ایجاد می شود که طرف مقابل در حالت Desirable باشد.

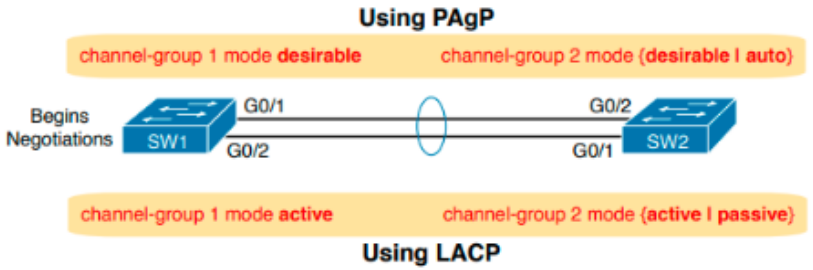
Desirable : به صورت فعال شروع به مذاکره با طرف مقابل برای ایجاد Channel می کند و در صورتی که طرف مقابل در حالت Auto یا Desirable باشد Channel تشکیل خواهد شد.

LACP-Link Aggregation Control Protocol: پروتکل استاندارد و عمومی می باشد که مشابه PAgP می باشد و دارای سه حالت زیر است:

On : در این حالت برای ایجاد Channel مذاکره نمی کند و برای ایجاد Channel باید طرف مقابل نیز در حالت on باشد.

Passive : مذاکره برای ایجاد Channel را با طرف مقابل شروع نمی کند ولی در صورت دریافت پیام PAgP به آن پاسخ می دهد. در صورتی Channel ایجاد می شود که طرف مقابل در حالت Active باشد.

Active : به صورت فعال شروع به مذاکره با طرف مقابل برای ایجاد Channel می کند و در صورتی که طرف مقابل در حالت Active یا Passive باشد Channel تشکیل خواهد شد.



LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

Static Persistance

	On
On	Yes

Port Aggregation Control Protocol

- CISCO Prop.
- Auto / Desirable
- Auto Not send , just accept
- Desirable Send and Accept
- Max 8 port

Link Aggregation Control Protocol

- IEEE 802.3ad
- Passive / Active
- Passive Not send , just accept
- Active Send and Accept
- Max 16 port but 8 port active

Layer 2 EtherChannel

```
Switch(config)#interface port-channel 1
Switch(config-if)#exit
Switch(config)#interface range fast 0/1-2
Switch(config-if-range)#channel-group 1 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
```

```
Switch(config)#int range fastEthernet 0/1-2
Switch(config-if-range)#channel-protocol ?
  lacp  Prepare interface for LACP protocol
  pagp  Prepare interface for PAgP protocol
```

```
SW1# show etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)           -        Fa0/14(P) Fa0/15(P)
```

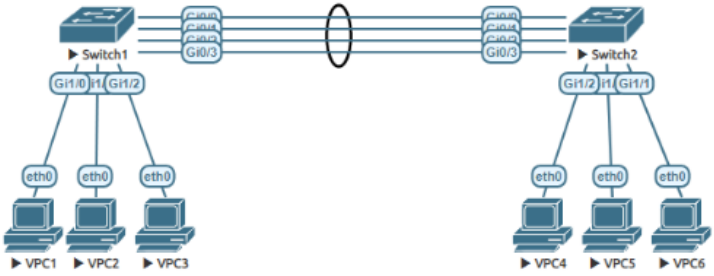
```
SW1# show spanning-tree vlan 3

VLAN0003
 Spanning tree enabled protocol ieee
 Root ID     Priority    28675
             Address     0019.e859.5380
             Cost        12
             Port        72 (Port-channel1)
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID   Priority    28675 (priority 28672 sys-id-ext 3)
             Address     0019.e86a.6f80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Po1                 Root FWD 12        128.64   P2p Peer(STP)
```

EtherChannel Load Distribution

```
SW1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source MAC address
  IPv4: Source MAC address
  IPv6: Source MAC address

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1111
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1112
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1113
Would select Gi1/0/22 of Po1
```

Configuration Keyword	Math Uses...	Layer
src-mac	Source MAC address	2
dst-mac	Destination MAC address	2
src-dst-mac	Both source and destination MAC	2
src-ip	Source IP address	3
dst-ip	Destination IP address	3
src-dst-ip	Both source and destination IP	3
src-port	Source TCP or UDP port	4
dst-port	Destination TCP or UDP port	4
src-dst-port	Both source and destination TCP or UDP port	4

```
SWH(config)# port-channel load-balance <>
```



MAC1 1111.1111.1111
MAC2 2222.2222.2222
MAC3 3333.3333.3333
MAC4 4444.4444.4444
MAC5 5555.5555.5555
MAC6 6666.6666.6666

Layer 3 EtherChannel


```
switch(config)# interface TYPE MOD/NUM
switch(config-if)# no switchport
switch(config-if)# ip address A.B.C.D  E.F.G.H

sw1(config)# interface gi0/1
sw1(config-if)# no switchport
sw1(config-if)# ip address 192.168.1.1 255.255.255.0

sw2(config)# interface gi0/1
sw2(config-if)# no switchport
sw2(config-if)# ip address 192.168.1.2 255.255.255.0
```

Routing-Protocol

```
switch(config)# interface TYPE MOD/NUM
switch(config-if)# no switchport

Manual/PAgP/LACP

switch(config-if)# channel-group GRP_NUM mode on
switch(config-if)# ip address A.B.C.D E.F.G.H
```

پیکربندی EtherChannel

به طور ساده اگر بخواهیم نحوه تنظیم EtherChannel را عنوان کنیم به این صورت است که شما باید یک اینترفیس منطقی ایجاد و اینترفیس های فیزیکی مد نظر را به ان اضافه کنید. برای ایجاد Port Channel از دستور زیر استفاده می کنیم:

Switch(config)#interface port-channel 1

برای ایجاد EtherChannel لایه سه از دستور زیر استفاده می کنیم:

Switch(Config-if)#no switchport

Switch(Config-if)#ip address 192.168.1.1 255.255.255.0

برای اضافه کردن پورت های مورد نظر از دستور زیر استفاده می کنیم:

Switch(Config)#interface fast 0/1

Switch(Config-if)#channel-protocol pagp

Switch(Config-if)#channel-group 1 mode auto

جهت دیدن وضعیت EtherChannel از دستورات زیر استفاده کنید.

Switch#show etherchannel

Switch#show etherchannel summary

Switch#show etherchannel load-balance

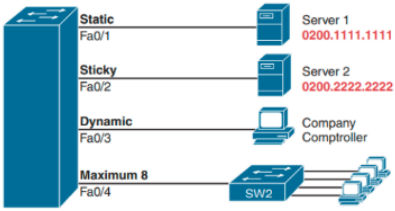
Port Security

Port Security یک قابلیت و امکان امنیتی است که به ما کمک می کند در لایه دو کنترل مناسبی داشته باشیم و بتوانیم جلوی بسیاری از حملات را بگیریم. Port Security کنترل می کند که چند MAC address روی یک پورت اجازه استفاده دارند. بر اساس طراحی سه لایه ای سیسکو دسترسی ها از طریق لایه Access ایجاد می شود که عمده مشکلات امنیتی به دلیل عدم کنترل این دسترسی ها صورت می پذیرد.

برای جلوگیری از اینکه کاربر دستگاه های مختلف را به سوئیچ وصل کند می توان از port security استفاده کرد و براساس MAC address این محدودیت برای هر پورت اعمال کرد. همچنین port security می تواند شبکه را در برابر نرم افزارهای مخرب که می توانند هزاران فریم را در شبکه با MAC Address های متفاوت ارسال کنند محافظت کند. با اینکار مهاجم با استفاده از این نرم افزار مخرب جدول MAC سوئیچ را تحت تاثیر خود قرار می دهد ، جدول MAC سوئیچ دارای ظرفیت محدودی است و این ظرفیت با MAC address های جعلی پر می شود.

در نتیجه MAC address های درست سایر تجهیزات نمی تواند در این جدول قرار بگیرد و زمانی که یک فریم به دست سوئیچ می رسد نمی تواند پورت خروجی برای مقصد فریم را پیدا کند و مجبور می شود این فریم را روی تمام پورت های خود ارسال کند و در اینجا مهاجم می تواند با Sniff کردن بسته ها به اطلاعات تمام دستگاه ها دسترسی پیدا کند. این حمله به عنوان CAM table overflow یا MAC Flooding Attack شناخته می شود. همچنین Port security می تواند از DHCP server محافظت کند. یک مهاجم با ارسال هزاران درخواست DHCP با MAC address متفاوت می تواند DHCP pool را خالی کند و سرویس دهی DHCP server را مختل کند و DHCP server دیگر نتواند به سایر دستگاه ها IP اختصاص دهد ، به این حمله DHCP starvation گفته می شود.

با فعال کردن Port Security روی یک پورت به صورت پیش فرض یک MAC address می تواند از آن استفاده کند که می توان این MAC address را به صورت دستی یا sticky برای پورت مشخص کرد البته می توان با استفاده از دستور maximum تعداد را افزایش داد. اگر تعداد MAC address های مورد استفاده از پورت ، بیشتر از مقدار مشخص شده بیشتر شود یا MAC address غیر از MAC address مجاز از پورت استفاده کند اقدامی که برای مقابله آن درنظر گرفته شده است به صورت پیش فرض shutdown است که باعث خاموش شدن و در حالت err-disable قرار گرفتن پورت می شود. البته می توان بجای shutdown از حالت های دیگر مثل Protect یا restrict استفاده کرد. در حالت protect پورت را خاموش نمی کند و اجازه عبور را به فریم های مربوط به MAC address های غیر مجاز را نمی دهد. Restrict عملکرد مشابه protect دارد با این تفاوت که log نیز تولید می کند.



Should be configured Interface as a trunk or access

SWH(config)# interface TYPE MOD/NUM

SWH(config-if)# switchport port-security
By Def.=Disable

SWH(config-if)# switchport port-security maximum <MAX number>
By Def.=1

SWH(config-if)# switchport port-security mac-address <MAC ADDRESS | Sticky >
If don't set will work Dynamic

SWH(config-if)# switchport port-security violation {shutdown | restrict | protect }
By Def.=shutdown

نحوه اجرای port security در مثال زیر نمایش داده شده است :

```
SW(config)#interface fastethernet 0/1
SW(config-if)#switchport port-security
SW(config-if)#switchport port-security maximum 3
SW(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac-address sticky
```

همچنین از دستورات زیر برای بررسی وضعیت port security می توان استفاده کرد :

```
SW#show port-security
```

مشاهده جدول port-security address table که از چه Vlan ای چه Mac address ای را چگونه از روی چه پورتی یاد گرفته است.

SW#show port-security address
SW# show port-security interface fa0/1

نکته : حالت Shutdown پیش فرض می باشد.

Protect در این حالت ترافیک مربوط به دستگاه غیر مجاز Drop می شود.

Restrict همانند حالت قبل ترافیک مربوط به دستگاه غیر مجاز Drop می شود و علاوه بر این Log نیز تولید می کند.

ShutDown سخت گیرانه ترین حالت می باشد که با دریافت ترافیک غیرمجاز پورت مربوطه در حالت Err-Disable قرار می گیرد و پورت خاموش می شود و برای خارج کردن آن از این حالت باید وارد تنظیمات سوئیچ شد و پورت مورد نظر را خاموش و روشن کرد.

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

نکته : پورت نباید Dynamic port باشد ، باید حتما Access باشد.

نحوه فعال کردن Port Security

اولین کار قرار دادن پورت در حالت Access است:

Switch(config)#interface fastethernet 0/1

Switch(config-if)#switchport mode access

بعد باید این قابلیت را فعال کنیم:

Switch(config-if)#switchport port-security

سپس MAC آدرس های مجاز را تعیین می کنیم که به دو صورت امکان پذیر است :

بصورت دستی:

Switch(config-if)#switchport port-security mac-address AD49.FB36.3596

استفاده از ویژگی Sticky :

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

نکته : در حالت sticky نیاز به وارد کردن MAC ادرس نیست و سوئیچ MAC ادرس را از روی اولین بسته دریافتی برمیدارد.

تعیین یکی از سه حالت موجود :

Switch(config-if)#switchport port-security violation portect

تعیین تعداد دستگاه های مجاز جهت استفاده از پورت:

Switch(config-if)#switchport port-security maximum 2

نکته : پیش فرض مقدار یک است و تا 132 می توان آن را مقداردهی کرد.

Port Security T-shoot

جهت مشاهده و بررسی تنظیمات از دستورات زیر استفاده می کنیم:

Switch#show port-security

Switch#show port-security address

show mac address-table **show port- security** **show port- security interface TYPE MOD/NUM** **show mac address-table secure** **show interface status err-disable** **Clear port-security**

errdisable recovery cause psecure-violation	Global command that enables the automatic recovery from err-disabled state for ports that reach that state due to port security violations
errdisable recovery interval *seconds*	Global command that sets the delay, in seconds, before a switch attempts to recover an interface in err-disabled mode, regardless of the reason for that interface being in that state
shutdown **no shutdown**	Interface subcommands that administratively disable and enable an interface, respectively

نکته : در صورتی که بخواهیم MAC آدرس هایی که از طریق Sticky آنها را پیدا کرده ایم را حذف کنیم از دستورات زیر استفاده می کنیم:

Switch#clear port-security all

Switch#clear port-security sticky interface fastEthernet 0/1

تنظیمات Port Security

با استفاده از Port Security در واقع ما به سویچ می گوییم که فقط اتصلات را از MAC Address هایی که ما تعیین می کنیم بپذیر. در نتیجه این کار، در صورتی که فرد مهاجم بتواند به تجهیزات شبکه داخلی ما دسترسی داشته باشد باز هم نمی تواند وارد شبکه داخلی ما شود. در حالت کلی Port Security در سه حالت زیر کار می کند:

Dynamic حالت معمولی که تمام MAC Address ها یاد می گیرد و اجازه اتصال می دهد اما اگر دستگاه reload شود پاک می شود.

Static تنها به MAC Address هایی که ما تعیین می کنیم اجازه دسترسی می دهد.

Sticky به صورت اتوماتیک MAC Address ها را ثبت می کند با این تفاوت که این تعداد آدرس ها ثبت شده محدود هستند.

سوالی که این جا پیش می آید این است که اگر یک دستگاه با MAC Address غیر مجاز به شبکه متصل شود چه اتفاقی می افتد. جواب این سوال در تعریف Violation Mode ها هستند Violation Mode ها در واقع عملی هستند که سویچ در مقابله با اتصال یک دستگاه با MAC Address غیر مجاز انجام می دهند که شامل سه حالت زیر هستند:

واضح است که بهترین روش Shutdown است.

دستورات مشاهده تنظیمات:

Switch#show port-security interface fastEthernet 0/1

Switch#show port-security address

Switch#show interfaces status

نکته: در صورت Shut Down شدن یک اینترفیس به دلیل نقض Port Security شما باید وارد آن اینترفیس شوید و یک بار آن را خاموش و روشن کنید.

نکته: با دستور زیر می توانید این کار را به صورت خودکار انجام دهید:

Switch(config)#errordisable recovery cause psecure-violation

Switch(config)#errordisable recovery interval <time>

مشاهده تنظیمات مربوط به:error disable

Switch#show errordisable recovery

Shutdown پورت را خاموش می کند.

Restrict بسته ها را drop می کند و همچنین شمارنده Security Counter را اضافه می کند به نوعی log ثبت می کند.

Protect تنها بسته ها را drop می کند اما هیچ log ای را ثبت نمی کند.

Show Port-security address

```
Switch#show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
1          000C.8529.B678         DynamicConfigured      FastEthernet0/1
-
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Dynamic Host Configuration Protocol (DHCP)

پروتکل DHCP یکی دیگر از پروتکل های مدل TCP/IP میباشد که در لایه application مورد استفاده قرار میگیرد.

هر دستگاه یا هر اینترفیس که از TCP/IP استفاده می کند ، برای استفاده از شبکه و ارتباطات خود نیاز به یک IP دارد، که این IP را می توان به دو صورت زیر به دستگاه اختصاص داد:

1. Static
2. Dynamic

1. Static

در این حالت اختصاص IP به صورت دستی انجام می گیرد یعنی روی هر دستگاه کاربر خودش یک IP مشخص کند.
اختصاص IP به صورت Static مزایای و معایب خاص خودش را دارد که به برخی از آنها اشاره می کنیم:

مزایا:

هر دستگاه دقیقا مشخص است که از چه IP استفاده می کند.

به لحاظ امنیتی استفاده از روش Static بهتر است چون در این روش کلاینت ها را بهتر می توان کنترل کرد.

نیاز به راه اندازی و استفاده از سرویس خاصی ندارد.

نگه داری و عیب یابی ساده تر انجام می شود.

معایب:

برای آینده نگری و عدم بروز مشکل باید برای سیستم آدرس دهی ، یک برنامه دقیق و مشخص داشته باشیم.

در صورتی که تعداد دستگاه زیاد باشند نیاز به وارد کردن IP به صورت دستی روی تک تک دستگاه است که کار مشکلی است.

احتمال استفاده شدن یک IP برای دو دستگاه وجود دارد که نتیجه آن IP Conflict و مختل شدن عملکرد دستگاه ها است.

در صورت نیاز به تغییر در سیستم آدرس دهی این تغییرات باید روی تک تک دستگاه ها انجام شود.

نکته: معمولا دستگاه هایی که در شبکه یک سرویس خاص را ارائه می دهند از IP Static استفاده می کنند، چون کلاینت ها از این سرویس استفاده می کنند درنتیجه نباید IP این دستگاه ها تغییر کند، روترها و سرور ها از این دسته می باشند.

Dynamic.2

در این حالت اختصاص IP به صورت خودکار و توسط سرویس DHCP (Dynamic Host configuration Protocol) انجام می گیرد. این پروتکل وظیفه مدیریت سیستم آدرسی دهی شبکه را برعهده می گیرد. DHCP این اجازه را به دستگاه های شبکه می دهد که درخواست برای دریافت IP داشته باشند. DHCP را می توان روی تجهیزات مختلف مانند روتر ، سوئیچ ، ویندوز سرور ، مودم و ... راه اندازی کرد و به آن DHCP Server گفته می شود و کلاینتی که درخواست IP می کند را DHCP client می نامند.

نحوه عملکرد DHCP

برای DHCP Server یک رنج IP مشخص می شود که از این رنج IP برای اختصاص به کلاینت ها استفاده می کند. DHCP Server علاوه بر مشخص کردن IP برای کلاینت می تواند IP Gateway ، DNS و ... را به کلاینت اعلام کند. برای دریافت IP بین DHCP Client و DHCP Server چهار بسته رد و بدل می شود.

زمانی که یک کلاینت به شبکه متصل می شود از رنج IP شبکه و DHCP Server بی خبر است یک بسته به عنوان DHCP Discover به آدرس MAC مقصد ffff.ffff.ffff و IP مبدا 0.0.0.0 و IP مقصد 255.255.255.255 به صورت Broadcast روی شبکه ارسال می کند. DHCP Server با دریافت این بسته به عنوان پاسخ یک بسته به عنوان offer ارسال می کند که حاوی اطلاعات مانند IP، Default Gateway و ... می باشد. DHCP Client با دریافت بسته offer و بررسی اطلاعات آن به عنوان تایید یک بسته Request ارسال می کند. DHCP Server با دریافت بسته Request به عنوان تایید این مراحل و اختصاص IP یک بسته Ack ارسال می کند و به این ترتیب مراحل اختصاص IP پایان می پذیرد.

معایب و مزایای استفاده از DHCP

مزایا:

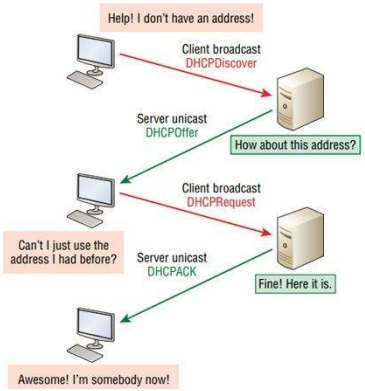
آدرس دهی به صورت خودکار و سریع انجام می شود.

برای مکان هایی که کاربران آن افراد ثابتی نیستند بسیار مناسب است.

مدیریت سیستم آدرسی دهی و رنج IP آدرس مورد استفاده توسط سرویس DHCP به صورت خودکار انجام می شود.

احتمال IP Conflict و مختل شدن عملکرد دستگاه ها بسیار کم است.

در صورت نیاز به تغییر در سیستم آدرس دهی این تغییرات به سادگی انجام می شود



معایب:

نیاز به نگه داری دارد.

دستگاه ها ، IP مشخصی ندارند در نتیجه کنترل آنها مشکل است.

امکان حمله DHCP Spoofing برای این سرویس وجود دارد.

برای راه اندازی نیاز به یک DHCP Server داریم در صورتیکه تجهیزات موجود در شبکه این را قابلیت نداشته باشند باید یک دستگاه به این منظور تهیه شود.

برای همه تجهیزات مثل سرورها نمی توان از DHCP استفاده کرد.

فعال کردن DHCP در تجهیزات سیسکو

از تجهیزات سیسکو مانند روتر و سوئیچ می توان به عنوان DHCP Server استفاده کرد. برای اینکار از دستورات زیر استفاده می کنیم:

در ابتدا یک Pool ایجاد می کنیم:

```
Switch(config)# ip dhcp pool VLAN_30
```

حالا باید رنج شبکه ای که می خواهیم از آن به کلاینت IP اختصاص دهیم را مشخص کنیم:

```
Switch(dhcp-config)# network 192.168.30.0 255.255.255.0
```

بادستور default-router جهت تنظیم Default Gateway :

```
Switch(dhcp-config)# default-router 192.168.30.1
```

بادستور domain-name جهت تنظیم dns-server :

```
Switch (dhcp-config)# domain-name 9.9.9.9
```

مدت زمان نگه داری IP را براساس روز مشخص می کنیم:

```
Switch (dhcp-config)# lease 9
```

اگر بخواهیم بخشی از رنج IP را برای موارد خاص مثل سرورها رزرو کنیم از دستور زیر استفاده می کنیم:

Switch (config)# ip dhcp excluded-address 192.168.30.1 192.168.30.9

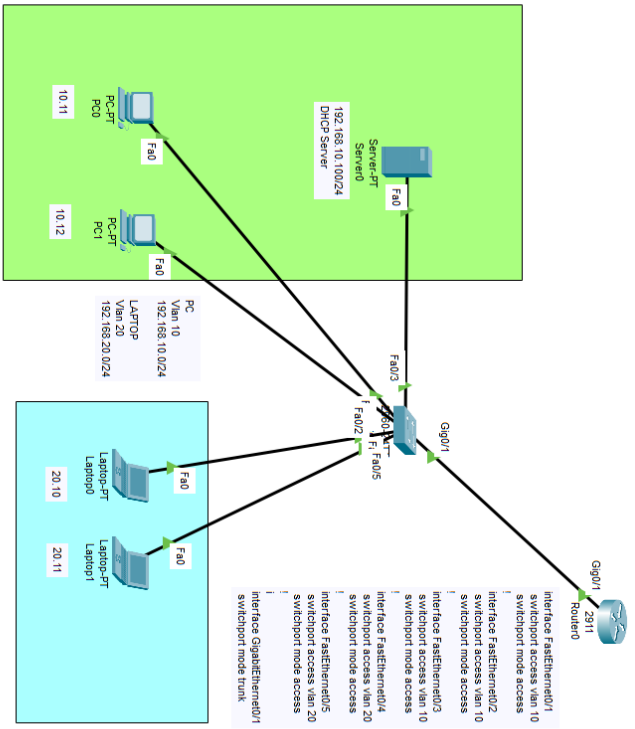
Switch (config)# ip dhcp excluded-address 192.168.30. 20192.168.30.255

دستورات مشاهده تنظیمات:

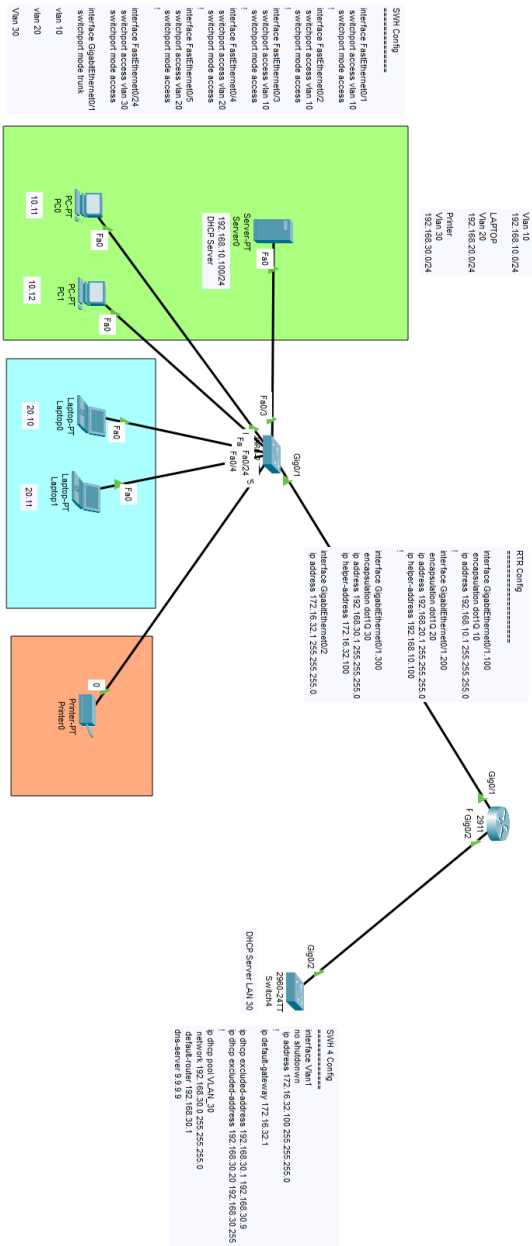
Switch#Show ip dhcp pool

```
Switch#sh ip dhcp pool

Pool VLAN_30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range
Leased/Excluded/Total
 192.168.30.1         192.168.30.1     - 192.168.30.254    0
/ 2     / 254
Switch#
```

DHCP and Relay Agent Scenario



DHCP and Relay Agent Scenario 2



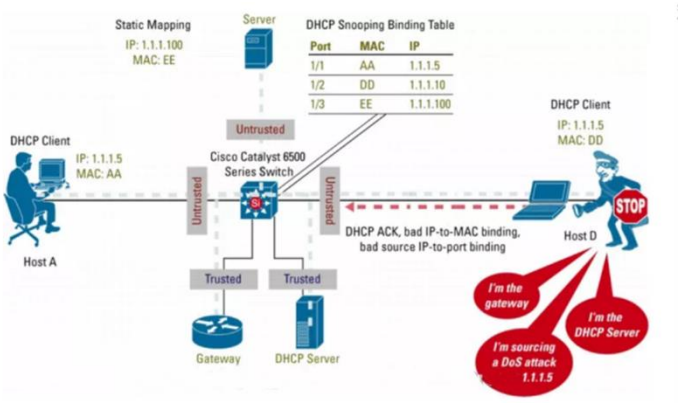
DHCP Snooping Configure and Trouble shooting

```
switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping vlan <VLAN_ID>

If switch is not Relay Agent :
switch(config)#[no] ip dhcp snooping information option

Trust Interface :
switch(config)#interface <>
switch(config-if)#ip dhcp snooping trust

Untrust Interface :
switch(config)#interface <>
switch(config-if)#ip dhcp snooping limit rate <PKTS>  (per second)
```

```
#show ip dhcp snooping
#show ip dhcp snooping statistics
#show ip dhcp snooping binding
```

DHCP Spoofing حمله ای است که عملکرد سرویس DHCP را مختل می کند.

این حمله به دو صورت می تواند به وجود اید:



DHCP Server Spoofing :

در حالت اول مهاجم به بسته های DHCP Request گوش می کند و بلافاصله به آنها جواب می دهد و IP Address و مشخصات مورد نظر خود را برای قربانی ارسال می کند به این نوع حملات man in the middle گفته می شود. به طور مثال IP خود را به عنوان Gateway به قربانی اعلام می کند در نتیجه قربانی بسته هایی که مقصد آنها خارج از شبکه هستند را به مهاجم تحویل می دهد و مهاجم اطلاعات مورد نظر خود را از این بسته استخراج می کند و سپس بسته را به سوی مقصد واقعی ارسال می کند و قربانی از این اتفاق بی خبر است.

DHCP Starvation :

حالت دوم جهت از کار انداختن سرویس DHCP مورد استفاده قرار می گیرد به این صورت که مهاجم تعداد زیادی DHCP Request جعلی ایجاد می کند و باعث می شود که کل محدود IP تعیین شده برای DHCP سرور پر شود یا تعداد این DHCP Request انقدر زیاد می شود که سرور توان پاسخگویی به آن را نداشته باشد.

نکته : در صورتی که DHCP سرور روی سوئیچ فعال باشد حمله حالت اول رخ نخواهد داد.

برای جلوگیری از این حملات از DHCP Snooping استفاده می کنیم و به صورت زیر عمل می کند:

برای جلوگیری از حالت اول پورتی که متصل به DHCP سرور ما است را به عنوان Trust معرفی می کنیم در نتیجه تنها این پورت اجازه دارد به بسته های DHCP Request پاسخ دهد. برای جلوگیری از حالت دوم برای پورت ها مشخص می کنیم که در هر ثانیه اجازه دارد چند DHCP Request دریافت کند و یا استفاده از قابلیت Port Security.

نحوه تنظیم DHCP Snooping در سوئیچ های سیسکو:

در ابتدا DHCP Snooping را فعال می کنیم.

```
Switch(config)#ip dhcp snooping
```

سپس VLAN مربوطه را مشخص می کنیم.

```
Switch(config)#ip dhcp snooping vlan 1
```

وارد اینترفیس متصل به DHCP سرور می شویم و آنرا به عنوان trust معرفی می کنیم.

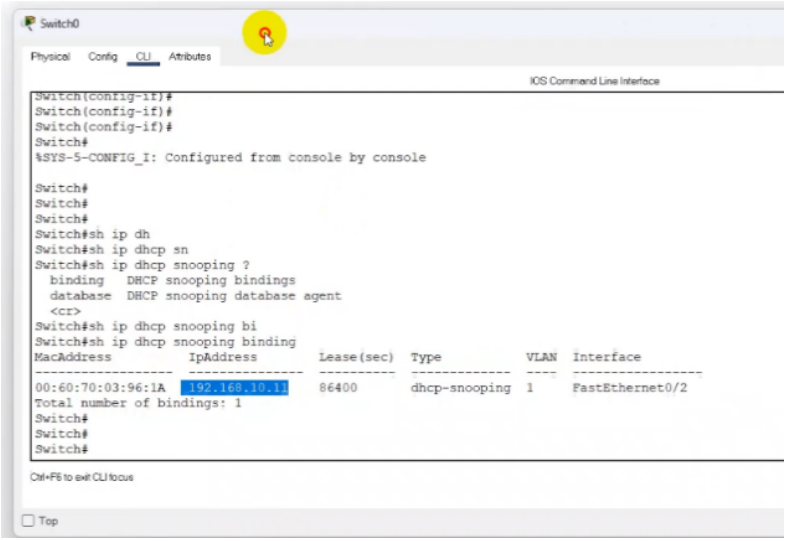
```
Switch(config)#interface fastethernet 0/24
Switch(config-if)# ip dhcp snooping trust
```

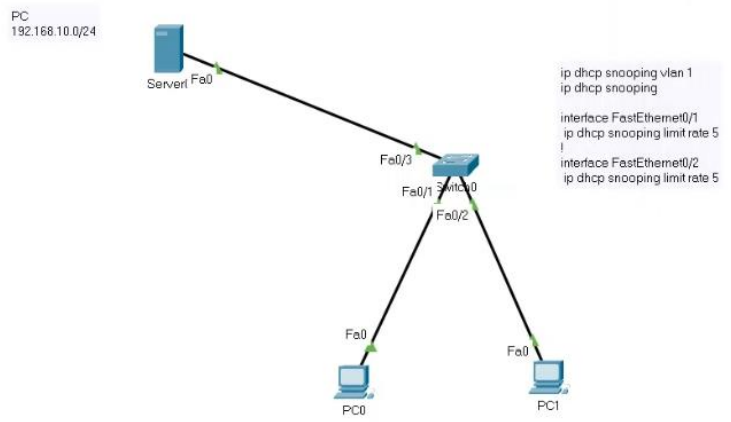
حالا باید مشخص کنیم که باقی پورت ها در هر ثانیه اجازه ارسال چند DHCP Request را دارند.

Switch(config)#interface range fastethernet 0/1-23

Switch(config-if)#ip dhcp snooping limit rate 3

Switch#show ip dhcp binding





Gratuitous ARP (GARP)

GARP یک ARP Request است که به صورت broadcast در شبکه منتشر میشود. وقتی کامپیوتر به صورت static یا dynamic دارای یک آدرس IP جدید میشود؛ آن را از طریق پیام GARP به تمام کامپیوترهای حاضر در broadcast domain و vlan خود خبر میدهد. در پیام GARP کامپیوتر به دنبال فهمیدن MAC هیچ کامپیوتری نیست؛ بلکه هدف از ارسال پیام GARP این است که جدول ARP کامپیوترهای شبکه بروزرسانی شود.

```
Ethernet II, Src: 00:53:ff:ff:bb:bb, Dst: ff:ff:ff:ff:ff:ff
  Destination: ff:ff:ff:ff:ff:ff
  Source: 00:53:ff:ff:bb:bb
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
```

```
Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: 00:53:ff:ff:bb:bb
    Sender IP address: 10.0.0.22
    Target MAC address: ff:ff:ff:ff:ff:ff
    Target IP address: 10.0.0.22
```

اگر GARP ارسال نشود

فرض کنید آدرس آی پی ۱۹۲.۱۶۸.۱.۱۰ متعلق به PC1 است. ادمین شبکه این آدرس IP را از تنظیمات کارت شبکه PC1 حذف میکند و همین آدرس را به کامپیوتر PC2 اختصاص میدهد. دیگر کامپیوترهای حاضر در شبکه LAN، از قبل در جدول ARP خود آدرس ۱۹۲.۱۶۸.۱.۱۰ را مرتبط با آدرس مک کامپیوتر PC1 ثبت کرده اند. حالا اگر PC2 آدرس IP جدیدش را همراه با آدرس مک خود برای سایر کامپیوترها broadcast نکند، سوییچ اترنت ترافیک ارسالی به مقصد ۱۹۲.۱۶۸.۱.۱۰ را بر اساس مک آدرس PC1 مسیردهی میکند. بنابراین ترافیک برای PC2 ارسال نمیشود.

معرفی حمله ARP Spoofing و ARP Poisoning و روش مقابله با آن

پروتکل Address resolation protocol (ARP) عمل تبدیل IP به MAC را برای ما انجام می دهد و مهاجم از این پروتکل برای حمله خود سود می برد. در این روش مهاجم با استفاده از پروتکل ARP یک بستهGARP ارسال می کند. به طور مثال IP Address گیت وی شبکه را با MAC آدرس خود اعلام می کند و سیستم های موجود در شبکه اطلاعات مربوط به ARP خود را با اطلاعات جدید بروز می کند و از این پس ترافیک خارج از شبکه خود را تحویل مهاجم می دهند و اگر مهاجم بعد از بدست آوردن اطلاعات مورد نیاز خود ترافیک به گیت وی اصلی ارسال کند کاربران از این اتفاق بی خبر خواهند بود (man in the middle).

Dynamic ARP inspection(DAI)

برای جلوگیری از این حمله از Dynamic ARP inspection استفاده می شود. Dynamic ARP inspection می تواند با DHCP Snooping کار کند تا جلوی این حمله را بگیرد. در Dynamic ARP inspection پورت های trusted و untrusted مشخص می شود و IP Address و MAC بسته های دریافتی ARP را با استفاده از دیتابیس DHCP Snooping بررسی می کند. پورت های Access باید به عنوان untrusted و پورت های متصل به روتر و دستگاه های که نمی خواهد بسته های ARP آنها چک شوند را در حالت trusted قرار می دهیم.

زمانی که ARP inspection را فعال می کنیم چه اتفاقی می افتد؟

مجدد همه پورت های سوییچ untrusted می شود و زمانی که روی هر پورت یک بسته ARP ارسال شود سوییچ هدر بسته را باز می کند و طبق جدول dhcp binding بررسی میکند که Mac بسته و Mac که در جدول قرار دارد یکی باشد در غیر این صورت بسته را دور میریزد.

Switch(config)# ip arp inspection vlan 1

با استفاده از دستور زیر پورت را در حالت trusted قرار داده می شود.

Switch (config)#interface fastethernet 0/1
Switch(config-if)# ip arp inspection trust

مشاهده تعداد بسته های Forward,Drop,DHCP Drop,ACL Drop

Switch#show ip arp inspection statistics

Switch#show ip arp inspection interface fast 0/1

بصورت پیشفرض روی هر اینترفیس که inspection فعال می کنیم اینتروالی که دارد در لحظه 15 بسته می تواند ارسال کند اگر بیشتر ارسال کند drop می شود.

برای تغییر محدودیت از دستور زیر استفاده می شود که در packet tracer غیر فعال است:

ip arp inspection limit rate <count>

```
#show ip arp incpection
#show ip arp incpection statistics
#show ip arp inspection interfaces
```

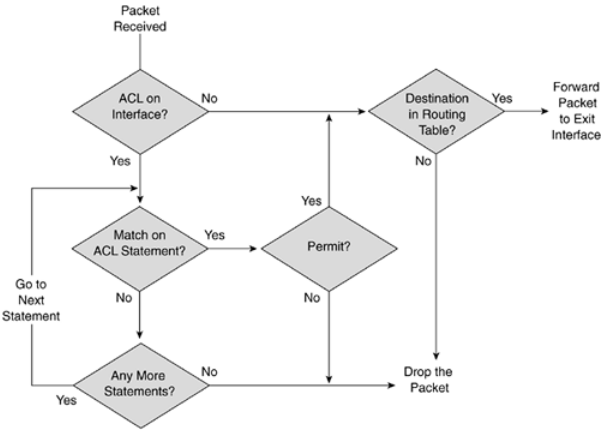
```
switch(config)#ip arp inspection vlan <VLAN_ID>

Trust Interface :
switch(config)#interface <>
switch(config-if)#ip arp inspection trust
switch(config-if)#ip arp inspection limit rate <COUNT>
<BURST INTERVALL> (default 15/sec)

Untrust Interface :
switch(config)#interface <>
switch(config-if)#ip arp inspection untrust
switch(config-if)#ip arp inspection limit rate <COUNT>
<BURST INTERVALL>  (default 15/sec)
```

Access Control Lists (ACL)

Access Control List یا ACL یک فیلتر است که به وسیله آن می توانیم جریان ترافیک را کنترل کنیم که چه بسته هایی اجازه ورود یا خروج از شبکه را دارند یا خیر. این فیلتر معمولا توسط مدیر شبکه تعیین و مورد استفاده قرار می گیرند تا به این وسیله بتواند کنترل و امنیت بیشتر را برای شبکه خود فراهم کند. این فیلترها را می توان روی بسیاری از دستگاه های شبکه مانند روتر و سوئیچ مورد استفاده قرار داد.

نحوه عملکرد ACL

ACL ها با استفاده از آیتم های مختلف مانند آدرس مبدا و مقصد ، پورت مبدا و مقصد ، نوع پروتکل و ... می تواند عمل فیلترینگ را روی بسته های ورودی یا خروجی یک پورت برای ما انجام دهد. زمانی که یک بسته به دستگاه می رسد در صورت وجود ACL ، اطلاعات موجود در Header بسته را بررسی می کند و با آیتم های تعریف شده در ACL مقایسه می کنند و نسبت به آن اجازه یا عدم اجازه عبور به بسته را می دهد.



چه زمانی از ACL استفاده می کنیم؟

جهت مقاصد امنیتی

محدود کردن ترافیک برای افزایش کارایی شبکه

جهت کنترل بسته های مربوط به پروتکل های مسیریابی

چه نوع ترافیکی اجازه عبور یا عدم عبور دارند

جداسازی برخی ترافیک های خاص به منظور عملیات خاص مانندQoS

اعمال محدودیت های زمانی

و ...

معرفی انواع Access Control List

Standard ACLs

Extended ACLs

Reflexive ACLs

Time-Base ACLs

Established ACLs

سیسکو دو نوع Access list با نام های Standard ACL و Extended ACL معرفی کرده است Standard ACL قدیمی ترین و ساده ترین نوع Access List است که در نسخه IOS 8.3 سیسکو ارائه شده است.

: Standard ACL

ترافیک بسته ها را به وسیله مقایسه آدرس مبدا (source IP) با آدرس تعریف شده در ACL کنترل می کند و action که می تواند داشته باشد Permit/Deny است. در همه نسخه ها ، برای Standard ACL می توان یک عدد از 1 تا 99 در نظر گرفت. از نسخه IOS 11.2 سیسکو امکان تعریف Standard ACL به وسیله نام فراهم شد و همچنین از نسخه IOS 12.0.1 سیسکو محدوده عددی بین 1300 تا 1999 برای Standard ACL اضافه شد.

Router(config)#Ip access-list

ساخت اکسس لیست 10 Router(config-std-nacl)# Ip access-list standard 10

عدم دسترسی Router(config-std-nacl)#deny host 192.168.10.10

دسترسی Router(config-std-nacl)#permit host 192.168.10.11

هر اکسس لیست می‌تواند چندین فرمان داخل خود داشته باشد. هر خط فرمان دارای شماره‌ای به نام sequence است که ترتیب اعمال آن‌ها را مشخص می‌کند. به صورت پیش فرض زمانی که چندین دستور در یک لیست وارد می‌کنیم، sequence ها با فاصله‌ی 10 تایی انتخاب می‌شوند. شماره sequence ها را می‌توان به دلخواه تعیین کرد.

به این دلیل شماره گذاری شده که دستورات لیست، به ترتیب اجرا شود، روی روتر یک standard access list در جهت in bound تعریف شده، SRC Ip که بسته ارسال کرده را خط به خط با access list بررسی می کند با اولین خطی که match شود طبق آن action انجام می دهد (deny/permit)

مشاهده اکسس لیست Show ip access-list

نحوه تعریف Standard ACL در حالت عددی:

Ip access-list stadard {number}

access-list-number عدد بین 1 تا 99 یا 1300 تا 1999

permit|deny عملی که در هنگام تطبیق بسته باACL نسبت با آن گرفته می شود(اجازه عبور یا عدم اجازه)

host-source-wildcard-any مشخص کردن IP به یکی از سه روش زیر:

Host یک ادرس IP مشخص می کنیم مانند Host 192.168.1.1

Any هر IP آدرسی

source source-wildcard تعیین یک IP به همراهWildcard Mask

نحوه تعریف Standard ACL با استفاده از نام:

IP Access-list {standard|extended} name

{permit|deny} {host|source source-wildcard|any}

سپس آن را به اینترفیس مورد نظر با استفاده از دستور زیر اختصاص می دهیم:

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip access-group 101 in

نکته : برای هر یک از جهت های ترافیک تنها یک ACL می توان در نظر گرفت در نتیجه حداکثر به یک اینترفیس می توان دو ACL اختصاص داد.

ACL ها در global configuration mode ایجاد شده و سپس آنها را باید فعال نمود. برای کنترل ترافیک انتقالی از راه اینترفیس ها، ACL ها را باید روی اینترفیس موردنظر فعال نماییم. در هنگام فعال نمودن ACL های ایجاد شده باید نوع ترافیکی را که تحت تاثیر قرار خواهد گرفت را مشخص نماییم. ترافیک عبوری را میتوان در دو گروه عمده قرار داد:

ترافیک ورودی یا Inbound

ترافیک خروجی یا Outbound

در ترافیک ورودی روتر اطلاعات رسیده را ابتدا با ACL های تعیین شده در روی اینترفیس مربوطه مقایسه کرده و سپس اقدام به ارسال آنها به مقصد خود می کند. اما در ترافیک خروجی یا outbound ، روتر اطلاعات رسیده را ابتدا به مقاصد خود ارسال کرده و سپس اقدام به مقایسه آنها با ACL مربوطه می نماید. یکی از محدودیت هایی که استفاده از ACL داراست این است که نمی توان ترافیکی که خود روتر آنها را ایجاد کرده به وسیله ACL ها فیلتر نمود.

برای مثال اگر از دستورات ping و یا traceroute در روی روتر استفاده کرده و یا اقدام به برقراری ارتباط telnet از روتر خود به سمت دستگاههای دیگر نماییم، نمی توان این ترافیک ها را به وسیله ACL ها فیلترگذاری کرد. اما اگر روتر دیگری اقدام به ping کردن و یا برقراری ارتباط telnet با روتر ما نماید و یا از طریق روتر ما، دستگاه دیگری را هدف قرار دهد، می توان از ACL بهره برد.

جهت مدیریت band with و resourse ها بهتر است تا جای ممکن فیلترینگ در نزدیکترین دستگاه در مبدا صورت گیرد که منابع سخت افزاری و پهنای باند کمتری اشغال شود.

Router(config)#int gig 0/0

Router(config-if)#ip access-group {number} {in|out}

اصلاح access list نوشته شده

Router(config)#ip access-list standard 10

Router(config-std-nacl)#no 5 خط 5 پاک می شود

Router(config)#15 permit host 192.168.10.12 اصافه کردن خط 15

حذف access list10 و access list LAN_A را جایگزین آن کنیم

Router(config)#int gig 0/0

Router(config-if)#no ip access-group 10 in

Router(config)#no ip access-list standard 10

Router(config)#int gig 0/0

Router(config-if)#ip access-group LAN_A in

اگر access list خالی بنویسیم در واقع خالی نیست اما آن را خالی می بینیم، بصورت پیشفرض انتهای هر access list یک خط نا نوشته وجود دارد (deny any) اگر لیست بررسی شد و هیچ خطی match نشده خط آخر deny any اجرا می شود.

استراتژی در نوشتن اکسس لیست

برای نوشتن اکسس لیست و مشخص کردن استراتژی، در ابتدا باید احتیاجات امنیتی یا security requirments را شناسایی کنیم، سپس براساس سبک ترین و کم تعدادترین خطوط اکسس لیست به تعریف انواع اکسس لیست بپردازیم.

اولویت لیست‌ها، از بالا به پایین می‌باشد. روش متداول در نوشتن لیست‌ها به صورت نوشتن لیست‌های permit و سپس لیست‌های deny می‌باشد.

هر اکسس لیست می‌تواند چندین فرمان داخل خود داشته باشد. هر خط فرمان دارای شماره‌ای به نام sequence است که ترتیب اعمال آن‌ها را مشخص می‌کند. به صورت پیش فرض زمانی که چندین دستور در یک لیست وارد می‌کنیم، sequence ها با فاصله‌ی 10 تایی انتخاب می‌شوند. شماره sequence ها را می‌توان به دلخواه تعیین کرد.

آموزش راه اندازی Extended ACL

در Standard ACL ما تنها می توانیم بر اساس آدرس مبدا ، بسته ها را کنترل کنیم ولی Extended ACL می تواند کنترل را براساس آدرس مبدا و مقصد ، شماره پورت مبدا و مقصد ، نوع پروتکل انجام دهد، در نتیجه Extended ACL به عنوان یک ابزار قدرتمند برای مدیران برای کنترل ترافیک محسوب می شود. در همه نسخه ها ، برای Extended ACL می توان یک عدد از 100 تا 199 در نظر گرفت. از نسخه IOS 11.2 سیسکو امکان تعریف Extended ACL به وسیله نام فراهم شد و همچنین از نسخه IOS 12.0.1 سیسکو محدود عددی بین 2000 تا 2699 برای Extended ACL اضافه شد.پارامترهای که می توان توسط Extended ACL کنترل کرد:

آدرس IP مبدا

آدرس IP مقصد

شماره پورت مبدا

شماره پورت مقصد

نوع پروتکل

نحوه تعریف Extended ACL با استفاده از نام :

Router(config)#IP Access-list {standard|extended} name

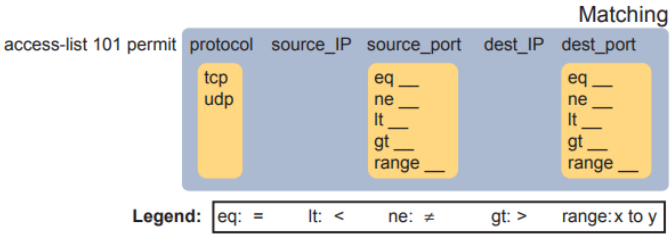
Router(config-ext-nacl)# {permit|deny} protocol source [Source port] destination [destination port]

سپس آنرا به اینترفیس مورد نظر با استفاده از دستور زیر اختصاص می دهیم:

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 101 in
```

هنگامی که یک دستور Extended ACL شامل کلمه کلیدی tcp یا udp باشد، به DST PORT/SRC PORT اشاره دارد.

برای انجام مقایسه شماره پورت از کلمات کلیدی: equal, not equal, less than, greater than, range استفاده می شود.



لیست پورت های مهم و شناخته شده UDP وTCP

Table 3-3 Popular Applications and Their Well-Known Port Numbers

Port Number(s)	Protocol	Application	access-list Command Keyword
20	TCP	FTP data	**ftp-data**
21	TCP	FTP control	**ftp**
22	TCP	SSH	**—**
23	TCP	Telnet	**telnet**
25	TCP	SMTP	**smtp**
53	UDP, TCP	DNS	**domain**
67	UDP	DHCP Server	**bootps**
68	UDP	DHCP Client	**bootpc**
69	UDP	TFTP	**tftp**
80	TCP	HTTP (WWW)	**www**
110	TCP	POP3	**pop3**
161	UDP	SNMP	**snmp**
443	TCP	SSL	**—**
514	UDP	Syslog	**—**
16,384–32,767	UDP	RTP (voice, video)	**—**

Wilcard Mask

عمده کاربرد Wilcard Mask در IOS های سیسکو در ACL ها است که نشان می دهد چه آدرسهای IP دسترسی وچه آدرس هایی دسترسی ندارند. از WildCard Mask به عنوان ماسک معکوس یاد می شود. دلیل اصلی این امر این است که برخلاف Subnet Mask است.

محاسبه Wilcard Mask:

فرض کنید ما یک شبکه با 10.0.0.0 و Subnet mask 255.255.255.240 داریم. ما می خواهیم یک ACL (Access list) برای این شبکه ایجاد کنیم که کل شبکه به یکسری منابع دسترسی نداشته باشند. برای این کار در ACL ما نیاز به اختصاص دادن Wilcard Mask برای آن Subnet داریم. ابتدا باینری Subnet mask به صورت زیر محاسبه میکنیم:

255.255.255.240=11111111.1111111.1111111.11110000

در مرحله بعد یه جمع ساده می سازیم ،به آخرین Octet نگاه کنید. برای Wilcard Mask فقط صفرها را جمع می بندیم.

8+4+2+1=15

بنابر این WilcardMask ما 0.0.0.15 خواهد بود.

یک مثال دیگر:

ما یک شبکه 10.0.0.0 با مسک 255.255.248.0 داریم:

مرحله اول:

255.255.248.0=11111111.11111111.11111000.00000000

مرحله دوم:

فقط صفرها رو محاسبه میکنیم

4+2+1.128+64+32+16+8+4+2+1

Wildcard Mask 0.0.7.255

یک روش ساده تر برای محاسبه نیز هست:

برای مثال:

255.255.240.0

هر Octet رو از 255 کم میکنیم:

255-255=0

255-255=0

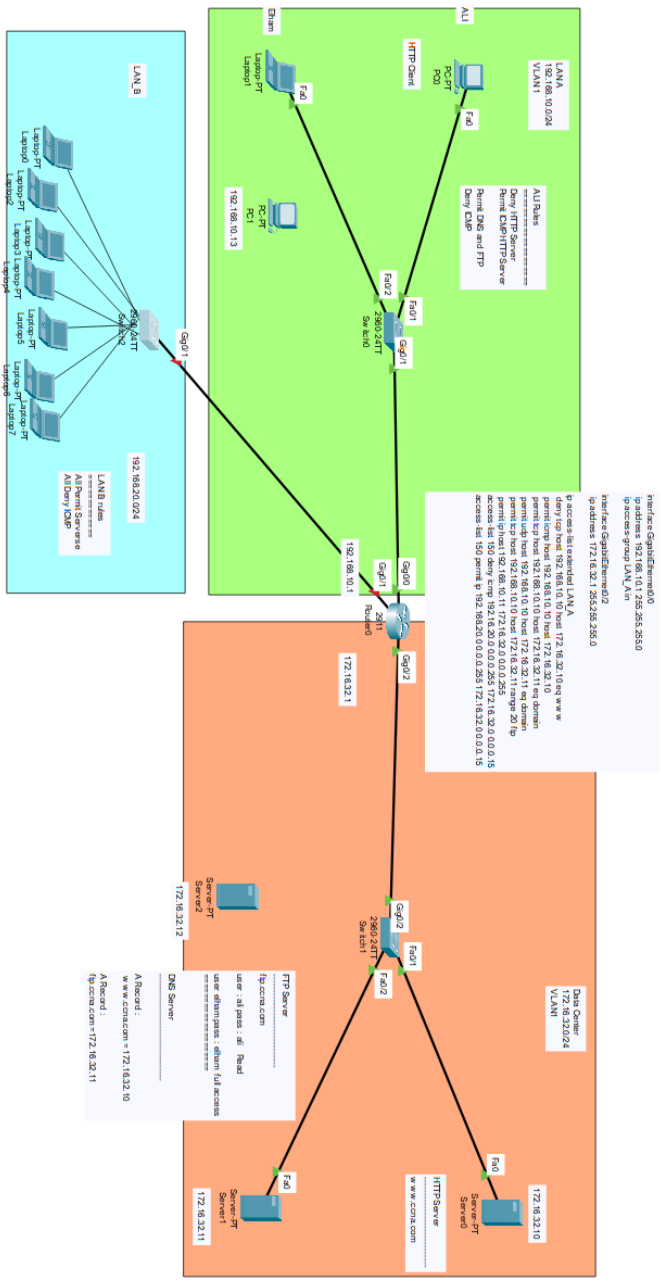
255-240=15

255-0=255

بنابراین Wilcard Mask

0.0.15.255

Extended ACL Scenario and Concept



Enterprise Campus Network Design

طراحی شبکه دولایه و سه لایه

Two-Tier Campus Design (Collapsed Core)

مدل دو لایه بهترین گزینه برای شبکه های کوچک یا متوسط در نظر گرفته می شود و معمولاً به عنوان هسته فروپاشیده شناخته می شود. این نوع طراحی اصولا برای مکان هایی در نظر گرفته می شود که تعداد End-Device ها در این نوع از شبکه ها به تعداد حداکثر 200 میرسد.

لایه Core و Distribution با یکدیگر ادغام می شوند و تشکیل لایه جدیدی به نام Collapsed را می دهند. و از دستگاه های کمتری استفاده می کنند که باعث کاهش هزینه ها شده.

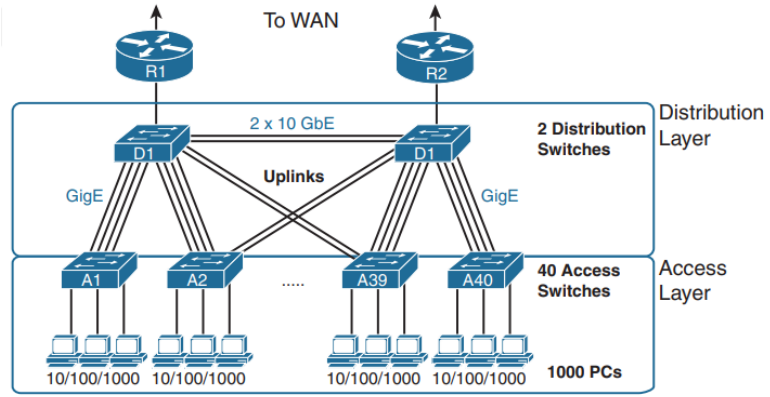
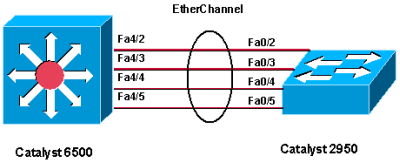


Figure 13-1 *Campus LAN with Design Terminology Listed*

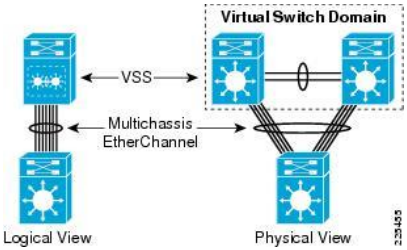
راهکارهای غلبه بر محدودیت پروتکلstp

در سال 2010 ، شرکت سیسکو از فناوری‌های vPC (Virtual-port-channel) و Multichassis EtherChannel برای غلبه بر محدودیت stp رونمایی کرد. یک EtherChannel عادی دو یا چند لینک فیزیکی بین یک جفت سوییچ با استفاده از پروتکل lacp .

(Link Aggregation Control Protocol) را پیاده‌سازی می‌کند. شکل زیر عملکرد این فناوری را نشان می‌دهد.



حال اگر به دنبال معماری کارآمدتری به منظور مدیریت پهنای باند باشیم، باید mec (Multichassis EtherChannel) استفاده کنیم. در روش mec یک EtherChannel بین یک جفت سوئیچ قرار می‌گیرد، اما از سوییچ سومی در ارتباط با لینک‌ها استفاده می‌کنیم تا ارتباط EtherChannel را تجمیع کند. به بیان دیگر از یک ترفند (سوییچ سوم) استفاده می‌کنیم تا نشان دهیم تنها یک سوییچ در مدار وجود دارد. شکل زیر این معماری را نشان می‌دهد.

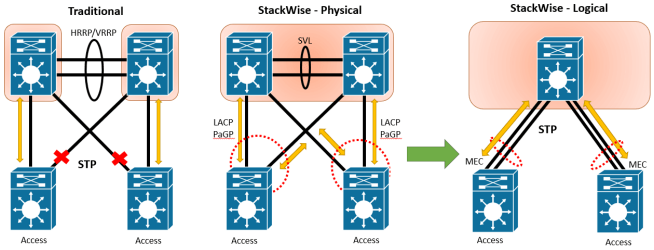


سوئیچ‌های Cisco Catalyst 6500 از ویژگی سوئیچینگ مجازی vss (Virtual Switching System) برای ساخت mec پشتیبانی می‌کنند.

خانواده سوئیچ‌های Cisco Nexus از ویژگی کانال پورت مجازی vPC (virtual Port Channel) برای ساخت MECپشتیبانی می‌کنند.

سوئیچ‌های Cisco Catalyst 3850 نیز قادر به پشتیبانی از معماری MEC هستند. البته در این حالت باید از StackWise برای اتصال سوییچ‌ها به Stack استفاده کنید.

کانال پورت مجازی (VPC) قابلیتی است که امکان تنظیم PortChannel میان چند سوییچ را فراهم می‌کند، مسئله پورت‌های مسدود شده توسط stp را حل می‌کند، دستیابی به مسیرهای آپ‌لینک active-active سوییچ‌های لایه دسترسی به لایه توزیع شده را امکان پذیر می‌کند و اجازه می‌دهد از پهنای باند موجود به بهترین شکل استفاده کرد. جالب آن‌که هنگام استفاده از فناوری VPC بازهم قادر به استفاده از پروتکل stp به عنوان راهکاری برای غلبه بر مشکل ایجاد حلقه در شبکه و fail-safe هستید. شکل زیر معماری مبتنی بر VPC را نشان می‌دهد.



با توجه به این‌که سوییچ‌های سری نکسوس سیسکو که برای مراکز داده طراحی شده‌اند از فناوری VPC پشتیبانی می‌کنند، عملکرد مراکز داده کوچک که بیشتر ترافیک آن‌ها از کرانه‌های شمالی و جنوبی (northbound و southbound) میان کلاینت‌ها و سرورها مبادله می‌شود به شکل بهتری مدیریت شده و در عمل عملکرد این مراکز داده نیز بهبود پیدا کرده است.

با استفاده از معماری leaf-spine ، مهم نیست چه سوییچی در لایه leaf به کدام سوییچ از لایه spine متصل شود، زیرا ترافیک همواره از دستگاه‌های مشخصی عبور می‌کند تا به سرور مقصد برسد. راه‌حل فوق باعث می‌شود تا تاخیر همواره در سطح قابل پیش‌بینی باقی بماند، زیرا بسته‌های داده تنها برای یک سوییچ spine و سوییچ leaf ارسال می‌شوند تا در نهایت به مقصد برسند.

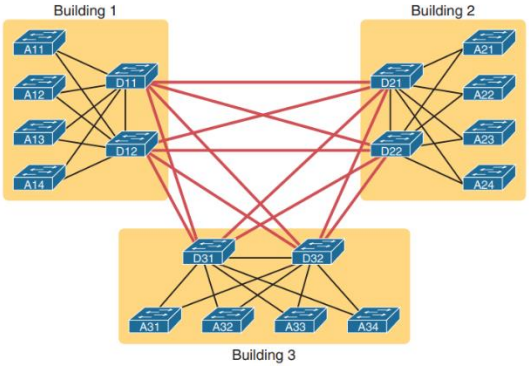


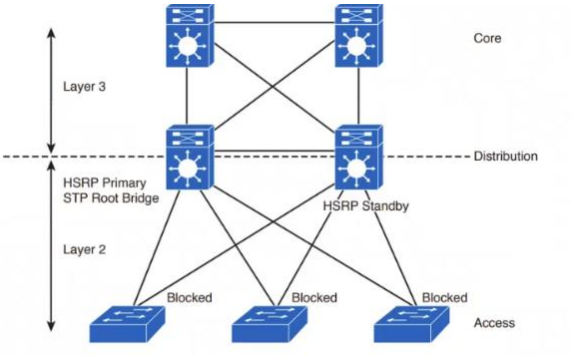
Figure 13-4 *Two-Tier Building Design, No Core, Three Buildings*

جهت ارتباط بین سوییچ ها و برای داشتن REDUNDANCY باید ارتباط Full Mesh برقرار کنیم، با این کار تعداد پورت های سوییچ های distribution هدر می رود و از یه جایی به بعد محدود می شویم و نمی توانیم شبکه را توسعه دهیم، به همین دلیل یک معماری سه لایه Three-Tier Campus Design طراحی شد.

شکل زیر مدل سه لایه درختی را نشان میدهد که شامل 3 لایه زیر می باشد:

- **Core**
- **Distribution**

- **Access**



سوییچ های مورد استفاده در لایه Access

Table 1-3 *Common Access Layer Switch Platforms*

	Catalyst Model	Max Port Density	Uplinks	Max Backplane	Other Features
	2960-X	384 (Up to 8 48-port switches in a stack)	2 10GE or 4 1 Gigabit Ethernet per switch	80 Gbps	RIP, OSPF available for routed access layer; PoE+
	3650	432 (Up to 9 48-port switches in a stack)	2 Gigabit Ethernet or 4 10GE	160 Gbps	Full-featured routing available, integrated wireless controller, PoE+
	3850	432 (Up to 9 48-port switches in a stack)	4 Gigabit Ethernet, 4 10GE	480 Gbps	Full-featured routing available, integrated wireless controller, PoE+, UPoE
	4500E	384 (Up to 8 48-port modules per chassis)	Up to 12-port 10GE per module	928 Gbps	Dual supervisors, full-featured routing available, integrated wireless controller, PoE+, UPoE

سوییچ های مورد استفاده در لایه Distribution

Table 1-4 *Common Distribution and Core Layer Switch Platforms*

	Catalyst Model	Max Port Density	Max Backplane	Other Features
	4500-X	80 10GE	1.6 Tbps	Dual-chassis Virtual Switching System (VSS) redundancy
	4500E	96 10GE or 384 Gigabit Ethernet	928 Gbps	Dual supervisors
	6807-XL	40 40Gbps, 160 Gigabit Ethernet, 480 Gigabit Ethernet	22.8 Tbps	Dual supervisor, dual-chassis VSS redundancy

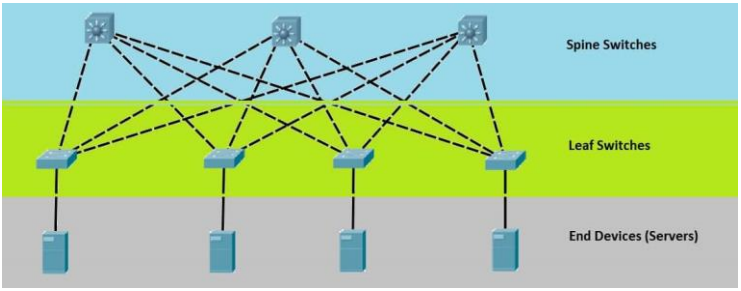
در این طراحی که بعنوان روشی رایج در معماری شبکه است، شامل 3 لایه اصلی میباشد: لایه Core شبکه ، لایه Distribution شبکه و لایه Access شبکه. هرچند که این طراحی تا به امروز نیازهای شبکه ها را برطرف کرده است و وظایف زیرساخت های شبکه را دسته بندی کرده است، نقاط ضعف مشخصی نیز دارد.

در این طراحی بهترین و هزینه برترین روترها در لایه Core و یا لایه Backbone شبکه قرار میگیرد و وظیفه انتقال اطلاعات با سریع ترین حالت ممکن و با کمترین Latency را عهده دار هستند. لایه Distribution که عمدتا شامل سوئیچ های پرقدرت لایه سه هستند مسئول اعمال سیاست های مختلف از قبیل ACL ها (Access List) ، SLA (Service Level Agreements)، QoS (Quality of Service)و غیره میباشنند. در آخر سوئیچ های Access شبکه با اتصال به کلاینت های شبکه از قبیل کامپیوتر و یا پرینترها مسئول تحویل بسته های ترافیکی به این دستگاه ها می باشند.

از مزیت های این روش میتوان به در دسترس بودن (Availability) ، امنیت ، مقیاس پذیری اشاره کرد. همچنین محدودیت پهنای باند در دسترس، Latency، محدود شدن ارتباطات پشتیبان بوسیله پروتکل Spanning-tree و محدودیت VLAN های موجود (4096 تا) از معایب این معماری میباشند که در شبکه های بزرگ مانند دیتاسنترهای پیشرفته که انتقال اطلاعات بین اپلیکیشن ها، ماشین های مجازی و سرورهای ذخیره ساز (Data Storage) بشدت نمود پیدا میکنند.

برای این منظور، شرکت سیسکو طراحی نوآورانه Spine and Leaf و با اتکا به سوئیچ نکسوس سیسکو سری 9000 را بعنوان راهکاری که تمامی نقاط ضعف نام برده شده را برطرف کند، پیشنهاد می دهد.

طراحی Spine and Leaf



این طراحی زیرساختی برای پیاده سازی مفهوم Cisco ACI و یا Application Centric Infrastructure بحساب می آید. در این زیرساخت مدیریت ارتباطات و ترافیک بین سرویس ها ، نرم افزارها و اپلیکیشن های موجود در شبکه بشدت ارتقا می یابد تا آنها بتوانند بدون اختلال و با بیشترین بازدهی فعالیت کنند.

در این طراحی که شامل دولایه می شود، هر سوئیچ Spine که در لایه ی بالایی قرار میگیرد بصورت Full-mesh به تمامی سوئیچ های Leaf که در لایه زیرین قرار دارند متصل می گردند و این سوئیچ های Leaf هستند که اطلاعات را به سرورها و بقیه سرویس های شبکه تحویل خواهند داد. لازم بذکر است که هیچ ارتباطی بین سوئیچ های Leaf و یا Spine در هرلایه نباید وجود داشته باشد. در این روش مسیر انتقال اطلاعات بصورت تصادفی انتخاب میگردد تا load balancing و استفاده از ظرفیت تمامی اتصالات به بهترین شیوه انجام شود.

در طراحی سه لایه سنتی از پروتکل STP برای پیشگیری از loop استفاده می کند که بر اساس شناسایی loop در شبکه، لینک های افزونه را مسدود می کند. در نتیجه یک سوییچ access که دارای دو عدد uplink است تنها از یکی از آنها می تواند بهره ببرد. معماری leaf-spine پروتکل های جایگزین جدیدتری به نام SPB(Shortest path bridging) و TRILL (Transparent Interconnection of Lots of Links) را برای پیشگیری از ایجاد loop به کار می برد. این پروتکل ها اجازه خواهند داد که تمام لینک های بین leaf و spine برای ارسال ترافیک استفاده شوند. پروتکل SPB و TRILL با به کارگیری پروتکل مسیریابی لایه 3 برای دستگاه های لایه 2 ای، این مسئله را برطرف کرده است و دستگاه های لایه 2 اجازه خواهند داد که فریم های اترنت را مسیریابی نمایند. حذف پروتکل STP در این معماری به افزایش پایداری در شبکه منجر می شود و با بهره مندی از ابزارهای جدید و در کنار راهکارهای دیگری همچون(SDN (Software-Defined Networking ، منجر به بهبود شبکه های Enterprise و پیشرفته خواهد شد.

همچنین در این طراحی ترافیک همواره باید از تعداد دستگاه های یکسانی گذر کند تا به سرور مقصد برسد. این رویکرد منجر خواهد شد که تاخیر (Latency) همیشه در سطحی قابل پیش بینی باقی بماند چرا که بسته های داده تنها به سمت یک سوییچ spine و سوییچ leaf دیگر حرکت می کنند تا به مقصد خود برسند.

سوئیچ Spine سیسکو

خانواده سوئیچ های 9000 نکسوس سیسکو شامل مدل های مختلفی از سوئیچ های ثابت مانند سیسکو نکسوس 9300 و سوئیچ های ماژولار مانند نکسوس سیسکو 9700 میشوند که بعنوان سوئیچ Spine در شبکه راه اندازی میشوند. این سوئیچ ها قابلیت های اتومات و براساس سیاست های درنظر گرفته شده را در بستر سیسکو ACI محقق می سازند. لازم بذکر است با فعال کردن این خانواده از سوئیچ ها با استفاده از لایسنس PLR سوئیچ نکسوس 9000 سیسکو تمامی ویژگی های این دستگاه ها، برای پیاده سازی در حالت ACI-mode ، بصورت دائمی و بدون نیاز به اینترنت فعال میگردد.

دومدل سوئیچ ماژولار نکسوس سیسکو N9K-C9508-B2 و N9K-X9736PQ از سری 9700 و سوئیچ ثابت نکسوس سیسکو N9K-X9336PQ از سری 9300 برای بکارگیری در این لایه پیشنهاد میگردند.

Router VS Switch :

■ User and Enable (privileged) mode

■ Entering and exiting configuration mode, using the configure terminal, end, and exit commands and the Ctrl+Z key sequence

■ Configuration of console, Telnet (vty), and enable secret passwords

■ Configuration of Secure Shell (SSH) encryption keys and username/password login credentials

■ Configuration of the hostname and interface description

■ Configuration of Ethernet interfaces that can negotiate speed using the speed and duplex commands

■ Configuration of an interface to be administratively disabled (shutdown) and administratively enabled (no shutdown)

■ CLI help, command editing

■The meaning and use of the startup-config (in NVRAM), running-config (in RAM)

■ The configuration of IP addresses differs in some ways, with switches using a VLAN interface and routers using an IP address

configured on each working interface.

■ Many Cisco router models have an auxiliary (Aux) port, intended to be connected to an external modem and phone line to allow

remote users to dial in to the router, and access the CLI, by making a phone call. Cisco switches do not have auxiliary ports.

■ Router IOS defaults to disallow both Telnet and SSH into the router because of the typical router default setting of transport input

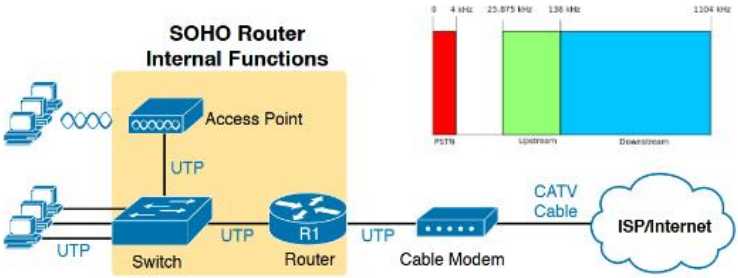
none in vty configuration mode.

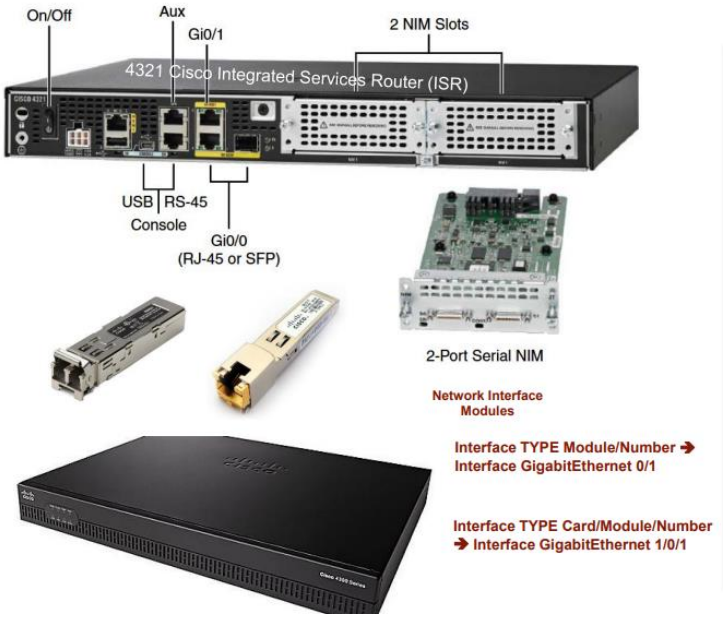
■ Cisco Layer 2 switches support the show mac address-table command, while Cisco routers do not.

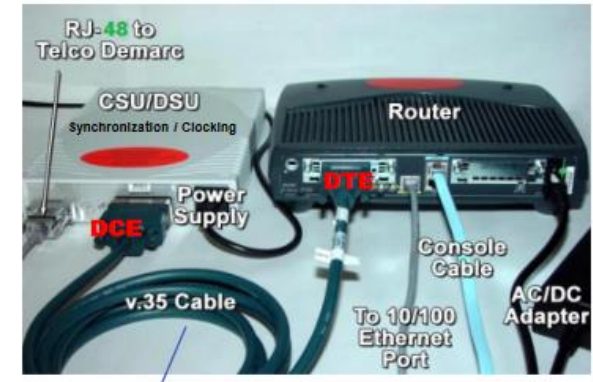
■ Cisco routers support the show ip route command, while Cisco Layer 2 switches do not.

■ Cisco Layer 2 switches use the show interfaces status command to list one line of output per interface (and routers do not), while

routers use the show ip interface brief command to list similar information (but switches do not)


SOHO Router
Internal Functions
Access Point
UTP
UTP
UTP
UTP
Switch
R1
Router
Cable Modem
CATV
Cable
ISP/Internet
0
4 kHz
25.875 kHz
138 kHz
1104 kHz
PSTN
Upstream
Downstream


On/Off
Aux
Gi0/1
2 NIM Slots
4321 Cisco Integrated Services Router (ISR)
USB
RS-45
Console
Gi0/0
(RJ-45 or SFP)
2-Port Serial NIM
Network Interface
Modules
Interface TYPE Module/Number
Interface GigabitEthernet 0/1
Interface TYPE Card/Module/Number
Interface GigabitEthernet 1/0/1



Telco Demarcation Point
(CSU/DSU) ➔ Channel Service Unit / Data Service Unit
DTE ➔ Data Service Unit ➔ Router
DCE ➔ Data Communications Equipment ➔ CSU/DSU

تفاوت روترهای سری ISR و سریASR:

ISR مخفف عبارت Integrated Services Router می باشد.

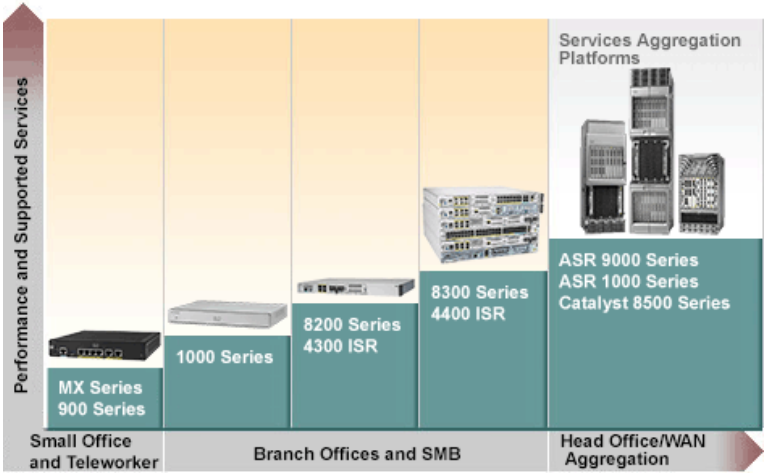
ASR مخفف عبارت Aggregation Services Router می باشد.

تفاوت اصلی این دو رده از روتر در این است که روتر سری ISR در مکان‌هایی استفاده می‌شود که نیازمندی های آن شبکه کوچک و کم هستند ، مانند مشاغل و دفاتر کوچک یا متوسط ، شعب شرکت ها و بانک ها و ... و این در حالی است که سری ASR برای نیاز شبکه های مقیاس بزرگ همانند شرکت‌های بسیار بزرگ یا ارائه دهندگان خدمات اینترنت و ... استفاده می‌شود.

سری ISR در مکان هایی که معمولا نیازمند سرویس و پهنای باند کم هستند ، استفاده می شود و چندین سری روتر ISR وجود دارد که توسط شرکت سیسکو معرفی شده است که شامل سری800 ISR ، سری1900 ISR ، سری ISR 2900، سری ISR 3900 و سری ISR 4000 و ... هستند و سیستم عامل آن ها IOS نامیده می شود.

روتر سری ASR در مکان هایی که معمولا نیازمند سرویس و پهنای باند بالا هستند ، استفاده می شود و چندین سری روتر ASR وجود دارد که توسط شرکت سیسکو معرفی شده است که شامل سری ASR 900 ، سری ASR 1000 و سری ASR 5000 و ... هستند و سیستم عامل آن ها IOS XE نامیده می شود.

روترهای سری ASR	روترهای سری ISR	پارامترهای ساده مقایسه
طراحی شده جهت شبکه های بزرگ و ارائه دهنگان خدمات اینترنتی	طراحی شده جهت شبکه های کوچک و متوسط	موارد قابل استفاده
سیسکو IOS-XE و IOS-XR	سیسکو IOS	سیستم عامل مورد استفاده
عدم دسترسی به سیستم ابری (در بعضی مدل ها قابلیت دسترسی)	قابلیت دسترسی به سیستم ابری	دسترسی به سیستم ابری
قابلیت پردازش سرعت تا 100 گیگابیت بر ثانیه (متفاوت در برخی مدل ها)	قابلیت پردازش سرعت تا 10 گیگابیت بر ثانیه (متفاوت در برخی مدل ها)	قابلیت پردازش سرعت
تعداد پورت زیاد و قابلیت افزایش پورت (توسط ماژول)	تعداد پورت کم و قابلیت کم افزایش پورت ها (توسط ماژول)	تعداد پورت ها و قابلیت افزایش دادن پورت ها (توسط ماژول)



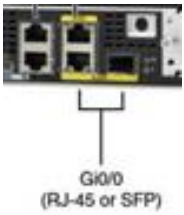
برقراری ارتباط از طریق پورت Console

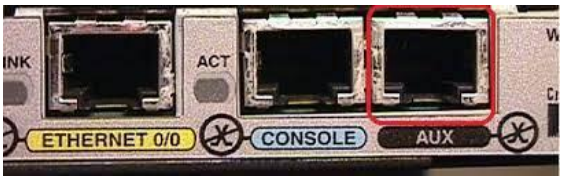
پورت کنسول زمانی مورد استفاده قرار می گیرد که شما نمی توانید تحت شبکه به روتر خود متصل شوید ، معمولا زمانی که برای اولین بار روتر خود را می خواهید پیکربندی کنید و در مدار شبکه قرار دهید از این پورت استفاده می کنید.

برقراری ارتباط از طریق پورت Auxiliary

با استفاده از این پورت شما می توانید یک دستگاه مودم را به روتر خود وصل کنید و شخصی که قصد پیکربندی روتر را دارد نیز با استفاده از مودمی که در اختیار دارد به مودمی که به پورت AUX روتر متصل شده است ، وصل می شود و می توانند همانند حالتی که با استفاده از پورت کنسول شما روتر را پیکربندی می کنید از طریق مودم خود و از راه دور روتر را پیکربندی کند . در واقع این پورت برای برقراری ارتباط با روتر از راه دور اما بدون استفاده از بستر شبکه ای می باشد.

شاید برای شما هم با توجه به تصویر زیر جای تعجب باشد که چگونه کابل شبکه به مودم متصل می شود زیرا اندازه پورت AUX همانند کابل های شبکه است ، مودم با استفاده از یک Connector خاص یا بهتر بگوییم یک مبدل به روتر متصل می شود و کار می کند که شما احساس کنید با پورت کنسول روتر کار می کنید ، به تصویر زیر دقت کنید که یک پورت AUX را نشان می دهد که با استفاده از یک کابل RJ به روتر متصل شده است.





روی پورت های روتر که مشترک هستند Media Type بصورت پیش فرض RJ45 می باشد. جهت تغییر به فیبر باید از دستور: media-type sfp استفاده کنیم و یا بلعکس تغییر به RJ45 .

هر روتر بصورت پیشفرض networkهایی که به آن متصل هستند را متوجه می شود و ip هایی که در همان network روی هر دست روتر ست شده را می داند.

جدول مسیریابی routing table, or routing information base (RIB)

#show ip route

روتر ها برای مسیریابی از جداول روتینگ استفاده می کنند. تمامی Router ها و بطور کلی دستگاه هایی که می توانند وظیفه مسیریابی بسته های اطلاعاتی را در شبکه برعهده بگیرند و در نتیجه از پروتکل IP پشتیبانی می کنند دارای Routing Table می باشند. جدول مسیریابی شامل اطلاعات ضروری برای ارسال بسته اطلاعاتی به سمت بهترین مسیر به مقصد آن است.

هر بسته اطلاعاتی شامل مبدا و مقصد آن می باشد. وقتی بسته اطلاعاتی توسط گیرنده (که میتواند روتر باشد) دریافت می شود و آن بسته اطلاعاتی یا پکت را باز میکند و اگر مشاهده کرد که آدرس مقصد در جدول مسیریابی اش قرار دارد آن را به شبکه مورد نظر هدایت میکند اما اگر بسته اطلاعاتی مربوط به آن شبکه نبود آن را به بهترین مسیر برای رسیدن آن بسته به مقصدش هدایت می کند. جدول مسیریابی همچنین دارای اطلاعاتی مثل Hop می باشد که روتر های بعدی را از رسیدن بسته به مقصد مطلع می سازند.

Hop نشان دهنده تعداد روتر هایی است که بسته اطلاعاتی برای رسیدن به مقصد نهایی اش باید از آنها عبور کند.

یک جدول مسیریابی ساده شامل اطلاعات زیر می باشد:

Destination یا مقصد : بیانگر آدرس IP مقصد بسته اطلاعاتی است.

Next hop : آدرس IP روتری که بسته اطلاعاتی باید به آن فوروارد یا ارسال شود.

Interface : آدرس IP اینترفیس یا پورتی که روتر پس از دریافت بسته اطلاعاتی به آن ارسال میکند تا به دست دیگر روتر (Hop) ها در شبکه برسد.

Metric : متریک به زبان ساده پارامتری است که بهینه ترین Route برای هدایت بسته اطلاعاتی انتخاب می شود. هر چه میزان cost کمتر باشد آن بسته توسط Route مربوط به مقصد ارسال می شود.

Subnet : که بیانگر آدرس زیر شبکه یا Subnet Mask ای است که به اینترفیس روتر تخصیص داده شده است.

جداول مسیریابی هم به صورت دستی یا static می توانند نگهداری و مدیریت شوند و هم بصورت dynamic (خودکار). جداول مسیریابی که در دستگاه های روتر به صورت دستی یا static تعریف میشوند تنها توسط مدیر شبکه قابل تغییر است. اما در Dynamic routing جداول مسیریابی توسط پروتکل های مسیریابی که روی روتر ها راه اندازی و پیکربندی میشود ایجاد و نگهداری می شوند.

Static Route

Static routing نوعی از مسیریابی است که دستگاه روتر با استفاده از Route هایی که در Routing Table آن دارد و بصورت دستی در روتر Learn یا تعریف شده است بسته اطلاعاتی را به سمت مقصد هدایت می کند. در بسیاری از موارد static route ها به صورت دستی توسط مدیر شبکه در Routing Table روتر پیکربندی می شوند. بر خلاف Dynamic routing مسیریابی استاتیک ثابت هستند و تا زمانی که تغییری در ساختار فیزیکی شبکه (مانند اضافه شدن یا حذف شدن یک روتر از شبکه) بوجود نیامده است بدون تغییرات باقی می مانند.

مزایای استفاده از Static routing

1- از static routing می توان برای تعیین یک مسیر پیشفرض خروج بسته اطلاعاتی در صورت نبود آدرس مقصد آن بسته در Routing Table روتر استفاده کرد. که به این مسیر پیشفرض Default Route نیز می گویند.
2- از static routing می توان در شبکه های کوچک که نیاز به یک یا دو Route دارند استفاده کرد.
3- از Static routing می توان در مواقعی استفاده کرد که Dynamic routing در دسترس نباشد به این معنی که می توان به عنوان یک Backup routing یا بهتر است بگوییم به عنوان یک مکمل در کنار Dynamic routing از آن استفاده کرد.
4- از static routing می توان به عنوان یک کمک برای انجام عملیات Routing از یک پروتکل مسیریابی به پروتکل مسیریابی دیگر بهره برد. (Routing Redistribution) .
5- سربار روی CPU روتر وجود ندارد.
6- پهنای باند بلا استفاده بین پیوندها وجود ندارد.
7- فقط مدیر شبکه می تواند مسیرها را اضافه کند.

معایب استفاده از Static routing

1- Human error در بسیاری از موارد static route ها بصورت دستی در روتر تعریف می شود که این خود مستعد بروز اشتباهات فردی است. اگر تنها یک Route به اشتباه در روتر وارد شود عملیات مسیریابی در کل شبکه از کار می افتد.
2- Fault tolerance مسیریابی استاتیک از قابلیت fault tolerant یا تحمل خرابی پشتیبانی نمی کند. به این معنی که اگر یکی از روتر ها در شبکه خراب شود یا تغییری در ساختار فیزیکی شبکه ایجاد شود دیگر ترافیک قابل مسیریابی در شبکه نمی شود. در نتیجه شبکه غیر قابل استفاده میشود و تا زمانیکه مشکل برطرف نشده باشد کل شبکه فلج می شود.
3- Administrative distance مسیر های استاتیک یا Static route ها بر dynamic route ها تقدم دارند به این معنی که Static route ها ممکن است مانع از کارکرد مناسب پروتکل های مسیریابی یا Routing Protocol ها شود. که راهکار این مشکل تغییر دادن مقدار Administrative distance پروتکل مسیریابی است.
4- Administrative overhead مسیر های استاتیک یا Static route ها در هر روتر باید بصورت دستی پیکربندی شود. این پیکربندی ها مدت زمان زیادی صرف می کند در صورتیکه تعداد روتر ها در شبکه زیاد باشد. همچنین تغییر دادن این تنظیمات نیز میتواند مستعد اشتباهات زیادی باشد.
5- سرپرست باید نحوه اتصال هر روتر را بداند.
6- گزینه ایده آل برای شبکه های بزرگ نیست زیرا زمان زیادی را صرف می کند.
7- هرگاه لینک خراب شود تمام شبکه از کار می افتد که در شبکه های کوچک امکان پذیر نیست.

نحوه پیکربندی Static routing در روتر های سیسکو

در محیط CLI یا خط فرمان روتر سیسکو ابتدا با دستور Enable وارد Enable mode شوید :

Router> enable

Router# configure terminal

Router(config)# interface s0/0/0

Router(config)# ip route 10.10.20.0 255.255.255.0 192.168.100.1

در دستور فوق ابتدا وارد محیط enable mode شدیم و سپس با دستور configure terminal وارد محیط global configuration شدیم سپس وارد محیط اینترفیس serial مربوطه شدیم تا بر روی آن اینترفیس یا پورت Static route مان را تعریف کنیم. آدرس 10.10.20.0 همان آدرس Destination یا مقصدی است که بسته اطلاعاتی قصد رسیدن به آن را دارد و آدرس 192.168.100.1 آدرس IP اینترفیسی است که بسته های اطلاعاتی می توانند از آن عبور کنند به این آدرس Default-Gateway نیز می گویند. توجه کنید که این آدرس آدرسی نیست که ما در حال حاضر روی اینترفیس مان پیکربندی انجام می دهیم بلکه آدرسی است که به اینترفیس روتر مجاورمان اختصاص داده شده است.

برای نوشتن یک دستور ip route ساده تنها نیاز است که فرمان ip route را نوشته و ابتدا آدرس network و یاhost مقصد (prefix) را وارد کنیم. در ادامه باید که subnet mask مربوط به مقصد (mask) را نوشت.

نکته: برای یک host خاص باید subnet mask مربوط به آن را 255.255.255.255 بنویسیم.

در صورتی که subet خود را برای ip یک host هر subnet بجز /32 وارد شود پیغام خطای %Inconsistent address and mask نشان داده خواهد شد . در گام بعدی می بایست ip address مربوط به روتر next-hop و یا interface که packet ها می توانند برای رسیدن به next-hop استفاده کنند نوشته شود.

دستور زیر یک مثال ساده از نوشتن Ip route می باشد:

Ip route 172.16.0.0 255.255.0.0 Ethernet 0

Ip route 172.16.0.0 255.255.0.0 192.168.1.2

اما یکی از تفاوت های اصلی این دو فرمان در نحوه نمایش route مورد نظر در routing table است. برای مشاهده static route ها به تنهایی می توان از فرمان show ip route static استفاده کرد. هنگامی که ازexit interface استفاده شود ، router به شکل Directly Connected در routing table نمایش داده می شود.

Prefix/mask is directly connected, exit-interface example: 172.16.0.0/24 is directly connected, Serial1/0

اما زمانی که از next-hop استفاده شود ، route مورد نظر در جدول routing به شکل زیر نمایش داده می شود .

prefix [AD/metric]via ip-next-hop example : 15.1.1.0 [1/0] via 172.16.0.2

همانطور که از مثال بالا مشخص است metric مربوط به static route ها برابر صفر و AD آنها برابر 1 می باشد. اما علاوه بر نحوه نمایش ، استفاده از interface و next-hop در نوشتن static routes تفاوت های محسوسی با یکدیگر دارد. هنگامی در نوشتن static route از next-hop استفاده شود روتر به طور پیش فرض هر 60 ثانیه یکبار next-hop را چک می کند و در صورت عدم دریافت جواب route را از routing table حذف می کند . برای تغییر این زمان می توان از فرمان زیر استفاده کرد.

Ip route static adjust-time number

در دستور فوق ، number عددی بین 1 تا 60 ثانیه است. در صورت استفاده از exit-interface تنها زمانی route از routing tableحذف می شود که exit interface به نحوی fail شود به طور مثال interface مربوطه shutdown شود.

همانطور که اشاره شد در نوشتن static route می توان هم به exit interface مثل Serial0 و هم next-hop استفاده کرد. اما همیشه استفاده از next-hop به جای exit interface پیشنهاد می شود . در صورتی که static route به یک broadcast interface مثل Ethernet اشاره کند route مربوط به آن تنها زمانی در routing table قرار می گیرد که interface مربوط به آن up باشد. به علاوه router فرض می کند محدوده تمام ip هایی که از طریق static route اشاره شده به صورت directly connect هستند و روتر برای ارسال به هر destination که در static route به آن اشاره شده است یک ARP ارسال می کند. نمونه چنین route زیر می باشد:

Ip route 0.0.0.0 0.0.0.0 Ethernet 0

در صورتی که packet های زیادی برای دستیابی به destination های کثیری از این فرمان استفاده کنند ، CPU Utilizationروتر بسیار بالا می رود و یک جدول arp cache بسیار بزرگ ایجاد می شود که می تواند حتی روتر را overloadکند . اضافه کردن numerical address و به بیان واضح تر IP مربوط به next-hop دو مزیت عمده دارد. یکی از ارسال arp ها جلوگیری می کند و دوم اینکه در صورت down شدن آن interface از طریق recursive route سعی در پیدا کردن route دسترسی به آن ip می کند. برای نوشتن این نوع route می بایست که interface و next-hop هر دو نوشته شوند. مثال آن در زیر نوشته شده است.

Ip route 0.0.0.0 0.0.0.0 Ethernet 0 172.16.0.2

استفاده از exit interface به تنهایی فقط زمانی پیشنهاد می شود که نوع interface خروجی point-to-point می باشد. یکی از مرسوم ترین point-to-point interfaceها serial interface ها می باشد.

یکی دیگر از کاربرد های static route استفاده در کنار Dynamic routing protocol می باشد و یک route جایگزین و redundant را در صورت down شدن مسیر advertised شده معرفی می کند که در اصطلاح به آن floating static route گفته می شود . در حالت عادی static route ها دارای Administrative Distance (AD) عدد 1 می باشند که مقدم بودن آنها را بر Dynamic Routing Protocols را اثبات می کند. در صورتی که شما AD مربوط به route نوشته شده را به عدد بیشتری از AD مربوط به Dynamic route اختصاص دهید در صورت fail شدن آن route از از static route نوشته شده استفاده می کند. بطور مثال فرض کنید شما از پروتکل EIGRP در شبکه خود استفاده می کنید که دارای AD برابر با 90 می باشد . در صورتی که شما AD مربوط به static route خود را به عددی بزرگتر از 90 قرار دهید می تواند نقش floating route را برای شما ایفا کند. همانطورکه می دانید محدود قابل اختصاص AD عددی بین 0 تا 255 می باشد . اما به این نکته داشته باشید که اختصاص AD عدد 255 آن route رو به عنوان Unreachable route در نظر گرفته می شوند و لذا این route هیچگاه در routing table قرار نمی گیرد. برای تعیین metric مربوط به static route مورد نظر تنها نیاز است تا در ادامه دستورات قبلی ، عدد metric مورد نظر وارد شود.

Ip route 172.16.0.0 255.255.0.0 192.168.1.2 150

با کمک کلمه name می توان برای route یک نام تعیین کرد. استفاده از نام تعیین شده کمک می کند تا زمانی که route های زیادی داریم به راحت تر آنرا در configuration file پیدا کنیم. مثال زیر کاربرد این فرمان را نشان می دهد.

ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Tehran2Shiraz

show running-config | in Tehran2Shiraz

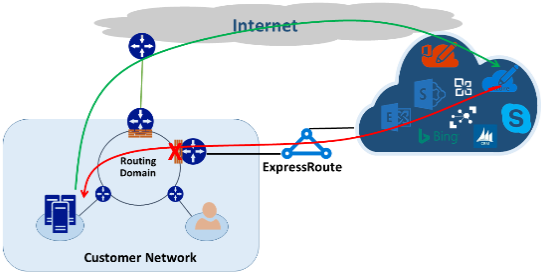
استفاده از کلمه permanent در ip route این امکان را می دهد که در صورت shutdown شدن exit interface همچنان route در routing table باقی بماند و remove نشود.

ip route 10.1.1.1 255.255.255.255 serial0 permanent

منظور از Equal-Cost Multipath یا به اختصار ECMP آن است که اگر به ازای یک مقصد یکسان چندین مسیر با cost یکسان وجود داشته باشد، تمام این مسیرها کشف شده و بین آن ها برای ارسال ترافیک load sharing صورت گیرد. پس در این روش، هر forwarder (روتر) به ازای هر مقصد معینی چندین next-hop داشته و از روش هایی به منظور مشخص کردن آن که از کدام next-hop برای ارسال یک پکت مشخص باید استفاده شود، استفاده می نماید.

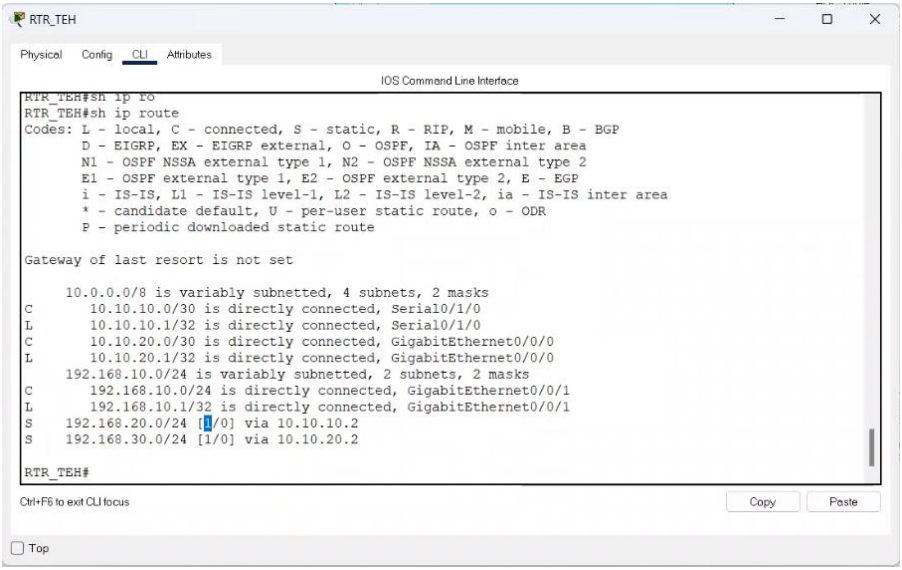
ساده ترین روش برای انجام این عمل آن است که مثلا پکت اول از لینک اول، پکت دوم از لینک دوم و الی آخر ارسال شوند. اصطلاحا به این روش per-packet load balancing گفته می شود .

در Asymmetric زمانی به مشکل بوجود می آید که در بین روتر ها فایروال یا cash server داشته باشیم. ارتباطی برقرار می شود که اگر درخواستی از روی یک ip و پورت رفت جوابش هم جوابش هم از روی همون برگرده، در غیر این صورت اگر ارتباط یک طرفه بیاد سمتش فکر میکنه attack و آن بسته را drop میکنه.



بررسی قابلیت Administrative Distanc

داخل براکت دو عدد وجود دارد که قسمت اول آن Administrative Distance هست.



بیشتر پروتکل های مسیریابی برای خود یک ساختار Metric و الگوریتم خاص دارند که شاید اصلا با پروتکل های دیگر تناسبی نداشته باشد. در شبکه ای که از چندین پروتکل مسیریابی مختلف استفاده می شود ، تبادل اطلاعات در خصوص مسیرهای موجود و همچنین قابلیت تشخیص بهترین مسیر از بین چندین پروتکل مسیریابی موجود مهمترین اولویت است.

Administrative Distance قابلیتی است که روترها با استفاده از آن می توانند بهترین مسیر در میان دو یا چندین شبکه ای که از پروتکل های مسیریابی مختلف استفاده می کنند برای رسیدن به یک مقصد مشخص را بیابند.

Administrative Distance در واقع میزان reliability یا قابلیت اعتماد به یک پروتکل مسیریابی را تعیین می کند. هر یک از پروتکل های مسیریابی موجود با استفاده از مکانیزم Administrative Distance از نظر سطح reliability یا قابلیت اعتماد اولویت بندی می شوند و به هر کدام از آنها یک مقدار یا Value اختصاص پیدا می کند.

اول Next hop باید reachable باشد و interface up باشد، دوم route ای بهتر است که specific تر باشد حالا اگر چند تا route به ازای مقصد داشته باشیم route ای ارجح تر میباشد که Administrative Distance کمتری داشته باشد. Route هایی که بصورت استاتیک استفاده می کنیم بصورت پیشفرض یک هستند، connected بصورت پیشفرض صفر است، به همین دلیل اگر static route خواستیم بزنیم interface انتخاب کنیم و connected شود Administrative Distance صفر می شود و میتواند loop ایجاد کند بنابر این اصولا next hop استفاده می کنیم.

بررسی قابلیت Administrative Distance

پارامتر Administrative Distance اولین شرطی است که یک Router زمانیکه دو پروتکل مسیریابی مختلف، اطلاعات مسیریابی مربوط به یک مقصد مشخص را ارائه می کنند، برای پیدا کردن بهترین مسیر از بین این دو یا چند پروتکل مسیریابی بررسی می کند. در واقع معیاری برای درست بودن و موثق بودن مبدا اطلاعات مسیریابی می باشد، نکته مهم در Administrative Distance این است که Local Significance است یعنی اهمیت و معنی آن فقط روی همان روتر معتبر است و با Update شدن Routing به روترهای دیگر Advertise نمی شود.

هر چقدر مقدار یا Value ای که به پروتکل در Administrative Distance داده می شود کمتر باشد به معنی این است که پروتکل مورد نظر قابل اعتماد تر است، برای مثال اگر یک روتر یک Route به یک شبکه مشخص دریافت کند که در آن هم پروتکل OSPF با Administrative Distance پیشفرض ۱۱۰ وجود داشته باشد و هم IGRP با Administrative Distance پیشفرض ۱۰۰ ، روتر مورد نظر ما مسیری که IGRP به آن معرفی می کند را به دلیل Reliability بیشتر انتخاب می کند و این بدین معناست که روتر نسخه Route مربوط به IGRP را در Routing Tableخود اضافه می کند.

اگر به هر دلیلی شما موفق به دریافت اطلاعات مربوط به IGRP نشدید (مثلا روتر در آن لحظه خاموش شده باشد) نرم افزار بصورت خود کار اطلاعات مربوط به مسیرهایی که OSPF ایجاد کرده است را استفاده می کند تا زمانیکه اطلاعات IGRP مجددا در دسترس باشند.

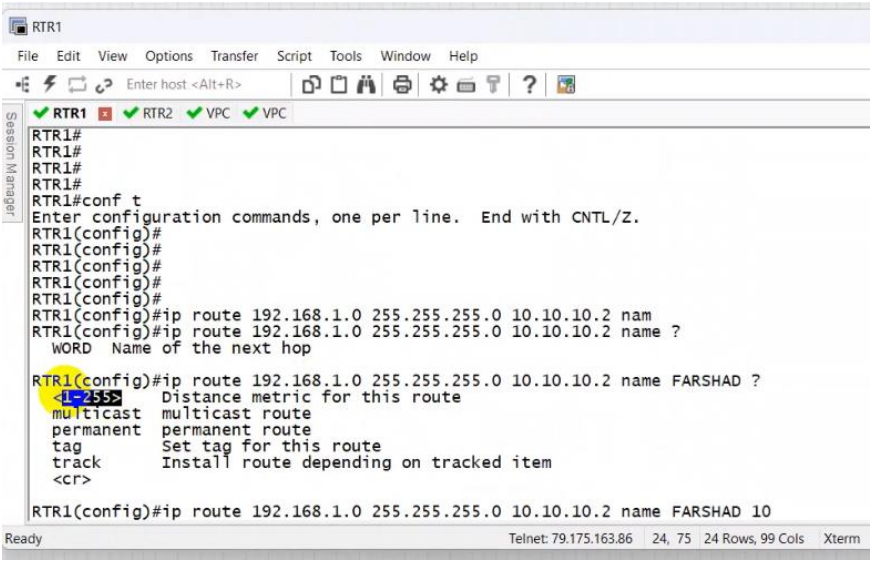
مقادیری که به عنوان Value به پروتکل های مختلف بصورت پیشفرض داده می شود از عدد ۰ تا ۲۵۵ متغیر می باشد عدد ۰ بالاترین اولویت و به معنای بالاترین Reliability و عدد ۲۵۵ به معنای پایین ترین حد Reliability می باشد. در static Route سعی می کنیم زیر 80 انتخاب کنیم چون در Dynamic Route مقدار value از 90 به بالا می باشد.

جدول زیر لیست مقادیر AD پیشفرض پروتکل هایی است که سیسکو از آنها پشتیبانی می کند:

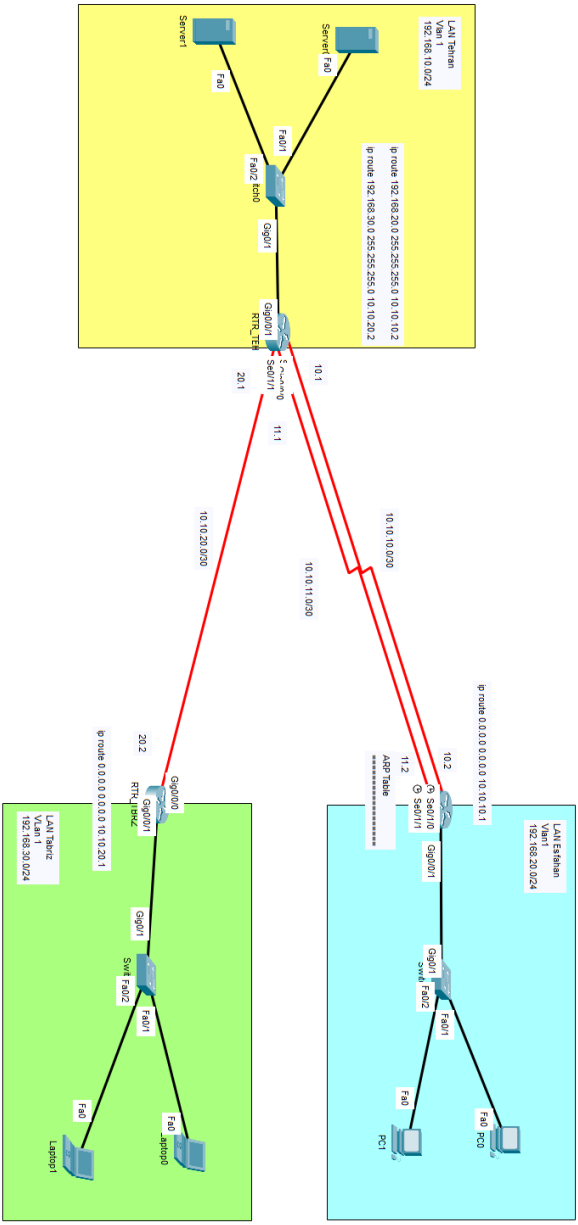
Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

اگر بخواهید اولویت های این پروتکل ها را در Administrative Distance ها تغییر دهید باید بصورت دستی مقادیر پیشفرض را عوض کنید.

تغییر Administrative Distance بصورت دستی



Static Route Scenario - ECMP



Floating Static Route

یعنی یک Route را شناور بذاریم، می تواند چند Static Route با Administrative Distance های متفاوت نوشت یا میتوان یک چند Static Route به همراه یک Dynamic Route بنویسیم. در داینامیک Administrative Distance ها متفاوت است و الویت هایش از 90 به بالا شروع می شود.

برای مثال ، در یک شبکه ، یک آپلینک اینترنت و یک لینک بکاپ وجود دارد ، میخواهیم ، در صورت قطع ارتباط اصلی ، ارتباط از طریق لینک بکاپ برقرار شود.

یکی از سناریو های پر کاربرد در ایران ، بدین ترتیب است که اکثر ISP ها ، علاوه بر ارتباط رادیویی با uplink خود که مثلا میتواند ماکروویو باشد ، یک ارتباط اینترانتی نیز بر روی فیبر هم با ISP بالادست خود ، یا مخابرات دارند ، خب البته که ماکروویو ارجح است ، چون تاخیر کمتری داشته و همچنین به ISP ، بار اضافی over head تحمیل نمی کند ، ولی در هر صورت ، اگر این لینک down شود ، می بایست ترافیک به شکل خودکار از روی لینک فیبر و یا همان اینترنت ، یا هر لینک دوم دیگری ، عبور کند ، البته هم برای send این کار را کرد و هم receive که می تواند BGP peering باشد .

permanent

کلمه permanent یا persistent باعث می شود route ای که شما اضافه می کنید در routing table روتر حتی بعد از خاموش و روشن شدن یا دچار مشکل شدن روتر باقی بماند .

SLA

باید در نظر داشت که SLA یک مفهوم مختص Cisco نیست و یک مفهوم عمومی در فناوری اطلاعات می باشد که توافق نامه سطح خدمات (Service Level Agreement) نام دارد. این توافق نامه در بیشتر مواقع بین خدمات دهنده و خدمات گیرنده امضا می گردد. در این توافق نامه یک سرویس با شرایط دسترسی، مدت زمان دسترسی و مدت زمان تضمینی قطعی سرویس خاص در اختیار کاربر قرار می گیرد. با ادغام قابلیت SLA در روتر های سیسکو این امکان را برای ما فراهم می آورد تا مدت زمان Uptime سرویس را نظارت و بررسی نماییم. در واقع به واسطه SLA یک مکانیزم تست و بررسی را ایجاد می نماییم . همچنین این امکان وجود دارد که داده های مورد نظر را به سیستم مانیتورینگ ارسال نماییم. و حتی این قابلیت وجود دارد تا به واسطه SLA یک مکانیزم فعال جهت تصمیم گیری انتخاب مسیر در روتر ایجاد نماییم. در سناریویی که ممکن است چندین مسیر Static وجود داشته باشد و در مسیر های Static وقتی یک لینک Down می شود روتر توجهی به اتفاق پیش آمده نخواهد کرد و تصمیمی اتخاذ نخواهد نمود. در چنین شرایطی می توان از SLA استفاده نمود. SLA با ارسال ترافیک به سمت مقصد از صحت اتصال اطمینان حاصل می نماید و به محض اینکه به هر دلیل پاسخی دریافت نکرد Static Route مورد نظر را از جدول مسیریابی حذف و مسیر Static دیگری را جایگزین می نماید. دقت داشته باشید این سناریو تعریفی فقط یکی از موارد استفاده SLA می باشد و در بسیاری از سناریو های مختلف می توان از این قابلیت بهره برد.

Dynamic Routing Protocol

طبقه بندی پروتکل های مسیریابی :

پروتکل های مسیریابی را می توان با توجه به ویژگی های آنها به گروه های مختلف طبقه بندی کرد:

Purpose: شامل Interior Gateway Protocol (IGP) یا Exterior Gateway Protocol

Operation: شامل Distance vector protocol ، link-state protocol یا path-vector

Behavior: شامل Classful (legacy) یا classless protocol

پروتکل های مسیریابی شامل سه دسته یDistance Vector، Link State و Advance Distance Vector می باشند. هر کدام از این بخش ها عمل روتینگ را با معیار ها و فاکتور های خاصی انجام می دهند که از نظر الگوریتمی که استفاده می کنند و رفتاری که بر اساس آن الگوریتم نشان می دهند.

انواع پروتکل مسیریابی بر اساس عملکرد :

پروتکل های Distance Vector:

پروتکل های Distance Vector با استفاده از دو فاکتور مسافت (Distance) و جهت (Vector) کار روتینگ را انجام می دهند. پروتکل های Distance vector جدول مسیریابی خود را برای تمامی همسایگانی که به طور مستقیم به آن ها متصل هستند، در فواصل زمانی مشخص و با پهنای باند بالایی انتشار می دهند و به آرامی همگرا می شوند. هنگامی که یک مسیر از دسترس خارج می شود، تمام روترهای شبکه باید جدول های مسیریابی خود را بر اساس اطلاعات جدید به روز کنند.

متریک آن Hop Count است ومشکل این پروتکل ها این است که هر روتر مجبور است که اطلاعات جدیدی را به همسایگان خود اطلاع دهد، در نتیجه مدت زمان زیادی طول می کشد تا همه روترها دید دقیقی از شبکه داشته باشند. این پروتکل ها از subnet mask های ثابت استفاده می کنند که مقیاس پذیر نیستند و حداکثر از Metric Value 15 پشتیبانی می کند یا به عبارتی فقط 15 عدد Hop Count را پشتیبانی می کند. اگر تعداد Hop Count ها بیشتر از عدد 15 شود این شبکه را به عنوان شبکه غیر قابل دسترس یا Unreachable در نظر می گیرد.

این پروتکل از الگوریتم بلمن فورد(Bellman-Ford) برای محاسبه مسیر استفاده میکند. الگوریتم بلمن فورد یک الگوریتم برای محاسبه کوتاه ترین مسیر است .

این پروتکل خیلی کند هستند (slow convergence) یعنی اگر تغییری در شبکه اتفاق بیوفتد خیلی دیر متوجه می شوند اما simple هستند و راحت پیاده سازی و اجرا می شوند و ادمین زیاد درگیر دیزاین نمی شود.

پروتکل های Link State:

Link State از سه فاکتور **ترافیک شبکه، سرعت Link** و **فاصله** به طور هم زمان و نه مجزا برای انتخاب بهترین مسیر استفاده می کند و همین عوامل باعث می شوند که Link State بسیار پیچیده تر از Distance Vector باشد و متریک آن cost هست و از الگوریتم دایجسترا (Dijkstra) استفاده می کند.

پروتکل های Link state اطلاعات مسیریابی را تنها در زمان بروز تغییرات انتشار می دهند، به همین دلیل به صورت موثر از پهنای باند استفاده می کنند. در این حالت روترها به جای جدول مسیریابی، تنها تغییرات را انتشار می دهند، در نتیجه باعث افزایش سرعت همگرایی می شود.

پروتکل مسیریابی اطلاعات جدید را در اختیار تمام همسایگان در یک شبکه قرار می دهد و تلاش می کند تا با اطلاعات مسیریابی جدید شبکه را همگرا کنند. این پروتکل ها از subnet masks با طول متفاوت استفاده می کنند که هم مقیاس پذیر هستند و هم مسیریابی را بهتر انجام می دهند. آنها همچنین نسبت به پروتکل های مسیریابی distance-vector به CPU و حافظه بیشتری نیاز دارند و پیکربندی آن سخت تر می باشد. از پروتکل های Link State معمولاً در شبکه های بزرگ و متوسط استفاده خواهد شد.

(Hybird) Advance Distance Vector

متریکی که استفاده می کند ترکیبی از چند پارامتر است و ترکیبی از پروتکل های Distance Vector و Link State هستند به همین دلیلی با آن Hybird می گویند. هر کدام از این دو نوع دارای مزایایی می باشند که در اینجا پروتکل های ADV مجموعه ای از مزایای دو پروتکل را در خود دارند و به همین دلیل امروزه در اکثر شبکه های بزرگ از این دسته پروتکل ها برای روتینگ استفاده می شود.

از چند پارامتر استفاده می کند و در فرمول قرار میدهد که عدد بدست آمده متریک آن می شود و بهرین مسیر را انتخاب می کند اما دید کاملی از کل توپولوژی شبکه ندارد.

K1 = Bandwidth [1]
K2 = Load [0]
K3 = Delay [1]
K4 = Reliability [0]
K5 = Additional Reliability [0]

$$\text{Metric} = \left[\left(K1 \times \frac{10^7}{BW_{min}} + \frac{K2 \times BW_{min}}{256 - load} + K3 \times \sum delays\right) \times \frac{K5}{K4 + reliability}\right] \times 256$$

With $K5$ defaulted to 0, the equation $\frac{K5}{K4 + reliability}$ will be set to 1

$$\text{Metric} = \left[\left(1 \times \frac{10^7}{BW_{min}} + \frac{0 \times BW_{min}}{256 - load} + 1 \times \sum delays\right) \times 1\right] \times 256$$

$$\text{Metric} = \left(1 \times \frac{10^7}{BW_{min}} + \frac{0 \times BW_{min}}{256 - load} + 1 \times \sum delays\right) \times 256$$

$$\text{Metric} = \left(\frac{10^7}{BW_{min}} + \sum delays\right) \times 256$$

Competitive Metric

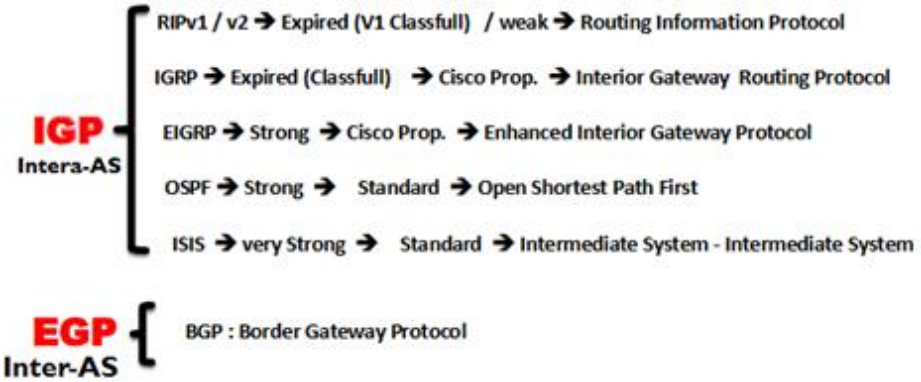
اگر به ازای رسیدن به یک مقصدی بیش از یک مسیر داشته باشم یکی از آنها Best اما مسیر بکاپ رو هم در توپولوژی نگه می دارد اما در DV و LS اینطور نیست.

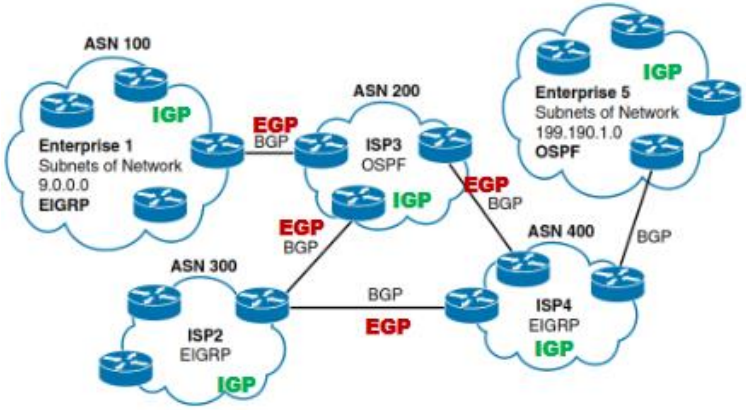
Path Vector :

رفتار آنها شبیه به DV هست اما اینجا متریک نداریم و پارامتر های مختلف که شبیه به متریک هستند رو داریم.

Autonomous System Number

Autonomous System یا AS به مجموعه ای از شبکه ها گفته می شود که در یک حوزه مدیریتی واحد قرار دارند این مجموعه می تواند شبکه های موجود در یک سرویس دهنده اینترنتی یا ISP باشد یا یک شبکه WAN بزرگ سازمانی.



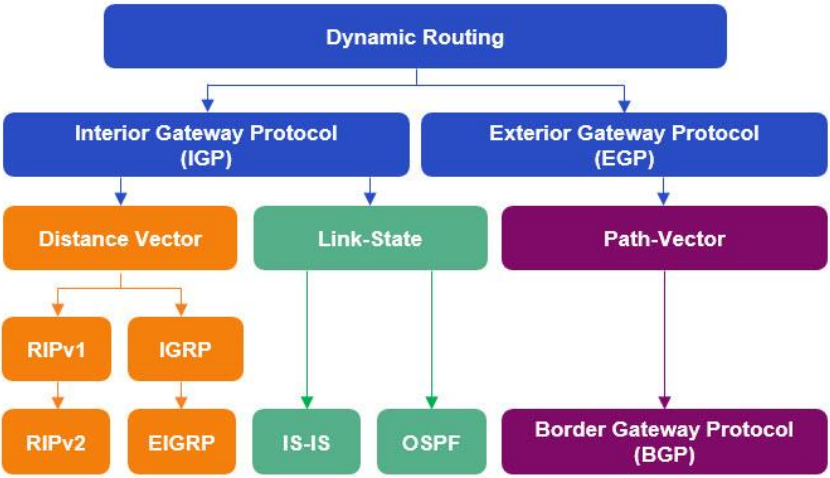


(IGP)Interior Gateway Protocol

درون یک AS استفاده می شوند که (DV,ADV,LS) جزو این دسته هستند.

(EGP) Exterior Gateway Protocol

بین AS ها استفاده می شوند که Path Vector جزو این دسته هست.



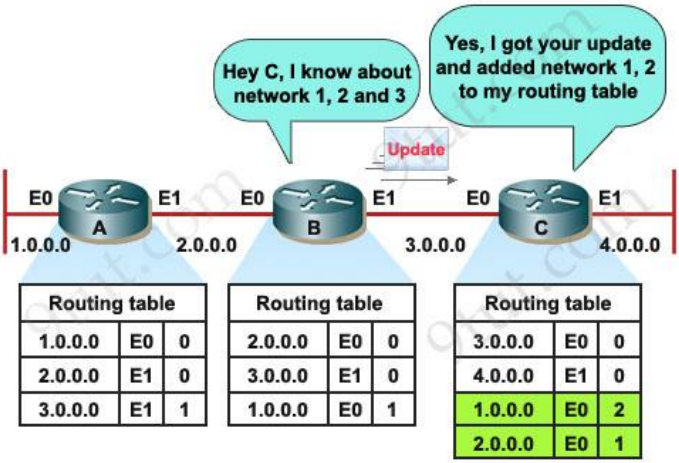
RIP

RIP یک پروتکل قدیمی و عمومی می باشد که جزء دسته پروتکل های Interior Gateway Protocol هست که در شبکه هایی با اندازه کوچک کارایی بالایی دارد و از رده پروتکل های Distance-Vector می باشد و فاقد مکانیزم احراز هویت می باشد یعنی اگر روتری این پروتکل را فعال کند می تواند کل Routing شبکه را داشته باشد.

ملاک انتخاب بهترین مسیر در این پروتکل hop count می باشد که بیشترین مقداری که برای متریک در این پروتکل در نظر گرفته شده 15 می باشد و در صورتی که از این مقدار بیشتر شود، مسیر غیرقابل دسترس خواهد بود.

full update در این پروتکل هر 30 ثانیه یک بار در شبکه به صورت Broadcast از اینترفیس های متصل به روتر خارج شده و به روتر های مجاور ارسال می شود.

در صورتی که روتر چند مسیر با متریک یکسان به یک شبکه پیدا کند، ترافیک را بین این مسیرها تقسیم می کند. بنابراین در این حالت از منابع شبکه و پهنای باند موجود به خوبی استفاده می شود. RIP به صورت پیش فرض توانایی پشتیبانی 4 مسیر با متریک یکسان جهت load balancing را دارد.



RIP Version 2

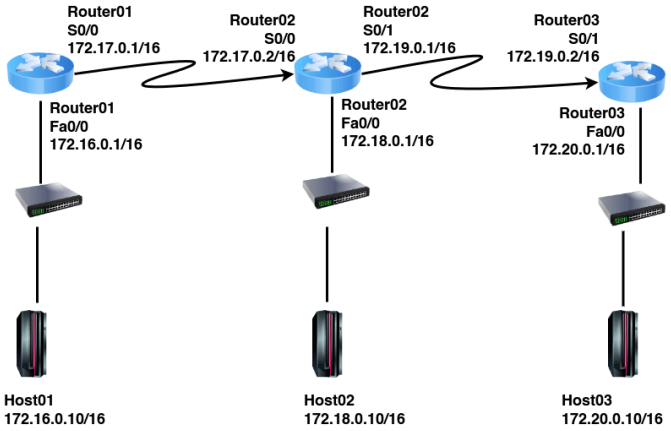
این پروتکل هم از نوع Distance Vector می باشد ولی پیشرفته تر از RIP Ver1 است. پروتکل RIP Ver 2 از Multicasting به جای Broadcast استفاده می کند اما قابلیت کار به صورت Broadcast را نیز دارا می باشد. پروتکل RIP ver2 یک پروتکل Classless می باشد و VLSM را پشتیبانی می کند.

RIP Ver2 همچنین از احراز هویت پشتیبانی می کند که این توانمندی باعث می شود که روترها قبل از آپدیت جدول مسیریابی و رد و بدل کردن اطلاعات مسیریابی یکدیگر را احراز هویت نمایند و بعد از تکمیل پروسه احراز هویت جدول های مسیریابی را بین یکدیگر مبادله کنند. در این پروتکل انتخاب بهترین مسیر بر اساس HOP Count با تعداد روترها موجود در مسیر محاسبه می شود.

Interior Gateway Protocol (IGP)

IGRP یک زیرمجموعه از پروتکل distance-vector interior gateway است که توسط CISCO توسعه یافته است. برای غلبه بر محدودیت های RIP معرفی شده است. معیارهای مورد استفاده عبارتند از بار، پهنای باند، تاخیر، MTU و قابلیت اطمینان. به طور گسترده ای توسط روترها برای تبادل داده های مسیریابی در یک سیستم autonomous استفاده می شود.

این نوع پروتکل مسیریابی برای اندازه شبکه های بزرگ از RIP بهتر است زیرا پس از هر 90 ثانیه پخش می شود و حداکثر تعداد 255Hop دارد. این به شما کمک می کند تا شبکه های بزرگتری را در مقایسه با RIP مدیریت کنید. IGRP همچنین به طور گسترده ای مورد استفاده قرار می گیرد زیرا در برابر ایجاد حلقه Loop در مسیریابی مقاوم است زیرا هنگام تغییر مسیر در شبکه خاص به طور خودکار به روز می شود. همچنین گزینه ای برای بارگیری تعادل ترافیک در مسیرهای هزینه متریک مساوی یا نابرابر ارائه شده است.



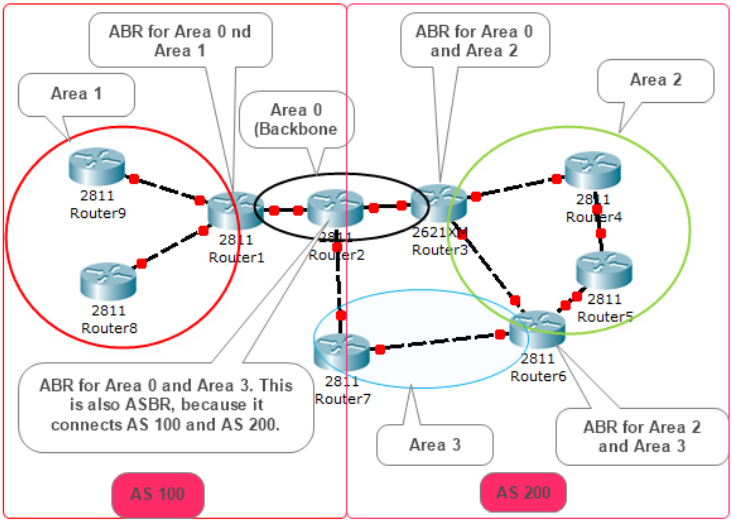
Open Shortest Path First (OSPF)

یک پروتکل مسیریابی Link state است که می تواند ترافیک های مربوط به پروتکل IP را مدیریت کند. تقریبا همه روترهایی که در دنیا وجود دارند از پروتکل OSPF پشتیبانی می کنند. از پروتکل های خانواده IGP می باشد که توسط EITF به عنوان یک استاندارد عمومی ارائه شد. این پروتکل قدرتمند به این دلیل طراحی شد که پروتکل RIP توانایی کار کردن در شبکه بزرگ را نداشت. این پروتکل برای شبکه های IP طراحی شد و از Subnetting پشتیبانی می کند.این پروتکل مسیریابی از الگوریتم Shortest Path First یا SPF برای جلوگیری از به وجود آمدن Routing Loopدر توپولوژی شبکه ها استفاده می کند و به نوعی یک شبکه Loop Free ایجاد می کند. OSPF فرآیند Convergenceسریعی دارد و از طرفی قابلیتIncremental Update را نیز با استفاده از Link State Advertisementیا LSA فراهم می کند.

مجموعه روترهایی که OSPF را اجرا می کنند به بخش هایی تحت عنوان Area تقسیم می شوند. یک شبکه OSPF باید یک Area 0 داشته باشد و علاوه بر آن می تواند Area های دیگری نیز داشته باشد. الگوریتم SPF در هر Area اجرا می شود و همچنین مسیر های ناحیه ای بینArea ها رد وبدل می شوند. به صورت پیش فرض توانایی پشتیبانی 4 مسیر با متریک یکسان جهت load balancing را دارد.

در OSPF دو سطح وجود دارد:

Area 0 به عنوان ناحیه انتقال طراحی شده است و Area های دیگر به آن متصل می شوند. Area ها دیگر باید به صورت مستقیم به Area 0 متصل شوند و از طریق Area 0 به دیگر Areaها دسترسی پیدا کنند.



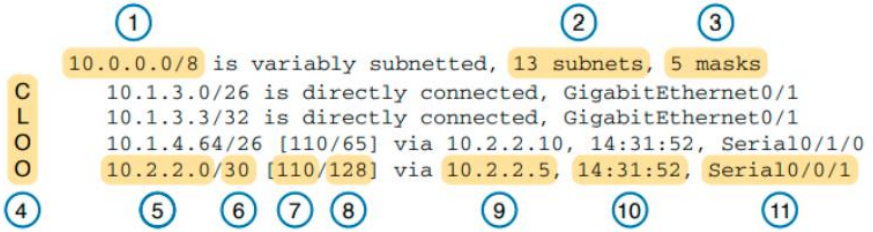
Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP یک پروتکل مسیریابی ترکیبی است که پروتکل های مسیریابی distance vector و پروتکل های مسیریابی link-state را ارائه می دهد. پروتکل مسیریابی فرم کامل EIGRP پروتکل مسیریابی پیشرفته داخلی است. پروتکل های مشابهی را که IGRP با استفاده از معیارهای ترکیبی مشابه IGRP هدایت می کند، هدایت می کند، که به شبکه کمک می کند بهترین مقصد مسیر را انتخاب کند.

Border Gateway Protocol (BGP)

BGP آخرین پروتکل مسیریابی اینترنت است که به عنوان DPVP (distance path vector protocol) طبقه بندی می شود. این نوع پروتکل مسیریابی هنگام ایجاد تغییرات، داده های جدول روتر به روز شده را ارسال می کند. بنابراین هیچ auto-discovery از تغییرات توپولوژی وجود ندارد، به این معنی که کاربر باید BGP را به صورت دستی پیکربندی کند.

Router# show ip route



Item	Idea	Value in the Figure	Description
1	Classful network	10.0.0.0/8	The routing table is organized by classful network. This line is the heading line for classful network 10.0.0.0; it lists the default mask for Class A networks (/8).
2	Number of subnets	13 subnets	The number of routes for subnets of the classful network known to this router, from all sources, including local routes—the /32 routes that match each router interface IP address.
3	Number of masks	5 masks	The number of different masks used in all routes known to this router inside this classful network.
4	Legend code	C, L, O	A short code that identifies the source of the routing information. *O* is for OSPF, *D* for EIGRP, *C* for Connected, *S* for static, and *L* for local. (See Example 16-8 for a sample of the legend.)
5	Prefix (Subnet ID)	10.2.2.0	The subnet number of this particular route.
6	Prefix length (Mask)	/30	The prefix mask used with this subnet.
7	Administrative distance	110	If a router learns routes for the listed subnet from more than one source of routing information, the router uses the source with the lowest administrative distance (AD).
8	Metric	128	The metric for this route.
9	Next-hop router	10.2.2.5	For packets matching this route, the IP address of the next router to which the packet should be forwarded.
10	Timer	14:31:52	For OSPF and EIGRP routes, this is the time since the route was first learned.
11	Outgoing interface	Serial0/0/1	For packets matching this route, the interface out which the packet should be forwarded.

Route Type	Administrative Distance
Connected	0
Static	1
BGP (external routes [eBGP])	20
EIGRP (internal routes)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (external routes)	170
BGP (internal routes [iBGP])	200
DHCP default route	254
Unusable	255

The Various Routing Protocols

Features	RIP v1	RIP v2	IGRP	OSPF	EIGRP
Classful / Classless	Classful	Classless	Classful	Classless	Classless
Metric	Hop	Hop	Composite (bw and delay)	Cost 100,000/BW	Composite (bw and delay)
Periodic Advertisement	30 seconds	30 seconds	90 seconds	none	30 seconds
Advertising Address	255.255.255.255 (broadcast)	224.0.0.9 (multicast)	255.255.255.255 (broadcast)	224.0.0.5 224.0.0.6 (multicast)	224.0.0.10 (multicast)
Administrative Cost	120	120	100	110	Internal: 90 External: 170
Category	Distance Vector	Distance Vector	Distance Vector	Link State	Hybrid

Open Shortest Path First (OSPF)

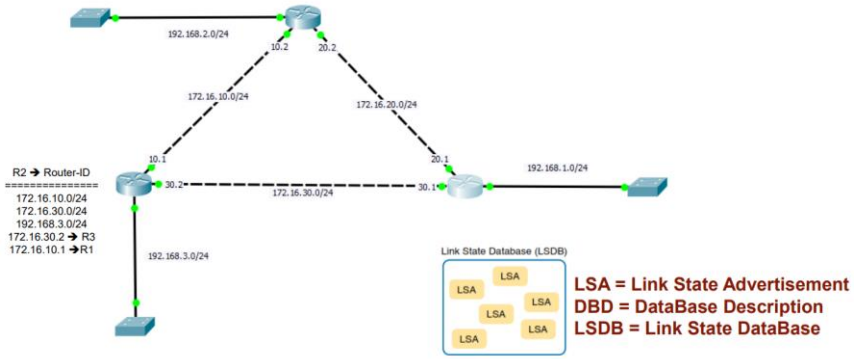
Open Shortest Path First
SPF Algorithm ➔ Dr. Dijkstera
OSPF V1 ➔ Expired
OSPF V2 ➔ IPV4
OSPF V3 ➔ IPV6 - IPV4/IPV6
IGP ➔ Link State (LS)
AD = 110
Metric = Cost ⇔ BW

$$\text{Default Cost} = \frac{8}{\frac{10}{BW}}$$

در زمان طراحی ospf سرعت شبکه 100Mbps بوده = 10^8

Router ID

هر روتری که در شبکه های OSPF قرار بگیرد به یک OSPF Router ID یا Identifier منحصر به فرد نیاز دارد. Router ID برای شناسایی یک روتر در شبکه های مبتنی بر پروتکل مسیریابی OSPF استفاده می شود و هر روتر برای اینکه در شبکه بصورت مشخص شناسایی شود برای خود دارای یک Router ID است. Router ID یک عدد خاص نیست بلکه یک آدرس IP v4 است (یک عدد 32 بیتی باینری) ، این آدرس IP به هر روتری که بر روی آن پروتکل OSPF پیکربندی شده باشد اختصاص پیدا می کند.



پروتکل OSPF از دسته ی IGP(Interior Gateway Protocol) است، یعنی پروتکلی است که درون یک AS(Autonomous System) کار می کند. این پروتکل استاندارد RFC2328 است، یعنی همه ی تجهیزات می توانند از آن استفاده کنند. این پروتکل می تواند تغییرات را به سرعت در شبکه اعمال کند، همچنین قابلیت triggered update دارد یعنی پس از هر تغییر یک آپدیت جدید ارسال و به همه خبر می دهد که این تغییر در Routing ما انجام شده است.

همچنین قابلیت periodic update دارد یعنی هر چند دقیقه یکبار هم یک آپدیت کلی ارسال می کند.(پیشفرض هر30دقیقه) پیغام هایی که OSPF ارسال می کند LSA(Link State Advertisement) نامیده می شوند، اما در برخی منابع نیز PDU(Protocol Data Unit) نامیده شده است. اگر تغییری در شبکه اتفاق بیافتد، در قالب پیغام های LSA اطلاع رسانی می شود. پیغام های LSA روی آدرس Multicast 224.0.0.5 ارسال می شود، یعنی درون فایروال باید این آدرس را برای OSPF باز بگذارید.

هر روتر LSA دریافتی را پس از ذخیره کردن برای همسایه ها Forward می کند، منتها محدوده ی Forward درون همان Area است. روترهاLSA ها را درون LSDB(Link State Data Base) روی روتر ذخیره می کنند.

LSDB)معادل همانTopology Table درون EIGPR می باشد (درون LSDB الگوریتم Dijkstra's (یکی از الگوریتم های پیمایش گراف) بهترین مسیرها را برای مقصدهای مختلف بدست می آورد و این مسیرهای منتخب درون Routing Table قرار می گیرند.

هر روتر براساس موقعیت و مکان خودش، بهترین مسیر را از LSDB انتخاب می کند، بهترین مسیر برای همه ی روترها همیشه یکسان نیست بلکه براساس Position و شرایط آن روتر انتخاب می شود. بهترین مسیرها درون Routing Table قرار میگیرد که به آن Forwarding Database هم گفته می شود.

روتری که در OSPF شرکت می کند، اولین کاری که باید انجام دهد این است که اطلاعات همسایه ها را نگهداری کند. برای این کار قطعا یک Neighbor Data Base خواهد داشت.(که Adjacency Data Base هم نامیده می شود) بعد از شناختن همسایه هایی که روی آنها OSPF اجرا شده است و در حال ارسال و دریافت LSA هستند، LSDB و به تبع آن Routing Table هم تکمیل می شود. (هنگام T-Shoot در OSPF ابتدا باید دید که Neighborها را شناخته باشد).

از ساختار Area برای جلوگیری از بزرگ شدن LSDB استفاده می کند. تعداد روتر توصیه شده برای هر Area حداکثر 50 روتر می باشد. نمی شود گفت که OSPF برای مدیریت شبکه به دنبال ساختار Area رفته است، چراکه وقتی حجم LSDB بالا برود کار الگوریتم برای محاسبه دشوار می شود زیرا شبکه خیلی پیچیده شده و تغییرات زمان بر است که این مطلوب نیست.

علاوه براین LSDB یک سری attribute برای هر مسیر دارد که resource فراوانی را اشغال می کند، زیرا برای انتخاب بهترین مسیر این attribute روی RAM دستگاه قرار می گیرد و هنگام اعمال الگوریتمRAM و CPUفراوانی اشغال می شود. ساختار Area درون OSPF دو لایه ای است: لایه اول Backbone Area ، لایه دوم Regular Area .

Backbone که همان Area 0 می باشد در واقع هسته ی اصلی Routing Protocol ما است . روترهای درون Area 0 باید از قدرت بالایی برخوردار باشند چراکه تمام ترافیک Routing شبکه باید از آن عبور کند حداکثر تعداد روتر توصیه شده درون یک area 50 روتر می باشد Area 0 هسته است اما نه هسته ی شبکه بلکه هسته ی Routing Protocol است، یعنی ترافیک سایر Routing protocol ها کاری با Area 0 ندارند.

Regular Area که Normal Area یا None-Backbone هم نامیده می شود سایرArea ها می باشند که فقط با Area 0 در ارتباط اند. یک Normal Area نمی تواند به صورت پیشفرض ترافیک سایرNormal Area ها را عبور دهد. هر Area یک LSDB منحصربه خود دارد که روی تمام روترهای عضو آن باید یکسان باشد.

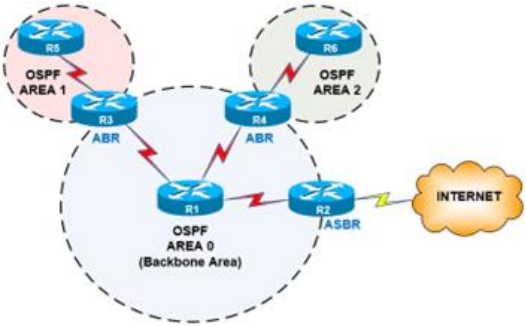
LSDB یک Area با هیچ Area دیگری یکسان نیست. بین دو Area جزئیات تمام مسیرها ردوبدل نمی شود چون کاربردی نیست بلکه تنها اطلاعات بهترین مسیر مدنظر داده می شود. توصیه شده است که یک روتر حداکثر عضو سه Area باشد. برای هر روتر بسته به ویژگی ها و وظیفه ای که درون OSPF برعهده دارد نام های زیر در نظر گرفته می شوند:

Internal Router به روتری که همه ی interface های آن درون تنها یک Area باشد، گفته می شود.

Backbone Router روتری که حداقل یک interface آن درون 0 Area باشد.

ABR(Area border Router) روتری که interface های آن درون Area های مختلف است و به ازای هر Area یک LSDB جداگانه دارد. معمولا ABR بین 0 Area و Normal Area ها می باشد.

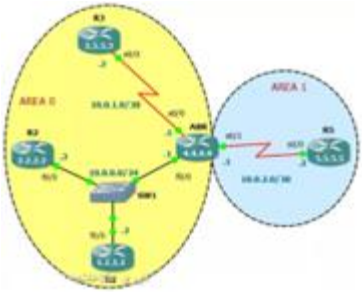
ASBR(Autonomous System Boundary Router) روتری که حداقل یک interface آن به یک Routing Domain دیگر متصل باشد.



برای ایجاد همسایگی روترها ابتدا روی آدرس Multicast پیغام Hello ارسال می کنند. درون این پیغام یک سری اطلاعات راجع به OSPF ارسال می شود. اولین شرط همسایگی این است که این دو روتر حتما درون یک Area باشند. درون یک Area وقتی یک روتر جدید اضافه می شود پس از ایجاد همسایگی، باید تمام LSDB این Area برای روتر جدید ارسال شود. اما گاهی ارتباط این همسایه ها P2P نیست و ممکن است چند روتر از یک Area مثلا به یک سوئیچ متصل باشند وNetwork Type ما Broadcast Domain باشد. نحوه ی رفتار OSPF نسبت به این دو نوع شبکه کاملا متفاوت خواهد بود:

حالت P2P در OSPF : زمانی که دو روتر با یک لینک سریال به هم متصل شده اند و پروتکل HDLC یا PPP روی آن اجرا شده است، در این حالت قطعا LSDB ها جابجا می شوند و یکبار هم بیشتر این کار انجام نمی شود.

حالت Broadcast در OSPF : زمانی که چند روتر از طریق سوئیچ به هم متصل هستند، در این حالت اگر روترها بخواهند دو به دو با هم LSDB جابجا کنند حجم زیادی دیتا باید ردوبدل شود که مطلوب نیست.



در این ساختارها یک روتر به عنوان DR در نظر گرفته می شود، سایر روترهایی که درون این Broadcast Domain هستند، LSDB های خود را به DR ارسال می کنند. روتر DR یک نقش مرکزی دارد که آپدیت ها را از سایر روترها جمع آوری می کند و در اختیار روترهایی قرار می دهد که نیاز دارند.

یک روتر هم نقش BDR را برعهده می گیرد تا زمانی که DR از کار افتاد به عنوان جایگزین ادامه ی کار را برعهده گیرد. هدف از این مکانیزم بالابردن بازدهی شبکه است. سایر روترها که نه DR است و نه BDR هستند، در این ساختارDRouter نامیده می شوند. اگر یک روتر جدید به این سوئیچ متصل شود با سایر روترها همسایه می شود اما برای تکمیل LSDB خود فقط با DR کار دارد. محاسبه ی Metric در OSPF براساس Cost است. هر چه BW بیشتر باشد، Cost پایین تر می آید.

به عبارت دیگر Metric بر این اساس انتخاب می شود که کدام مسیر Cost کمتری دارد. مسیری Cost کمتری دارد که BW بیشتری داشته باشد، یعنی ملاک اصلی انتخاب Metric در OSPF همان BW است. لینک سریال، اگر Kbps56 باشد، Cost آن 1785 است، اگر Kbps64 باشد، Cost آن 1562 است. اگر E1 باشد48 ، اگرEthernet باشد 10 و اگر Fast Ethernet باشد 1 است.

در OSPF ما با پیغام های LSA سروکار داریم، LSA روشی دارد که reliable باشد. هر LSA یک Sequence Number دارد که براساس آن Sequence Number جواب های Acknowledge ارسال می شود یعنی در LSA برای تشخیص جدیدترین آپدیت ها از Sequence Number استفاده می شود. همچنین هر LSA یک MaxAge دارد یعنی مدت زمانی که آن LSA معتبر خواهد بود که به صورت پیشفرض یک ساعت است اگر آپدیتی دریافت نکند، پس از 60 دقیقه آن LSA نامعتبر می شود. به صورت پیشفرض هر 30دقیقه یکبار OSPF کل LSDB ای که دارد را درون شبکه Deploy می کند.

یک پیغام به نام LSU(Link State Update) وجود دارد که آپدیت های Routing را ارسال می کند، هر LSU می تواند شامل چندین LSA باشد. وقتی که روتر یک LSU دریافت می کند ابتدا تک تکLSA های درون آن را بررسی می کند که آیا این آپدیت ها را در LSDB خود دارد یا خیر، مثلا فرستنده ی LSU می خواهد بگوید که به سمت شبکه ی 40.0.0.1 یک Route دارداگر روتر گیرنده ی LSU آن Route را نداشته باشد.

آن LSA (همان 40.0.0.1) را ذخیره کرده و یک Ack برای فرستنده ارسال کرده و سپس الگوریتم روی LSDB اجرا می شود تا Routing Table با توجه به آپدیت های جدید چیده شود. ممکن است پیش بیاید که یک LSU دریافت کنیم که آپدیت جدیدش برای LSA ای باشد که در LSDB ما از قبل موجود است.

(مثلا روتر من 40.0.0.1 را از قبل دارد)، حال باید Sequence Number این LSA دریافتی با Sequence Number آن LSA ای که از قبل در LSDB ما موجود بوده مقایسه شود، اگر Sequence Number دریافتی بزرگتر باشد پس روتر آن را Add کرده و Ack را نیز می فرستد. اگر کوچکتر باشد پس روتر وقتی که می بیند بسته های قدیمی بدستش می رسد یک LSU از آن موارد ساخته و برای Source ای که LSU قدیمی را فرستاده بود، می فرستد تا LSU آن هم آپدیت شود.

انواع Packet در OSPF

Hello : هر 10 ثانیه دوره ای ارسال می شود تا همسایه ها را پیدا کرده و ارتباط را برقرار کند. اگر hello ها دریافت نشوند همسایگی از بین می رود. هر روتر یک Dead Interval دارد که به صورت پیشفرض چهار برابر زمان ارسال دوره ای Hello Packet آن می باشد (پیشفرض 40 ثانیه) و مشخص می کند که چه مدت باید منتظر دریافت Helloاز سمت Neighbor بمانیم و پس از گذشتن این مدت همسایگی از بین می رود. علت استفاده از Dead Intervalاین است که بلافاصله پس از دریافت نکردن یک hello کل توپولوژی به هم نخورد، روتر باید منتظر بماند چراکه شاید Packet Lost اتفاق افتاده باشد یا مشکل موقتی دیگری است. توصیه می شود جایی که شبکه ی ما زیاد Stable نیست مقدار Dead Interval را بیشتر بگذاریم.

DBD(Data Base Description) : وقتی دو روتر تازه همسایه شدند، باید چک شود که آیا این ها LSDB هایشان یکی هست یا خیر. به عبارت دیگر کاربرد DBD برای Data Base Synchronization است DBD کل LSDB را نمی فرستد بلکه تنها یک خلاصه ای از آن را ارسال می کند.

LSR (Link State Request) : وقتی که روتر دنبال یک LSA می گردد و اطلاعات آن را از همسایه ها درخواست می کند. مثلا زمانی که یک DBD دریافت می شود ممکن است تعدادی از اطلاعات درون آن برای روتر شناخته باشد پس یک LSR برای فرستنده ی DBD ارسال می شود تا در قالب یک LSU اطلاعات کامل مسیرهای خواسته شده دریافت شود.

LSAck : زمانی که قرار است Acknowledge ارسال شود. این LSAck بحث reliable بودن OSPF را تصدیق می کند.

LSU : زمانی که قرار است آپدیت ارسال شود LSU گاهی یک جواب برای LSR است.

پیغامی مثل Hello نیاز به Ack ندارد چون مداوم در بازه های زمانی ارسال می شود، اما وقتی LSU داریم حتما باید در جواب Ack بفرستیم. تمامی پنج Packet توی OSPF به صورت لایه سومی توسط بسته های IP ارسال می شوند یعنی OSPF از UDP و TCP استفاده نمی کند و مکانیزم خاص خود را دارد. شما یک Frame دارید که Header و trailer دارد، داخل Frame یک قسمتی به نام IP Header وجود دارد و درون آن Protocol ID Number مشخص شده است که مقدار آن 89 می باشد تا هر روتری که این بسته را گرفت بفهمد که OSPF است.

پارامترهای دیتا در پروتکل OSPF

Version Number : برای IPv4 ورژن 2 و IPv6 هم از ورژن 3 استفاده می کند.

Type : نوع OSPF Packet ارسالی را مشخص می کند.

Length : طول بسته را نشان می دهد.

Router ID : یک مقدار 32بیتی اندازه IPv4 که می تواند به صورت دستی تنظیم شود، پیشفرض اگر اینترفیس Loopbackداشته باشیم مقدار Router ID همان IP آن اینترفیس است وگرنه IP اینترفیسی برای Router ID انتخاب می شود که عدد شماره اش بیشتر است و آن اینترفیس فعال است. علت اولویت Loopback این است که هیچ وقت خاموش نمی شود یا هست یا نیست. برای ایجاد همسایگی ابتدا روتری که Router ID بالاتری دارد، DBD را ارسال می کند Router ID .تنها فرمتش مانند IPv4 است و هیچ ارتباط دیگری با هم ندارند.

Area ID : یک شناسه 32بیتی

Checksum :برای error detection استفاده می شود. و در موارد که دو LSA دارای SeqNumber برابر باشند، ملاک بعدی برای تعیین جدیدترین LSA همین Checksum است.

AuType :نوع Authentication می تواند یاnull باشد یعنی بدون رمز، یا رمز ساده باشد و یا از الگوریتم MD5 برای کدنگاری استفاده کند.

Authentication :یک فیلد 64بیتی برای ذخیره ی رمز

اما درون IP Packet پس از Header نوبت به فیلد دیتا می رسد:

اگر Packet Type از نوع Hello باشد، پس فیلد دیتا شامل لیستی از همسایه ها است.

اگر Packet Type از نوع DBD باشد، شامل خلاصه ای از LSDB است.

اگر LSR باشد، شامل نوع LSU های درخواست شده است.

اگر LSAck باشد، فیلد دیتا خالی است

شرط اول همسایگی، برابری Area ID است. همچنین مقدار MTU نیز در هر دو طرف لینک برای ایجاد همسایگی باید یکسان باشد. اگر مقدار Dead Interval برای Hello Packet روی دو روتر یکسان نباشد همسایگی برقرار نمی شود. همچنین AuType و رمز هم بین دو طرف باید یکسان باشد.

توصیه می شود همیشه ابتدا شبکه را اندازی کنیم و سپس به فکر Authentication باشیم. برای همسایگی فقط primary IP addressدر نظر گرفته می شود و خیلی از سرویس ها روی secondary IP address اجرا نمی شوند. معمولا از secondary IP address به عنوان یک نقش کلاینتی استفاده می شود. همچنین برای همسایگی Subnet Maskها نیز باید یکی باشند.

هر روتر یک Router Priority دارد، که برای انتخاب DR و BDR در یک Broadcast Domain استفاده می شود. DRوBDR هم برای آپدیت کردن از Multicast استفاده می کنند اما نه از 224.0.0.5 بلکه از 224.0.0.6. پس ما باید در تنظیمات فایروال و ACL این IP را باز گذاشته باشیم. به عبارت دیگر ارتباط روترها با DR روی آدرس 224.0.0.6 است.

معرفی وضعیت های مختف روتر در پروتکل OSPF برای رفع اشکال

Down State: یعنی همسایگی برقرار نیست. مثلا پیش می آید که شما تمام تنظیمات را درست انجام داده اید و حتی ping همسایه را هم دارید ولی وضعیت همسایگی برقرار نیست، در این حالت قطعا Hello Packet ها در طول مسیر Drop شده اند و رنج Multicast 224.0.0.5 باز نیست.

Initialize: یعنی برای اولین با یک Hello Packet دریافت شده است. پس از اینکه روتر دوم اولین Hello را دریافت کرد، برای فرستنده ی آن یک hello از جنس Unicast می فرستد تا درخواست همسایگی اجابت شود. به همین علت است که Hello Packet ها نیاز به LSAck ندارند.

Two Way: یعنی هر دو طرف قبول کردند که باهم همسایه باشند.

Exstart: علت استفاده از الویت Router ID در این مرحله انتخاب شروع کننده ی ارسال DBD است چون هر دو روتر همزمان نمی توانند برای هم DBD ارسال کنند و یکی باید فرآیند را آغاز کند.

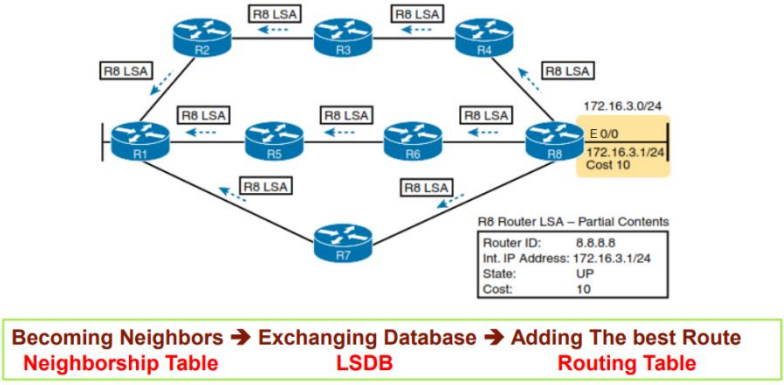
Exchange State: پس از همسایگی نوبت به همگام سازی LSDB ها رسیده است. حالت Exchange هنگامی است که بالاترین Router ID شروع به ارسال DBD می کند. هر دو روتر پس از دریافت DBD برای هم LSAck می فرستند.

Loading State: در این مرحله چک می شود که با LSR چه اطلاعاتی را باید درخواست دهد و از LSU دریافت کند. پس از این که هر روتر خلاصه ای از LSDB همسایه اش را دریافت کرد، حال آن Record هایی که ندارد را درخواست می کند.

Full: یعنی LSDB ها هم همگام سازی شده اند.

خلاصه ای از وضعیت LSA ها هر 30 دقیقه یکبار در شبکه ارسال می شود. تا هر روتری که دید Record خاصی را ندارد با LSR درخواست کند تا با LSU دریافت کند. وقتی که یک LSA مجددا دریافت می شود Life Time آن Refreshمی شود MaxAge .برای هر LSA پیشفرض 60 دقیقه است، یعنی اگر پس از 60 دقیقه LSA ای Refreshنشود، آن LSA از درون LSDB حذف می شود.

قبلا گفتیم که برای پیدا کردن بروزترین LSA باید SeqNumber ها چک شود، اما اگر SeqNumber ها برابر باشد، باید CheckSum های آن ها مقایسه شود و آن LSA ای که عدد CheckSum بالاتری داشته باشد، بروزتر است. اگر CheckSum ها نیز یکی بود، Age Time بررسی می شود که کدام Age کمتری دارد. لازم به ذکر است که SeqNumber یک عدد 32 بیتی است و به صورت هگزادسیمال نمایش داده می شود.



لحظه خروج از اینترفیس Cost محسابه می شود یا روی آن قرار داده می شود.

انجام تنظیمات مربوط به پروتکل OSPF روی روتر

با استفاده از دستورات زیر و قالب دستوری زیر می توانید این پروتکل را روی روترهای خود پیاده سازی کنید:

Router(config)# router ospf process_ID

Router(config-router)# network network_id wildcard_mask area area#_

Router>enable

Router #configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router (config)#router ospf 1 انتخاب پروتکل و پروسس آیدی از 1 تا 65535

بعد از انتخاب پروسس آیدی روتر برای خودش روتر آیدی تعریف می کند اما میتوانیم دستی تعریف کنیم،روتر آیدی باید یونیک باشد اگر نه همسایگی رقرار نمی شود.

Loopback Interfaceیک Interface مجازی یا Logical است که روی روترهای سیسکو تعریف می شود . Loopback Interfaceمانند Interface های فیزیکی مثل Fast Ethernet یا Gigabit Ethernet نیست و تنها interface هست که می توان به آن 32/ به آن ip بدهیم.

این Interface نه به پورت ها یا Interface های فیزیکی روتر سیسکو متصل می شود و نه شبکه ای می تواند به آن متصل شود و مهمترین ویژگی این Interface این است که هیچوقت down نمی شود مگر اینکه خود دستگاه بصورت کامل خاموش شود. یکی از پرکاربردترین استفاده هایی که از Loopback Interface می شود در پروتکل مسیریابی OSPF است.

همانطور که اشاره کردیم loopback interface همیشه up است و به همین دلیل به پروتکل Border Gateway Protocol یا BGP اجازه می دهد که neighborship بین دو روتر در شبکه را حتی زمانیکه یک interface فیزیکی down شده است up نگه دارد. کاربرد دیگر loopback interface در پروتکل های RSRB و DLSW است که در این پروتکل ها به عنوان Termination Point یا نقطه پایانی مورد استفاده قرار می گیرد. دقت کنید که حتی اگر Interface فیزیکی روتر شما down باشد loopback interface روتر فعال است و همیشه در دسترس می باشد.

Router (config-router)#router-id 1.1.1.1 یک عددی شبیه به آی پی

اگر روتر آی پی را ما انتخاب نکنیم روتر انتخاب می کند واگر چند اینترفیس لوپ بک وجود داشت، بزرگارین آی پی اینترفیس لوپ بک رو استفده میکند برای روتر آی دی و اگر اینترفیس لوپ بک نداشتیم بزرگترین آی پی از اینترفیس های فیزیکال را بعنوان روتر آی دی انتخاب می کند. اینجا ما 1.1.1.1 دستی انتخاب کردیم.

Router2 (config)#interface loopback 100

Router2 (config-if)#ip address 2.2.2.2 255.255.255.255

Router2 (config-if)#router ospf 200

با این دستور هر پروتکلی فعال کرده باشیم نمایش می دهد Show ip protocol

یا این دستور Show ip ospf

Show ip ospf neighbor

برقراری همسایگی بین روتر ها بصورت traditional

RTR_ESF(config-router)#network 10.10.10.0 0.0.0.3

بدلیل اینکه این پروتکل سنگین هست، area بندی کرده شبکه را، وقتی میخواهیم همسایگی برقرار کنیم باید تعریف کنیم که در کدام areaیا کدام دست روتر قرار دارد.

RTR_ESF(config-router)#network 10.10.10.0 0.0.0.3 area 0

و بعد network هایی که روی هر روتر وجود دارد را توی ospf به بقیه advertise کنیم.

RTR_ESF(config)# router ospf 200

RTR_ESF(config-router)#network 192.168.20.0 0.0.0.255 area 0

هر نتورکی که زیر این اینترفیس باشد را انگار با دستور نتورک وارد ospf می کند. که به این روش explicit می گویند.

RTR_TBRZ(config)# int g 0/0/1

RTR_TBRZ(config-if)#ip ospf 200 area 0

خلاصه عملکرد ospf

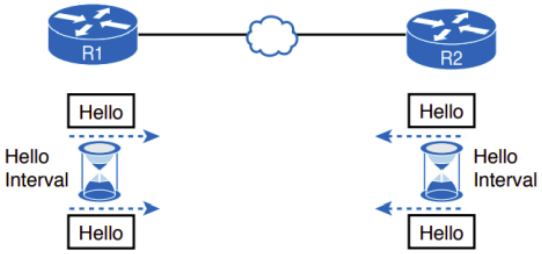
یاد گرفتیم چطور ospf را فعال کنیم و Router ID چطور انتخاب میشه که سه روش دارد:

```
1 - Manually Configured
2 - Highest IP Address of Loopback interface [up/up]
3 - Highest IP Address of  Non-Loopback interface [up/up]
```

1-دستی

2-بزرگترین ip از interface loopback در صورت وجود

3-اگر وجود نداشت از Non-Loopback interfaceکه میتواند از vlan,physycal,subinterface یا هرچیزی که up/upباشد.



Ospfبعد از اینکه up شد وهمسایگی برقرار شد هر 10 ثانیه یکبار بسته های Hello برای یکدیگر ارسال می کنند ، اگر 4 تا Hello فرستاد و طرف مقابل جواب نداد (dead time)متوجه می شود که روتر طرف مقابل از دسترس خارج شده و هر route که ازش یاد گرفته بود رو از روی lsdb پاک میکند و درنتیجه د ر routing table نمیبینم.

Ospf در indirect/direct topology change ممکن هستن در بعضی مواد مشکلاتی داشته باشد برای مثال بین دو روتر سوییچ قرار دارد و اگر روتر مقابل شات شود مسیر down می شود و مسر دیگر را جایگزین می کند و روتر همسایگی را بعد از dead time میتواند downکند به دلیل اینکه ارتباط directly نیست.

BFDمکانیزم تشخیص سریع Down شدن همسایگی است .BFD با ارسال بسته های Hello در بازه های زمانی بسیار کوتاه، در صورت عدم دریافت Hello در چند بازه زمانی متوجه Down شدن همسایگی می شود. بازه زمانی بسیار کوتاه و معمولا 50 میلی ثانیه است.

که اگر بخواهیم با زمان چندین ثانیه در پروتکل های مسیریابی مقایسه نماییم، بسیار قابل توجه است. ضمنا BFD مکانیزم مشترک ما بین همه پروتکل های مسیریابی است. بدین معنی که همه پروتکل های مسیریابی می توانند از این مکانیزم بهره ببرند و زمان همگرایی خود را کاهش دهند.

OSPF Metric

نحوه جابجایی مسیر ترافیک در OSPF

برای اینکه یک مسیر را بهتر یاد بدتر کنیم که مسیر ترافیک را جابجا کنیم میتوانیم متریک را تغییر دهیم و cost رو بیشتر کنیم باید BW اینترفیس رو کمتر کنیم اما این کار پیشنهاد نمی شود زیرا تغییر BW زیر اینترفیس هیچ تاثیری روی ترافیکی که روی آن اینترفیس رد میشود ندارد اما در پروتکل هایی که استفاده میکنیم مثل stp این BW لحاظ می شود .برای این کار روشی هست که در ospf میتوانیم مستقیم روی همان اینترفیس costرا تغییر دهیم و این کار را لوکالی انجام می دهد یعنی روی روتر های دیگر اعمال نمیشود.

BW که برای اینترفیس سریال در نظر گرفته شده 1544 هست که با دستور زیر میتوانیم مشاهده کنیم:

Show interface serial 0/0/1

تغییر BW با دستور زیر:

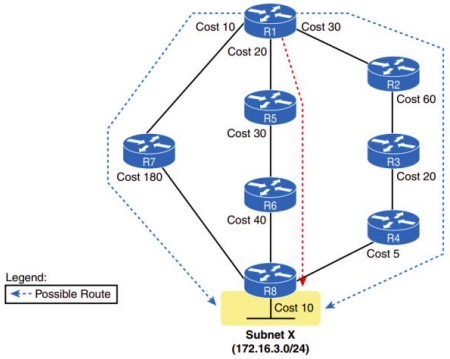
RTR_ESF(config)#Interface serial 0/1/1

RTR_ESF(config-if)#bandwidth 500

تغییر Cost با دستور زیر:

TRT_TBRZ(config)#interface serial 0/1/1

RTR_ESF(config-if)#ip ospf cost 100



Change Cost of interface :
R1(config)#interface <type> <>
R1(config-if)#ip ospf cost <1-65535>

Change Maximum-Path in ospf:
R1(config)#router ospf <>
R1(config-router)#maximum-paths <1-32>

مراحل اجرای OSPF

تشکیل جدول همسایگی

تشکیل جدول توپولوژی

اجرای الگوریتم SPF و بروز رسانی جدول مسیریابی

شرایط تشکیل همسایگی

داشتن Hello interval برابر

داشتن Dead interval برابر

داشتن شماره Area یکسان

داشتن Sunbnet mask یکسان

داشتن Subnet number یکسان

داشتن Authentication مشابه

نداشتن RID برابر

نحوه تبادل اطلاعات Topology

در شبکه های زیر این تبادل اطلاعات با کمی تفاوت انجام می شود:

شبکه های Point to Point

شبکه های Multi Access (Broadcast)

نکته : از روی نوع لینک امکان تشخیص شبکه فراهم می شود به طور مثال Fastethernet به عنوان یک شبکه Multi Access و Serial به عنوان یک شبکه Point to Point در نظر گرفته می شود.

بررسی مفهوم DR و BDR و نحوه انتخاب آنها در OSPF

در شبکه هایی که بستر ارتباطی بین روترهای شبکه مشترک است انجام عمل همسایگی و تبادل اطلاعات بین همه ارتباط باعث ایجاد بار زیاد و درگیر کردن تجهیزات می شود برای جلوگیری از این مشکل ، ارتباط و تبادل اطلاعات دو به دو انجام نمی شود و یک روتر به عنوان Designated Router یا DR انتخاب می شود و وظیفه بروز نگه داشتن همه روترها را دارد در این حالت DR یک نقطه حساس در شبکه است و اگر این روتر از کار بیافتد شبکه نیز مختل می شود برای جلوگیری از این مشکل یک روتر به عنوان Backup Designated Router یا BDR در نظر گرفته می شود و به طور دائم ، فعال و زنده بودن DR را چک می کند و در صورت بروز مشکل اطلاعات لازم برای DR شدن را دارد.به طور ساده می خواهیم تعریفی از DR داشته باشیم می گویم DR را به عنوان ریشه یک درخت در نظر بگیرد که همه روترها (شاخه ها) به آن متصل می شوند و از طریق آن اطلاعات را ردوبدل می کنند. زمانی که روی هر روتری روی هر دست آن همسایگی را فعال می کنیم یک multicast ip 224.0.0.5 در کنار unicast ip که ما ست کردیم فعال می شود .

به ترتیب براساس یکی از شرایط زیر DR انتخاب می شود:

روتری که دارای Priority بالاتر است بصورت پیشفرض 1 هست.

روتری که دارای RID بالاتری است.

اصولا روتری را DR میکنند که ظرفیت و پرفورمنس بیشتری دارد و Network Connection بیشتری دارد.

نکته :DR,BDR election قابلیت مقایسه یا preemption ندارد یعنی اگر روتری DR شد و روتر بعدی شد BDR اگر روتری اضافه شود که شرایط بهتری روی اینترفیس آن داشت یعنی priority بیشتری داشت یا Router ID بزرگتری داشت در DR,BDR سریع تغییری ایجاد نمی شود، تا وقتی که DR وجود دارد و کار می کند سرجای خود قرار دارد اما وقتی down شد مجدد election انجام می شود. یکی از راهکار ها این است که ospf را suspend کنیم:

```
RTR(config)#router ospf 25184
RTR(config-router)#shutdown
RTR(config-router)#no shutdown
```

DR,BDR به ازای اینترفیس انتخاب می شود، ممکن است روی دست های دیگر روتر ارتباط P2P داشته باشیم و ما نمیخواهیم همسایگی روی دست های دیگر روتر که ارتباط سریال دارد down شود و میخواهیم همسایگی ها up,down شود بجای این کار از دستور:

```
RTR#clear ip ospf 25184 process
```

نکته: ملاک انجام انتخاب DR,BDR در ospf بررسی Media Type هست. اگر بخواهیم به ازای یک اینترفیس DR,BDR election نداشته باشیم میتوانیم priority را صفر قرار دهیم. مثلا دو روتر ارتباط P2P دارند و از طریق فیبر به هم وصل شدند که بصورت پیشفرض DR,BDR election را انجام می دهد اما نیازی نداریم و همسایگی دیر تر up می شود میتوانیم priority را روی اینترفیس ها صفر بذاریم یا Network type را point-to-point تنظیم می کنیم اما روتر طرف مقابل هم باید حتما Network Type را تغییر دهیم یا حتی میتوان به ازای پروسس آیدی Network Type را تغییر دهیم چون ممکن است اینترفیس مورد نظر در ospf های مختلف مشارکت داشته باشد.

RTR(config)#int g 0/1

RTR(config-if)#ip ospf network point-to-point

نکته : اگر Priority یک روتر 0 باشد به عنوان DR یا BDR انتخاب نمی شود .

نکته: انتخاب DR و BDR در OSPF به ازای interface اتفاق می افتد نه به ازای کل روتر، ممکن است یک دست روتر ارتباط سریال (P2P) باشد یک دست دیگر ارتباط فیبر (broadcast) .

نکته : Priority می تواند بین 0 تا 255 مقدار بگیرد و پیش فرض آن 1 می باشد.

نکته : انتخاب DR و BDR غیر رقابتی است یعنی یکبار این انتخاب انجام می شود و حتی یک روتر با Priority بهتر در شبکه حضور پیدا کند باز هم همان روترهای قبلی به عنوان DR و BDR خواهند بود مگر اینکه پروسه OSPF ریست شود.

وضعیت های که روترها سپری می کنند تا همسایه شوند به صورت زیر است:

Down

Initialize

Two way

Exstart

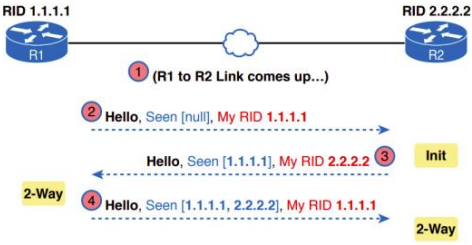
Exchange

Loading

OSPF Neighbor States

بررسی شبکه های Point to Point

early neighbor states



در این حالت بین دو روتر یک لینک اختصاصی وجود دارد مانند اینترفیس سریال و DR,BDR نیاز ندارد. در این شبکه ها مراحل همسایگی و تبادل اطلاعات توپولوژی به صورت زیر است:

مرحله اول همسایگی: بطور کل در همه igp ها فقط با روتری میتوان همسایگی برقرار کرد که آن روتر directly connected باشد اگر بین دو روتر دستگاه لایه دویی باشد مشکلی نیست اما اگر دستگاه لایه سه ای باشد دیگر نمیتوان بین دو روتر همسایگی را برقرار کنیم.

در این شبکه ها مراحل همسایگی و تبادل اطلاعات توپولوژی به صورت زیر است:

Down : هنوز OSPF روی روتر اجرا نشده و هیچ بسته ای در رابطه با OSPF رد وبدل نمی شود.

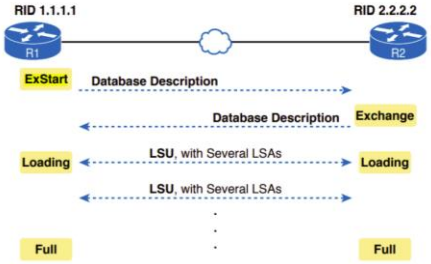
Initialize : در این وضعیت OSPF اجرا شده و روتر شروع به ارسال Hello به آدرس 224.0.0.5 که multicast است می کند. داخل بسته Hello روتر آیدی خودش و روتر هایی که با آن ها همسایگی برقرار کرده وجود دارد. روتر مقابل بررسی می کند اگر در بسته روتر آیدی خودش وجود نداشته باشد متوجه می شود که با روتر همسایه نیست و روتر آیدی خودش را در بسته قرار میدهد و ارسال می کند.

Two way : در این وضعیت روتر یک Hello که حاوی RID خودش است دریافت می کند. در صورت تطبیق شرایط مورد نیاز همسایگی با روتر مقابل همسایه شده و به آن با قرار دادن RID روتر مقابل پاسخ می دهد در این مرحله ارتباط به صورت unicast انجام می شود.

نکته: قبل از انجام Database exchange و انتخابات DR,BDR در این مرحله MTU Discovery انجام می دهد و MTU مسیربین دو روتر باید یکسان باشد ، اگر MTU یکسان نباشد همسایگی برقرار می شود و تا مرحله Two Way پیش می رود اما دیگر قادر به exchange دیتابیس نیستند.این کار را بدلیل performance انجام می دهد، MTU مسیر را Discovery می کند که بداند سایز دیتابیس هایی میخواهد بین خود و طرف مقابل جابجا کند ماکزیمم چقدر می تواند باشد اگر یک بسته ای را با یک سایزی ارسال کنیم و طرف مقابل MTU کمتری داشته باشد و در نتیجه MSS آن هم کمتر می شود و بخواهد بسته را Segmentation انجام دهد Performance کاهش می یابد پس در نتیجه برای اینکه سایز بسته هایی که ما ارسال می کنیم برای طرف مقابل با سایز بسته هایی که قرار هست دریافت کند یکی باشد و نخواهد Segmentetion انجام دهد MTU باید یکسان باشد.

Database exchange

سه مرحله اول انجام شد و همسایگی برقرار شد حالا برای اینکه Database exchange کنیم قبل از آن اگر Network Type ما broadcast باشد DR,BDR election انجام می شود یعنی بعد از 2way و ایجاد همسایگی قبل از اینکه مرحله بعدی همسایگی شروع شود. اگر نه باطرف مقابل شروع به ارسال اطلاعات می کند.



Exstart : در این مرحله کسی که قرار است تبادل اطلاعات توپولوژی را شروع کند مشخص می شود که در اینجا کسی که RID بزرگتری دارد اینکار را شروع می کند.

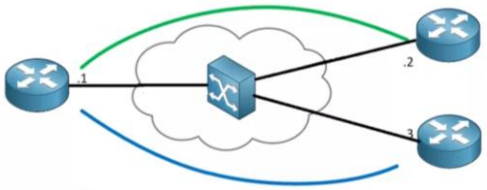
Exchange : در این مرحله روتر انتخاب شده در مرحله قبل اقدام به ارسال یک بسته DBD می کند که شامل خلاصه ای از شبکه های متصل به آن روتر می باشد سپس روتر مقابل نیز اینکار را انجام می دهد و هر روتر بعد از دریافت بسته DBD یک بسته ACK به منظور تایید دریافت بسته ارسال می کند. اینکار توسط روتر مقابل نیز انجام می شود.

Loading : روتر که بسته DBD را دریافت کرد آن را با شبکه هایی که دارد مقایسه می کند و برای شبکه هایی که آنها را ندارد توسط بسته LSR درخواست ارسال می کند که اطلاعات کامل آنها را می خواهد. روتر مقابل اطلاعات

کامل را توسط یک بسته LSU ارسال می کند و بعد از دریافت LSU یک بسته ACK به منظور تایید دریافت ارسال می کند. این عمل توسط روتر مقابل نیز انجام می شود.

Full : حالا اطلاعات جدول توپولوژی کامل شده و هر روتر به صورت جداگانه الگوریتم SPF را اجرا می کنند و جدول مسیریابی خود را بروز می کنند.

شبکه های Multi Access (Broadcast)



Multi Access لینک هایی هستند که به صورت اشتراکی مورد استفاده قرار می گیرند. مانند Ethernet در این نوع شبکه ها ارتباط و تبادل اطلاعات دو به دو انجام نمی شود و یک روتر به عنوان Designated Router یا DR انتخاب می شود و وظیفه بروز نگه داشتن همه روترها را دارد در این حالت DR یک نقطه حساس در شبکه است و اگر این روتر از کار بیافتد شبکه نیز مختل می شود برای جلوگیری از این مشکل یک روتر به عنوان Backup Designated Routerیا BDR در نظر گرفته می شود و به طور دائم ، فعال و زنده بودن DR را چک می کند و در صورت بروز مشکل اطلاعات لازم برای DR شدن را دارد. در شبکه های Multi Access همه روترها فقط با روتر DR و BDR مراحل برقراری و تبادل اطلاعات را که در شبکه های Point To Point گفته شد انجام می دهند و در این شبکه ها روترهایDROther یا همان NON DR بسته های خود را به آدرس 224.0.0.6 ارسال می کنند و 224.0.0.5 توسط DR برای ارسال بسته ها مورد استفاده قرار می گیرد و BDR فقط گوش می دهد.

نکته : بهتر است در انتخاب DR و BDR ما نقش داشته باشیم و بهترین روترها را برای اینکار انتخاب کنیم مثلا روترهایی که توانا بالاتری دارند یا به همه روترها لینک مستقیم دارند.

نکته : سایر روترها به عنوان DRother در نظر گرفته می شوند.

دستور نمایش فقط قسمت روتر ospf

RTR#show run | section router ospf

RTR2(config-router)#router ospf 25184

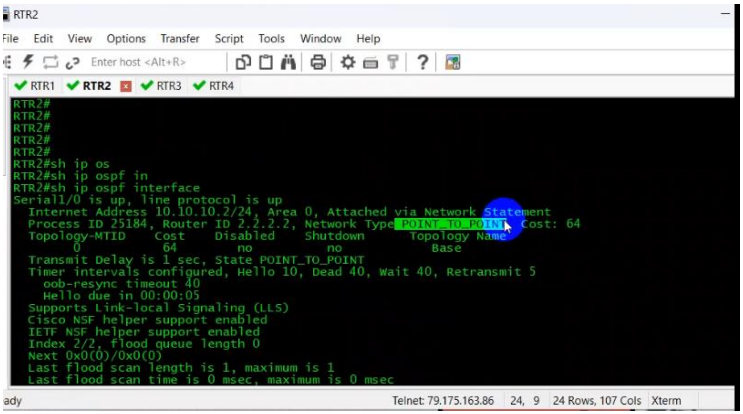
RTR2(config-router)#router-id 2.2.2.2

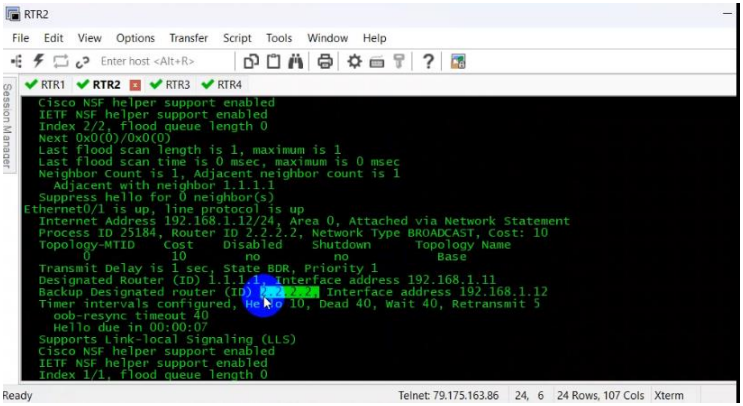
RTR2(config-router)#network 0.0.0.0 0.0.0.0 area 0 همسایه شو هر آی پی داری روهرچیزی که

این روش زیاد مناسب نیست و سطح امنیت پایینی دارد زیرا اگر یک روتر دیگر اضافه کنیم آن هم میتواند همسایه شود، اگر طرف مقابل هکر باشد بسته های hello ارسالی را دریافت می کند و میتواند روی روتر خود ospf اجرا کند و دیتا بیس را دریافت کند و توپولوژی شبکه ما را بدست میاورد.

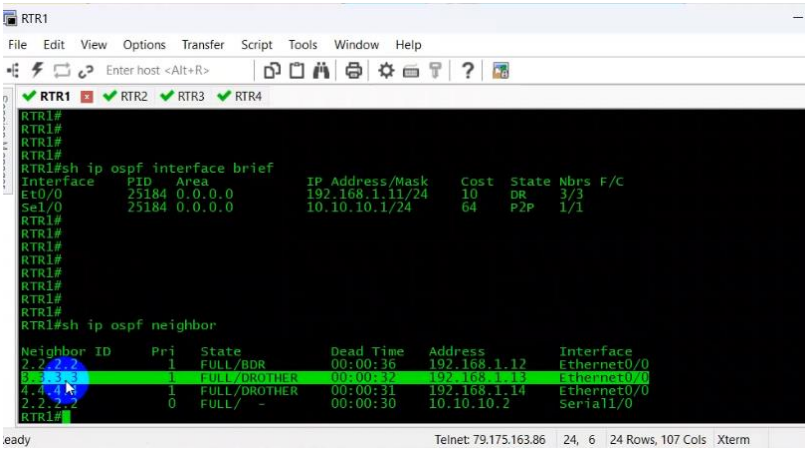
دستور مشاهده Network Type

RTR2#sho ip ospf interface

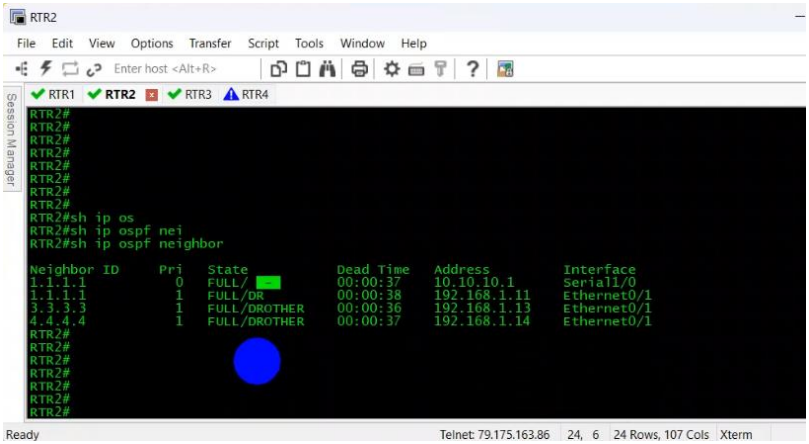




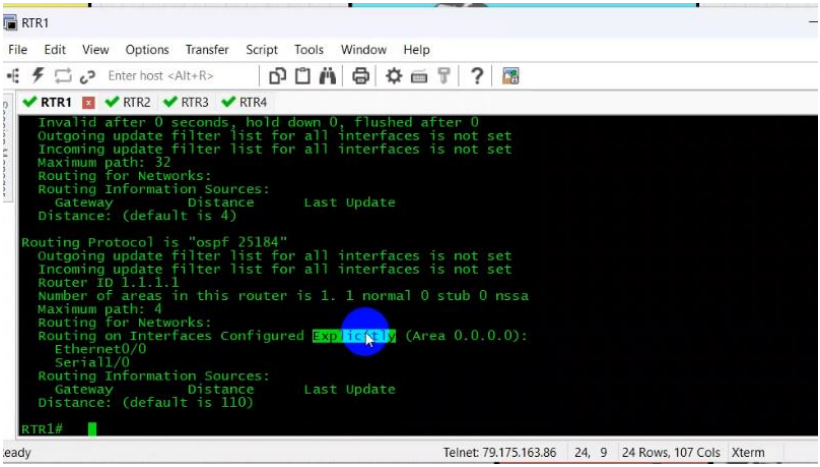
#show ip ospf neighbor



انتخاب DR و BDR انجام نشده زیرا ارتباط سریال است



#sho ip protocol



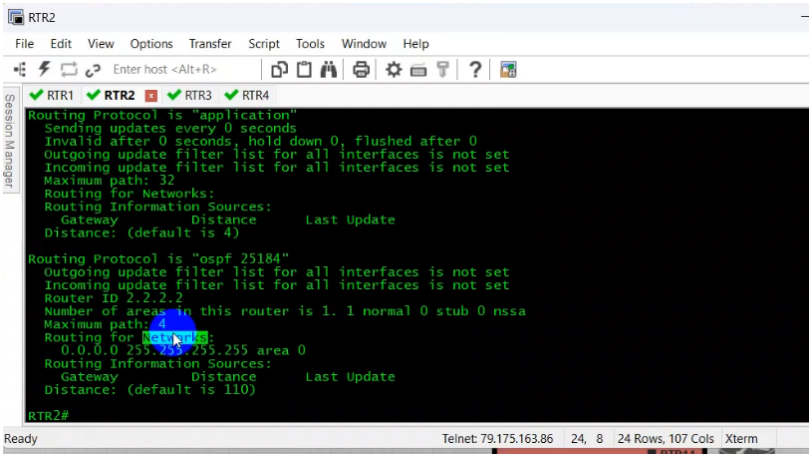


Table 20-3 Faster Interfaces with Equal OSPF Costs

Interface	Interface Default Bandwidth (Kbps)	Formula (Kbps)	OSPF Cost
Serial	1544 Kbps	100,000 / 1544	64
Ethernet	10,000 Kbps	100,000 / 10,000	10
Fast Ethernet	100,000 Kbps	100,000/100,000	1
Gigabit Ethernet	1,000,000 Kbps	100,000/1,000,000	1
10 Gigabit Ethernet	10,000,000 Kbps	100,000/10,000,000	1
100 Gigabit Ethernet	100,000,000 Kbps	100,000/100,000,000	1

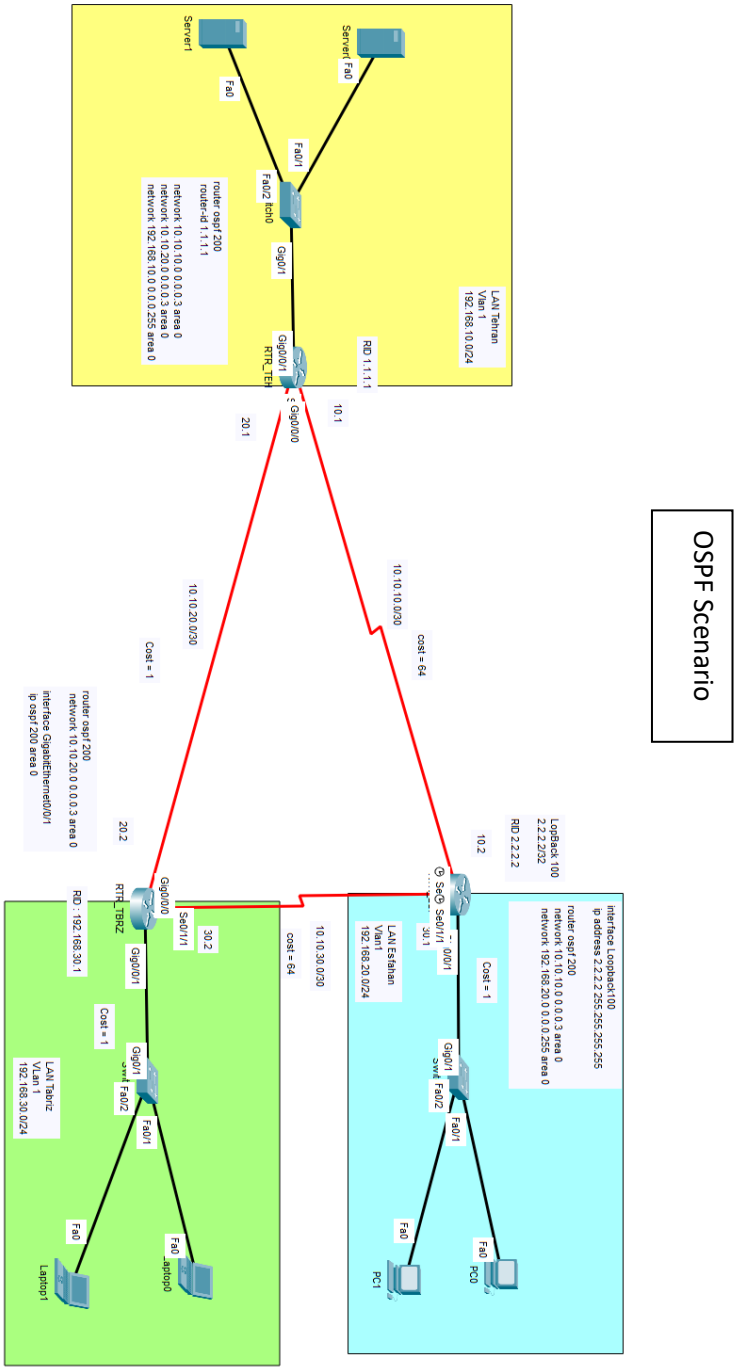
ملاک متریک که بر اساس fast ethernet 10^8 هست را عوض می کنیم. پیشفرض روی مگابیت هست یعنی 100 چون ارتباط گیگ داریم 1000 تنظیم میکنیم اما برای اینکه متریک دقیق تر داشته باشیم مقدار را بیشتر و روی 10000 تنظیم می کنیم و دقت داشته باشید که روی همه روتر ها باید اعمال شود که متر شاخص داشته باشیم.

RTR(config)#router ospf 25184

RTR(config-router)#auto-cost reference-bandwidth 10000

R1(config-router)#auto-coust refrence-bandwidth REF-BW[M}

OSPF Scenario



ساختار OSPF

مجموعه روترهایی که OSPF را اجرا می کند به بخش هایی تحت عنوان Area تقسیم می شوند. یک شبکه OSPF باید یک Area 0 داشته باشد و علاوه بر آن Area 0 می تواندArea های دیگری نیز داشته باشد. الگوریتم SPF در هر Area اجرا می شود و همچنینRoute های ناحیه ای بینArea ها ردوبدل می شوند.در OSPF دو سطح وجود دارد:

Backbone areaیا همان ناحیه صفر

Standard area

Area 0 که به عنوان ناحیه انتقال طراحی شده است و Area های دیگر به آن متصل می شوند.

Area ها دیگر باید به صورت مستقیم به Area 0 متصل شوند و از طریق Area 0 به دیگرArea ها دسترسی پیدا می کنند.

در هر Area روترها باید دیتابیس یکسانی داشته باشند. به طور معمول هر Area حداکثر 50 تا 100 روتر می تواند داشته باشد. که به شرایط شبکه بستگی دارد. Standard areaها باید بصورت مستقیم به area0 متصل شوند و هیچ standard area نباید صورت مستقیم یا به اصطلاح Back to Back به هم وصل شوند.

ویژگی های تقسیم بندی Area

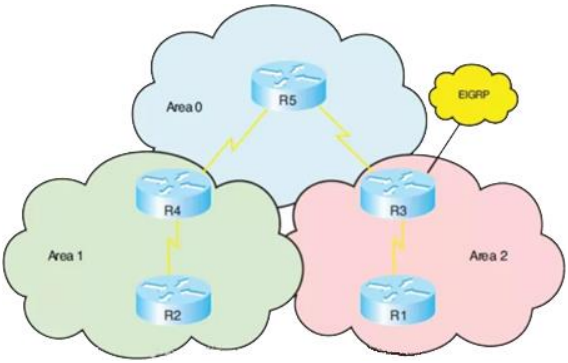
به حداقل رساند تعداد رکوردهای جدول مسیریابی

کنترل شدن ارسال LSA در هر ناحیه

به حداقل رساندن تاثیر تغییرات در شبکه

اجرای مدل سلسه مراتبی در طراحی شبکه

نقش روتر های در OSPF



Internal Router یک روتر داخلی تمام اینترفیس های آن در یک Area قرار دارد در شبکه بالا روتر های 1 و 2 و 5 به عنوان روتر داخلی محسوب می شوند.

Backbone Router روتر Backbone حداقل یک اینترفیس آن به 0 Area متصل است در شکل بالا روترهای 3 و 4 و 5 به عنوان روتر Backbone محسوب می شوند.

Area Border Router (ABR) روترهای که به دو یا چند Area متصل باشند در شکل بالا روترهای 3 و 4 به عنوان روتر ABR محسوب می شوندABR .ها مرز ارسال LSA را مشخص می کنند و می توانند Summarization را برای ما انجام دهند و یا به عنوان Default Route معرفی شوند. این روترها برای هر Area که به آن متصل است یک دیتابیس ایجاد می کند. در واقعABR ها Area مختلف را به یکدیگر متصل می کنند.

Autonomous System Boundary Router (ASBR) این روترها از یک سمت به شبکه OSPF و از طرف دیگر به شبکه دیگر متصل است در شکل بالا روتر 3 به عنوان روتر ASBR شناخته می شود. چون از یک سمت به شبکه OSPFو از سمت دیگر به یک شبکه EIGRP متصل است ASBRوظیفه اتصال شبکه OSPF را به دیگر شبکه های دارد.

نکته : یک روتر می تواند چند نقش داشته باشد.

Link State Advertisements (LSA)

هر روتر برای هر Area یک دیتابیس تحت عنوان link-state database (LSDB) ایجاد می کند که حاوی اخرین LSA دریافتی می باشد. در تعریف دیگر OSPF با کمک LSA از توپولوژی شبکه آگاه می شود و دیتابیس خود را براساس آن می سازد.

عملکرد LSA در OSPF

هر LSA دارای یک شماره و یک طول عمر است که به طور پیش فرض 30 دقیقه می باشد. زمانی که یک LSA دریافت می شود با دیتابیس LSDB مقایسه می شود. اگر LSA جدید بود به دیتابیس اضافه می شود و الگوریتم OSPF اجرا می شود. اگر LSA از یک Router ID که قبلا در دیتابیس موجود است باشد Sequence Number آن مقایسه می شود و اگر قدیمی تر بود از آن صرفه نظر می شود. اگر LSA قدیمی تر باشد LSA جدیدتر که در حافظه موجود است برای فرستنده LSA ارسال می شود Sequence Number 32 بیتی می باشد. اولین مقدار Sequence Number برابر x800000010 می باشد Sequence Number.به یکی از دو دلیل زیر تغییر می کند:

زمانی که یک Route اضافه یا حذف می شود.

طول عمر LSA تمام شود.

با استفاده از دستور زیر می توانید طول عمر و Sequence Number را ببینید:

Router#show ip ospf database

انواع LSA درOSPF

OSPF برای Advertise از LSA متفاوت برای Route مختلف مثل Area داخلی یا خارجی استفاده می کند. بعضی از آنها با نماد خاصی در جدول مسیریابی نمایش داده می شوند. در جدول زیر انواع LSA را می بینیم:

LSA Name	LSA Type	Primary Purpose	Contents of LSA
Router	1	Describe a router	RID, interfaces, IP address/mask, current interface state (status)
Network	2	Describe a network that has a DR	DR and BDR IP addresses, subnet ID, mask
Summary	3	Describe a subnet in another area	Subnet ID, mask, RID of ABR that advertises the LSA

Type 1 : Router LSA، هر روتر در داخل Area خودش یک type 1 router LSA بصورت Multicast برای روتر های همان Area که از پروتکل OSPF استفاده میکنند ارسال میکند. در این LSA میتوانید لیستی از تمامی لینک های Connected به روتر را مشاهده کنید.

Type 2 : Network LSA، روتری که نقش DR را دارد این LSA را تولید می کند و در Area آن را پخش می کند.

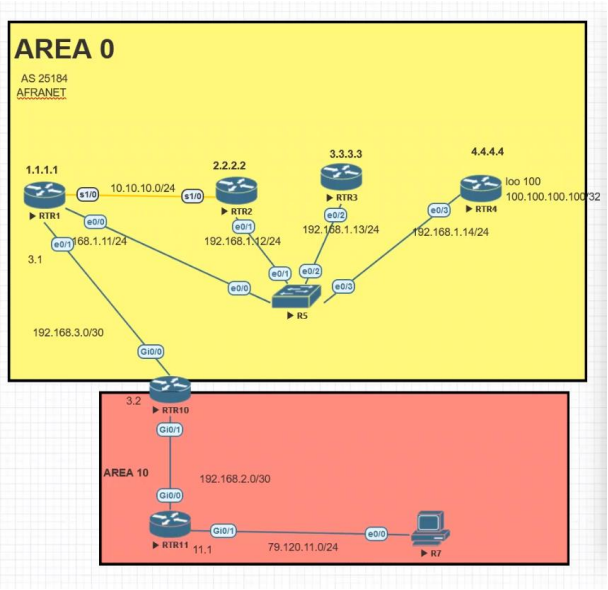
Type 3 : Summary LSA ، توسط روترهای ABR تولید می شود و شامل مسیرهایی است که از طریق ABR می توان به آن رسید.

نکته: اگر در یک Area نتورک تایپ Point To Point باشد فقط LSA Type1 داریم.

نکته: اگر در یک Area نتورک تایپ علاوه بر اینکه Point To Point باشد Broadcast باشد LSA Type1 و LSA Type2 داریم.

نکته: اگر در یک Multy Area OSPF داشته باشیم یعنی یک روتر در نقش ABR باشد این روتر برای اینکه آپدیت های داخل Area خودش را به Area0 یاد دهد که Area0 به بقیه یاد دهد با LSA Type3 این کار را انجام می دهد.

Multi Area OSPF



RTR10(config)#Int g 0/0

RTR10(config-if)#no sh

RTR10(config-if)#ip address 192.168.3.2 255.255.255 .252

Exit

RTR1 (config)#int e 0/1

RTR1 (config-if)#no sh

RTR1 (config-if)#ip address 192.168.3.1 255.255.255.252

Exit

RTR1#ping 192.168.30.2

RTR1 (config)#int e 0/1

RTR1 (config-if)#ip ospf 25184 area 0

RTR1#sh run Ethernet0/1 بررسی دستورات روی اینترفیس

RTR10(config)#Int g 0/0

RTR10(config-if)#ip ospf 25184 area 0

Router(config)#hostname PC7

PC7(config)#int e 0/0 no sh

PC7(config-if)#ip address 79.120.11.17 255.255.255.0

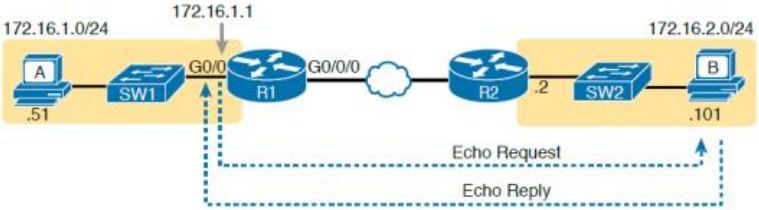
PC7#ping 79.120.11.1 ping gateway

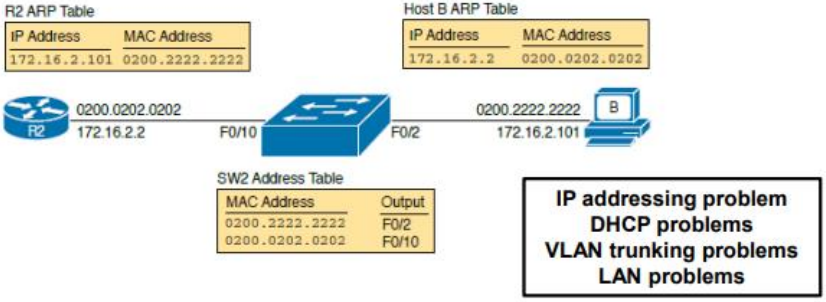
زمانی که روی PC ما gateway تنظیم کنیم بصورت خودکار یک deafault route به سمت gateway ما inject می کند.

PC7(config)#ip route 0.0.0.0 0.0.0.0 79.120.11.1

Extended PING

می توان از سورس و پورت دلخواه ping انجام داد.






```
R1# ping
Protocol [ip]:
Target IP address: 172.16.2.101
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.101, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

RTR4(config)# int loopback 100

RTR4(config-if)#ip address 100.100.100.100 255.255.255.255

RTR4(config-if)#ip ospf 200 area 0

PC7(config)#int e 0/0

PC7(config-if)#ip ospf 500 area 10

OSPF Passive Interface

Pc می تواند routing شبکه را بدست بیاورد یکی از راه حل های جلوگیری از آن OSPF Authentication است. بین دوتا همسایگی که می خواهیم برقرار کنیم یک پسوورد ست می کنیم که اگر روتر جدا شد و روتر دیگری جایگزین آن شود پسوورد من رو بداند که بتواند با من همسایه شود اما این روش برای ارتباطی است که ما می دانیم که می خواهیم با آن همسایه شویم اما بین روتر و PC نمی خواهیم همسایگی برقرار شود که روی آن پسوورد ست کنیم و در این سناریو کاربردی نیست. مجبور هستیم اینترفیس را در OSPS قرار دهیم. زمانی که این کار را می کنیم بسته های OSPF روی لینک ارسال و دریافت می شود . باید از ارسال بسته های Hello جلوگیری کنیم از این طریق همسایگی برقرار نمی شود.

RTR11(config)#router ospf 25184

RTR11(config-router)#passive-interface g 0/1

ممکن است تعداد passive interface ها زیاد باشد .

RTR11(config)#router ospf 25184

RTR11(config-router)#passive-interface default

RTR11(config-router)#no pasive-interface g 0/0

OSPF Authentication

احراز هویت درOSPF : در محیط های سازمانی این احتمال وجود دارد تا افراد غیر مجاز با اهدافی، قصد ایجاد همسایگی و دسترسی به شبکه با استفاده از پروتکل های مسیریابی را داشته باشند. این افراد ممکن است با ایجاد همسایگی بین روتر های سازمان مسیر های نادرستی را در سطح شبکه Advertise و منتشر نمایند. به منظور جلوگیری از انجام چنین اعمالی در شبکه می توان از احراز هویت بین روتر هایی که در OSPF مشارکت دارند استفاده نمود.

انواع احراز هویت در OSPF

به صورت کلی سه حالت احراز هویت در OSPF وجود دارد:

No-Authentication در این حالت هیچ احراز هویتی انجام نخواهد گرفت و روتر ها بدون توجه به احراز هویت، همسایگی را شکل خواهند داد.

Type 1 در این روش از احراز هویت که از آن به عنوان Simple Authentication نیز یاد می گردد، احراز هویت به صورت غیر امن و تنها به صورت Clear Text انجام خواهد گرفت.

Type 2 در این روش، احراز هویت OSPF با رمزنگاری MD5 انجام خواهد شد.

به صورت پیش فرض هیچ احراز هویتی در OSPF انجام نمی گیرد. باید دقت داشت چنانچه قصد استفاده از احراز هویت در OSPF را داریم، روتر ها باید بر سر نوع احراز هویت اتفاق نظر داشته باشند. این قابلیت وجود دارد که بنا به نیاز یکی از مکانیزم های احراز هویت را فقط روی یکی از اینترفیس های روتر فعال نمود تا احراز هویت OSPF تنها بر روی یک اینترفیس انجام پذیرد. همچنین این نکته حائز اهمیت است، چنانچه احراز هویت را به صورت عمومی فعال نمایید و در عین حال بر روی اینترفیس هم احراز هویت فعال شود، اولویت با تنظیمات اینترفیس خواهد بود. همواره به دلیل رمزنگاری استفاده از احراز هویت Type 2 که از MD5 بهره می گیرد، پیشنهاد می شود.

Two types of authentication can be used:

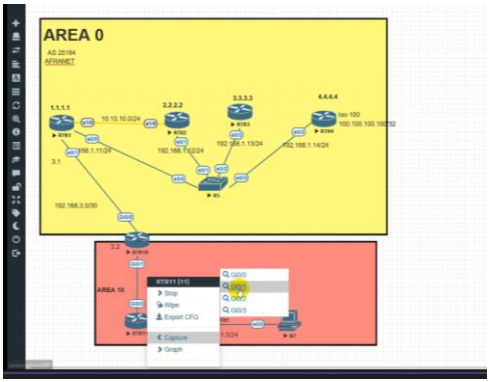
1. **clear text authentication** – clear text passwords are used

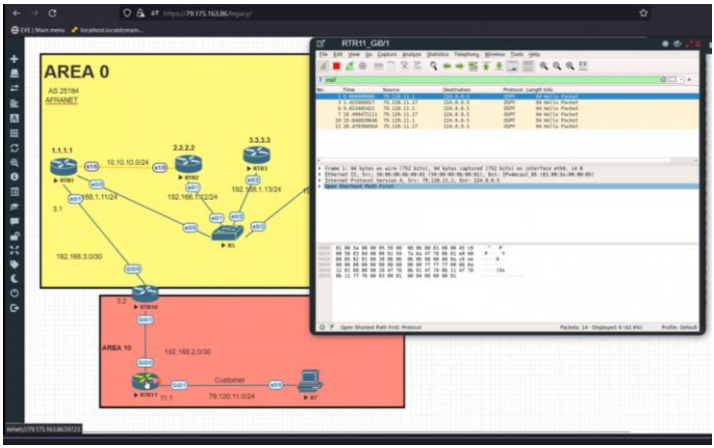
Router(config-if)#ip ospf authentication-key PASSWORD
Router(config-if)# ip ospf authentication

2. **MD5 authentication** – MD5 authentication is used. This type of authentication is more secure because the

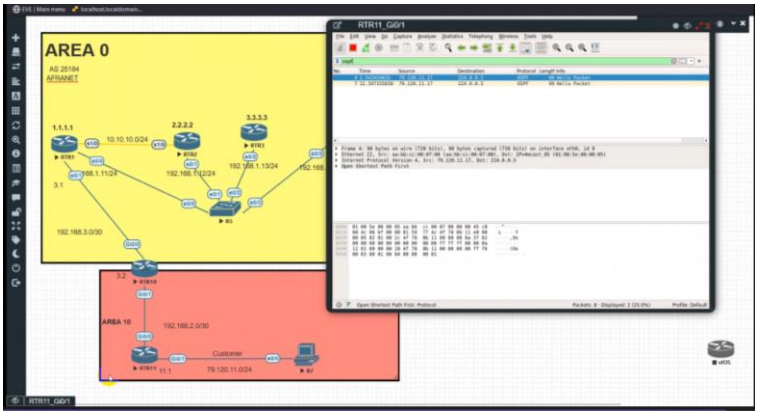
Router(config-if)# ip ospf message-digest-key <> md5 <VALUE>
Router(config-if)# ip ospf authentication message-digest

کپچر کردن یک اینترفیس با استفاده از نرم افزار Wireshark

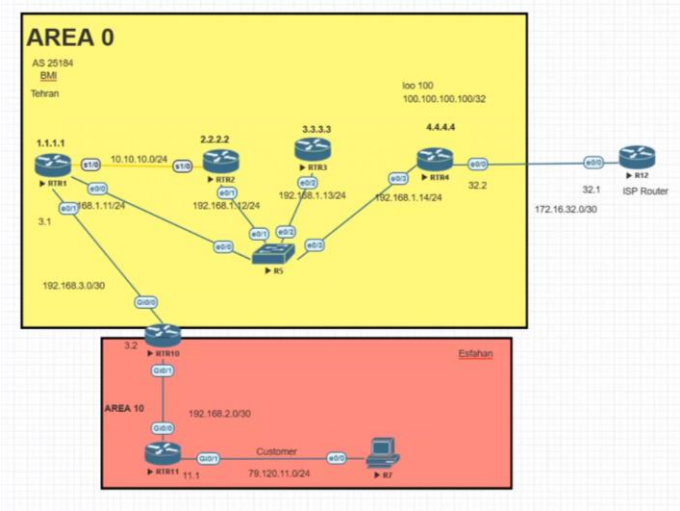




بعد از اجرای دستور RTR11(config-router)#passive-interface g 0/1



Default route



RTR4(config)#int e 0/0

RTR4(config-if)#ip address 172.16.32.2 255.255.255.252

RTR4(config-if)#no sh

ROUTER(config)#hostname ISP_RTR

ISP_RTR (config)#int e 0/0

ISP_RTR (config-if)#no sh

ISP_RTR (config-if)#ip address 172.16.32.1 255.255.255.252

ISP_RTR (config-if)#do ping 172.16.32.2

RTR4(config)#ip route 0.0.0.0 0.0.0.0 172.16.32.1 name TO_PROVIDER
default route ایجاد یک

روتر R4 از طریق جدول مسیر یابی مسیر های استاتیک و داینامیکی که می داند را مسیر یابی می کند و مسیر هایی که نمی شناسد را از default route استفاده می کند.

روتری که به شبکه خارجی متصل شده یعنی edge شبکه می باشد(جایی که سرویس را به یوزر delivere می کنیم یا به شبکه دیگری وصل می شویم که به آن لبه شبکه می گویند) .

روی روتر edge نیاز داریم که به بقیه اعلام کند که به یک شبکه دیگر وصل می باشد و ارتباط از طریق default route می باشد، به بقیه هم اعلام کن که یک default route به سمت من که اگر نیاز باشد مسیر یابی به سمت مقصدی که در جدول مسیریابی وجود نداشت با این default route بتواند match شود و دیگر نیاز نباشد روی همه روترها default route بصورتی دستی inject شود.

RTR4(config)#router ospf 200

RTR4(config-router)#default-information orginate

OSPF Neighbor Relationship

Requirement	Required for OSPF	Neighbor Missing if Incorrect
Interfaces must be in an up/up state.	Yes	Yes
Access control lists (ACL) must not filter routing protocol messages.	Yes	Yes
Interfaces must be in the same subnet.	Yes	Yes
They must pass routing protocol neighbor authentication (if configured).	Yes	Yes
Hello and hold/dead timers must match.	Yes	Yes
Router IDs (RID) must be unique.	Yes	Yes
They must be in the same area.	Yes	Yes
OSPF process must not be shut down.	Yes	Yes
Neighboring interfaces must use same MTU setting.	Yes	No
Neighboring interfaces must use same OSPF network type.	Yes	No

```
--> OSPF Configuration

    1) Network-Command (Classic)
    2) Interface-Based     (Explicit)

-----------------------------------------

router(config)# router ospf PROCESS_ID
router(config-router)#
  network INTERFACE_IP  WC_MASK  area AREA_ID


router(config)# interface INT_NAME
router(config-if)# ip ospf PID area AREA_ID

-----------------------------------------

OSPF Router-ID -> A.B.C.D

1- Manual --> router(config-router)# router-id A.B.C.D
2- Highest IP Address of Loopback Interfaces [UP/UP]
3- Highest IP Address of Non-Loopback Interfaces [UP/UP]

router# clear ip ospf process
-----------------------------------------
METRIC ---> BW -----> TOTAL-COST

INTERFACE COST = (10^8)/INTERFACE-BW

FA=> Cost= 100000000/100M = 1
SE=> Cost= 100000000/1544000 = 64
LO=> Cost= 100000000/8000000000=1

router(config)# router ospf PROCESS_ID
router(config-router)#
  router-id A.B.C.D
  network INTERFACE_IP  WC_MASK  area AREA_
  passive-interface INT_NAME

  passive-interface default
  no passive-interface INT_NAME

router(config)# interface INT_NAME
router(config-if)# ip ospf PID area AREA_ID
router(config-if)# ip ospf hello-interval SEC
router(config-if)# ip ospf dead-interval SEC

router# show ip protocols
router# show ip ospf interface [INT_NAME][brief]
router# show ip ospf neighbors [ INT_NAME ]
router# show ip ospf database
router# show ip route [ospf]
```

Requirements for Neighbor Adjacency

- RIDs must be unique between the two devices
- The interfaces must share a common subnet
- The MTUs (maximum transmission units) on the interfaces must match.
- The area ID must match for the segment
- OSPF hello and dead timers must match for the segment
- Authentication type and credentials (if any) must match for the segment.(Clear-Text/Hash)
- The DR enablement must match for the segment

Internet Assigned Numbers Authority(IANA)

مرجع واگذاری اعداد در اینترنت، نهادی است که مسولیت سرپرستی IP Address و سیستم خودگردان (Autonomous System) تخصیص داده شده.

پیش از برپایی ICANN برای این منظور، IANA در ابتدا به وسیله جان پوستِل از مؤسسه علوم اطلاعات دانشگاه کالیفرنیای جنوبی، تحت قرارداد USC/ISI با وزارت دفاع ایالات متحده مدیریت می‌شد، تا اینکه آیکان برای دریافت این مسئولیت تحت قراردادی با وزارت بازرگانی ایالات متحده ایجاد شد.

کل کره زمین به پنج region جداگانه تقسیم بندی شده که به آن Regional Internet Registry گفته می شود.

در سطح کره زمین پنج RIP وجود دارد: APNIC, ARIN, RIPE NCC, LACNIC, AFRINIC

IR → ICANN / IANA

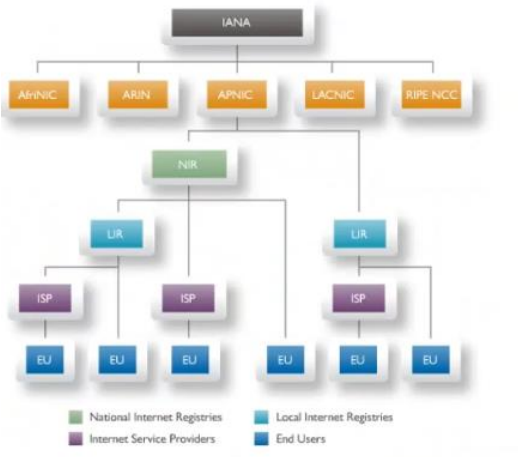
Regional Internet Registry (RIR)
Local Internet Registry (LIR)

www.iana.org

- Number Resources (AS / IP)
- Protocol Assignment
- Domain Names

یک شرکت را در نظر بگیرید مثلا اسنپ که سرویسی را می خواهد ارائه کند دو راه کار دارد:

اول اینکه به یک Provider وصل می شود حال برای اینکه سرویس را در سطح اینترنت Publish کند دو روش دارد، یا IP را از Provider اجاره کند یا AS/IP مستقل داشته باشد و مالکیت آن را داشته باشد و هزینه بیشتری باید بپردازد اما اگر Service Provider دچار اختلال و قطعی شد امکان جابجایی ترافیک شبکه را دارد و همیشه سرویس در دسترس است.

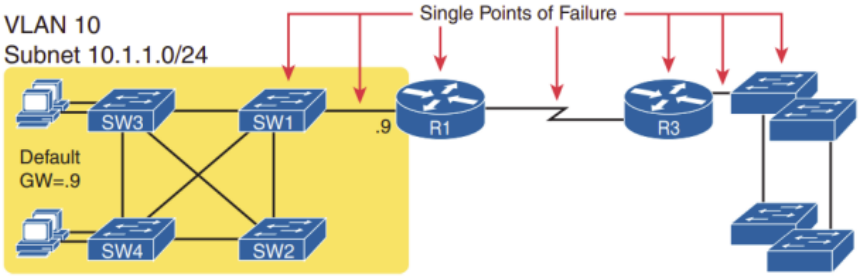


First Hop Redundancy Protocol (FHRPs)

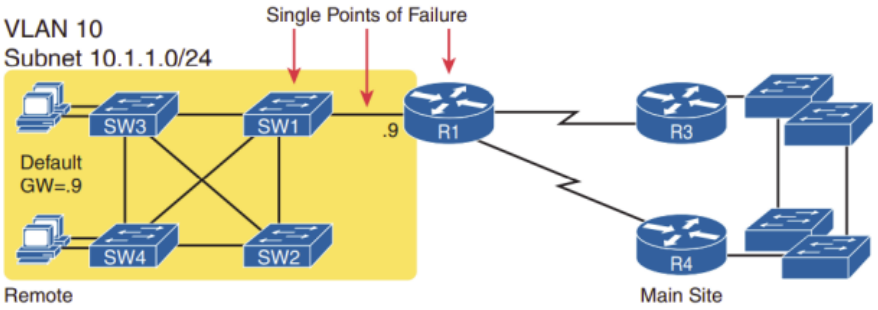
در شبکه های با مقیاس بزرگ از مدل طراحی سه لایه ای سیسکو که شامل لایه های Core, Distribution و Access هست استفاده شده و برای افزایش Availability یا در دسترس بودن از تکنیک های مختلف Redundancy استفاده می شود. در اکثر این شبکه ها Redundancy در لایه های Distribution و Core دیده می شود .

بعضاً در سازمان ها با وجود قابلیت استفاده از پروتکل های FHR در سوییچ های لایهDistribution ، از تکنیک تنظیم چندین Default Gateway روی کلاینت های مختلف استفاده می شود، یعنی روی بخشی(معمولاً نصفی) از کلاینت ها آدرس آی پی اینترفیس یکی از سوییچ های لایه Distribution را تنظیم می کنند و روی بخش دیگری از کلاینت ها آدرس آی پی اینترفیس سوییچ دوم را تنظیم می کنند. اگرچه این روش باعث ایجاد Load Balancing و تا حدودی Redundancy در شبکه می شود ولی در صورت قطعی یکی از لینک ها یا خرابی یکی از سوییچ ها، دسترسی نصف کلاینت ها به کل شبکه قطع خواهد شد.

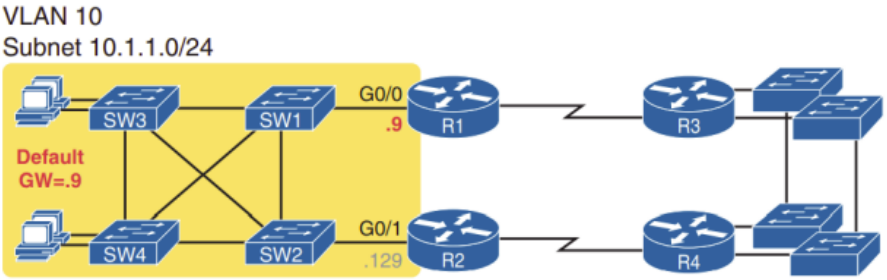
FHRPها پروتکل هایی هستند که با ایجاد یک اینترفیس مجازی این مشکل را حل کرده و باعث ایجاد Redundancy و در نتیجه High Availability در لایه Distribution می شوند. عملکرد هر سه پروتکل HSRP, VRRP و GLBP از دید کلاینت ها تقریباً شبیه به هم بوده و کلاینت ها این دو یا چند سوییچ لایه توزیع را به صورت یک سوییچ می بینند.در حالت کلی در تمامی این سه پروتکل یک IP Address و Mac Address به صورت مجازی انتخاب می شود.



شناسایی SPF



اضافه کردن یک Provider



اضافه کردن یک روتر جهت Redundancu

با اضافه کردن روتر مشکل حل نشد و روی client ها نمی تواند دو Default Gateway تنظیم کند و پروتکل HSRP را جهت رفع مشکل پیاده سازی می کند.

پروتکل های FHRP :

پروتکل HSRP – Hot Standby Router Protocol که اختصاصی سیسکو است در سال 1998 معرفی شده است.

پروتکل VRRP – Virtual Router Redundancy Protocol که یک پروتکل استاندارد است

پروتکل GLBP – Gateway Load Balancing Protocol یک پروتکل جدیدتر از سیسکو می باشد.

Hot Standby Router Protocol (HSRP)

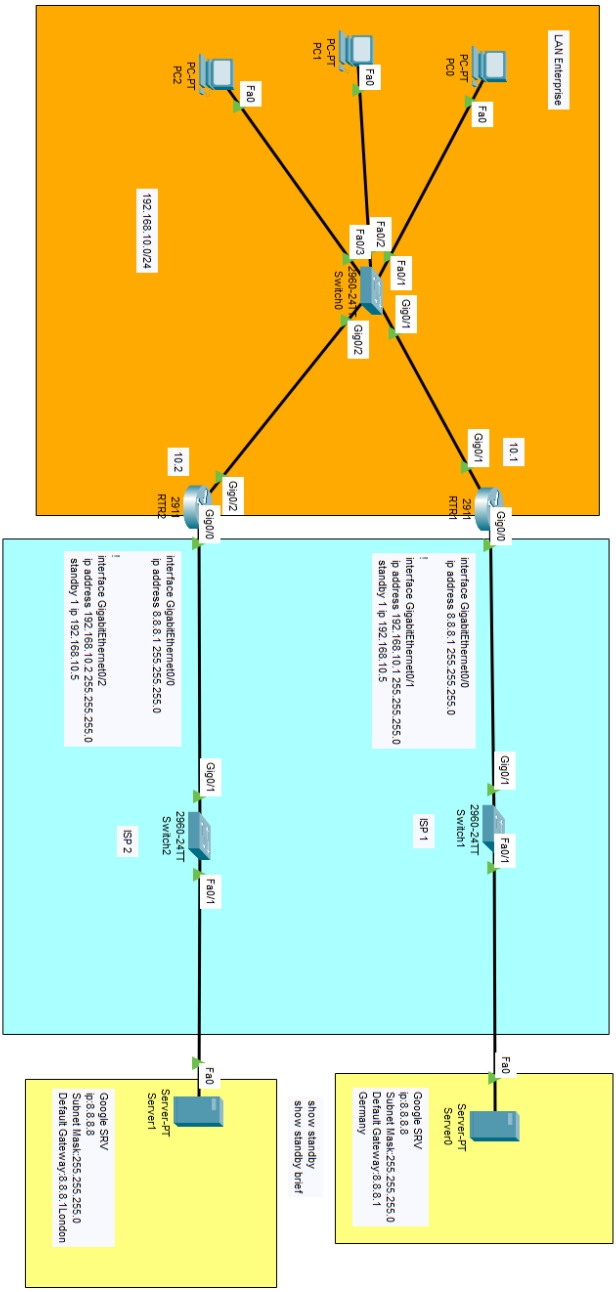
یک پروتکل استاندارد سیسکو است؛ که جهت ایجاد High Availability (HA) در شبکه ارائه شده است، این پروتکل از طریق ایجاد Redundancy درFirst-Hop ، برای IP هاست‌های رویLAN 802 IEEE ، با یک Gateway پیش‌فرض تنظیم شده است. در واقع HSRP ترافیک IP را بدون هیچگونه وابستگی به در دسترس بودن هر یک از روترها، مسیریابی می‌نماید .این امر باعث فعال نمودنِ گروهی ازInterface های روتر می شود که ظاهر یک روتر مجازی یا Gateway پیش‌فرض را به هاست‌های روی یک LAN می‌دهد .هنگامی‌که HSRP روی یک شبکه یا Segment پیکربندی می‌گردد، یک آدرس مجازی MAC و یک IP آدرس می‌سازد که در گروهی از روترهای پیکربندی‌شده به اشتراک گذاشته می‌شود. HSRP به دو یا چند روتر پیکربندی‌شده بر اساس HSRP اجازه می‌دهد که از MACیا IP یک روتر مجازی استفاده نمایند .در واقع، این روتر مجازی وجود ندارد، بلکه هدف مشترک روترهایی است که برای ارائه‌ی پشتیبانی به یکدیگر، تنظیم شده‌اند .یکی از روترها به عنوان روتر Active و دیگری به‌عنوان روتر Standby انتخاب می‌شود، روترStandby ، کنترل MAC گروه و IP را، در صورتی که روتر Active از کار بیافتد، به‌عهده می‌گیرد.

پیکربندی HSRP

یکی از راه‌های رسیدن به Uptime تقریباً ۱۰۰ درصدی، استفاده از HSRP است که Redundancy شبکه را برای شبکه‌های مبتنی بر IP فراهم کرده و رفع مشکل ارسال و دریافت ترافیک کاربر پس از خرابی اولینHop ، در تجهیزات Edge شبکه و مدارهای دسترسی را تضمین می‌نماید.

برای انتخاب حالت active,standby روتر دو قسمت در نظر گرفته می شود. قسمت اول priority عددی بین 0 تا 255 که بصورت پیشفرض روی همه روتر ها عدد100 در نظر گرفته شده که ادمین قادر به تغییر این مقدار می باشد، روتری Active می شود که prority بالا تری داشته باشد، اگر با priority نتوانست انتخاب کند بزرگترین IP Interface را در نظر می گیرد اما قابلیت preemtion فعال نیست یعنی اگر روتری که IP کمتری دارد Active شود و روتری که IP Interface بزرگتری دارد وارد شود تا زمانی که روتری که Active هست fail نشود اتفاقی نمی افتد. هر 3ثانیه یکبار بین یکدیگر بسته های Hello ارسال می کنند و 10ثانیه Dead Time در نظر گرفته شده که قابل تنظیم می باشد.

HSRP Scenario 1



روی روتر یک مقدار priority را بصورت دستی تغییر می دهیم اما تا زمانی که قابلیت مقایسه یا preemtion فعال نشود اتفاقی نمی افتد.

```
RTR1(config)#int g 0/1
RTR1(config-if)#standby 1 priority 105
RTR1(config-if)#standby 1  preempt
```

روی روتری که می خواهیم اکتیو باشد و الویت بالاتری دارد قابلیت مقایسه را فعال می کنیم .

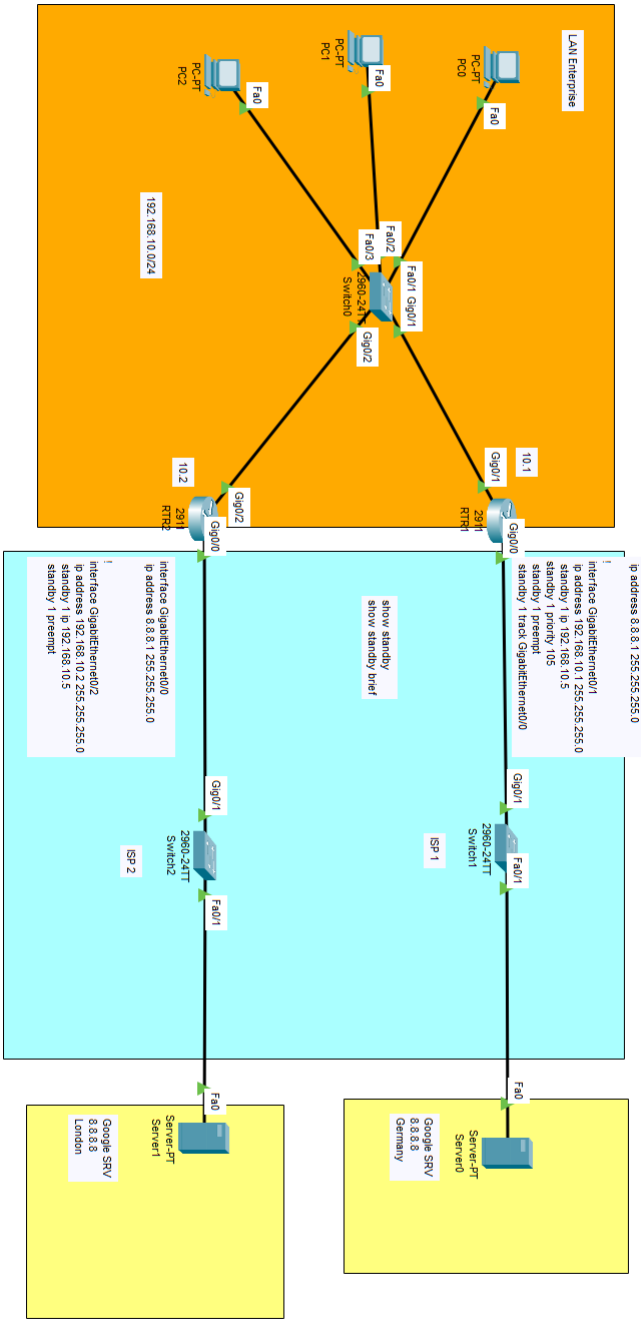
Redundancy در سطح Gateway

اگر دست دیگر روتر یعنی اینترفیسی که سمت Provider هست قطع شود درکی از آن ندارد. برای حل این مشکل از راهکار زیر استفاده می کنیم.

زمانی که اینترفیس Not Connected یا Shutdown شود بصورت خودکار از مقدار priority 10تا کم می کند که جای Activeو Standby تغییر کند.

```
RTR1(config)#int g 0/1
RTR1(config-if)# standby 1 track GigabitEthernet0/0

RTR2(config)#int g 0/2
RTR2(config-if)#standby 1  preempt
```

HSRP Scenario 2

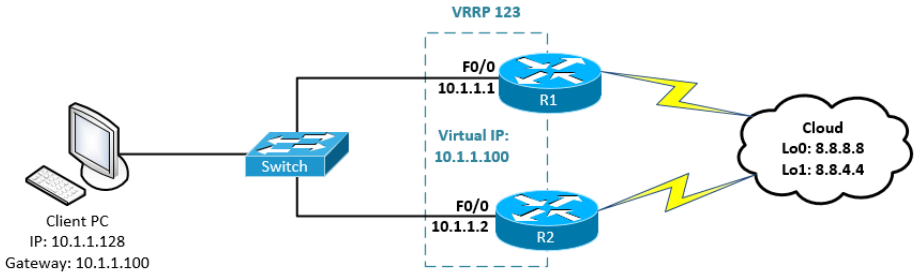


Acronym	Full Name	Origin	Redundancy Approach	Load Balancing Per...
HSRP	Hot Standby Router Protocol	Cisco	active/standby	subnet
VRRP	Virtual Router Redundancy Protocol	RFC 5798	active/standby	subnet
GLBP	Gateway Load Balancing Protocol	Cisco	active/active	host

```
(config) # interface <TYPE> <>
(config-if) # standby <> ip <Virtual_IP>
(config-if) # standby <> priority <>
(config-if) # standby <> preempt

# Show standby
# Show standby brief
```

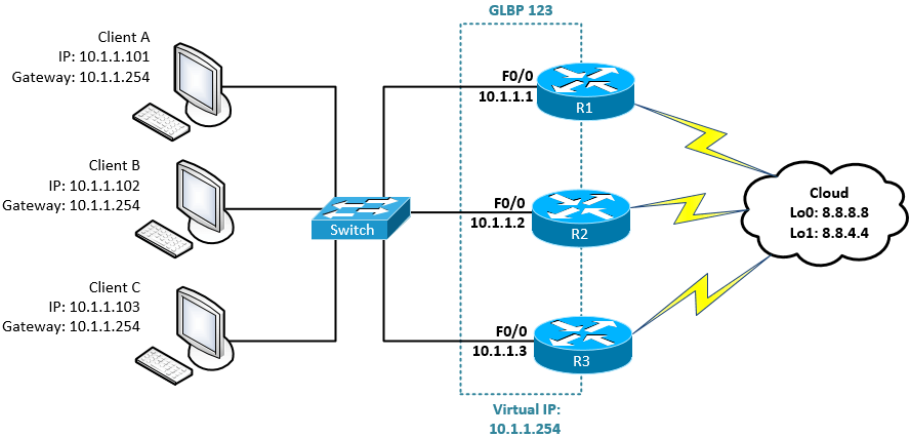
Version	HSRP V1 (Default)	HSRP V2
Group numbers	0 to 255	0 to 4095
Multicast address	224.0.0.2	224.0.0.102 or FF02::66
Virtual MAC address	0000.0C07.AC00 - 0000.0C07.ACFF (last two digits group number)	**IPv4** 0000.0C9F.F000 to 0000.0C9F.FFFF **IPv6** 0005.73A0.0000-0005.73A0.0FFF (last three digits group number)
Support for MD5 authentication	No	Yes

پروتکل Virtual Router Redundancy Protocol – VRRP



این پروتکل توسط IETF به صورت عمومی منتشر شده و قابل استفاده در تمامی سوییچ ها با هر برندی می باشد. نحوه عملکرد کلی آن شبیه HSRP بوده و در موارد جزئی تفاوتی با آن دارد .در این پروتکل می توان از آدرس اینترفیس فیزیکی هم به عنوان آدرس انتخابی مجازی استفاده کرد ولی در HSRP چنین قابلیتی وجود نداشت . هرچند این کار توصیه نمیشه ولی می توان استفاده کرد. همچنین در این پروتکل بر خلاف HSRP چندین سوییچ یا اینترفیس می توانند در گروه به صورت Standby منتظر به دست گرفتن کنترل اینترفیس مجازی بمانند.

پروتکل GLBP – Gateway Load Balancing Protocol



پروتکل GLBP ، پروتکل اختصاصی شرکت سیسکو است و بصورت دیفالت از 3 روش برای LOAD-BALANCE استفاده می کند. این پروتکل را در سطح روتر در خیلی از IOS ها می توانیم داشته باشیم اما در زمینه MLS ها ما به سوئیچ های 4500,6500 محدود شده ایم. این پروتکل برای برداشتن محدودیت هایی که در پروتکل HSRP و VRRPبا آن مواجه بودیم معرفی شد.

در پروتکل های HSRP و VRRP ما تنها یک روتر ACTIVE داشتیم که ترافیک از طریق آن به خارج از شبکه (اینترنت) ارسال می شد و سایر روتر ها منتظر بودند تا روتر ACTIVE ی ، FAIL شود تا جایگزین آن شوند.

همچنین در پروتکل های مزبور HSRP و VRRP وقتی کلاینت هایی که برای GATEWAY آنها VIRTUAL IP تخصیص داده شده بود و حالا برای VIRTUAL MAC آنها، ARP REQUEST ارسال می کردند، تنها روتر ACTIVE در HSRP وMASTER درVRRP جوابگو بودند و برای آنها در ARP REPLY ارسالی، VIRTUAL MAC را معرفی می کردند.

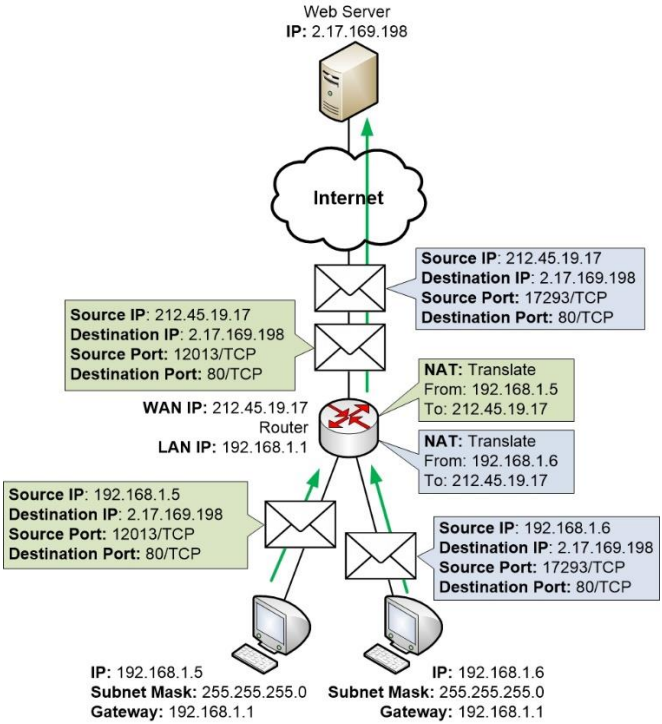
اما در پروتکل GLBP ، وقتی کلاینت ها برای مک VIRTUAL IP ای ، ARP REQUEST ارسال می کنند، روتر AVG پاسخگو است و در هر بار ARP REQUEST کلاینت ها VIRTUAL MAC یکی از FORWARDER ها را معرفی می کند که البته براساس یکسری الگوریتم، این روش اختصاصVIRTUAL MAC متفاوت است.

Network Address Translation (NAT)

IPv4 نسخه چهارم پروتکل اینترنت نسبت به تقاضای فعلی شبکه به لحاظ تعداد IP محدود می باشد. به همین دلیل امکان درنظر گرفتن IP برای تمام تجهیزاتی که به اینترنت می خواهند متصل شود وجود ندارد. علاوه بر این محدودیت ، استفاده از IP های معتبر موجود در اینترنت نیاز به پرداخت هزینه است.

Netwrok Address Translate (NAT) برای برطرف شدن این مشکلات ارائه شد. در شبکه های محلی از Private IP استفاده می شود و برای شبکه تعداد محدودی IP معتبر (Public)گرفته می شود و با استفاده از سرویس NAT ارتباط دستگاه ها به اینترنت برقرار می شود.

NAT یک IP به IP دیگر را تبدیل می کند یا عبارتی Private IP را به Public IP تبدیل می کند. به طور مثال یک شبکه را در نظر بگیرد که دارای 20 دستگاه است که می خواهند از اینترنت استفاده کنند با استفاده از سرویس NAT به جای اینکه برای هر دستگاه یک Public IP تهیه شود کلا یک Public IP تهیه می شود و برای دستگاه ها Private IP در نظر گرفته می شود و این دستگاه ها با استفاده از یک Public IP به اینترنت متصل می شوند. با اینکار در مصرف IP و هزینه صرفه جویی می شود.



محدوده آدرسهای آی پی Private IP

10.0.0.0 تا 10.255.255.255

172.16.0.0 تا 172.31.255.255

192.168.0.0 تا 192.168.255.255

موارد استفاده از NAT

صرفه جویی در مصرف IP و هزینه

زمانی که بخواهیم IP را به دلایلی عوض کنیم

زمانی که شبکه داخلی از Private IP استفاده می کند.

برقراری ارتباط بین دو شبکه که دارای رنج IP یکسانی هستند

نخواهیم رنج IP که در شبکه مورد استفاده قرار می گیرد از بیرون دیده شود

زمانی که مقصد ، رنج IP داخلی شبکه ما را نمی شناسد

معرفی مفاهیم NAT

Inside Local Address : آدرس هایی که برای شبکه داخلی مورد استفاده قرار می گیرد(Private IP).

Inside Global Addres : آدرس هایی که دستگاه های داخلی شبکه با آن از بیرون دیده می شوند(Public IP) .

Outside Local Address : آدرسی هایی که دستگاه های داخل شبکه ، دستگاه های خارج از شبکه را با آن می بینیم و می تواند آدرس Private باشد. نکته ای که وجود دارد این آدرس از طریق شبکه داخلی قابل مسیریابی است.

Outside Global Address : آدرس های Public مربوط به دستگاه های بیرون از شبکه ، که ما با آنها ارتباط برقرار می کنیم مانند Public IP سرور سایت.

کاربردهای اصلی NAT

Source NAT : امکان ایجاد ارتباط یک دستگاه که دارای Private IP است را به اینترنت فراهم می کند.

Destination NAT : امکان ایجاد ارتباط به یک دستگاه که دارای Private IP است را از اینترنت فراهم می کند.

انواع NAT

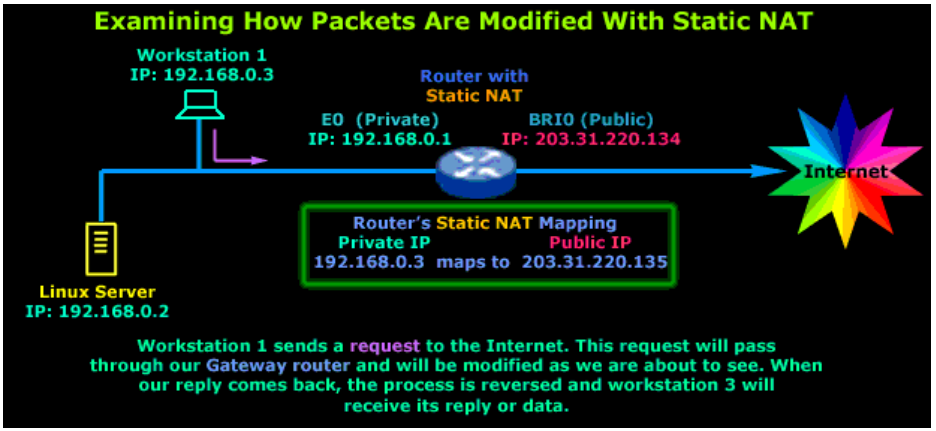
Static NAT

Dynamic NAT

Overloaded (PAT)

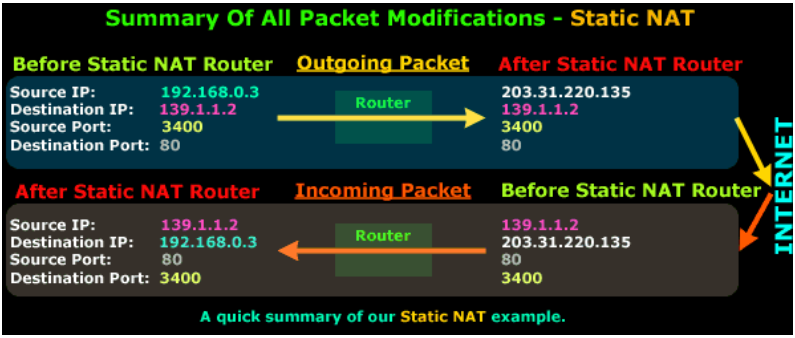
Static NAT

در این روش یک آدرس Private را تبدیل به یک آدرس Public می کند یا به عبارتی یک دستگاه از شبکه داخلی به یک IP از شبکه خارجی تبدیل می شود.



در این روش NAT به صورت یک به یک انجام می شود. اگر شما 100 کاربر داخلی و 100 ادرس global داشته باشید. می توانید از این روش استفاده کنید و برای هر یوزر مشخص کنید از چه آدرس global می تواند استفاده کند. به صورت معمول ما به اندازه کافی آدرس global برای هر کاربر نداریم. استفاده معمول از روش static NAT برای

یک سرور در شبکه داخلی یا محیط DMZ است و می خواهیم به کاربران سطح اینترنت دسترسی به این سرور را بدهیم و با استفاده از static NAT می توانیم این دسترسی را فراهم کنیم.



Static NAT Scenario

Router0

Router(config)#int g 0/1

Router(config-if)#no sh

Router(config-if)#ip add 192.168.10.1 255.255.255.0

Router(config-if)#exit

Router(config)#hostname RTR_EDGE

RTR_EDGE (config)#int g 0/0

RTR_EDGE (config-if)#no sh

RTR_EDGE (config-if)#ip add 79.120.11.100 255.255.255.0

RTR_EDGE (config-if)#exit

Provider یک IP از طریف DHCP یا بصورت دستی به ما اختصاص داده، در این سناریو:

79.120.11.100 255.255.255.0

Router1

Router(config)#hostname RTR_PROVIDER

Router(config)#int g 0/0

Router(config-if)#no sh

Router(config-if)#ip add 79.120.11.1 255.255.255.0

Router(config)#int g 0/1

Router(config-if)#no sh

Router(config-if)#ip add 8.8.8.1 255.255.255.0

SERVER

IP 8.8.8.8

Subnet Mask 255.255.255.0

Default Gateway 8.8.8.1

برای اینکه PC بتواند با سرور ارتباط برقرار کند باید روی روتر route مورد نظر را وارد کنیم.

هر مسیری که در جدول مسیریابی نداشت به provider می دهد

Router0

RTR_EDGE (config)#ip route 0.0.0.0 0.0.0.0 79.11.120.1

Provider یک Access list standard به نام Customer نوشته که اگر هر بسته ای با Source 16/ یا /8

RTR_PROVIDER(config)ip access-list standard CUSTOMER

RTR_PROVIDER(config-std-nacl)deny 192.168.0.0 0.0.255.255

RTR_PROVIDER(config-std-nacl)deny 10.0.0.0 0.255.255.255

RTR_PROVIDER(config-std-nacl)permit any

RTR_PROVIDER(config)int g 0/0

RTR_PROVIDER(config-if)ip access-group CUSTOMER in

Router0

RTR_EDGE (config)#int g 0/1

RTR_EDGE (config-if)#ip nat inside

RTR_EDGE (config-if)#exit

RTR_EDGE (config)#int g 0/0

RTR_EDGE (config-if)#ip nat outside

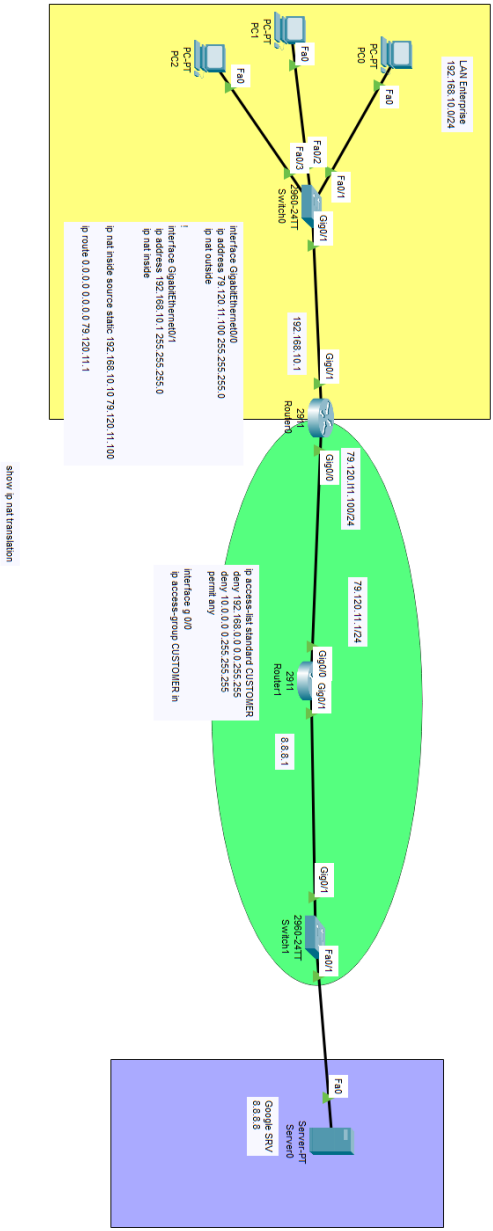
RTR_EDGE (config-if)#exit

RTR_EDGE (config)#ip nat inside source static 192.168.10.10 79.120.11.100

RTR_EDGE #show ip nat

در روش استاتیک مشکل رفع شد اما به ازای هر کلاینت باید یک Public IP تهیه کنیم که منطقی نیست.

Static NAT


LAN Enterprise
192.168.10.0/24
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
Fa0
Fa0
Fa0
Fa0/2
Fa0/3
Fa0/1
2960-24TT
Switch0
Gig0/1
192.168.10.1
Gig0/1
2911
Router0
Gig0/0
79.120.11.100/24
interface GigabitEthernet0/0
ip address 79.120.11.100 255.255.255.0
ip nat outside
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip nat inside
!
ip nat inside source static 192.168.10.10 79.120.11.100
!
ip route 0.0.0.0 0.0.0.0 79.120.11.1
show ip nat translation
ip access-list standard CUSTOMER
deny 192.168.0.0 0.0.255.255
deny 10.0.0.0 0.255.255.255
permit any
!
interface g 0/0
ip access-group CUSTOMER in
79.120.11.1/24
Gig0/0
Gig0/1
2911
Router1
8.8.8.1
Gig0/1
2960-24TT
Switch1
Fa0/1
Fa0
Server-PT
Server0
Google SRV
8.8.8.8

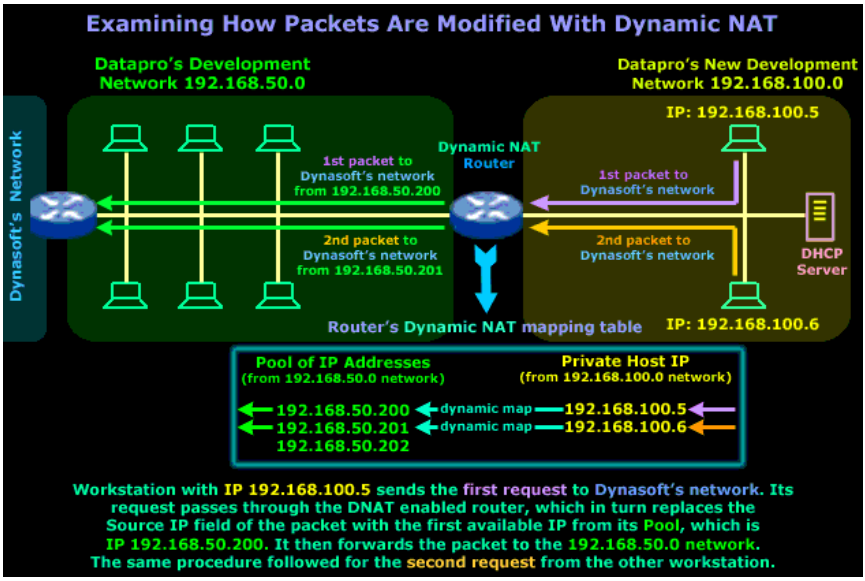
Dynamic NAT

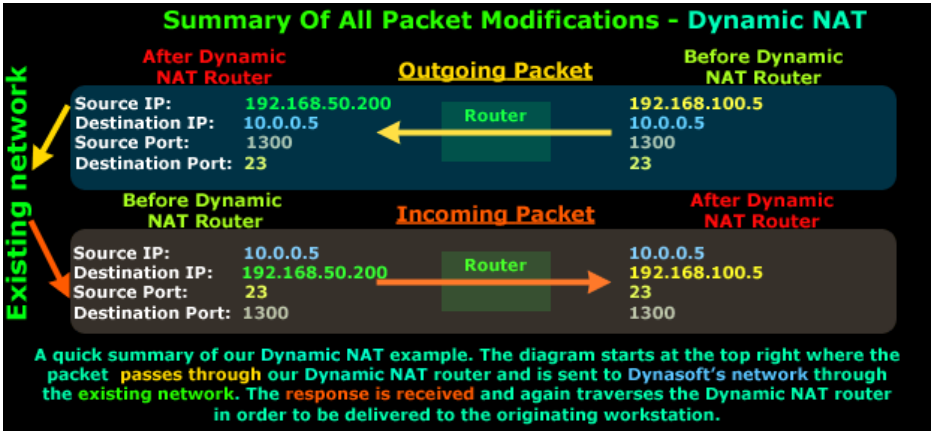
IP هایی که از Provider گرفته شده را در NAT Pool قرار می دهیم.

در این روش یک pool (رنج) از آدرس های Public را به یک رنج از Private IP شبکه داخلی اختصاص می دهیم.
در این حالت تعداد IPهای داخلی و خارجی باید برابر باشد.

نکته : NAT کردن براساس پارامترهای دیگر مانند پروتکل ، اینترفیس ، مقصد و ... امکان پذیر است برای این حالت ، به جای Standard ACL از Extended ACL استفاده می کنیم.

در این حالت ما یک رنج از آدرس های global داریم و تنها این رنج آدرس ها را به شبکه داخلی اختصاص می دهیم تا زمانیکه هر دستگاه نیاز به استفاده از اینترنت را داشت از آنها استفاده کند. به طور مثال ، یک کاربر می خواهد از اینترنت استفاده کند با شروع به کار او یک آدرس global از این رنج به او اختصاص داده می شود و این کاربر با استفاده از این آدرس global ارتباطش با اینترنت برقرار می شود بعد از یک بازه زمانی کاربر کارش با اینترنت به اتمام می رسد و دیگر نیاز به استفاده از اینترنت را ندارد. در این دستگاهی مثل روتر که عمل NAT را انجام می دهد بعد از یک بازه زمانی مشخص در صورت عدم استفاده آدرس global این آدرس را آزاد خواهد کرد که سایر دستگاه ها بتوانند از آن استفاده کنند. تعداد آدرس های global با تعداد دستگاه های شبکه داخلی که می خواهند از اینترنت استفاده کنند باید برابر باشد.





Dynamic NAT Scenario

Ip هایی گه از Provider گرفتیم را در Nat Pool قرار می دهیم.

RTR_EDGE (config)#ip nat pool INTERNET 79.120.11.100 79.120.11.101 network 255.255.255.0

یک Access List Standard به نام NAT می نویسم

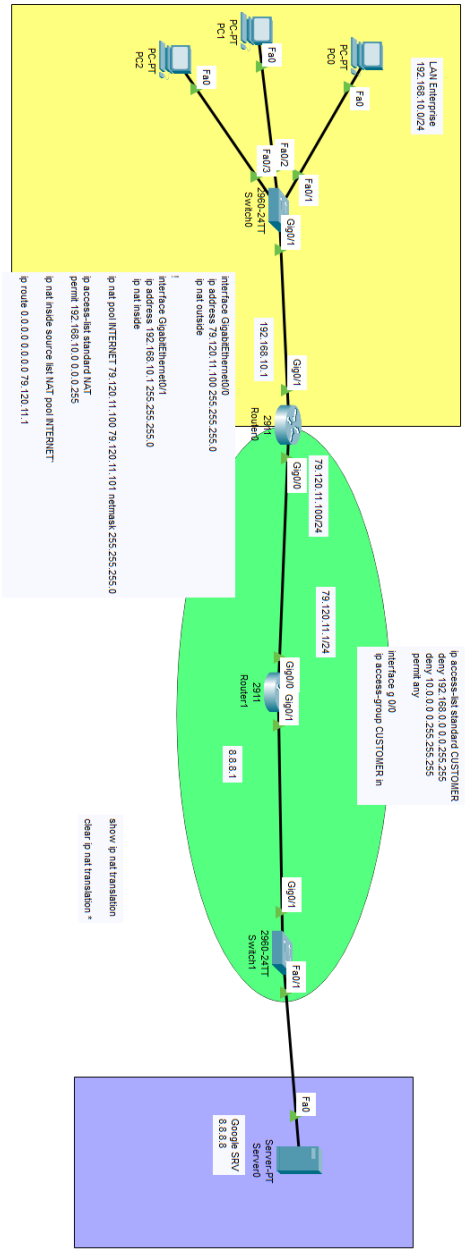
RTR_EDGE (config)no ip nat inside source static 192.168.10.10 79.120.11.100

RTR_EDGE (config)#ip access-list standard NAT

RTR_EDGE (config-std-nacl)#permit 192.168.10.0 0.0.0.255

RTR_EDGE (config)#ip nat inside source list NAT pool INTERNET

Dynamic NAT

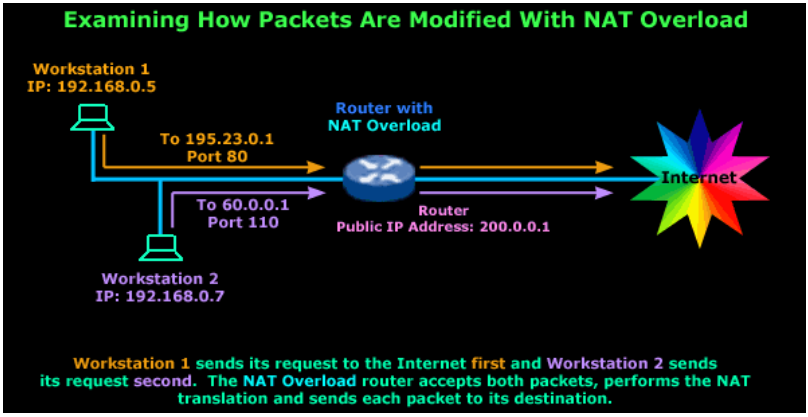

LAN Enterprise
192.168.10.0/24
PC-PT
PC1
PC-PT
PC2
PC-PT
PC0
Fa0
Fa0
Fa0
Fa0/2
Fa0/3
Fa0/1
2960-24TT
Switch0
Gig0/1
192.168.10.1
Gig0/1
2911
Router0
Gig0/0
79.120.11.100/24
79.120.11.1/24
Gig0/0
Gig0/1
2911
Router1
8.8.8.1
Gig0/1
2960-24TT
Switch1
Fa0/1
Fa0
Server-PT
Server0
Google SRV
8.8.8.8
interface GigabitEthernet0/0
ip address 79.120.11.100 255.255.255.0
ip nat outside
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip nat inside
ip nat pool INTERNET 79.120.11.100 79.120.11.101 netmask 255.255.255.0
ip access-list standard NAT
permit 192.168.10.0 0.0.0.255
ip nat inside source list NAT pool INTERNET
ip route 0.0.0.0 0.0.0.0 79.120.11.1
ip access-list standard CUSTOMER
deny 192.168.0.0 0.0.255.255
deny 10.0.0.0 0.255.255.255
permit any
interface g 0/0
ip access-group CUSTOMER in
show ip nat translation
clear ip nat translation *

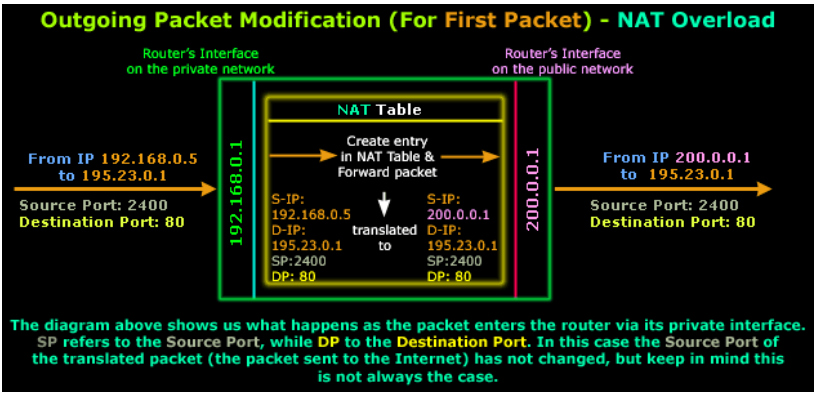
PORT ADDRESS TRANSLATION(PAT) / NAT OVERLOAD

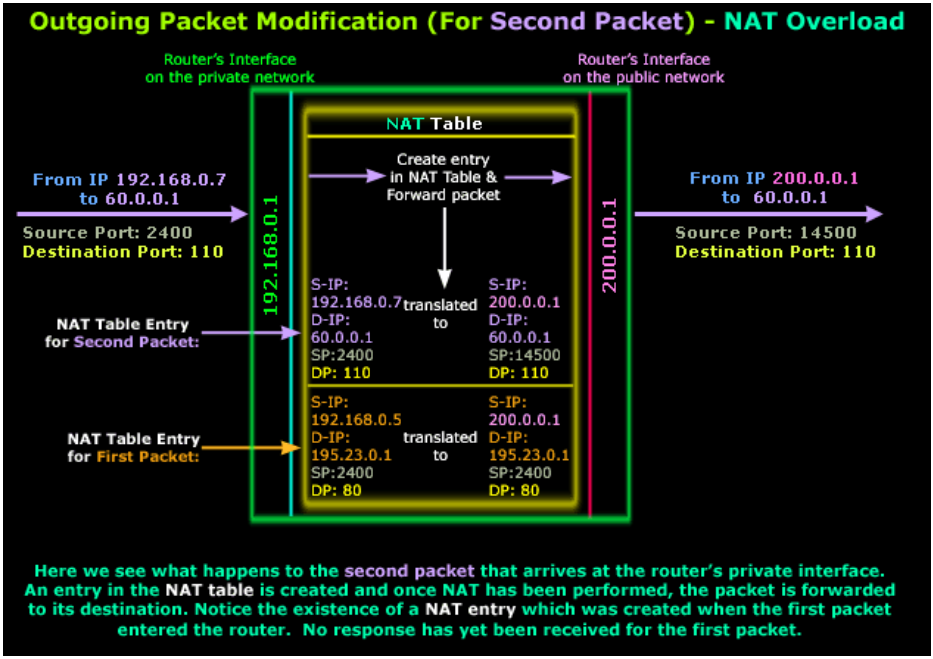
این روش مشابه Dynamic NAT می باشد با این تفاوت که به تعداد دستگاه هایی که می خواهند از اینترنت استفاده کنند نیاز به IP نداریم و تعداد می تواند کمتر و یا حتی یک عدد باشد.

این روش برای بیشتر کاربرانی که به اینترنت متصل می شوند استفاده می شود. در این روش از مزیت Dynamic NAT که تنها به کاربرانی که نیاز به استفاده از اینترنت دارند آدرس Global اختصاص داده می شود استفاده می کند و در کنار آن با استفاده از شماره پورت های مورد استفاده در ارتباط ، امکان استفاده چندین کاربر را از یک آدرس Global فراهم می کند. در این روش دستگاهی که عمل PAT را انجام می دهد اطلاعات پورت و IP ها را ردیابی می کند و براساس آنها جدول NAT را تشکیل می دهد.

مقدارپورت کنار IP قرار داده می شود که 16 بیت می باشد یعنی 2^{16}=65536 حالت در نتیجه با یک IP Public که از Provider می گیریم این تعداد Client را می توانیم NAT کنیم.







چون یک IP از Provider گرفتیم دیگر نیازی به NAT Pool نداریم. اگر بخواهیم NAT Pool را حذف کنیم باید کانفیگ NAT را پاک کنیم زیرا در حال حاضر NAT Pool ما Used هست اجازه پاک کردن آن را نمی دهد.

خطا: %pool INTERNET use,cannot destroy

در نتیجه اول خط NAT را پاک می کنیم

RTR_EDGE (config)#clear ip nat translation *

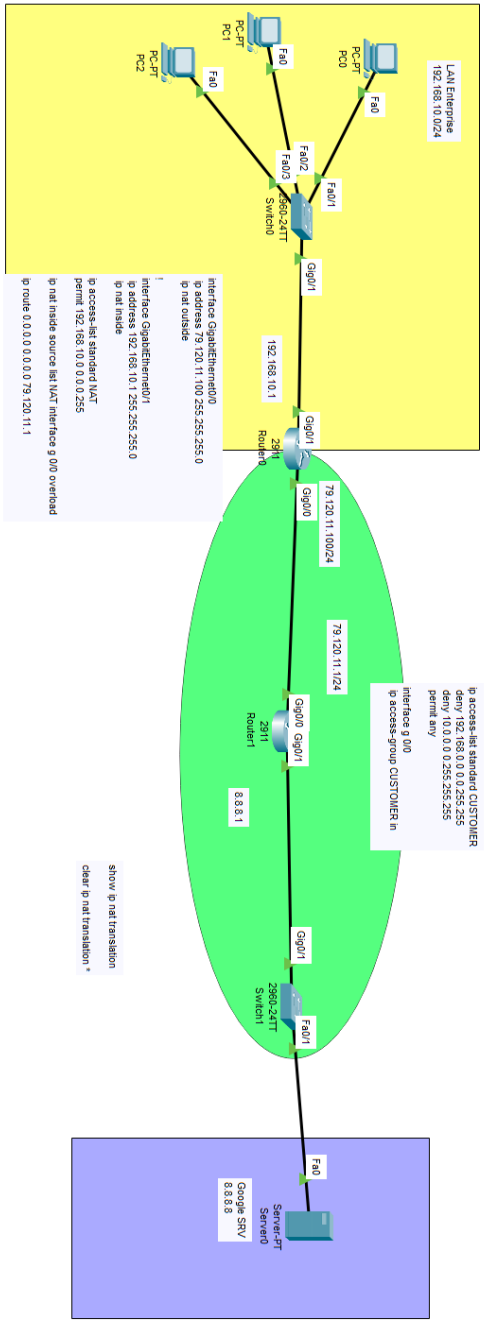
RTR_EDGE (config)#no ip nat inside source list NAT pool INTERNET

RTR_EDGE (config)#no ip nat pool INTERNET 79.120.11.100 79.120.11.101 network 255.255.255.0

NATهمان Access-list که نوشتیم می باشد

RTR_EDGE (config)#ip nat inside source list NAT interface g 0/0 overload

Overload NATNAT



CGNAT

ماژول CGNAT (CGN) امکان پیاده سازی انواع مختلفی از تکنیکهای Tunneling مورد استفاده بین شبکه های IPv4 و IPv6 شامل DS-lite، RD6، MAP، MAP-E، و LW4O6 را فراهم می نماید. این ماژول با ارائه کارایی بسیار بالا در شبکه های Enterprise و Carrier-grade، به خوبی نیازمندی های مرتبط با یک شرکت ارائه دهنده سرویس های اینترنتی را برآورده می کند. همچنین با استفاده از ماژول CGN، امکان پیکربندی و پیاده سازی انواع مختلفی از تکنیکهای Address Translation شامل NAT44 و NAT64 با استفاده از تکنیک های Deterministic، NAPT (Network Address & Port Translation) و PBA (Port Block Allocation) بصورت Reverse-proxy و Forward-proxy فراهم خواهد شد. علیرغم آنکه امکان استفاده از ماژول CGN به تنهایی نیز وجود دارد، ولی استفاده از این ماژول در کنار ماژول LTM و AFM نیز منجربه فراهم شدن قابلیت مجزا نمودن سرویس های مختلف و اعمال Security Policy مختلف به ازای هر سرویس و درنهایت ارسال/دریافت ترافیک به واسطه IPv4 Tunnels و یا IPv6 Tunnels تحت NAT Policy دلخواه می باشد.

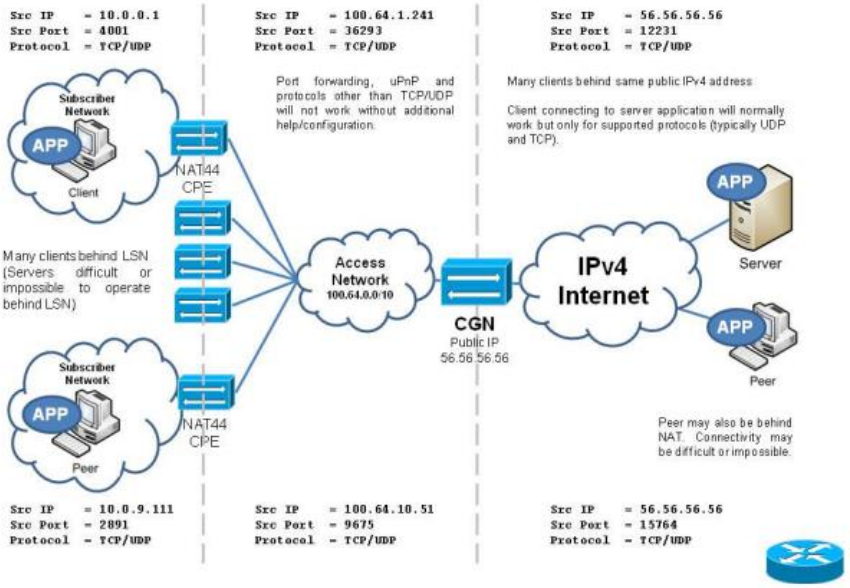


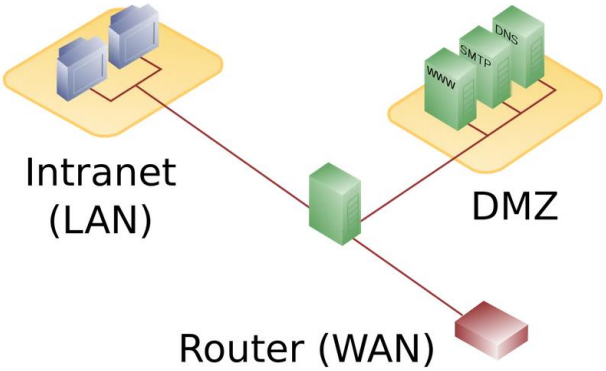
Figure 3.3 - The Internet and Access Networks with the Introduction of CGN

Demilitarized Zone (DMZ)

در جریان جنگی که بین کره شمالی و جنوبی پیش آمده بود (سال 1950 میلادی) ، در پیشنهادی که از طرف سازمان ملل به دو کشور شد ، قرار بر این شد که در میان مرز این کشور قسمتی را به عنوان منطقه غیرنظامی یا Demilitarized Zone انتخاب کنند تا مردم بتوانند از آن برای زندگی و امرار معاش بدون وارد شدن ساختار نظامی و جنگ استفاده کنند و همین مورد بین دو کشور توافق شد . مردم از این منطقه به عنوان منطقه ارتباطی بین دو کشوری که در حال جنگ بودند و به یکدیگر اعتماد نداشتند استفاده می کردند اما در محیطی که به هیچیک از دو کشور صدمه ای وارد نشود.

در یک ساختار DMZ ساده در یک شبکه معمولی ، یک سرور یا کامپیوتر که در اینجا به عنوان Host معرفی می شود در محیط DMZ قرار می گیرد و تمامی درخواست هایی که کاربران داخلی برای برقراری ارتباط با خارج از شبکه دارند را دریافت می کند ، این سرور بعد از دریافت این بسته های درخواست (مثلا درخواست وب سایت) آنها را به سمت شبکه عمومی یا اینترنت هدایت می کند و سپس پاسخ این درخواست ها را در همان Session ای که توسط کاربر داخلی ایجاد شده بود برای وی ارسال می کند ، توجه کنید که در این طراحی ساده ، هیچگونه ترافیکی نمی تواند از شبکه بیرونی به شبکه داخلی وارد شود.

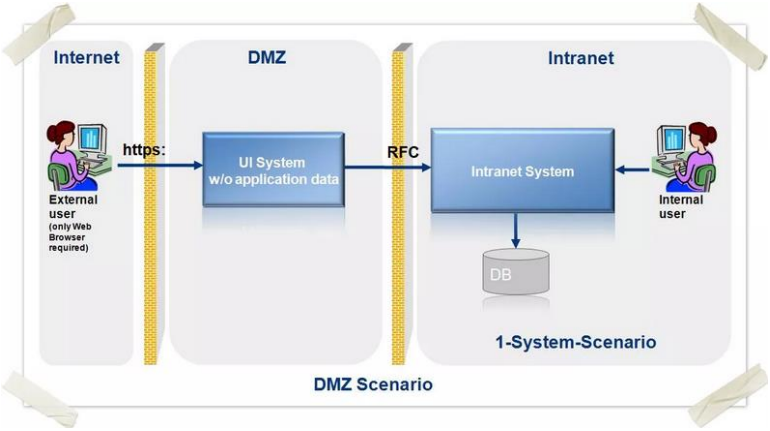
کاربرانی که در شبکه اینترنت یا خارجی قرار دارند صرفا می توانند به Host ای که برای DMZ استفاده می شود دسترسی پیدا کنند و به هیچ عنوان به شبکه داخلی دسترسی نخواهند داشت. یکی دیگر از کارهایی که در این Host می تواند انجام شود این است که صفحات وب ای که قرار است از طرف سازمان بر روی اینترنت در معرض دسترسی قرار بگیرند می توانند بر روی این Host قرار بگیرند. اما توجه کنید که DMZ به شبکه داخلی نیز در این حالت دسترسی نخواهد داشت. شما فرض کنید که در این حالت یک هکر قصد حمله به وب سایت سازمان را دارد ، حتی اگر موفق به هک این صفحات شود ، به اطلاعات خاصی در خصوص شبکه داخلی و اطلاعات خصوصی سازمان دست پیدا نخواهد کرد. بدون شک یکی از بهترین تجهیزات شبکه ای که برای استفاده ویژه در ساختار DMZ مورد استفاده قرار می گیرد تجهیزات فایروال شرکت سیسکو می باشد.



اگر بخواهیم از نظر امنیتی DMZ را تعریف کنیم ، می توان آن را به نوعی تنظیمات پیشرفته در فایروال های شبکه نیز معرفی کنید. در تنظیمات DMZ اکثر کامپیوترهایی که در شبکه LAN قرار گرفته اند در پشت فایروال قرار می گیرند که این فایروال به شبکه اینترنت یا شبکه عمومی متصل شده است . از طرفی یک یا چندین سرور نیز در محلی بعد از فایروال قرار می گیرند ، یعنی در شبکه داخلی نیستند ، این سرورهایی که در بعد از فایروال قرار می گیرند ، درخواست های کاربران داخلی را همانطور که اعلام شد از شبکه داخلی دریافت کرده و سپس آنها را به شبکه اینترنتی که به آن متصل هستند ارسال می کنند ، این دقیقا همان مفهوم امنیتی است که مد نظر است ، خاطرتان هست که در جنگ بین کره شمالی و جنوبی یک شهر به عنوان محل رابط بین دو کشور انتخاب شد که در آن جنگی در کار نبود ، این را دقیقا در شبکه نیز می توانید تصورکنید.

توجه کنید که شما واژه DMZ را در بسیاری از تجهیزات شبکه اعم از روترهای اینترنتی خانگی نیز مشاهده می کنید اما آنها واقعا DMZ نیستند بلکه صرفا قابلیت پشتیبانی از این نوع تنظیمات هستند که در تجهیزات شبکه دیده شده است . این نوع تجهیزات با طراحی واقعی DMZ در ساختار های سازمانی به کلی تفاوت دارند ، آنها صرفا چند Rule ساده در تنظیمات روتر خانگی هستند ، اما در DMZ های سازمانی ، سرورها و تجهیزات حرفه ای در طراحی DMZ استفاده می شود.

در حوزه امنیت اطلاعات ممکن است DMZ به عنوان Perimeter Network نیز مطرح شود که نام دیگر همین نوع طراحی شبکه است. در اکثر سازمان های دولتی و حتی شرکت ها ، سرویس هایی وجود دارد که سازمان ها قصد دارند به بیرون از شبکه ارائه دهند ، مثلا وب سایت یا پورتال سازمانی ، سرویس ایمیل ، سرویس میزبانی وب یا حتی سرویس DNS . فرض کنید که این سرویس ها را در درون شبکه داخلی قرار بدهید و به کاربرانی که از اینترنت قصد استفاده از این سرویس ها را دارند اجازه ورود به شبکه داخلی را بدهید ، این خود یک نقطه ضعف امنیتی می باشد ، بنابراین همیشه برای اینگونه سرویس های عمومی استفاده از طراحی DMZ توصیه می شود.



در چنین شرایطی شما سرویس ها و سرورهای مورد نظر خود را در محیط DMZ قرار می دهید و ارتباط محدودی با شبکه داخلی برای آنها ایجاد می کنید ، ارتباطی که در سطح بسیار کم و با درصد خطر کمتری نسبت به ارتباطات معمول شبکه باشد. طراحی DMZ برای محافظت از حملاتی است که از بیرون سازمان به سرویس ها انجام می شود و معمولا در این نوع طراحی خطرات شبکه داخلی سازمان از جمله Spoofing و Sniffing و ... آنها دیده نمی شود.

سرویس هایی که نیازمند دسترسی عمومی می باشند را در این منطقه از شبکه قرار می دهیم ، مهمترین و معروف ترین سرویس هایی که در قسمت DMZ شبکه قرار می گیرند به شکل زیر می باشند:

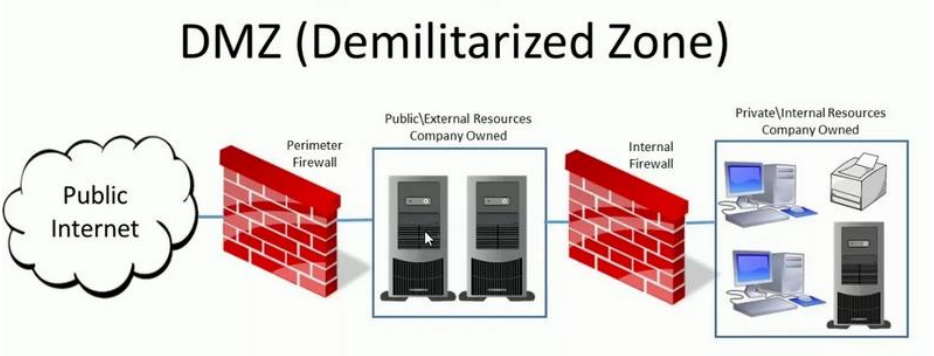
سرویس دهنده های وب یا Web Server ها

سرویس دهنده های ایمیل یا Mail Server ها

سرویس دهنده هایVoip

سرویس دهنده هایFTP

نکته ای که در اینجا بسیار مهم است ، این است که وب سرورهای سازمانی معمولا صفحات ایستا نیستند که صرفا چند صفحه باشند ، بلکه صفحات دینامیکی هستند که در پس زمینه خود دارای یک پایگاه داده اطلاعاتی می باشند ، این وب سرور ها بایستی بتوانند از این پایگاه داده استفاده کنند ، قاعدتا اگر این پایگاه داده را در خود محیط DMZ قرار بدهید ، کار اشتباهی خواهد بود ، در این حالت پایگاه داده مورد نظر را یا در شبکه داخلی و پشت فایروال قرار می دهند و یا در پشت یک فایروال و در شبکه ای در همان طراحی DMZ قرار می دهند. در این حالت اگر هکری موفق به نفوذ به وب سایت شود ، صرفا به صفحات وب سایت دسترسی پیدا می کند و نمی تواند داده ها و اطلاعات موجود در پایگاه داده را که در پشت فایروال دیگری قرار دارد را مورد هجوم قرار دهد.



سرویس های ایمیل یا همان Email Server ها نیز دارای اطلاعات کاربری و پایگاه داده خاص خود می باشند که آنها نیز بایستی محافظت شوند. همانطور که در طراحی قبلی اشاره کردیم آنها را نیز در پشت یک فایروال جداگانه قرار می دهیم ، توجه کنید که معمولا سرویس دهنده های ایمیل از سرویسی به نام Webmailپشتیبانی می کنند که می توان از طریق وب به آنها دسترسی داشت ، شما می توانید ایمیل سرور خود را در پشت فایروال DMZ قرار داده و از طریق امکانی به نام Publishing صفحه وب ایمیل را برای دسترسی عمومی Publish کنید.

توجه کنید که ایمیل سرور هایی که به این شکل هستند هم ترافیک ورودی و هم ترافیک خروجی ایمیل ها را بایستی به درستی مدیریت کنند ، طراحی DMZ ها با توجه به سرویس های موجود در شبکه متعیر هستند و DMZ یک ساختار ایستا و ثابت نمی باشد. به دلیل مسائل امنیتی و همچنین مسائل مانیتورینگ در یک محیط تجاری ، بیشتر سازمان ها و شرکت ها در محدوده DMZ خود یک Proxy Server راه اندازی می کنند ، راه اندازی این سرور در این محیط دارای مزایا به شرح زیر می باشد:

- اجبار کردن کاربران داخلی برای استفاده از Proxy Server برای استفاده از اینترنت
- کاهش نیاز به پهنای باند اضافی بر روی شبکه اینترنت به علت استفاده از قابلیت cache در پروکسی سرور
- ساده سازی فرآیند ضبط و مانیتورکردن استفاده کاربران از اینترنت
- متمرکز سازی فرآیند فیلترکردن وب سایت ها و محتویات وب

ممکن است در اینجا این سئوال پیش بیاید که حال اگر نیاز به این باشد که کاربری بتواند از بیرون به شبکه داخلی دسترسی پیدا کند ، آیا ساختار DMZ این امکان را به وی می دهد یا خیر ؟ در پاسخ به این سئوال بایستی بگوییم که سرویسی به نام Reverse Proxy وجود دارد که امکان دسترسی پیدا کردن کاربران خارجی به منابع داخلی شبکه را فراهم می کند ، همانطور که Proxy Server به کاربران داخلی سرویس می دهد ، Reverse Proxyعکس این عمل را انجام می دهد ، یعنی به کاربران خارجی دسترسی داخلی را می دهد.

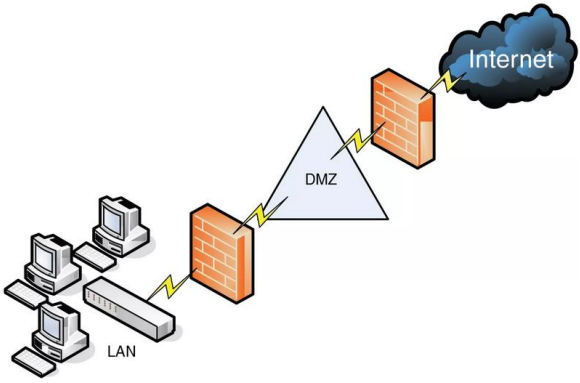
برای مثال فرض کنید که شما در ساختار DMZ خود یک سرویس ایمیل دارید ، و کاربران اینترنتی از آن استفاده می کنند ، اما مدیر همین سرور تصمیم می گیرد به این سرور که در شبکه داخلی قرار داشته و توسط فایروال Publish شده است دسترسی پیدا کند ، چه مشکلی پیش می آید ؟ با استفاده از Reverse Proxy شما می توانید به وی اجازه برقرار ارتباط Remote به سرور مورد نظر را بدهید . توجه کنید که در چنین حالت هایی برای کاهش خطرات موجود شما از فایروال های لایه هفتم یا Application Layer Firewall ها استفاده می کنید تا درصد بروز حملات به سرورها از طریق Reverse Proxy را کاهش دهید. این روش امن ترین روش برقراری ارتباط از خارج شبکه به داخل آن می باشد.

معماری ها مختلف در ساختار DMZ

همانطور که اشاره کردیم روش های زیادی برای طراحی DMZ وجود دارد و هر کس می تواند با توجه به شرایط موجود طراحی ویژه سازمان خود از این روش را داشته باشد. شما می توانید در طراحی های DMZ از یک فایروال با 3 کارت شبکه ، یا از چندین فایروال جداگانه استفاده کنید. البته اینها طراحی های ساده ای از DMZ هستند ، DMZ می تواند در ابعاد بسیار گسترده آنقدر بزرگ و پیچیده شود که واقعا در حد این مقاله نمی باشد. این که چگونه DMZ را طراحی می کنید کاملا به نیازمندی های سازمانی شما بستگی دارد. در ادامه دو نوع از روش های معمولی که DMZ طراحی می شود را برای شما شرح می دهیم:

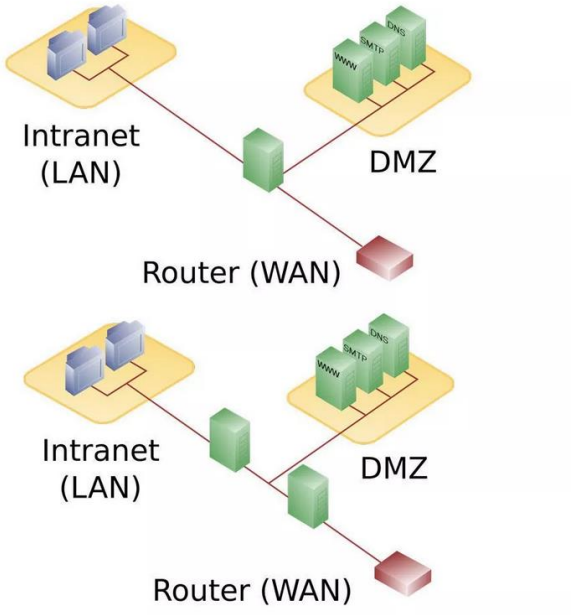
DMZ با استفاده از یک فایروال

در این حالت شما یک فایروال سخت افزاری یا نرم افزاری دارید که دارای حداقل سه کارت شبکه می باشد که طراحی DMZ شما در این سه کارت شبکه جای می گیرد. ارتباط خارجی شما که به اینترنت و شبکه ISP متصل می شود به درون کارت شبکه اول متصل می شود. شبکه داخلی شما به کارت شبکه دوم موجود و در نهایت شبکه DMZ شما نیز به کارت شبکه سومی که بر روی فایروال قرار دارد متصل می شود. در اینجا فایروال ما یک Single Point Of Failure ایجاد کرده است ، به این معنی که با از بین رفتن این فایروال یا بروز اختلال در آن کلیه شبکه هایی که به آن متصل شده اند دچار مشکل خواهند شد. همچنین اگر ترافیک بین شبکه ها زیاد باشد این فایروال به تنهایی ممکن است نتواند سرویس دهی را انجام دهد و شبکه شما کند شود. به هر یک از این کارت شبکه ها در اصطلاح یک Zone یا محدوده گفته می شود. معمولا برای نمایش این ساختار برای مستند سازی از رنگ بنفش برای شبکه داخلی ، سبز برای شبکه DMZ و قرمز برای شبکه اینترنت استفاده می شود.



DMZ با استفاده از دو فایروال

استفاده از دو عدد فایروال در طراحی DMZ یکی از امن ترین طراحی های موجود در DMZ را به شما ارائه می دهد. اولین فایروال که به آن front-end firewall هم گفته می شود به گونه ای تنظیم می شود که ترافیک را از شبکه اینترنت دریافت و به آن ارسال می کند ، این ترافیک قاعدتا ابتدا به Zone ای که به DMZ معروف است متصل می شود. فایروال دوم به گونه ای تنظیم می شود که ترافیک ورودی و خروجی به شبکه داخلی را مدیریت می کند و در اصطلاح به آن back-end firewall گفته می شود.



این طراحی از امنیت بیشتری برخوردار است ، دلایل مختلفی برای اثبات این موضوع وجود دارد. ایجاد مشکل و خرابکاری در دو فایروال طبیعی است که از یک فایروال سخت تر است و یک هکر به ناچار بایستی انرژی بیشتری برای هک این سرورها بگذارد. اگر فایروالهای مورد استفاده در این طراحی از دو نوع مختلف باشند ، درجه امنیتی را بالاتر خواهند برد ، وجود نقطه ضعف امنیتی در یکی از سرورها باعث بروز مشکل در سرور دیگری یا فایروال دیگری نخواهد شد.

برای مثال فرض کنید که در چنین طراحی ، به عنوان front-end فایروال نرم افزاری TMG و به عنوان فایروال داخلی یا back-end فایروال سیسکو ASA قرار داده اید ، حال اگر نقطه ضعف امنیتی بر روی TMG وجود داشته باشد و هکر بتواند به منطقه DMZ نفوذ کند ، به دلیل عدم وجود همین نقطه ضعف در فایروال ASA حمله در همین نقطه باقی خواهد ماند.

Data Center Design

دیتاسنتر و اتاق سرور استاندارد

سرورها باید در اتاق سرور استاندارد مستقر شوند چون امنیت فیزیکی و کنترل محیطی را به طور بهینه می توان ارائه کرد؛ سرور هایی که در این اتاق قرار می گیرند باید تمام الزامات امنیتی در آنها رعایت شود.

اتاق سرور

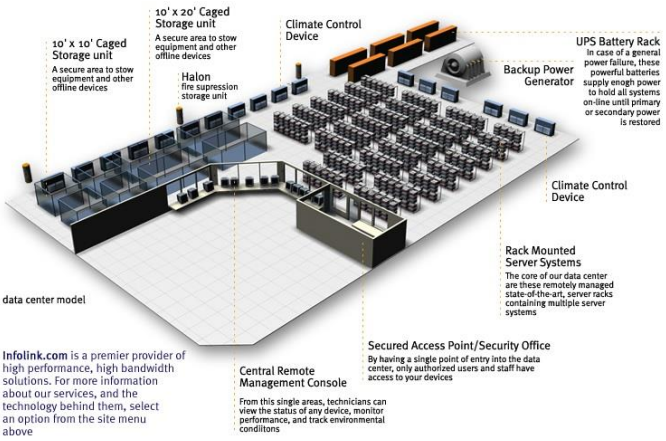
هر اتاقی که یک یا چند کامپیوتر برای ارائه خدمات برای گروهی از کاربران از طریق شبکه دارد، یک اتاق سرور نامیده می شود. این دامنه ای از اتاق سرور کوچک تا دیتاسنترهای بزرگ تر می باشد.

دیتاسنتر

دیتاسنتر یا مراکز داده مجموعه ای از تجهیزات سخت افزاری و نرم افزاری است با زیر ساخت های امنیتی ، اطلاعاتی که برای نگه داری و پشتیبانی از سرویس های تحت شبکه اینترنت ، اینترانت ، اکسترانت استفاده میشود ، دیتاسنتر یا مرکز داده و یا اتاق سرور در حقیقت محل نگه داری داده های تحت وب است.

شرکت های ارائه دهنده خدمات تحت وب با اجاره قسمتی از مراکز داده یا همان دیتاسنتر به صورت مستقیم یا غیر مستقیم ، قسمتی از دیتا سنتر را با نام سرور تهیه میکنند و اقداماتی در جهت بهینه سازی سرور تهیه شده انجام می دهند و با اتصال سرور به اینترنت امکان میزبانی وب سایت ها بر روی این فضا فراهم میشود.بنابراین دیتاسنتر محلی است که صدها و یا هزاران سرور را در رک ها rack ، کیج ها، Cageو اتاق های مختلف جای می دهد.

ساختمان دیتاسنتر از بخش های مختلفی مانند اتاق کنترل، اتاق سرور، ژانراتورها، تاسیسات خنک سازی، انبار سخت افزار، اتاق UPS و Battery backup ، اتاق نگه داری از وسایل اطفای حریق، اتاق مدیریت شبکه تشکیل می شود، هر چند که با توجه به نیازها، طراحی و امکانات و زیرساخت برای هر مرکز داده کاملا می تواند متفاوت باشد.



استانداردهای دیتاسنتر

دیتاسنتر بر اساس چندین نوع استاندارد تعبیه شده است .که اینک به بررسی دونوع TIA942 و BICSI می پردازیم: در سال 2010 استاندارد bicsi2010 منتشر شد و در سال 2011 نسخه نهایی اصلاح شده آن منتشر شد. استاندارد TIA942زمانی تنها مرجع استاندارد ساخت مرکز داده بود که به خودی خود تنها بخش های Telecommunication مرکز داده را پوشش می داد و اشاراتی نیز به سایر استاندارد ها داشت.

استاندارد TIA942 را زمانی که مطالعه کردیم تعداد زیادی علامت سوال در ذهن ها بوجود می آمد که برای رفع آنها نیاز بود به مراجع و مآخذ اعلام شده در استاندارد مراجعه نموده و پاسخ سوالات خود را در یابیم.

استاندارد BICSI محدوده وسیع تری را در حوزه دیتاسنتر پوشش می دهد . مثلا در استاندارد TIA942 اشاره مختصری به بحث سرمایش شده است اما در BICSI صفحات زیادی به توضیحات این مقوله اختصاص یافته است.

استاندارد BICSI برای ساخت یک دیتاسنتر تمام عیار منتشر شده است در این استاندارد به جزئیات زیادی توجه شده . مثلا به آب ورودی ساختمان ، قطر لوله و حتی محل جمع آوری زباله ها نیز توجه شده است . در ابتدا محدوده (Scope)تعریف و واحد های مورد استفاده توضیح داده شده و سپس به عنوان اولین مبحث Space Planning مطرح می گردد.

قبل از ایجاد دیتا سنتر باید موارد زیر را در نقشه آن به طور کامل در نظر بگیریم:

تهیه نقشه مهندسی ساختمان

مسیر گذاری کف وسقف جهت کابل کشی برق و شبکه

فاصله قرار گیری رک ها از هم

موقعیت

مکانی باید انتخاب شود که بتوان از کنترل های فیزیکی و محیطی مطمئن شد. مکان باید در برابر آتش، سیل و سایر خطرات مشابه، ایمن باشد. اتاق سرور استاندارد در جایی قرار دارد که سر و صدا در کار دفاتر و اتاق ها خلل ایجاد نکند.

امنیت محیط

تمام اتاق های سرور باید دیوارهای محکم از سقف تا کف داشته باشند. در بخش هایی که کف کاذب یک سقف کاذب وجود دارد، دیوار باید تا زیر کف کاذب و بالای سقف کاذب کشیده شود تا مانع از ورود اشخاص شود. رک های دارای قفل یا قفسه هم برای امنیت استفاده می شود.

دسترسی فیزیکی

دسترسی فیزیکی به اتاق سرور استاندارد باید تنها محدود به چند نفر شود که اجازه دسترسی را به طور قانونی دارند. استفاده از کارت خوان یا قفل الکترونیک برای اجازه دسترسی نسبت به کلیدهای مرسوم، پیشنهاد می شود؛ اگر از کلید استفاده می شود، باید عبارت "عدم کپی برداری"، روی آن حک شود. لیست افراد مجاز برای ورود باید حداقل هر فصل توسط صاحبان دیتاسنتر بررسی شود. باید کلیدها یا کارت های دسترسی گم شده یا دزدیده شده مشخص شوند. استفاده از دوربین های مدار بسته برای کنترل و ثبت ورود و خروج و کار در این فضا پیشنهاد می شود. ثبت زمان ورود، زمان خروج، هدف از دسترسی فیزیکی توسط بازدید کنندگان یا پرسنل مجاز باید مشخص شود. بازدیدکنندگان باید کارت شناسایی داشته باشند. بازدید کنندگان توسط پرسنل مجاز در تمامی زمان ها باید اسکورت شوند.

ملاحظات و بررسی های ساختاری

اتاق سرور استاندارد باید در جایی مستقر باشد که بتواند وزن تمام سیستم ها از جمله سیستم هایی که قرار است در آینده نصب شود را تحمل کند. اندازه چارچوب در باید مناسب بردن و آوردن تجهیزات باشد. برای ساختار جدید، درها باید ۴۲ اینچ عرض (106.48سانتیمتر) و ۹ فوت(274.32 سانتیمتر) ارتفاع داشته باشند. اگر لولا خارج از اتاق است، درها باید از پین های قفل لولا استفاده کنند.

سقف اتاق باید حداقل ۹ فوت ارتفاع داشته باشد.

اتاق سرور استاندارد نباید پنجره رو به بیرون داشته باشد.

ترتیب چیدمان تجهیزات باید به گونه ای باشد که فضای مناسب در اطراف رک ها داشته باشد.

4 فوت(121.92 سانتیمتر) از جلو و 3 فوت (91.44 سانتیمتر) از عقب پیشنهاد می شود.

برق اتاق سرور باید مدارهای مناسب برای تمام تجهیزات به همراه یک یا چند مدار اضافی در صورت آسیب رسیدن به مدار اصلی را داشته باشد. سیستم های مهم و اصلی باید به UPS و یا برق ژنراتور بسته به الزامات کسب و کار متصل باشد UPS و یا ژنراتور برق باید حداقل سالانه تست شود و بر اساس خصوصیات و ویژگی های تولید کننده نگهداری شود.

اتاق های بزرگ باید سوئیچ خاموش اضطراری داشته باشند. باید رویه های مربوطه در اتاق نصب شود و توضیح دهید که در هنگام قطعی برق چکار باید انجام داد. باید سیستم نورپردازی اضطراری هم داشته باشند.

کنترل درجه حرارت

اتاق سرور استاندارد باید کنترل درجه حرارت مناسب برای حفظ دمای اتاق بر اساس محدودیت تعریف شده برای سخت افزارهای موجود در اتاق را داشته باشد. باید تهویه هوای مناسب برای حفظ درجه حرارت بین ۶۵ – ۷۰ درجه فارنهایت (18.33 درجه سانتیگراد تا 21.11 درجه سانتیگراد) داشته باشد. کنترل های محیطی باید مجهز به سیستم های هشدار دهنده در هنگام بروز مشکل باشند. برای اتاق های بزرگ، سیستم ها و تجهیزات خنک کننده باید برای حداکثر سازی کارآیی نصب شود.

اتاق سرور ، قلب هر کسب و کار است. بدون مدیریت پیوسته و کارآمد داده، ذخیره و انتشار، بیشتر کسب و کارها نمی توانند به درستی کار کنند و اگر برای سیستم مشکلی ایجاد شود، نمی توان کار کرد. اهداف اساسی در خصوص طراحی اتاق سرور باید کارآیی و ثبات همراه با تجهیزات در سطوح بهینه باشد.

فضای باز، تمیز و با تهویه مناسب

اتاق سرور استاندارد باید تمیز، بدون گرد و غبار باشد و تهویه مناسب داشته باشد. سرورها و سایر کامپیوترها به طور طبیعی گرما ایجاد می کنند و تهویه نامناسب می تواند منجر به گرمای بیش از حد و خرابی شود. در طراحی اتاق سرور مطمئن شوید که فضای کافی بین واحدها برای نظافت منظم و دسترسی راحت برای تعمیر و نگهداری با حداقل فضاهای غیر قابل دسترسی که گرد و غبار روی هم انباشته می شود، وجود دارد.

کنترل های محیطی و لوازم خنک کننده مناسب

هر چه تهویه و خنک سازی بیشتری برای سرورها فراهم شود، کمتر احتمال دارد بیش از حد گرم شوند. مطمئن شوید که کنترل های محیطی و تخلیه موثر را برای طراحی اتاق سرور در نظر گرفته اید. لوازم جانبی بسیاری در بازار وجود دارند تا به تسهیل خنک سازی کمک کنند، از جمله کف کاذب، کابینت های خود خنک کننده و IRC.

تامین برق اضطراری

مهم است که سیستم الکتریکی اتاق سرور برای ادامه کار در حین اختلال در برق، طراحی شود. همچنین مهم است مطمئن شد که برق برای واحدهای شما، به درستی توزیع شده است. ژنراتورهای بک آپ و باتری ها به سالم ماندن تامین برق ادامه می دهند و واحدهای توزیع برق می توانند مقدار درستی از برق را در تمام زمان ها به مکان مناسب منتقل کنند.

جلوگیری از بهم ریختگی سیم ها

بخش کلیدی دیگر طراحی اتاق سرور، مسیریابی موثر و مناسب کابل و سیم ها است. در هم و برهمی سیم ها، حوادثی هستند که آماده هستند هر زمانی رخ دهند. مطمئن شوید که مسیر مناسبی مشخص کرده اید تا سیم ها و اتصالات بتوانند بدون خطر قطعی، کشیدن و کندن منتقل شوند و مطمئن شوید که نقشه اتصالات را ترسیم کرده اید تا متخصصین فناوری اطلاعات بدانند که در چه جایی مشکلات را شناسایی کرده و به آنها دسترسی پیدا کنند.

فراهم سازی محیط کار با کیفیت

در هنگام طراحی اتاق سرور استاندارد، فراموش نکنید که به فکر کارکنان فناوری اطلاعات باشید. مطمئن شوید که یک فضای کار با طراحی خوب، روشن و مطابق با ارگونومی فراهم می کنید تا کارکنان فناوری اطلاعات بتوانند به راحتی و به طور موثر بر آن نظارت داشته باشند.

مشخصات محیطی:

- اتاق نباید پنجره داشته باشد
- فضا به اندازه کافی برای رشد و توسعه آتی، بزرگ باشد
- سقف باید حداقل نه فوت ارتفاع داشته باشد

مشخصات تجهیزات:

- رک های کامپیوتر باید حداقل ۴۲ اینچ فاصله داشته باشند
- تمام رک ها باید مجهز به امکانات لرزه ای مناسب باشند
- تجهیزات محاسباتی باید حداکثر شدن الکتریکی ۳۰۰ وات در هر مربع فوت را داشته باشند
- در اتاق سرور باید بر آتش، دود، آب و رطوبت نظارت داشت

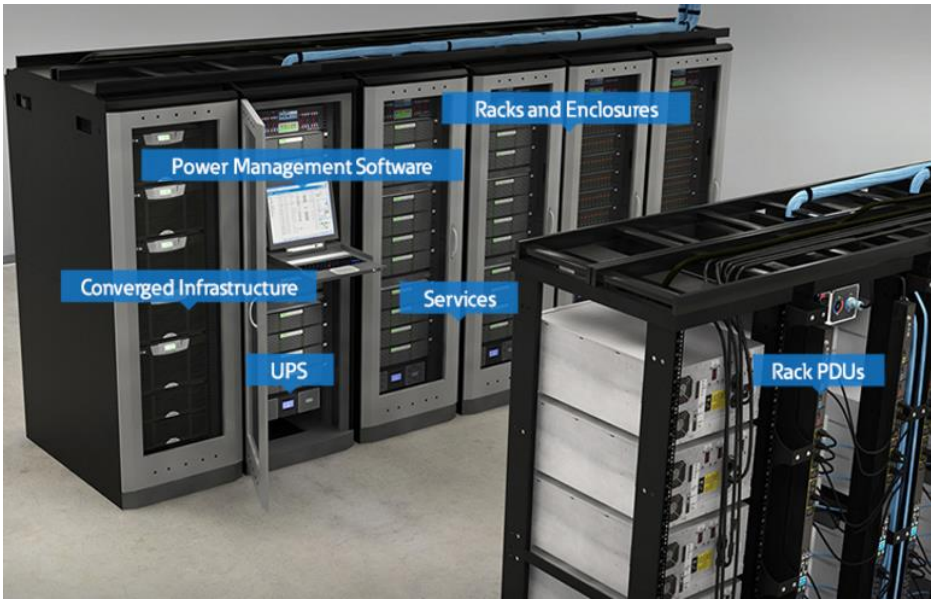
مشخصات خنک سازی:

- از تجهیزات خنک سازی با فن های متغیر سرعت استفاده شود
- سیستم های خنک سازی از کف با حداقل ارتفاع ۲۴ اینچ با توانایی تحمل بار رک های سرور و تجهیزات نیاز است

مشخصات سیستم های الکتریکی:

- تجهیزات کامپیوتری و HVAC باید پانل های برق جداگانه داشته باشند
- نباید هیچ تجهیزات پشتیبانی که گرما تولید می کند، وجود داشته باشد
- برق جداگانه باید برای دیتاسنتر موجود باشد.

تجهیزات اتاق سرور



هک و افشای داده ها، کسب و کارها را مجبور کرده تا درباره حریم خصوصی داده یا محرمانگی دوباره فکر کنند که چگونه می توانند داده ها را از دست هکرها حفظ کنند. با ایجاد بخش فناوری اطلاعات در شرکت به جای استفاده از خدمات آنلاین، می توان بسیاری از مسائل امنیتی مربوط به داده را حفظ کرد، این امر مستلزم استفاده از تجهیزات اتاق سرور استاندارد است. با تمرکز بر خدمات آنلاین، این کار می تواند برای کسب و کارهای کوچک، ترسناک باشد. علاوه بر این، منابعی که برای کمک طراحی شده اند می خواهند از تاسیسات در اندازه متوسط استفاده کنند که ممکن است ضرورتا برای اتاق سرور کوچک، به اندازه کافی خوب نباشد.

با درک برخی اصول، ایجاد اتاق سرور دیگر یک فرآیند محرمانه نخواهد بود. در اینجا به برخی نکات اشاره شده است:

تجهیزات رک ، اهمیت دارند

برای کسب و کارهای کوچک چندان رایج نیست تا عملیات خود را با استفاده از سخت افزار سرور و دستگاه های شبکه روی قفسه یا میز انجام دهند. اگرچه چنین کاری، ارزان است، اما مقداری زیادی از تجهیزات با رشد شرکت، توسعه می یابند. تجهیزات همچنین کاملا برای بررسی فیزیکی، باز هستند و گرد و غبار، ریختن مایعات یا حتی برخورد با سیم ها برای تجهیزات بسیار خطرناک است.

رک سرور، برای تمام فصول است

قبل از خرید رک سرور، خوب است که در ابتدا خصوصیات اصلی را درک کنید. رک های سرور با واحدهای رک سنجیده می شوند. یک واحد رک معادل ۱،۷۵ اینچ (۴۴،۴۵ میلی متر) ارتفاع دارد. سوئیچ های شبکه در کل ۱ تا ۲ واحد هستند. سرورها می توانند بین ۱ تا ۴ واحد داشته باشند.

سرورها را برای کاهش صدا، ایزوله کنید

سازمان ها بدون اتاق های اختصاصی برای تجهیزات سرور می خواهند صدا را کنترل کنند. یک اتاق کوچک با پارتیشن هم ارزش هزینه دارد. گذشته از کاهش یا حتی حذف صدای تجهیزات، اتاقی برای تجهیزات فناوری اطلاعات می تواند به جلوگیری از سرقت یا دستکاری تجهیزات کمک کند.

مدیریت سیم ها، ضروری است

تنظیم و راه اندازی رک سرور، چیزی بیشتر از بستن چند تا پیچ و مهره است. در مدیریت مناسب کابل ها نمی توان اغراق کرد چون هر بخش از تجهیزات در رک با کابل های اترنت بهم متصل شده اند. در کنار سیم کشی بین کابینت ها، رساندن کابل به نقاط LAN برای کامپیوترها، دوربین های مدار بسته و سایر تجهیزات شبکه در رک، اهمیت دارد. علاوه بر نصب پانل، همیشه یک بند کابل داشته باشید تا کابل ها را بهم ببندید. بند استاندارد کابل، ارزان هستند.

تمامی تجهیزات باید دارای برچسب باشند

یک پرینتر لیبل خریداری کنید. تمامی سرورها و تجهیزات شبکه باید با نام های توصیفی منحصر به فرد و آدرس های آی پی شان برچسب گذاری شوند. همچنین برای سایر تجهیزات اتاق سرور مثل کیبورد، سوئیچ ویدئو و ماوس، تجهیزات NAS، روترها، دستگاه های بک آپ داده و تجهیزات اتاق سرور دیگر هم باید برچسب داشته باشند.

توضیحات مشروح که رویه های مهم مرتبط با تجهیزات را توصیف می کند باید تایپ و به کابینت سرور با چسب یا آهنربا متصل شود. این نوشته ها باید به دستور العمل های عملیاتی مهم مرتبط با شبکه، بک آپ داده یا خاموش کردن تجهیزات در هنگام بروز قطعی برق اشاره کند.

اگر برنامه دارید تا از یک جفت سوئیچ شبکه و سیستم ذخیره (NAS) استفاده کنید، باید درجه حرارت را با تجهیزات مرتبط کاهش دهید، چرا که با افزایش درجه حرارت تجهیزات اتاق سرور، طول عمر آنها کم شده و باعث بروز قطعی یا خسارت می شود.

یکی دیگر از تجهیزات اتاق سرور ، سیستم تهویه هوا می باشد که کسب و کارها باید حداقل دو دستگاه در اتاق سرور با مدارهای جداگانه نصب کنند.

سینی کابل و لدر برای کابل کشی

سینی های کابل باید به نحوی اجرا شود که جلو مسیر هوا را در زیر کف کاذب سد نکند. سینی های زیر کف کاذب ممکن است به صورت چند طبقه طراحی شوند تا فضای کمتری را اشغال نموده و ظرفیت بیشتری را عرضه نماید . سینی های فلزی باید به سیستم ارت مرکز داده متصل شود.

سینی کابل حداکثر با عمق 15 سانتی متر مجاز است. مسیر سینی کابل های زیر کف کاذب در هنگام طراحی باید با سایر تاسیسات نصب شده زیر کف کاذب هماهنگی لازم را داشته باشد . کابل ها درون سینی باید فیکس شود و لیبل شماره کابل مطابق استاندارد نصب شود.

سینی ها باید در قالب چند استاندارد مهم پیاده سازی شوند ، از جمله:

–نارسانایی در برابر بارها
–تحمل وزن بالا
–غیر قابل اشتعال
–مقاومت در برابر ضربه
–دارای عمر مطلوب و بالا
–ایده آل برای انواع آب و هوا ها
–و سینی ولدرهای کابل با ورق استیل مقاوم در برابر مواد شیمیایی باشد.

کنترل تردد و دوربین های امنیتی

برای کنترل دسترسی ورودی و خروجی افراد مجاز و بر روی مبادی ورودی وبرخی از مبادی خروجی سایت مرکز داده سیستم های کنترل دسترسی نصب خواهد شد ، برای مبادی خروجی از کارت های مغناطیسی با بیومتریک استفاده یا از Push Button استفاده می شود.

همچنین دوربین های امنیتی نیز پوشش نسبتا کاملی با توجه به نیاز کارفرما در فضای مرکز خواهد داشت. صفحه نمایشی که برای نظارت تصاویر دوربین های مداربسته استفاده می شوند معمولا مانیتور های حادثه یا نقطه ای نامیده شده و اجازه می دهند که اطلاعات تصاویر بدون خطا ودر لحظه دیده بانی شوند و مانیتور های حادثه مستقیما باید روبروی اپراتور و در فاصله ی تقریبی 0.5 تا 1.5متری و با اندازه قطر 9-16 اینچی (22-40 سانتی متری) از وی نصب شوند.

درب اتاق سرور

امنیت اتاق سرور بسیار حائز اهمیت است از این رو باید اکثر الزامات ضروری در این اتاق رعایت شود تا از آسیب ها و خسارات احتمالی جلوگیری شود. گزینه های مختلفی برای سیستم های امنیتی درب اتاق سرور وجود دارد.

سه سیستم وجود دارد: قفل های صفحه کلید دار، قفل های کارتی و قفل های بیومتریک.

قفل های صفحه کلید دار، یک صفحه کلید عددی در نزدیکی دستگیره درب اتاق سرور دارند که کاربر باید یک پین کد برای باز کردن در وارد کند. قفل های کارتی که در بیشتر هتل ها استفاده می شود به یک کارت با نوار مغناطیسی برای باز کردن درب نیاز است مثل کارت های اعتباری. سیستم های بیومتریک معمولا سیستم خواندن اثر انگشت برای قفل دارند که کاربر انگشت خود را برای اجازه دسترسی روی آن قرار می دهد.

اگرچه تمام این سیستم ها اساسا مکانیکی هستند اما به کنترل های متمرکز نیاز دارند که معمولا می توان از طریق شبکه کامپیوتری انجام داد. بزرگ ترین مزیت کارت خوان ها این است که نوار مغناطیسی را می توان تنها برای اجازه دسترسی کارکنان خاصی فعال کرد. وقتی که آن کارکنان، شرکت را ترک کنند، کارت را می توان بدون دسترسی فیزیکی به قفل، غیر فعال کرد.

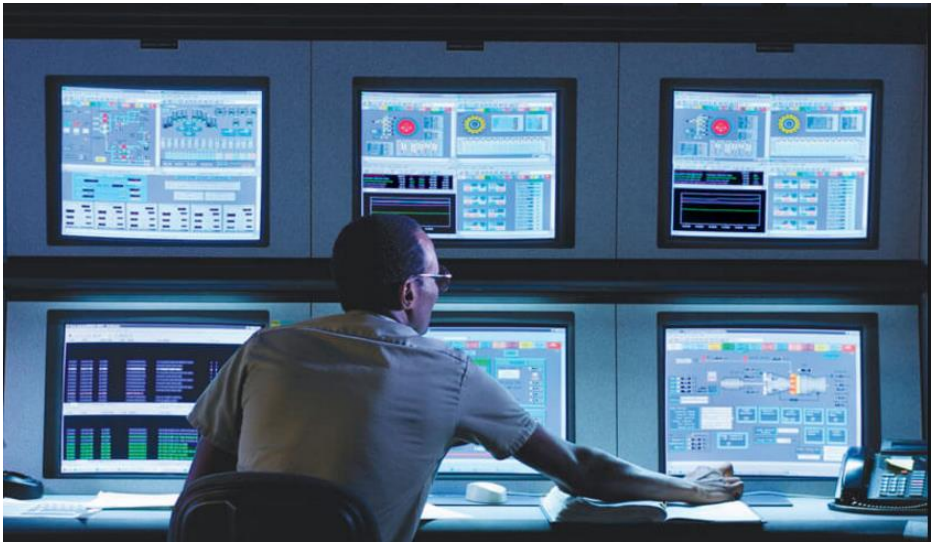
قفل های صفحه کلید دار هم به صورت مکانیک و هم به صورت الکترونیک هستند که هر قفل حدودا بین ۱۰۰ تا ۱۵۰ دلار بسته به برند و مارک آن قیمت دارد.

نکته: مطمئن شوید که صفحه کلیدهای مکانیکی، چندین گزینه تغییر راحت کد را داراست. این نوع قفل برای درب اتاق سرور اماکنی مناسب است که افراد کمی به آنجا تردد دارند مثل اتاق سرور مدارس.

قفل بدون کلید یا ورود با کد الکترونیک برای درب اتاق سرور امروزه بسیاری از اشکال قفل های بدون کلید و قفل های کد دار الکترونیک در ساختمان ها به چشم می خورد. برخی از آنها سیستم های پیچیده تری دارند که گران تر هم هستند. این سیستم ها به یک کاربر نیاز دارند تا کد ورودی را برای دسترسی جهت ورود وارد کند. آسیب پذیری مشهود این سیستم ها این است که اگر کد هیچ وقت تغییر نکند، کل افراد در نهایت کد را می دانند. وقتی این اتفاق رخ دهد، انگار که اصلا هیچ دربی وجود ندارد. تعیین یک فرد برای قفل ها یا امنیت خارجی به شما کمک می کنند تا اگر شما هم یکی از افرادی هستید که به اتاق سرور وارد می شوید، کد دسترسی خود را به صورت بازه ای از طریق سیستم های قفل بدون کلید تغییر دهید. با وجود چنین سیستم هایی، می توانید کدهای مختلف برای کارکنان مختلف تعیین کنید. بدین ترتیب، اگر کسی شرکت را ترک کند می توانید کد دسترسی او را غیر فعال کنید.

کارت های کنترل دسترسی قدرتمند ترین شیوه برای نظارت بر دسترسی به نقاط مهم و حساس، سیستم های کارتی کنترل دسترسی روی درب اتاق سرور است. سیستم هایی با ویژگی های کامل هستند که با ساختار ساختمان یکپارچه شده اند و حقوقی که برای یک شخص جهت ورود به اتاق سرور مشخص شده را رد یا تایید می کند (که به کدام شخص تخصیص یافته است). چنین سیستم هایی می توانند هر چیزی را از HVAC، آسانسورها و درب ها گرفته تا حتی سیستم های نور پردازی، پیکربندی کند. سیستم های کارتی کنترل دسترسی، بهترین مزیت را به شرکت های بزرگ ارائه می کنند. شرایط را در موقعیت های خاص، تغییر کارکنان و غیره کنترل می کنند. برخی حتی رابط های نرم افزاری دارند که از طریق آنها می توان کنترل کرد. سیستم های کارتی کنترل دسترسی، انعطاف پذیری بسیاری دارند. برخی از آنها با انواع جدیدتری از این تکنولوژی ها، دستگاه های رابط انسان دارند تا در ارتباط با سیستم های کارتی کار کنند.

سیستم مانیتورینگ اتاق سرور



بسیاری از حوادثی که در اتاق سرور رخ می دهد قابل پیشگیری می باشند نظارت و مانیتورینگ عوامل محیطی اتاق سرور نیز یکی از مهمترین وظایف مسئولین اتاق سرور است. سیستم مانیتورینگ اطلاعات لازم جهت کنترل وضعیت محیط را دراختیار شما قرارمی دهد و در مواقعی مانند نفوذ رطوبت گاز و دود قطع ولتاژ دمای بالا و ... هشدارهای لازم و از قبل تعیین شده را برای شما ارسال کند. این کارمی تواند توسط ارسال اخطار به نرم افزار مرکزی ارسال پیامک ایمیل فعال کردن زنگ هشدار و ...صورت پذیرد و یا اقدامی را در صورت رسیدن به آستانه بحران و خطر انجام دهد به عنوان مثال در صورت افزایش بیش از دما سیستم تهویه را فعال نماید .در صورت نیاز می توان برای تامین سطح امنیت بیشتر سیستم کنترل تردد و دوربین مدار بسته را به خدمت گرفت .

اتاق های سرور از معدود مکانهایی هستند که حساسیت ویژه ای دارند چرا که تمامی اطلاعات و ارتباطات یک مجموعه به اتاق سرور وابسته است.معمولا سرورهای موجود در شرکت ها و سازمان ها می بایست به صورت شبانه روزی سرویس دهی گردد ، این امر مستلزم ایجاد شرایط محیطی مناسب و نظارت مداوم می باشد. تا در صورت بروز هر گونه اشکال بلافاصله اقدامات لازم در خصوص فعال نگاه داشتن صورت پذیرد. از این رو استفاده ازسیستم کنترل و نظارت بر اتاق سرور امری ضروری می باشد.

– فعال شدن آزیر صوتی در محل و ارسال آلارم هشدار بر روی تلفن همراه و پنل کاربری در صورت افزایش دما ، رطوبت و یا مشکل در سیستم سرمایش.
– کنترل تردد و جلوگیری از ورود غیر مجاز با استفاده از درب های مجهز به قفل دیجیتالی با قابلیت شناسایی اثر انگشت و...
– اعمال فرایند های ویژه بصورت اتوماتیک و هوشمند برای کنترل دما : مانند روشن کردن کولر رزرو و یا هواساز، برای جلوگیری از خسارات وارده .
– دریافت دستور مدیر اتاق سرور را در برای قطع برق ، آب و راه اندازی مجدد و یا غیره .
– ارسال دما و رطوبت فعلی اتاق سرور بر روی تلفن همراه و پنل کاربری با قابلیت زمان بندی.
– دریافت آلارم از سنسورهای آتش و دود ، نشت گاز ، ضربه و ورود غیر مجاز ، قطع برق ، نوسان برق و ...–
کنترل برق اتاق سرور و نحوه کارکرد یو پی اس و تجهیزات برق اضطراری ، توسط تلفن همراه و پنل کاربری در شرایط بحرانی .
– کنترل و مدیریت دمای سویچ ها ، رکها و دیگر تجهیزات با قابلیت دریافت خطاهای شبکه و

امکانات سیستم :

–قابلیت کارکرد دستگاه بصورت آفلاین بدون نیاز به کامپیوتر
–امکان اجرای فرامینی خاص توسط اس ام اس
-امکان کنترل درب های ورودی با استفاده از قفل های دیجیتالی با امکان دسترسی به قفل با اثر انگشت ، اسکن چشم و کد 4 تا 8 رقم
-امکان کنترل عوامل محیطی مانند دما ، رطوبت ، دود و گاز
-امکان هشدار بصورت پیام کوتاه، تماس تلفنی، آژیر و ایمیل

-قابلیت فعال سازی سیستمهای مختلف توسط ارسال پیام کوتاه
-دارای چندین خروجی (رله) جهت کنترل ادوات جانبی
-امکان ثبت تصویر افراد وارد شده به اتاق سرور
-امکان تعریف و ارسال پیام کوتاه به چند نفر بطور همزمان
-امکان کنترل ارتباط و خاموش کردن چندین سرور توسط نرم افزار مرکزی در مواقع خاص
-مانیتور کردن ریست شدن سرور توسط نرم افزار و ارسال پیام کوتاه
–مانیتور کردن قطع و وصل شدن برق توسط نرم افزار و ارسال پیام کوتاه
-مانیتور کردن قطع و وصل شدن UPS توسط نرم افزار و ارسال پیام کوتاه
-قابلیت ارتباط با سیستم کنترل دسترسی و بازکردن در توسط پیام کوتاه
-قابلیت کنترل سرویس های ویندوز سرور اعم از DNS, DHCP و...
-امکان دریافت وضعیت اتاق سرور با استفاده از پیام کوتاه
-گزارش گیری های مختلف تحت وب و شبکه محلی

UPS اتاق سرور

یکی از دستگاه های اتاق سرور UPS است. این دستگاه که در اتاق های سرور به کار گرفته می شود موجب عملکرد نرمال سرورها حین قطع و وصل شدن جریان خواهد شد.

بسیاری از شرکت ها یا سازمان ها برای اتاق سرور خود یک UPS تهیه می کنند تا اتاق سرور آنها به عنوان اتاق سرور UPS شناخته شود. البته هزینه کمی نیز نداشته و یک گزینه بزرگ برای اتاق سرور است که با افزودن آن می توان ایمنی و استاندارد لازم را به اتاق سرور افزود. بنابراین می توان به کمک چنین دستگاهی شدت جریان برق را در سرورها به شکل نرمالی برقرار کرده و خطر قطعی را از دستگاه ها دور داشت.

در حقیقت اتاق سرور UPS به اتاقی گفته می شود که شامل دستگاه UPS برقرار کننده شدت جریان برق نرمال در حین قطعی کامل یا تغییر نوسان می شود. بنابراین وجود دستگاه UPS در کنار اتاق سرور ضروری بوده و موجب جلوگیری از بروز هرخطری ناشی از قطعی برق می شود.

برق امر حیاتی برای یک اتاق سرور محسوب می شود که نبود آن حتی موجب حذف حافظه بخشی از داده ها می شود که در نهایت ضررهایی را برای شرکت یا سازمان موردنظر به دنبال دارد. بنابراین نباید در هنگام ایجاد اتاق سرور از استفاده دستگاه UPS صرف نظر کرد.

این دستگاه مخفف Uninterruptible power supply که همان منبع تغذیه بی وقفه محسوب شده و مدت ها می تواند در کنار اتاق سرور به کار گرفته می شود.

دمای اتاق سرور

اتاق سرور، اتاقی است که هوای مطبوع دارد و به عملیات مداوم سرورهای کامپیوتری تخصیص یافته است. کل ساختمان یا ایستگاهی که به این کار اختصاص یافته، دیتاسنتر نام دارد. دمای اتاق سرور ، یکی از فاکتورهایی است که بر مصرف انرژی و اثر محیطی اتاق سرور تاثیر می گذارد. در نواحی که هوا خنک است و برق قابل تجدید بسیاری دارند، اثرات زیست محیطی معتدل تر است. از این رو کشورهایی با شرایط مطلوب مثل کانادا، فنلاند، سوئد و سوئیس سعی دارند شرکت های بیشتری را برای استقرار اتاق های سرور خود در این کشورها جذب کنند.

در سرتاسر دنیا، شرکت ها برای ذخیره و پشتیبانی از داده های حساس بی شمار به اتاق های سرور متکی هستند. به منظور برآورده سازی تقاضای مشتری، سرورها باید پیوسته آنلاین حفظ شوند. این تجهیزات، گرمای زیادی را ایجاد می کنند که اگر بررسی نشود، می توانند اثر معکوسی بر عملکرد آن داشته باشد. بنابراین اوپراتورهای اتاق های سرور باید دمای بهینه را حفظ کنند تا مطمئن شوند که این سیستم ها کار خود را به درستی انجام می دهند.

وقتی یک اتاق سرور، خیلی گرم باشد، تجهیزات خیلی راحت بیش از حد گرم می شوند و منجر به از بین رفتن داده های ذخیره شده می شود. این مشکل برای یک سازمان، فاجعه به حساب می آید که به این اطلاعات برای انجام کسب و کار خود متکی است. بنابراین در اتاق های سرور از سیستم های خنک سازی برای خنک کردن اتاق سرور و جلوگیری از گرمای بیش از حد تجهیزات استفاده می شود.

تجهیزات شبکه و کامپیوتر برای عملیات در یک دامنه دمایی نسبتا محدود طراحی شده است. برای اطمینان از عملیات قابل اعتماد و طولانی تر شدن عمر قطعات ، شما باید مطمئن شوید که دما در آن دامنه باقی می ماند. حتی چند درجه گرما می تواند یک تراشه سرور را از بین ببرد.

هزینه خرابی سرور می تواند قابل توجه باشد. فکر کنید به خاطر این خرابی چقدر ضرر می کنید؟ هزینه جایگزینی هم وجود دارد. تجارت الکترونیک را از دست می دهید، جزییات اطلاعات مشتریان را از دست می دهید، زمان کارکنان هدر می رود و متحمل خیلی هزینه های مرتبط دیگر می شوید.

توصیه های عمومی مطرح می کنند که دما نباید پایین تر از ۱۰ درجه سانتی گراد (۵۰ درجه فارنهایت) یا بالای ۲۸ درجه سانتی گراد (۸۲ درجه فارنهایت) باشد اما بهتر است که دما را بین ۲۰ – ۲۱ درجه سانتی گراد (۷۱-۶۸ درجه فارنهایت) نگه داشت.

نظارت بر دمای اتاق سرور

شما باید دمای اتاق سرور استاندارد را همیشه کنترل کنید و بر آن نظارت داشته باشید، به ویژه در شب و آخر هفته ها که هیچ کس در آنجا نیست. سیستم هایی برای این کار موجود است. باید دما را در نقاط مختلف اتاق بسنجید تا

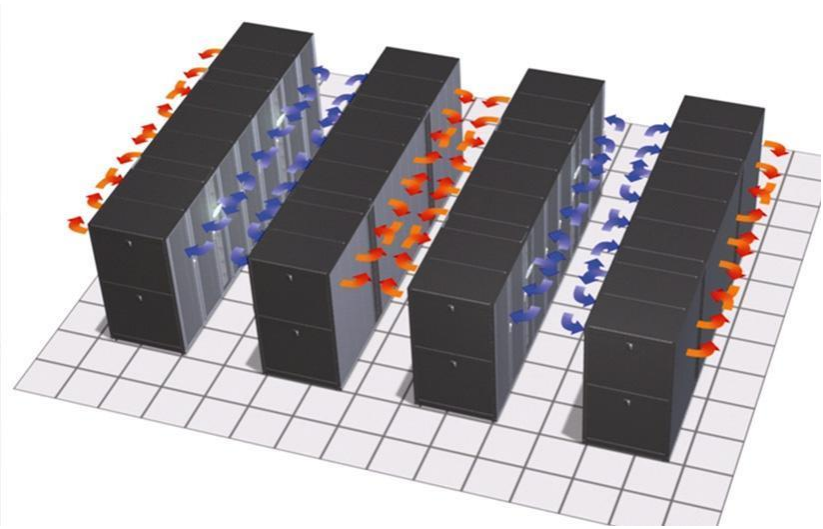
ببینید که کجا گرم است. سنجش دما باید خودکار و قابل اعتماد باشد. سیستم ها باید از هشدار به صورت های مختلف مثل ایمیل یا اس ام اس پشتیبانی کنند.

در تعیین بهترین دمای اتاق سرور، چندین فاکتور از جمله اندازه اتاق و تعداد سرورها باید در نظر گرفته شود. این اطلاعات می تواند به اوپراتورها در تصمیم گیری پیرامون بهترین دما کمک کند. وقتی که بهترین دما شناسایی شد، اوپراتورهای اتاق سرور باید بر سیستم های کنترل دما نظارت داشته باشند تا مصرف انرژی و خنک سازی حفظ شود.

سیستم تهویه

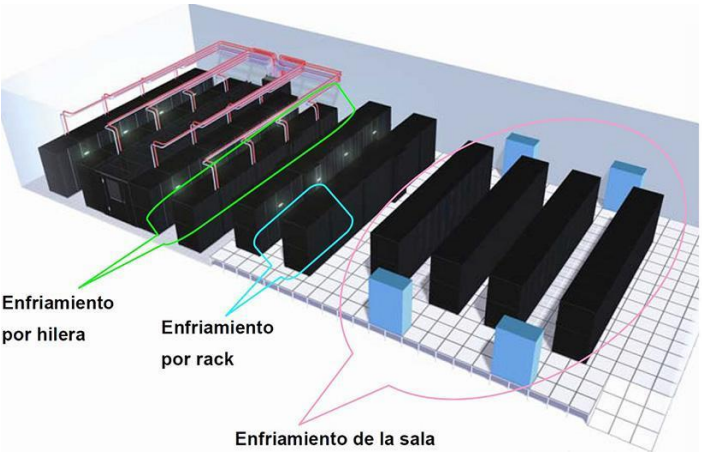
انتخاب سیستم خنک کننده بر اساس نوع و سطح درجه بندی مرکز داده انجام می گیرد. باید از تکنولوژی استفاده شود که قادر به کاهش بار تهویه هوا در اتاق سرور استاندارد باشد زیرا قبل از آنکه گرما در فضای اتاق سرور پخش شود جمع آوری و به خارج از اتاق سرور منتقل شود.
راه های توزیع هوای سرد به سه دسته براساس تجهیزات تقسیم بندی می شود:

Row oriented
سیستم توزیع سرمایش در میان رک ها بالا و پایین کف کاذب یا در بین ردیف ها استفاده میشود ، رک های ظرفیت بالاتر در یک ردیف و رک های با ظرفیت پایین در یک ردیف دیگر نگهداری می شود.



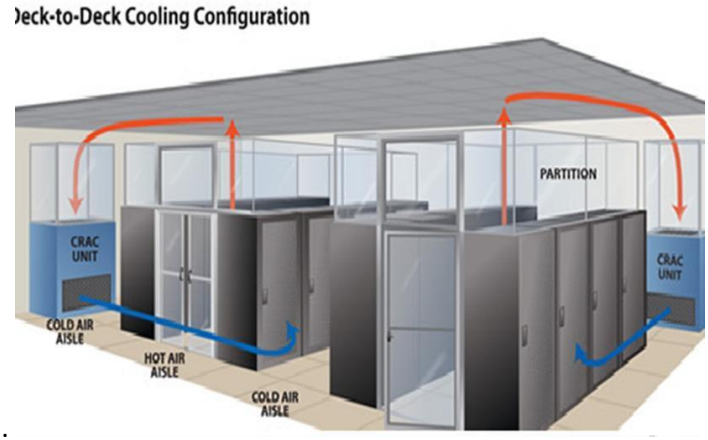
Room Oriented

سیستم سرمایشی که برای کل فضای دیتا سنتر در نظر گرفته می شود و به ساختار اتاق و ارتفاع سقف وابسته است.
مکانیزم آن به این شکل است که هوای گرم و سرد را با یکدیگر ترکیب می کند تا به دمای مناسب دیتا سنتر برسد.



Rack Oriented

سیستم سرمایش در داخل رک قرار می گیرد و وظیفه تنظیم دمای هر رک را به عهده دارد تا دمای رک را همواره در دمای تنظیم شده نگه دارد و به طور کلی فارغ از وابستگی به تغییرات دمای اتاق می باشد.



اتوماسیون اتاق سرور

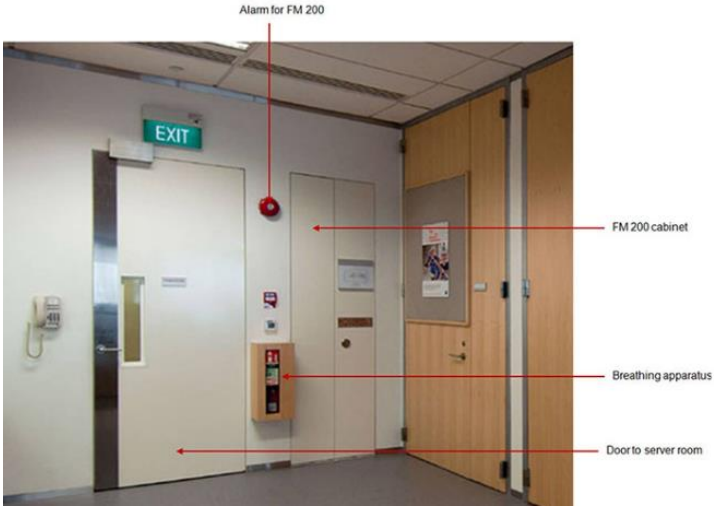
سیستم کنترل و نظارت یا همان اتوماسیون اتاق سرور استاندارد یکی از تجهیزات اصلی نگهداری اتاق های سروری شرکت ها و سازمان ها به شمار می روند، بنابراین بدون وجود آن خطر بزرگی این مکان ها را تهدید می کند و خسارت های بزرگی را نیز برای این کمپانی های به دنبال خواهد داشت. از این رو بایستی به طور حتم اتوماسیون ها در اتاق های سرور به کار گرفته شوند تا نظارت همیشگی روی سرورها داشت و مانع از به وجود آمدن مشکلات شد.

برخی از کمپانی هایی که فاقد چنین اتوماسیونی هستند نظارت ناقصی روی سرورها داشته و از این رو باید هزینه های بسیاری جهت حل مشکل متحمل شوند. هنگامی که مشکلی به وجود می آید سیستم نظارت یا همان اتوماسیون به شکل ارسال پیامک، برقراری تماس، ارسال ایمیل و برخی از این دست به افراد تعیین شده در سیستم ارسال می شود. از این رو افراد معین شده در صورت به وجود آمدن مشکلی در این رابطه اطلاعی کسب کرده و به حل سریع آن می پردازند.

یکی دیگر از ویژگی های بارز و قابل توجه این نوع سیستم خاموش و روشن نمودن سرور و روشن کردن تهویه با ارسال پیامک است که کمک شایانی جهت حل مشکل می کند.

بنابراین وجود اتوماسیون در اتاق سرور استاندارد می تواند موجب ایمنی کامل اتاق ها شده و نگهداری کاملی به دنبال خواهد داشت. اتاق های سرور همانطور که گفته شد مرکز اسناد و اطلاعات شرکت ها و سازمان ها به شمار می روند. از این رو بایستی نظارت کامل و حرفه ای روی آنها صورت گیرد و در غیر این صورت شاهد آشکار شدن مشکلات

سیستم های اطفاء حریق مناسب جهت دیتاسنترها و اتاق های سرور:



در درجه اول گازهای تمیز همچون FM-200، Novec 1230، Inert Gas و سایر گازهای ذکر شده دراستاندارد NFPA 2001، پیشنهاد می شود. همچنین استفاده از سیستم های Oxygen Reduction و Watermist جهت استفاده در اتاق سرور با محدودیت هایی روبرو است که می بایست مورد بررسی بیشتری قرار گیرد. استفاده از سیستم آیروسل (Aerosol) در اتاق سرور به عنوان گزینه اصلی توصیه نمی شود.

خصوصیات کلی یک سیستم اطفاء حریق مناسب از نوع Total Flooding در اتاق سرور استاندارد شامل موارد زیر است:

- قدرت اطفاء کنندگی در کلاس C و A حریق
- قابلیت نفوذ پذیری بالا
- نداشتن پسماند
- عایق الکتریسیته
- نداشتن خطر جانی برای افراد
- سرعت عملکرد و برگشتن سریع سیستم به حالت نرمال
- آسیب نرساندن به تجهیزات
- تناسب مالی با ارزش دیتا و سخت افزار مورد استفاده
- امکان جایگزینی سریع پس از عملکرد

مضرات اتاق سرور استاندارد

اتاق سرور یکی از بخش های مهم هر سازمان و شرکت محسوب می شود که باید نگهداری کاملی از آنها صورت گیرد. در این میان اگرچه فوایدی از اتاق سرور می توان مشاهده کرد امامضرات اتاق سرور را نیز باید در نظر گرفت. سازمان ها و شرکت ها باید توجه کاملی به مضرات اتاق سرور داشته باشند زیرا ممکن است در نهایت خطرات و ضررهای بزرگی را برای طرف های مقابل به دنبال داشته باشند.

از جمله مضرات اتاق سرور باید به تهدیداتی اشاره کرد که همیشه اتاق های سرور را دنبال می کنند. این تهدیدات که باید آنها را مضرات اتاق سرور نیز محسوب کرد شامل عوامل متعددی می شوند که باید به افزایش درجه دما، رطوبت بالا هوا، جنبش ، قطعی برق و سرقت اشاره کرد.

البته هر یک از عوامل فوق توضیحاتی داشته که در ادامه می توانید بیشتر درباره آنها اطلاعات کسب کنید:

۱– جنبش

حرکات ناخواسته در اتاق سرور استاندارد آسیبی به هارد سرورها وارد می کند که در نتیجه داده ها موجود در آن را با مشکل ایجاد خواهد کرد. حرکت افراد، حرکت وسایل نقلیه و برخی از این قبیل موجب می شود تا حرکت های ناخواسته ای را به دنبال داشته که- فرجام بدی دارد. این حرکت های ناخواسته که به آن ارتعاش نیز گفته می شود، درایوهای سرور را دچار اختلال می کند که این اختلال ممکن است به حذف داده های درون سرور بیانجامد. بنابراین نباید به حرکت کردن در اتاق های سرور پرداخت و بایستی بیشتر کارها را به شکل آهسته انجام داد.

۲– قطعی برق

قطع برق یکی از بزرگترین عوامل تهدید کننده اتاق سرور است. زیرا هارد درایو سرورها بوسیله برق می توانند انرژی داشته و فعال باشند و قطعی مکرر می تواند آسیب بزرگی را به این درایوها وارد کند. آسیبی که همچون جنبش می تواند موجب پاک شدن داده های درون هارد سرور شود. از این رو بایستی سیستم هوشمندی را به کار گرفته تا از قطعی برق جلوگیری کرده تا آسیبی متوجه سرورها نشود.

۳– رطوب هوا

رطوبت یکی از تهدیدات مهم هر اتاق سرور است. رطوبت بالای هوا موجب می شود تا سخت افزارهایی چون پردازنده و درایوهای سرور دچار پوسیدگی شده که در نهایت نابودی آنها را به دنبال دارد. بنابراین بایستی مانع از به وجود آمدن رطوب در این اتاق ها شد زیرا ضرر بزرگی را به وجود خواهد آورد.

۴- افزایش دما

دما یکی از مهم های تهدید اتاق سرور استاندارد به شمار می رود. با افزایش درجه دما اتاق سرور، سخت افزار سرورها دچار اختلالی شده که ناشی از افزایش دما آنها بوده و بایستی با استفاده از سیستم خنک کننده این موضوع را حل کرد. با افزایش دما سرورها ممکن است در سخت افزار آن مشکلی ایجاد شده و داده ها پاک شوند.

۵- سرقت

برخی افراد برای ضربه زدن به شرکت یا سازمانی سعی می کنند با رجوع به بخش اتاق سرور آن که داده های مهمی را در بر می گیرد، به این اتاق آسیبی وارد کرده و اطلاعات را به سرقت ببرد. از این رو موجب شده تا داده های مهم نابود و سرور دچار اختلالی شود که سازمان یا شرکت موردنظر را با مشکل بزرگی رو به رو خواهد ساخت. بنابراین باید افراد و سیستم نظارتی برای این نوع اتاق ها به کار گرفته شود.

Simple Network Management Protocol (SNMP)

در بسیاری از شبکه های کامپیوتری نرم افزار های مانیتورینگ وجود دارند. با این نرم افزارها می توان به بررسی اطلاعات کامل و دقیق از تمامی بخش های شبکه پرداخت. تمامی این نرم افزارها با استفاده از پروتکل های مختلفی مثل NetFlow، ICMP، ARP و از همه مهم تر SNMP اقدام به اسکن و بررسی شبکه می کنند.

پروتکل SNMP یکی از پروتکل های لایه Application است که امکان نقل و انتقال اطلاعات مدیریتی را بین عناصر شبکه ایجاد می کند و در واقع قسمتی از پروتکل TCP/IP می باشد. این پروتکل به طور وسیعی برای مانیتورینگ و مدیریت اجزاء شبکه استفاده می شود.

بسیاری از وندورها، تجهیزات تولیدی خود را به پروتکل SNMP مجهز می کنند تا امکان نظارت بر عملکرد آنها به کمک نرم افزارهای مانیتورینگ فراهم شود. در حال حاضر سه نسخه از پروتکل SNMP وجود دارد، SNMPv1، SNMPv2 و SNMPv3 .

SNMPv1

امنیت این ورژن پروتکل SNMP بسیار پایین است.

هنگامی که ارسال جواب از سمت SNMP Agent به NMS در حال انتقال است، به راحتی میتوان جواب را تغییر داد.

در واقع این نسخه فقط community-based است.

SNMPv2

این ورژن پروتکل SNMP شامل سه نوع است که در مجموع امنیت بهتری از ورژن 1 دارد:

SNMPv2c نسخه ای از ورژن 2 است که فقط community-based است.

SNMPv2u نسخه ای از ورژن 2 است که فقط user-based است. یعنی می‌توانید جهت احراز هویت، نام کاربری تعریف کنید.

نکته : این ورژن مشکل امنیتی ورژن 1 را حل کرده است. در این ورژن می‌توانید به جای ارتباط Read-Write به Read-Only بهره ببرید تا دیتا ها توانایی تغییر نداشته باشند.

SNMPv3

این ورژن ایمن ترین کامل ترین همچنین پر دردسر ترین ورژن پروتکل SNMP است.

در SNMPv3 بسته ها کاملا Encrypt (رمزنگاری) می شوند. همچنین user-based است و NMS نیاز به رمزی برای احراز هویت دارد.

اجزای اصلی پروتکل SNMP

SNMP Manager

Managed Devices

SNMP Agent

Management Information Base (MIB)

SNMP Manager

یک SNMP Manager که با نام Network Management System (NMS) هم شناخته می شود، وظیفه برقراری ارتباط و تبادل اطلاعات با SNMP Agent های فعال در تجهیزات شبکه را بر عهده دارد. به زبان ساده تر، یک SNMP Managerکامپیوتری است که بر روی آن یک نرم افزار مانیتورینگ شبکه نصب شده است و وظیفه مانیتورینگ شبکه را بر عهده دارد.وظایف یک SNMP Manager به طور عمده عبارتند از:

ارسال پرس و جو به Agent ها

دریافت پاسخ از Agent ها

سِت کردن متغیر ها در Agent ها

دریافت پیغام های Trap از Agent ها

Managed Devices

منظور از Managed Device همه دستگاه های شبکه هستند که بر روی آنها SNMP Agent فعال شده باشد، مثل روتر ها، سوئیچ ها، سرورها و فایروال ها.

SNMP Agent

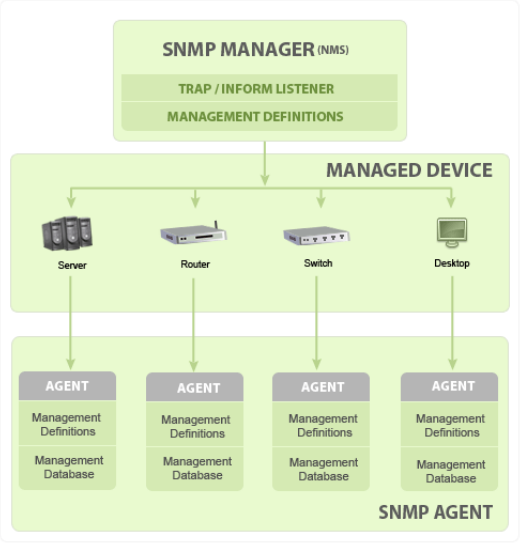
یک SNMP Agent در اصل برنامه ای است که بر روی تجهیزات شبکه کار گذاشته شده تا قابلیت SNMP را به آنها اضافه کند و وظیفه اصلی آن پاسخ دادن به درخواست های ارسال شده از طرف SNMP Manager است. وقتی SNMP Agentروی یک دستگاه فعال می شود، شروع به ثبت شاخص ها و اطلاعات دستگاه به صورت لوکال می کند و این اطلاعات را در دسترس NMS ها قرار می دهد.

این Agent ها می توانند استاندارد باشند مثل (Net-SNMP) یا مخصوص یک وندور باشند مثل (HP Insight Agent). به طور کلی وظایف یک SNMP Agent عبارتند از:

جمع آوری اطلاعات مدیریتی از دستگاهی که روی آن نصب شده است

نگه داری و فراخوانی اطلاعات مدیریتی بر اساس MIB مربوطه

ارسال سیگنال به NMS شبکه.



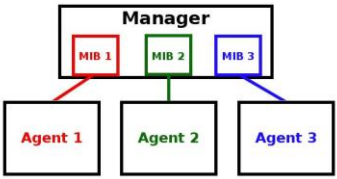
Management Information Base -MIB یا پایگاه داده اطلاعات مدیریتی

هر SNMP Agent دارای یک پایگاه داده برای معرفی و توصیف پارامتر های قابل نظارت و اندازه گیری است. به عبارتی SNMP Manager ها از این پایگاه داده جهت ارسال درخواست به Agent ها برای دریافت پارامتر های مورد نظر و همچنین تفسیر پاسخ ها مطابق با تعاریف صورت گرفته توسط وندور استفاده می کنند.

به زبان ساده، یک MIB یک پایگاه داده متنی است که فهرست پارامتر های قابل مانیتورینگ روی دستگاه را مشخص می کند و زبان مشترک بین Agent و Manager است، شاید بتوان گفت فایل های MIB مجموعه ای از سوالاتی است که یک NMS می تواند از دستگاه تحت مانیتورینگ بپرسد.

MIB

SNMP Agent شامل یک Database یا پایگاه است که به آن MIB یا Management Information Base می گویند.



تمامی اطلاعاتی یک دستگاه می‌تواند از خود به سمت NMS ارسال کند، به شکل یک Tree در آن قرار دارد .به هر یک از اطلاعاتی که در MIB قرار دارد OID یا Object identifier می گویند که شامل آدرس آن Tree می‌باشد. در نتیجه، تمامی اطلاعاتی که درون MIB وجود دارند، OID نام دارد. برای دریافت اطلاعات یک OID باید آدرس آن را به سمت SNMP Agent توسط پروتکل SNMP ارسال کنید.

انواع MIB ها در پروتکلSNMP

MIB ها به دو دسته Public و Private تقسیم می‌شوند.

MIBهای Public در تمام دستگاه ها قالب یکسانی دارند و پشتیبانی می‌شوند .مثل MIB های RFC1759 که برای تمامی پرینتر ها است و یا RFC1213 که اطلاعات شبکه ی دستگاه را می‌دهد که درون تمامی دستگاه ها وجود دارد.

MIBهای Private توسط کمپانی یا شرکت سازنده دستگاه ها ارائه می شوند و فقط در دستگاه های آن ها وجود دارد. مثل MIB ی CISCO-VTP-MIB که فقط درون دستگاه های سیسکو وجود دارد.

انواع درخواست های پروتکل SNMP

از NMS به SNMP Agent با استفاده از درخواست ها و فرمان های زیر می توان مقادیر MIB ها را دریافت کرد.

Get جهت دریافت دیتا یک OID خاص.

Get Next جهت دریافت دیتا یک آدرس بعد از آخرین آدرس GET شده.

Set برخی از OID ها در حالت Read-Write قرار دارند که از NMS میتوان مقدار آن OID را توسط این فرمان تغییر داد.

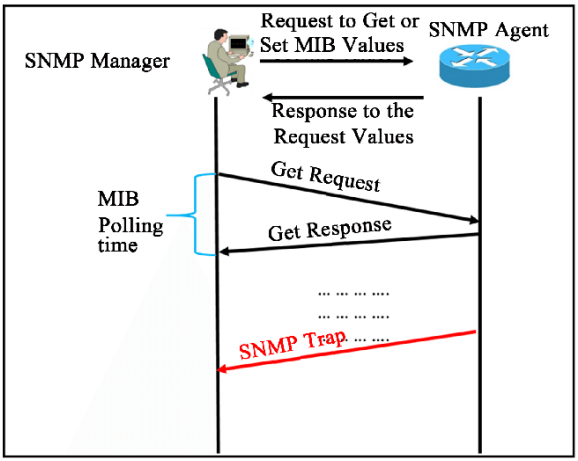
GetBulk جهت دریافت دیتا از جدولی که تعداد زیادی OID دارد که هر OID شامل چندین خروجی است.

Trap یک نوع Notification از وضعیت SNMP Agent برای NMS ها بدون .Acknowledge در ادامه اطلاعات بیشتری وجود دارد.

Inform همان Trap می باشد با این تفاوت که دارای Acknowledge است و می‌توانید از ارسال بسته اطمینان حاصل کنید.

SNMP Trap

یک سری دیتا مشخص شده می‌باشد که به صورت اعلان و به طور خودکار و بدون نیاز به ارسال درخواست، از SNMP Agent یا همان Managed Device برای NMS ارسال می‌شود.

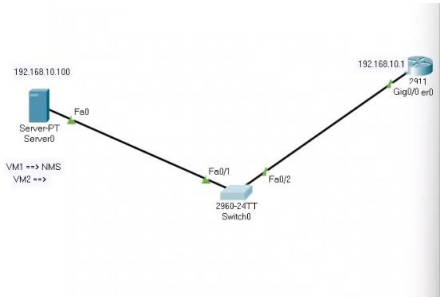


برای فعال سازی این ابزار باید آدرس NMS را به دستگاه بدهید تا بداند که دیتای Trap برای کی ارسال شود.

نکته :برای فعال سازی Trap در دستگاه ها و Managed Device ها باید SNMP فعال باشد.

Trap وضعیت روشن یا خاموش بودن Interface ها، خاموش یا روشن شدن دستگاه ها، مشکلات و وضعیت در لحظه تجهیزات و دستگاه ها را در لحظه به NMS ارسال می کند.

Time Setting Configuration



Server

IP: 192.168.10.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

Router(config)#int g 0/0

Router(config-if)#no sh

Router(config-if)#ip address 192.168.10.1 255.255.255.0

Router#show clock

Mon Mar 1 1993

Router#clock set 10:14:14 6 july 2023

```
Router(config)#clock timezone <TEH> <3 30>
Router#clock set 20:49:50 24 Sep 2015

Router#show clock
```

The following example specifies that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00. The **recurring** keyword indicates that the rules apply every year.

```
router(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

Network Time Protocol

Switch(config)#ntp server 192.168.10.100

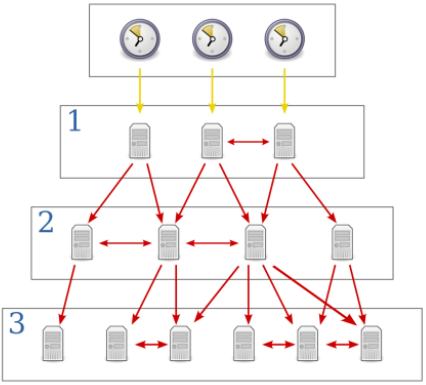
Switch(config)#int vlan 1

Switch(config-if)#no sh

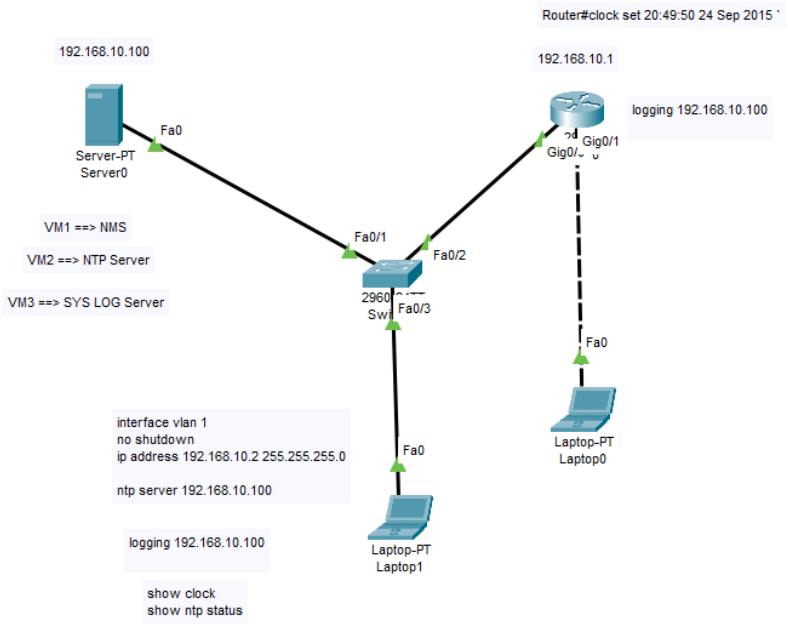
Switch(config-if)#ip address 192.168.10.2 255.255.255.0

```
Router(config)#ntp server <NTP IP ADDRESS> [prefer]

Router#show ntp status
Router#show ntp association
```

UDP 123



Syslog Server



روی سرور SYSLOG را ON می کنیم.

Router(config)#logging host 192.168.10.100

Logging Type

Keyword	Numeral	Description	
Emergency	0	System unusable	Severe
Alert	1	Immediate action required	
Critical	2	Critical Event (Highest of 3)	Impactful
Error	3	Error Event (Middle of 3)	
Warning	4	Warning Event (Lowest of 3)	
Notification	5	Normal, More Important	Normal
Informational	6	Normal, Less Important	
Debug	7	Requested by User Debug	Debug

Service	To Enable Logging	To Set Message Levels
Console	logging console	logging console *level-name* | *level-number*
Monitor	logging monitor	logging monitor *level-name* | *level-number*
Buffered	logging buffered	logging buffered *level-name* | *level-number*
Syslog	logging host *address* | *hostname*	logging trap *level-name* | *level-number*

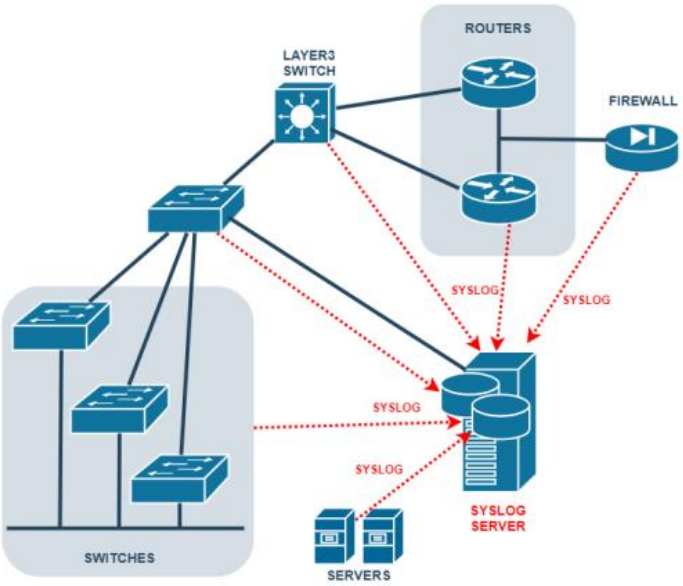
UDP 514

Log Message Format

*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down

Notice that by default on this particular device, we see the following:

A timestamp: *Dec 18 17:10:15.079
The facility on the router that generated the message: %LINEPROTO
The severity level: 5
A mnemonic for the message: UPDOWN
The description of the message: Line protocol on Interface FastEthernet0/0, changed state to down



Cisco Discovery Protocol (CDP)

سیسکو (Cisco Discovery Protocol (CDP را در سال 1994 معرفی کرد که یک مکانیزم برای مدیریت سیستم می باشد که بتواند به صورت خودکار در مورد دستگاه متصل به شبکه اطلاعات کسب کند. CDP روی دستگاه های سیسکو (روتر ، سوئیچ ، تلفن و ...) اجرا می شود. استفاده از CDP باعث می شود که دستگاه های شبکه به صورت دوره ای اطلاعات خود را به یک آدرس Multicast در شبکه ارسال کنند در نتیجه این امکان را برای سایر دستگاه ها یا نرم افزارها فراهم می کند که به اطلاعات ارسالی توسط این پروتکل دست پیدا کنند.به مرور زمان بهبودهایی در این پروتکل بوجود آمد تا قابلیت های آن افزایش یابد.

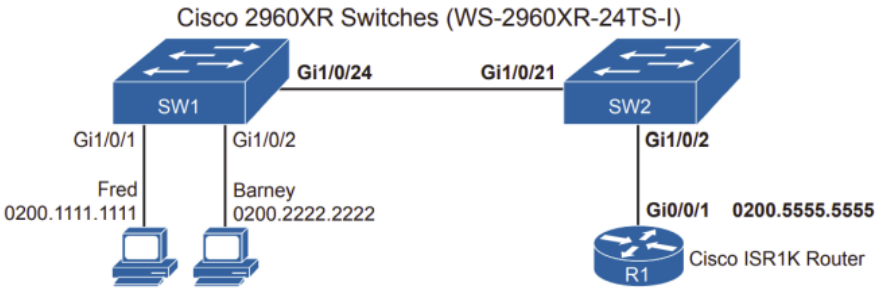
برنامه های کاربردهایی مانند Vocie به این پروتکل وابسته شدند تا بتوانند به درستی کار کنند این وابستگی باعث بروز مشکلاتی در ارتباط با سایر برندها شد. بنابراین برای ارتباط بین تجهیزات برندهای مختلف نیاز به یک پروتکل استاندارد احساس شد. پروتکل استانداردی که تعریف شد LLDP می باشد که به عنوان بخشی از 802.1 ABمی باشد که بصورت استاندارد قابلیت discovery را فراهم می کند. همچنین یک بهبود تحت عنوان Media Endpoint) Discovery (MEDبرای برنامه های Voice برای آن ارائه شد.

این پروتکل به صورت پیش فرض روی دستگاه ها فعال است و پیشنهاد می شود که CDP را روی پورت های غیرقابل اطمینان و پورت هایی که نیاز به این پروتکل ندارند غیر فعال شود .در لایه دو عمل می کند و می تواند اطلاعاتی مانند نوع دستگاه ، نسخه نرم افزار و سخت افزار ، اطلاعات IP و VLAN و ... را در اختیار مهاجم قرار دهد. در مثال زیر نحوی تنظیم و همچنین غیرفعال کردن CDP را به صورت global و به ازای اینترفیس نمایش داده است.

```
router(config)#no cdp run
router(config)#interface fastethernet 0/0
router(config-if)#no cdp enable
router#show cdp
```

علاوه برغیرغعال کردن CDP ، پیشنهاد می شود که LLDP را نیز در محلی که مورد نیاز نیست غیر فعال گردد. در مثال زیر نحوی غیر فعال کردن LLDP نمایش داده شده است.

```
router(config)#no lldp run
router#show lldp
```



```
SW2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW1              Gig 1/0/21        155              S I   WS-C2960X Gig 1/0/24
R1               Gig 1/0/2         131            R S I   C1111-8P  Gig 0/0/1

Total cdp entries displayed : 2
```

Command	Description
show cdp	States whether CDP is enabled globally and lists the default update and holdtime timers
show cdp interface [*type number*]	States whether CDP is enabled on each interface, or a single interface if the interface is listed, and states update and holdtime timers on those interfaces
show cdp traffic	Lists global statistics for the number of CDP advertisements sent and received

CDP (Cisco Discovery Protocol) is a Cisco proprietary protocol which has been in use on Cisco devices for many years. If CDP is enabled, a device will send out information about itself using the multicast MAC address 01-00-0c-cc-cc-cc

[no] cdp run	Global command that enables and disables (with the **no** option) CDP for the entire switch or router.
[no] cdp enable	Interface subcommand to enable and disable (with the **no** option) CDP for a particular interface.
cdp timer *seconds*	Global command that changes the CDP send timer (the frequency at which CDP sends messages).
cdp holdtime *seconds*	Global command that changes how long CDP waits since the last received message from a neighbor before believing the neighbor has failed, removing the neighbor's information from the CDP table.

LLDP (Link Layer Discovery Protocol) is a vendor-neutral standard defined by the IEEE in 802.1AB. It allows devices from different manufacturers to learn information about each other and behaves similarly to CDP. LLDP uses Ethernet frames and is usually sent to one of several multicast MAC addresses (01:80:c2:00:00:0e, 01:80:c2:00:00:03 or 01:80:c2:00:00:00) with the Ether type 0x88CC.

Command	Description
[no] lldp run	Global command to enable and disable (with the no option) LLDP for the entire switch or router.
[no] lldp transmit	Interface subcommand to enable and disable (with the no option) the transmission of LLDP messages on the interface.
[no] lldp receive	Interface subcommand to enable and disable (with the no option) the processing of received LLDP messages on the interface.
lldp timer *seconds*	Global command that changes the LLDP send timer (the frequency at which LLDP sends messages).
lldp holdtime *seconds*	Global command that changes how long LLDP waits since the last received message from a neighbor before believing the neighbor has failed, removing the neighbor's information from the LLDP table.

Password Recovery

ریکاوری پسورد روتر های سیسکو

پسورد روتر سیسکو یا همان کلمه عبور اولین لایه محافظت از روتر سیسکو در مقابل دسترسی های غیر مجاز است. گاها پیش آمده که نیاز به بازیابی کلمه عبور روتر سیسکو (ریست پسورد روتر سیسکو) داشته باشید برای مثال روتر سیسکو دست دوم خریداری کرده اید یا کلمه عبور روتر سیسکو فراموشتان شده.

مراحل بازیابی کلمه عبور روتر سیسکو بسیار آسان و سریع است مراحل کار بدین ترتیب است:

قدم اول: کابل کنسول را به روتر متصل کرده و نرم افزار putty را SecureCRT را باز کنید.

قدم دوم: روتر را خاموش و روشن کنید؛ پیش از decompress شدن IOS (حدودا 60 ثانیه اول روشن شدن روتر)، کلید Ctrl+PauseBreak یا Ctrl+Shift+C را بزنید تا وارد محیط Rommon شوید.

قدم سوم: دستور confreg 0x2142 را وارد کرده و با اجرای دستورreset ، روتر را دوباره راه اندازی کنید.

rommon 1>confreg 0x2142

rommon 2>reset

روتر ریبوت شده و فاقد تنظیمات بالا مي آید. حال وارد Enable Mode شده و دستور زیر را وارد کنید تا تنظیمات startup-config بر روی runnning-config کپی شود:

Router>enable

Router#copy startup-config running-config

نکته: توجه داشته باشید در صورتی که دستور را به صورت copy running-config startup-config وارد کنید، تمامی تنظیمات روتر پاک میشود.

پس از کپی شدن تنظیمات بر روی روتر، پسورد را تغییر دهید

Router(config)#enable password 1234

در مرحله آخر Config Register :را با استفاده از دستور زیر به حالت قبل برگردانید:

Router (config)#config-register 0x2102

Router #wr

نکته: تمامی اینترفیس های فیزیکی بعد از این عملیات به حالت administrative shut در خواهد آمد که نیاز به up کردن دستی خواهد داشت.

1 – To initiate the password recovery procedure, connect the rollover cable to the console port, then power the router off and back on. As soon as you receive a prompt showing the boot process, hit Ctrl-Break:

2 – Now, to skip our password-protected configuration, we instruct the router to by-pass the configuration located in NVRAM during bootup, and reset the router:

```
rommon 1 > confreg 0x2142     (by Def. 0x2102)
rommon 2 > reset
```

3 - The router will now reset and start its normal bootup process, however, the current configuration will be ignored. When the bootup is complete, you will be prompted to 'enter the initial configuration dialog', answer 'no':

```
Router> enable
Router# copy startup-config running-config
Destination filename [running-config]? (hit enter)

Router# configure terminal
Router(config)# enable password <>
Router(config)# enable secret <>
Router(config)# line console 0
Router(config-line)# password <>
Router(config)# username <> privilege 15 secret <>
```

4 – Lastly, we need to change the 'configuration register' so the router will load the newly modified configuration next time it reboots, save our settings and reboot the router

```
Router(config)# config-register 0x2102

Router(config)# exit
Router# copy running-config startup-config
Destination filename [startup-config]? (hit enter)
Router# reload
```

```
R1#show version | include register
Configuration register is 0x2102
```

The default value is 0x2102, what does this mean? Let's break it down:

Hexadecimal	2	1	0	2
Binary	0010	0001	0000	0010
Bit Number	15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0

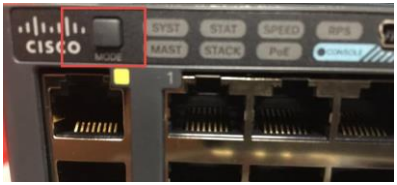
The 0x part means that we are looking at hexadecimal characters. 2102 is the default setting that tells the router to use a console speed of 9600 baud and to load the Cisco IOS image from flash memory.

- bit 13 tells the router to boot the default ROM software if network boot fails.
- bit 8 disables break.
- bit 1 tells the router to boot the first system image in onboard flash memory.

Bit 5, 11 and 12 are used to change the baud rate. If you don't touch these settings then the default will be 9600 baud.

ریکاوری پسورد سوئیچ سیسکو

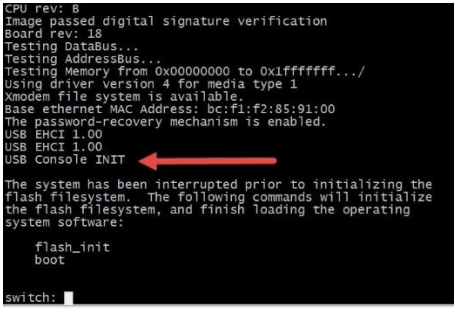
در برخی از موارد ممکن است پسورد ورود به کنسول سویچ سیسکو را فراموش کرده اید و یا شخص دیگری این پسورد را تعیین کرده و به او دسترسی ندارید. اگر به تنظیمات سوئیچ خود نیاز ندارید. در این شرایط یا باید کلید Mode سویچ را به مدت 15 ثانیه نگه دارید تا تمامی تنظیمات سویچ حذف شده و سویچ Factory reset شود یا سوئیچ عمالا به حالت کارخانه برگرد ولی اگر به تنظیمات سوئیچ نیاز دارید باید آن را password recovery کنید.



پسورد ریکاوری سویچ با روتر تفاوت دارد، برای پسورد ریکاوری سویچ مراحل زیر را انجام دهید:

1 .پورت کنسول را به سویچ متصل کرده و نرم افزار putty را SecureCRT را باز کنید.

2. سویچ را خاموش کرده، کلید Mode را بین 30 تا 40 ثانیه نگه داشته و سویچ را روشن کنید تا قبل از extract کردن IOS، وارد محیط ریکاوری شود. عبارت :switch بر روی کنسول مشاهده میکنید:



3. در این مرحله، سویچ هنوز Flash خود را detect نکرده است. با توجه به اینکه تنظیمات سویچ در Flash قرار دارد، با اجرای دستور زیر،flash را Detect خواهد کرد:

Switch: Flash_init

4 .پس از شناساییFlash ، محتویات آن را با اجرای دستور زیر مشاهده کنید:

Switch: dir flash:

```
switch: dir flash:
Directory of flash:/

2    -rwx  0         <date>              env_vars
3    -rwx  344       <date>              system_env_vars
4    -rwx  47        <date>              private-config.text
6    -rwx  8431      <date>              config.text
7                    <date>

10732544 bytes available (5266432 bytes used)
switch:
```

نکته: در صورتی که دستور no service password recovery بر روی سویچ اجرا شده باشد، پیغامی ظاهر میشود که password recovery غیرفعال شده و تنها راه Recoverکردن پسورد، حذف تمامی Config است.

5 .حال باید فایل Config.text را به نام دیگری Rename کنید، برای انجام این کار از دستور زیر استفاده کنید:

Switch: rename flash:config.text flash:config.old

Switch: boot

```
switch: rename flash:config.text flash:config.old
switch: boot
```

6.پس از Rename کردن فایلConfig ، با اجرای دستورreset ، سویچ را reboot کنید.

7. پس از بوت شدن سویچ، سویچ خام و فاقد تنظیمات میباشد، برای بازگرداندن تنظیمات، از دستورات زیر استفاده کنید، دستور اول نام فایل Config را به فرمت اصلی بر میگرداند و دستور دوم تنظیمات شما را که در فایل Config.txtقرار دارد به ممووری یا running-config منتقل می کند.

Switch# rename flash:config.old flash:config.text

Switch# copy flash:config.text system:running-config

8. پس از بازگرداندن تنظیمات، پسورد را تغییر داده و تنظیمات را ذخیره کنید.

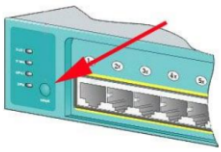
Step 1: Connect your PC or terminal into the switch console port with the blue console cable.

Step 2: Open up a Hyperterminal for emulation and set the speed to 9600 baud.

Step 3: Unplug the power cable to the switch.

Step 4: Press and hold the **MODE** button on the front of the switch and plug the power cable back into the switch at the same. After the power cable has been plugged in, wait a couple of seconds and then release the **MODE** button.

Step 5: Your display on your HyperTerminal should look like this… **switch:**



Step 6: Enter these commands into the switch
•switch: **flash _init**
•switch: **load_helper**
•switch: **dir flash:**

Directory of flash:
•13 drwx 192 Mar 01 1993 22:30:48 c2960-mz-124-0.0.53
•11 -rwx 5825 Mar 01 1993 22:31:59 config.text
•18 -rwx 720 Mar 01 1993 02:21:30 vlan.da

•switch: **rename flash:config.text flash:config.text.old**
•switch: **boot**

Step 7: Once the switch reboots, answer **NO** to "Would you like to enter system configuration dialog? [Yes/No]:

Step 8: Get into the privilege prompt.
•Switch**>enable**
•Switch**#rename flash:config.text.old flash:config.text**
•Switch**#copy flash:config.text system:running-config**
•Source filename [config.text]?
•Destination filename [running-config]?
•Press **Enter** to copy

Step 9: Get into global configuration
•Switch#conf t
•Switch (config)**#enable secret password**
•Enter the password you would like

Step 10: Return to Privilege mode and save your config
•Switch (config)**#exit**
•Switch**#copy run start**

IOS Upgrade / Downgrade

روترهای سیسکو هم مانند سیستم عامل هایی که استفاده می کنیم هر چند وقت یکبار باید بروز رسانی شوند و یا یک نسخه جدید از آنها روی روتر نصب شود. این فرآیند می تواند به دلایل مختلفی انجام شود برای مثال ممکن است شما سخت افزار یا ماژول جدیدی به روتر خود اضافه کنید و بر همین اساس IOS شما هم باید این ماژول را پشتیبانی کند و یا اینکه قابلیت جدیدی از نظر نرم افزاری به IOS ها اضافه شده است که شما با بروز رسانی به IOS جدید می توانید از این قابلیت جدید استفاده کنید و در نهایت اگر Bug ای در IOS های قدیمی وجود داشته است و در IOS جدید برطرف شده است.

شما می توانید با بروز رسانی به IOS جدید این Bug را برطرف کنید ، توجه کنید که IOS مثل ویندوز شما ممکن است بعد از مدت ها کارکرد دچار اختلال یه به اصطلاح فنی Corrupt شود و این بهترین گزینه است که بعد از چند وقت IOS خود را از اول نصب کنید. حتما به اندازه و ظرفیت حافظه Flash موجود روی روتر یا سویچ خود دقت کنید.

ممکن است اندازه حافظه Flash موجود روی روتر شما به اندازه ای نباشد که IOS جدید بتواند بر روی آن نصب شود بنابراین این مورد را حتما بررسی کنید. شما می توانید IOS خود را از طریق یک TFTP سرور موجود روی شبکه نصب و بروز رسانی کنید. نرم افزارهای رایگان زیادی وجود دارند که شما براحتی با استفاده از آنها می توانید یک TFTP سرور راه اندازی کنید .

دستورالعمل بروز رسانی IOS روترهای سیسکو با استفاده ازInternal Flash

با استفاده از تنظیمات پیشفرض یک ارتباط کنسولی با دستگاه برقرار کنید 9600 baud rate) ، 8 databit ، no flow control)

با استفاده از دستور Ping ارتباط بین روتر و TFTP سرور را آزمایش کنید. البته قبل از آن مطمئن شوید که Range آدرس IP شما با Range آدرس IP سرور TFTP یکسان باشد.

با توجه به اینکه فرآیند Upgrade در حافظه Flash انجام می شود و تنظیمات روتر در NVRAM ذخیره می شود ایندو چندان ارتباطی با هم ندارند اما بهتر است قبل از اینکه فرآیند Upgrade را انجام دهید از تنظیمات و پیکربندی های روتر خود Backup بگیرید. همچنین از IOS فعلی که بر روی روتر قرار دارد نیز یک Backup تهیه کنید تا زمانیکه در صورت احتمال IOS در زمان بروز رسانی دچار اختلال شد بتوانید از IOS قبلی استفاده کنید .

-با استفاده از دستور زیر فرآیند Upgrade را شروع کنید:

Router#copy tftp flash

حالاشمابه چیزی که در پایین مشاهده می کنید ، از شما آدرس IP سرور TFTP پرسیده خواهد شد:

Address or name of remote host []? XXX.XXX.XXX.XXX

بعد از وارد کردن آدرس TFTP سرور از شما نام فایل IOS ای که قرار است از TFTP کپی شود از شما مشابه پایین پرسیده می شود:

Source filename []? cXXXX-X-XX.XXX-XX.bin

به این نکته توجه کنید که اسم فایل IOS که می خواهید وارد کنید کاملا Case Sensitive است و باید دقت کنید که عین حروف را بدون کوچکترین تغییری وارد کنید.بعد از این مرحله از شما در خصوص نام فایلی که قرار است بر روی روتر مقصد قرار بگیرد سئوال خواهد شد ، همانطور که در پایین مشاهده می کنید:

Destination filename []? cXXXX-X-XX.XXX-XX.bin

پیشنهاد می شود که این فایل را نیز همانند همان فایلی نامگذاری کنید که در TFTP سرور قرار گرفته است تا به سادگی این فایل و فایلی که روی روتر قرار گرفته است را بتوانیم مقایسه کنیم. حالا همانطور که در پایین مشاهده می کنید از شما سئوال می شود که آیا می خواهید فایل های موجود در حافظه Flash حذف شود یا خیر ؟ اگر فضای خالی به اندازه کافی روی Flash دارید ، ترجیحا IOS قبلی را حذف نکنید ، ممکن است بعدا به آن نیاز پیدا کنید.

Erase flash: before copying? [confirm]

بعد از تایید روتر شروع به کپی کردن فایل Image مربوط به IOS از TFTP سرور به داخل روتر می شود و یا بر حسب انتخاب شما شروع به حذف و خالی کردن حافظه Flash می کند

```
Erasing the flash filesystem will remove all files! Continue? [confirm]y
Erasing device… eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeee …erased
Erase of flash: complete
Loading cXXXX-X-XX.XXX-XX.bin from XXX.XXX.XXX.XXX (via Ethernet0/0): !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - xxxxx/yyyyyyy bytes]

Verifying checksum…  OK (0xAC8A)
xxxxxx bytes copied in xx.xx secs (yyyy bytes/sec)
```

فرآیند کپی کردن IOS ممکن است چندین دقیقه بر حسب نوع شبکه ای که دارید زمان ببرد. در طی زمان کپی کردن پیام هایی نمایش داده می شود که نمایانگر فایل هایی است که به آنها دسترسی پیدا می شود. علامت تعجب یا ! به معنای این است که فرآیند کپی شدن در حال انجام است همانطور که در بالا مشاهده می کنید. هر کدام از علامت های تعجب به معنای کپی شدن 10 بسته اطلاعاتی یا Packet می باشد که با موفقیت کپی شده است. بعد از اینکه فرایند کپی به درستی انجام شد یک Checksum تایید یا Verification Checksum به داخل حافظه Flash روتر نوشته می شود.

قبل از اینکه روتر را Reload کنید بایستی از دو چیز مطمئن شوید.اولین نکته این است که باید مطمئن شوید که configuration register روتر شما مقدار 0×2102 است. برای بررسی این مورد کافیست دستور show version را وارد کنید. اگر configuration register شما مقدار 0×2102 را نمایش نمی دهد و هر چیزی به غیر از این است بایستی آن را بصورت دستی با استفاده از دستور زیر تبدیل به 0×2102 کنیم:

Router(config)#config-register 0×2102

دومین نکته ای که بایستی به آن توجه کنید البته زمانیکه به سیستم گفته اید که Flash را پاک نکند این است که روتر نباید از IOS قبلی بوت شود و شما باید به روتر بگویید از IOS قبلی استفاده نکند ، با استفاده از دستور اول زیر ، روتر شما از IOS قبلی سیستم دیگر استفاده نمی کند و با استفاده از دستور دوم روتر از IOS ای که برایش تعریف می کنید بوت خواهد شد:

```
Router(config)#no boot system
Router(config)#boot system flash cXXXX-X-XX.XXX-XX.bin
```

اگر دستور reload را در این مرحله وارد کنید روتر از شما می پرسد که آیا می خواهید تنظیمات را ذخیره کنم یا خیر ؟ در این مرحله شما باید بسیار دقت کنید و دلیلش هم این است که اگر روتر در boot mode قرار بگیرد ، روتر دیگر قادر به انجام عملیات routing نخواهد بود. بنابراین در این هنگام ترجیحا تمامی تنظیمات موجود در running configuration را بر روی startup configuration ذخیره کنید تا در زمان boot این تنظیمات از بین نرود. توجه کنید زمانی تنظیمات را ذخیره کنید که همه تنظیمات را می توانید در خروجی دستور show run مشاهده کنید. به هر حال تایید را با y انجام دهید و ادامه دهید.

```
Router#reload
System configuration has been modified. Save? [yes/no]: y
Building configuration…
[OK]
Proceed with reload? [confirm]y
```

برای اینکه مطمئن شوید Image جدید بصورت کامل در روتر Load شده است دستور show version را وارد کنید.

```
00:22:25: %SYS-5-CONFIG_I: Configured from console by console
Cisco Internetwork Operating System Software
IOS ™ CXXXX Software (CXXXX-X-X), Version XX.X(XX), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 25-Mar-02 20:33 by xxxxx
Image text-base: 0x80008088, data-base: 0x80828788

ROM: System Bootstrap, Version xx.x(x)XA4, RELEASE SOFTWARE (fc1)

XXXX uptime is 22 minutes
System returned to ROM by reload
System image file is “flash: cXXXX-X-XX.XXX-XX.bin “     <<< Check it here
```

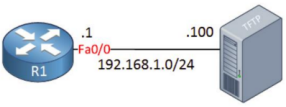
روتر شما به IOS جدید بروز رسانی شد

1 – Once you downloaded the IOS image, check if you have enough space left on your flash memory:

```
R1#show flash:
1     1119 Sep 29 2015 11:11:52 +00:00 r1-r2-r3.cfg
2     1184 Dec 3 2014 15:14:06 +00:00 R1-R2-ASA1-ASA2.cfg

3862364160 bytes available (137428992 bytes used)
```

2 – When we want to copy something to or from this router, we have to use the copy command:

```
R1#copy tftp: flash:
Address or name of remote host [ ]? 192.168.1.200
Source filename [ ]? c2800nm-adventerprisek9-mz.151-4.M12a.bin
Destination filename [c2800nm-adventerprisek9-mz.151-4.M12a.bin]?
```



3 - The transfer has completed, let's take a look at our flash memory:

```
R1#show flash: | include .bin
8     67926080 Apr 2 2015 14:21:46 +00:00 c2800nm-adventerprisek9-mz.151-4.M10.bin
25    67929600 Nov 4 2016 12:11:22 +00:00 c2800nm-adventerprisek9-mz.151-4.M12a.bin
```

4 – Most routers will select the first filename that they find on the flash memory so in our case, it means it would boot the older IOS image. We can change this with the boot system command:

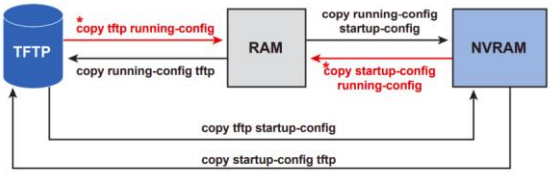
```
R1(config)#boot system flash:c2800nm-adventerprisek9-mz.151-4.M12a.bin
```

5 – Let's reload the router:

```
R1#reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
```

6 - Once the router has reloaded, verify that we are running the new IOS image:

```
R1#show version
```



1 - Traditional Configuration Backup and Restore with the copy Command

2 - Alternatives for Configuration Backup and Restore

2-1 – First we need to configure where we want to store our configuration archives. When you use the path command you can see what options we have:

```
Router(config)#archive
Router(config-archive)#path ?
  flash:  Write archive on flash: file system
  ftp:    Write archive on ftp: file system
  http:   Write archive on http: file system
  https:  Write archive on https: file system
  pram:   Write archive on pram: file system
  rcp:    Write archive on rcp: file system
  scp:    Write archive on scp: file system
  slot0:  Write archive on slot0: file system
  tftp:   Write archive on tftp: file system
```

2-2 – Normally an external location would be a good idea but to keep things simple I will use the flash memory of my router:

```
Router(config-archive)#path flash:router-backup
```

2-3 – I will also configure a schedule, for example to create a configuration archive each 24 hours:

```
Router(config-archive)#time-period 1440
```

BGP · PART 1

packetlife.net

Attributes

	Name	Description
Well-known Mandatory · Must be supported and propagated		
1	**Origin**	Origin type (IGP, EGP, or unknown)
2	**AS Path**	List of autonomous systems which the advertisement has traversed
3	**Next Hop**	External peer in neighboring AS
Well-known Discretionary · Must be supported; propagation optional		
5	**Local Preference**	Metric for internal neighbors to reach external destinations (default 100)
6	**Atomic Aggregate**	Includes ASes which have been dropped due to route aggregation
Optional Transitive · Marked as partial if unsupported by neighbor		
7	**Aggregator**	ID and AS of summarizing router
8	**Community**	Route tag
Optional Nontransitive · Deleted if unsupported by neighbor		
4	**Multiple Exit Discriminator (MED)**	Metric for external neighbors to reach the local AS (default 0)
9	**Originator ID**	The originator of a reflected route
10	**Cluster List**	List of cluster IDs
13	**Cluster ID**	Originating cluster
--	**Weight**	Cisco proprietary, not communicated to peers (default 0)

About BGP

Type	Path Vector
eBGP AD	20
iBGP AD	200
Standard	RFC 4271
Protocols	IP
Transport	TCP/179
Authentication	MD5

Terminology

Autonomous System (AS)
A logical domain under the control of a single entity

External BGP (eBGP)
BGP adjacencies which span autonomous system boundaries

Internal BGP (iBGP)
BGP adjacencies formed within a single AS

Synchronization Requirement
A route must be known by an IGP before it may be advertised to BGP peers

Packet Types

Open	**Update**
Keepalive	**Notification**

Path Selection

	Attribute	Description	Preference
1	**Weight**	Administrative preference	Highest
2	**Local Preference**	Communicated between peers within an AS	Highest
3	**Self-originated**	Prefer paths originated locally	True
4	**AS Path**	Minimize AS hops	Shortest
5	**Origin**	Prefer IGP-learned routes over EGP, and EGP over unknown	IGP
6	**MED**	Used externally to enter an AS	Lowest
7	**External**	Prefer eBGP routes over iBGP	eBGP
8	**IGP Cost**	Consider IGP metric	Lowest
9	**eBGP Peering**	Favor more stable routes	Oldest
10	**Router ID**	Tie breaker	Lowest

Neighbor States

Idle · Neighbor is not responding

Active · Attempting to connect

Connect · TCP session established

Open Sent · Open message sent

Open Confirm · Response received

Established · Adjacency established

Troubleshooting

```
show ip bgp [summary]
show ip bgp neighbors
show ip route [bgp]
clear ip bgp * [soft]
debug ip bgp […]
```

Influencing Path Selection

Weight	`neighbor 172.16.0.1 weight 200`	**Local Preference**	`bgp default local-preference 100`
MED	`default-metric 400`	**Route Map**	`neighbor 172.16.0.1 route-map Foo`
Ignore AS Path	`bgp bestpath as-path ignore`	**Ignore Cost Communities**	`bgp bestpath cost-community ignore`

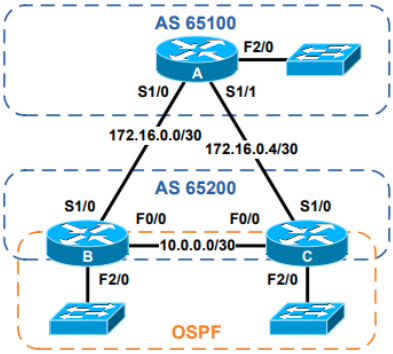
by Jeremy Stretch

v2.1-r1

BGP · PART 2

packetlife.net

Configuration Example



Router A

```
interface Serial1/0
 description Backbone to B
 ip address 172.16.0.1 255.255.255.252
!
interface Serial1/1
 description Backbone to C
 ip address 172.16.0.5 255.255.255.252
!
interface FastEthernet2/0
 description LAN
 ip address 192.168.1.1 255.255.255.0
!
router bgp 65100
 no synchronization
 network 172.16.0.0 mask 255.255.255.252
 network 172.16.0.4 mask 255.255.255.252
 network 192.168.1.0
 neighbor South peer-group
 neighbor South remote-as 65200
 neighbor 172.16.0.2 peer-group South
 neighbor 172.16.0.6 peer-group South
 no auto-summary
```

Router B

```
interface FastEthernet0/0
 description Backbone to C
 ip address 10.0.0.1 255.255.255.252
!
interface Serial1/0
 description Backbone to A
 ip address 172.16.0.2 255.255.255.252
!
interface FastEthernet2/0
 description LAN
 ip address 192.168.2.1 255.255.255.0
!
router ospf 100
 network 10.0.0.1 0.0.0.0 area 0
 network 192.168.2.1 0.0.0.0 area 1
!
router bgp 65200
 no synchronization
 redistribute ospf 100 route-map LAN_Subnets
 neighbor 10.0.0.2 remote-as 65200
 neighbor 172.16.0.1 remote-as 65100
 no auto-summary
!
access-list 10 permit 192.168.0.0 0.0.255.255
!
route-map LAN_Subnets permit 10
 match ip address 10
 set metric 100
```

Router C

```
interface FastEthernet0/0
 description Backbone to B
 ip address 10.0.0.2 255.255.255.252
!
interface Serial1/0
 description Backbone to A
 ip address 172.16.0.6 255.255.255.252
!
interface FastEthernet2/0
 description LAN
 ip address 192.168.3.1 255.255.255.0
!
router ospf 100
 network 10.0.0.2 0.0.0.0 area 0
 network 192.168.3.1 0.0.0.0 area 2
!
router bgp 65200
 no synchronization
 redistribute ospf 100 route-map LAN_Subnets
 neighbor 10.0.0.1 remote-as 65200
 neighbor 172.16.0.5 remote-as 65100
 no auto-summary
!
access-list 10 permit 192.168.0.0 0.0.255.255
!
route-map LAN_Subnets permit 10
 match ip address 10
 set metric 100
```

Router A Routing Table

```
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.0.4 is directly connected, S1/1
C       172.16.0.0 is directly connected, S1/0
C    192.168.1.0/24 is directly connected, F2/0
B    192.168.2.0/24 [20/100] via 172.16.0.2
B    192.168.3.0/24 [20/100] via 172.16.0.2
```

Router B Routing Table

```
     172.16.0.0/30 is subnetted, 2 subnets
B       172.16.0.4 [20/0] via 172.16.0.1
C       172.16.0.0 is directly connected, S1/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, F0/0
B    192.168.1.0/24 [20/0] via 172.16.0.1
C    192.168.2.0/24 is directly connected, F2/0
O IA 192.168.3.0/24 [110/2] via 10.0.0.2, F0/0
```

by Jeremy Stretch

v2.1-r1

Cisco IOS Versions

packetlife.net

IOS Nomenclature

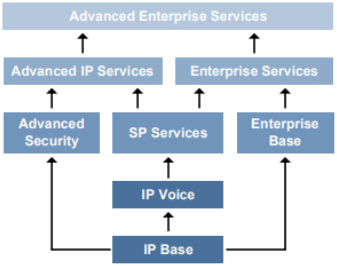
Mainline 12.4(7a)
- Maintenance Release
- Individual Release
- Numbered Version

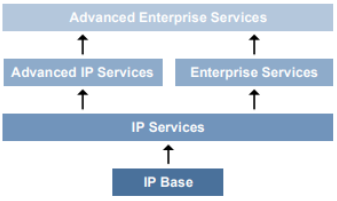
T Train 12.4(9)T1
- Maintenance Release
- Individual Release
- New Feature Identifier
- Numbered Version

S Train 12.2(25)SEB4
- Release
- Individual Release
- Numbered Version

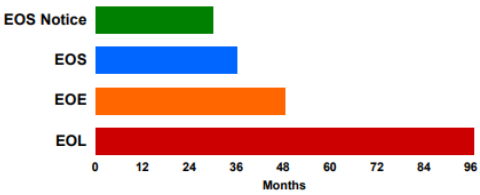
IOS XR 3.2.1
- Major Release
- Minor Release
- Maintenance Release

IOS Package Trees





Release Lifecycle



First Customer Shipment (FCS)
The release is made available to Cisco customers on CCO

EOS Notice
Notification of upcoming EOS

End of Sale (EOS)
The release is no longer orderable or included in manufactured shipments

End of Engineering (EOE)
The last day for software fixes; only TAC assistance is offered from this point

End of Life (EOL)
The last day for TAC support; release becomes obsolete; upgrade is only option for continued support

IOS Filename

c3725-entbase-mz.124-6.T.bin
- Hardware
- Feature Set
- Memory Location
- Compression Format
- Maintenance Release
- Individual Release
- T Designator

Deployment Classifications

Early Deployment (ED)
Offers new feature, platform, or interface support

General Deployment (GD)
A major release considered qualified for deployment on critical devices

Limited Deployment (LD)
A major release prior to reaching its GD milestone

Deferred (DF)
Known defective images; should not be installed

IOS Version Verification

```
show version
dir <filesystem>:
verify <filesystem>:<image>
```

by Jeremy Stretch v2.0

COMMON PORTS

packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

by Jeremy Stretch

v1.1

EIGRP

packetlife.net

Protocol Header

8	16	24	32
Version	Opcode	Checksum	
Flags			
Sequence Number			
Acknowledgment Number			
Autonomous System Number			
Type	Length		
Value			

Metric Formula

$$256 * (K_1 * \mathbf{bw} + \frac{K_2 * \mathbf{bw}}{256 - \mathbf{load}} + K_3 * \mathbf{delay}) * \frac{K_5}{\mathbf{rel} + K_4}$$

- **bw** = 10^7 / minimum path bandwidth in kbps
- **delay** = interface delay in µsecs / 10

EIGRP Configuration

Protocol Configuration

```
! Enable EIGRP
router eigrp <ASN>

 ! Add networks to advertise
 network <IP address> <wildcard mask>

 ! Configure K values to manipulate metric formula
 metric weights 0 <k1> <k2> <k3> <k4> <k5>

 ! Disable automatic route summarization
 no auto-summary

 ! Designate passive interfaces
 passive-interface (<interface> | default)

 ! Enable stub routing
 eigrp stub [receive-only | connected | static | summary]

 ! Statically identify neighoring routers
 neighbor <IP address> <interface>
```

Interface Configuration

```
! Set maximum bandwidth EIGRP can consume
ip bandwidth-percent eigrp <AS> <percentage>

! Configure manual summarization of outbound routes
ip summary-address eigrp <AS> <IP address> <mask> [<AD>]

! Enable MD5 authentication
ip authentication mode eigrp <AS> md5
ip authentication key-chain eigrp <AS> <key-chain>

! Configure hello and hold timers
ip hello-interval eigrp <AS> <seconds>
ip hold-time eigrp <AS> <seconds>

! Disable split horizon for EIGRP
no ip split-horizon eigrp <AS>
```

Attributes

Type	Distance Vector
Algorithm	DUAL
Internal AD	90
External AD	170
Summary AD	5
Standard	Cisco proprietary
Protocols	IP, IPX, Appletalk
Transport	IP/88
Authentication	MD5
Multicast IP	224.0.0.10
Hello Timers	5/60
Hold Timers	15/180

K Defaults	
K_1	1
K_2	0
K_3	1
K_4	0
K_5	0

Packet Types	
1	Update
3	Query
4	Reply
5	Hello
8	Acknowledge

Terminology

Reported Distance
The metric for a route advertised by a neighbor

Feasible Distance
The distance advertised by a neighbor plus the cost to get to that neighbor

Stuck In Active (SIA)
The condition when a route becomes unreachable and not all queries for it are answered; adjacencies with unresponsive neighbors are reset

Passive Interface
An interface which does not participate in EIGRP but whose network is advertised

Stub Router
A router which advertises only a subset of routes, and is omitted from the route query process

Troubleshooting

```
show ip eigrp interfaces
show ip eigrp neighbors
show ip eigrp topology
show ip eigrp traffic
clear ip eigrp neighbors
debug ip eigrp [packet | neighbors]
```

by Jeremy Stretch v2.1

First Hop Redundancy

packetlife.net

Protocols

Hot Standby Router Protocol (HSRP)
Provides default gateway redundancy using one active and one standby router; standardized but licensed by Cisco Systems

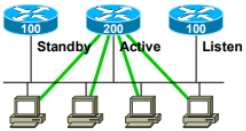
Virtual Router Redundancy Protocol (VRRP)
An open-standard alternative to Cisco's HSRP, providing the same functionality

Gateway Load Balancing Protocol (GLBP)
Supports arbitrary load balancing in addition to redundancy across gateways; Cisco proprietary

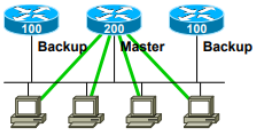
Attributes

	HSRP	VRRP	GLBP
Standard	RFC 2281	RFC 3768	Cisco
Load Balancing	No	No	Yes
IPv6 Support	Yes	No	Yes
Transport	UDP/1985	IP/112	UDP/3222
Default Priority	100	100	100
Default Hello	3 sec	1 sec	3 sec
Multicast Group	224.0.0.2	224.0.0.18	224.0.0.102

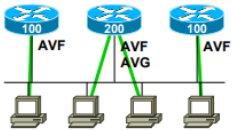
HSRP



VRRP



GLBP



HSRP Configuration

```
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 standby version {1 | 2}
 standby 1 ip 10.0.1.1
 standby 1 timers <hello> <dead>
 standby 1 priority <priority>
 standby 1 preempt
 standby 1 authentication md5 key-string <password>
 standby 1 track <interface> <value>
 standby 1 track <object> decrement <value>
```

VRRP Configuration

```
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 vrrp 1 ip 10.0.1.1
 vrrp 1 timers {advertise <hello> | learn}
 vrrp 1 priority <priority>
 vrrp 1 preempt
 vrrp 1 authentication md5 key-string <password>
 vrrp 1 track <object> decrement <value>
```

GLBP Configuration

```
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 glbp 1 ip 10.0.1.1
 glbp 1 timers <hello> <dead>
 glbp 1 timers redirect <redirect> <time-out>
 glbp 1 priority <priority>
 glbp 1 preempt
 glbp 1 forwarder preempt
 glbp 1 authentication md5 key-string <password>
 glbp 1 load-balancing <method>
 glbp 1 weighting <weight> lower <lower> upper <upper>
 glbp 1 weighting track <object> decrement <value>
```

HSRP/GLBP Interface States

Speak · Gateway election in progress

Active · Active router/VG

Standby · Backup router/VG

Listen · Not the active router/VG

VRRP Interface States

Master · Acting as the virtual router

Backup · All non-master routers

GLBP Roles

Active Virtual Gateway (AVG)
Answers for the virtual router and assigns virtual MAC addresses to group members

Active Virtual Forwarder (AVF)
All routers which forward traffic for the group

GLBP Load Balancing

Round-Robin (default)
The AVG answers host ARP requests for the virtual router with the next router in the cycle

Host-Dependent
Round-robin cycling is used while a consistent AVF is maintained for each host

Weighted
Determines the proportionate share of hosts handled by each AVF

Troubleshooting

```
show standby [brief]   show vrrp [brief]
show glbp [brief]      show track [brief]
```

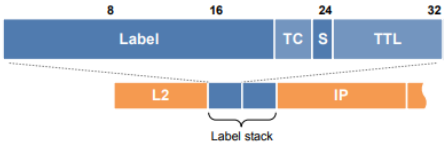
by Jeremy Stretch

v2.0

FRAME MODE MPLS

packetlife.net

Protocol Header



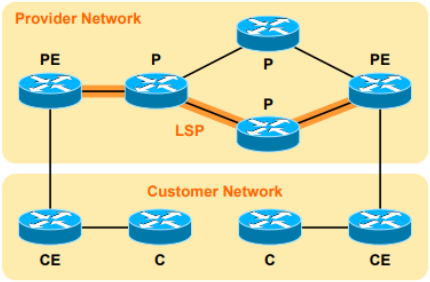
Label (20 bits) · Unique label value

Traffic Class (3 bits) · CoS-mapped QoS marking

Bottom of Stack (1 bit) · Indicates label is last in the stack

Time To Live (8 bits) · Hop counter mapped from IP TTL

Label Switched Path



Customer (C) · IP-only routers internal to customer network

Customer Edge (CE) · C routers which face PE routers

Provider Edge (PE) · LSRs on the MPLS-IP boundary

Provider (P) · MPLS-only LSRs in provider network

MPLS Configuration

```
! Enable CEF
ip cef

! Select label protocol
mpls label protocol ldp

! Enable MPLS on IP interfaces
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 mpls ip
 ! Raise MPLS MTU to accommodate multilabel stack
 mpls mtu 1512
```

Conceptual Components

Control Plane
Facilitates label exchange between neighboring LSRs using LDP or TDP (includes the LIB)

Forwarding/Data Plane
Forwards packets based on label or destination IP address (includes the FIB and LFIB)

Label Protocols

	LDP	TDP
Hello Address	224.0.0.2	255.255.255.255
Hello Port	UDP/646	UDP/711
Adjacency Port	TCP/646	TCP/711
Proprietary	No	Cisco

Terminology

Label Distribution Protocol (LDP)
Standards-based label distribution protocol defined in RFC 3036

Tag Distribution Protocol (TDP)
Cisco's proprietary predecessor to LDP

Label Switching Router (LSR)
Any router performing label switching (MPLS)

Label-Switched Path (LSP)
The unidirectional path through one or more LSRs taken by a label-switched packet belonging to an FEC

Forwarding Equivalence Class (FEC)
A group of packets which are forwarded in an identical manner, typically by destination prefix and/or traffic class

Label Information Base (LIB)
Contains all labels learned by an LSR via a label distribution protocol

Forwarding Information Base (FIB)
Routing database for unlabeled (IP) packets

Label FIB (LFIB)
Routing database for labeled (MPLS) packets

Interim Packet Propagation
An LSR temporarily falls back to IP routing while waiting to learn the necessary MPLS label(s)

Penultimate Hop Popping (PHP)
The second-to-last LSR in an LSP removes the MPLS label so the last LSR only has to perform an IP lookup

Troubleshooting

`show mpls interfaces`	`show mpls ldp bindings [detail]` (LIB)	`show ip cef [detail]` (FIB)
`show mpls ldp neighbors`	`show mpls forwarding-table [detail]` (LFIB)	`debug mpls […]`

by Jeremy Stretch v2.0

IEEE 802.1X

packetlife.net

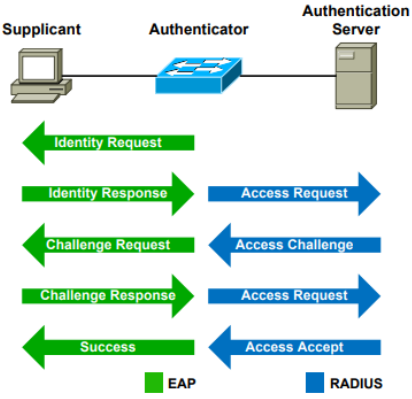
802.1X Header

1	1	2	
Version	Type	Length	EAP

EAP Header

1	1	2	
Code	Identifier	Length	Data

EAP Flow Chart



Configuration

Global Configuration

```
! Define a RADIUS server
radius-server host 10.0.0.100
radius-server key MyRadiusKey
! Configure 802.1X to authenticate via AAA
aaa new-model
aaa authentication dot1x default group radius
! Enable 802.1X authentication globally
dot1x system-auth-control
```

Interface Configuration

```
! Static access mode
switchport mode access
! Enable 802.1X authentication per port
dot1x port-control auto
! Configure host mode (single or multi)
dot1x host-mode single-host
! Configure maximum authentication attempts
dot1x max-reauth-req
! Enable periodic reauthentication
dot1x reauthentication
! Configure a guest VLAN
dot1x guest-vlan 123
! Configure a restricted VLAN
dot1x auth-fail vlan 456
dot1x auth-fail max-attempts 3
```

Terminology

Extensible Authentication Protocol (EAP)
A flexible authentication framework defined in RFC 3748

EAP Over LANs (EAPOL)
EAP encapsulated by 802.1X for transport across LANs

Supplicant
The device (client) attached to an access link that requests authentication by the authenticator

Authenticator
The device that controls the status of a link; typically a wired switch or wireless access point

Authentication Server
A backend server which authenticates the credentials provided by supplicants (for example, a RADIUS server)

Guest VLAN
Fallback VLAN for clients not 802.1X-capable

Restricted VLAN
Fallback VLAN for clients which fail authentication

802.1X Packet Types

0	EAP Packet
1	EAPOL-Start
2	EAPOL-Logoff
3	EAPOL-Key
4	EAPOL-Encap-ASF-Alert

EAP Codes

1	Request
2	Response
3	Success
4	Failure

Interface Defaults

Max Auth Requests	2
Reauthentication	Off
Quiet Period	60s
Reauth Period	1hr
Server Timeout	30s
Supplicant Timeout	30s
Tx Period	30s

EAP Req/Resp Types

1	Identity
2	Notification
3	Nak
4	MD5 Challenge
5	One Time Password
6	Generic Token Card
254	Expanded Types
255	Experimental

Port-Control Options

force-authorized
Port will always remain in authorized state (default)

force-unauthorized
Always unauthorized; authentication attempts are ignored

auto
Supplicants must authenticate to gain access

Troubleshooting

```
show dot1x [statistics] [interface <interface>]
dot1x test eapol-capable [interface <interface>]
dot1x re-authenticate interface <interface>
```

by Jeremy Stretch

v2.0

IEEE 802.11 WLAN · PART 1

packetlife.net

IEEE Standards

	802.11a	802.11b	802.11g	802.11n
Maximum Throughput	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz
Modulation	OFDM	DSSS	DSSS/OFDM	OFDM
Channels (FCC/ETSI)	21/19	11/13	11/13	32/32
Ratified	1999	1999	2003	2009

WLAN Types

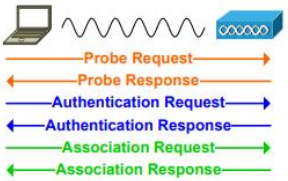
Ad Hoc
A WLAN between isolated stations with no central point of control; an IBSS

Infrastructure
A WLAN attached to a wired network via an access point; a BSS or ESS

Frame Types

Type	Class
Association	Management
Authentication	Management
Probe	Management
Beacon	Management
Request to Send (RTS)	Control
Clear to Send (CTS)	Control
Acknowledgment (ACK)	Control
Data	Data

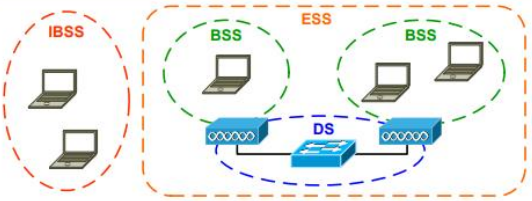
Client Association



Modulations

Scheme	Modulation	Throughput
DSSS	DBPSK	1 Mbps
	DQPSK	2 Mbps
	CCK	5.5/11 Mbps
OFDM	BPSK	6/9 Mbps
	QPSK	12/18 Mbps
	16-QAM	24/36 Mbps
	64-QAM	48/54 Mbps

WLAN Components



Basic Service Area (BSA)
The physical area covered by the wireless signal of a BSS

Basic Service Set (BSS)
A set of stations and/or access points which can directly communicate via a wireless medium

Distribution System (DS)
The wired infrastructure connecting multiple BSSs to form an ESS

Extended Service Set (ESS)
A set of multiple BSSs connected by a DS which appear to wireless stations as a single BSS

Independent BSS (IBSS)
An isolated BSS with no connection to a DS; an *ad hoc* WLAN

Measuring RF Signal Strength

Decibel (dB)
An expression of signal strength as compared to a reference signal; calculated as $10\log_{10}$(signal/reference)

dBm · Signal strength compared to a 1 milliwatt signal

dBw · Signal strength compared to a 1 watt signal

dBi · Compares forward antenna gain to that of an isotropic antenna

Terminology

Basic Service Set Identifier (BSSID)
A MAC address which serves to uniquely identify a BSS

Service Set Identifier (SSID)
A human-friendly text string which identifies a BSS; 1-32 characters

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
The mechanism which facilitates efficient communication across a shared wireless medium (provided by DCF or PCF)

Effective Isotropic Radiated Power (EIRP)
Net signal strength (transmitter power + antenna gain - cable loss)

by Jeremy Stretch v2.2

IEEE 802.11 WLAN · PART 2

packetlife.net

Distributed Coordination Function (DCF)

Interframe Spacing

Short IFS (SIFS)
Used to provide minimal spacing delay between control frames or data fragments

DCF IFS (DIFS)
Normal spacing enforced under DCF for management and non-fragment data frames

Arbitrated IFS (AIFS)
Variable spacing calculated to accommodate differing qualities of service (QoS)

Extended IFS (EIFS)
Extended delay imposed after errors are detected in a received frame

Encryption Schemes

Wired Equivalent Privacy (WEP)
Flawed RC4 implementation using a 40- or 104-bit pre-shared encryption key (deprecated)

Wi-Fi Protected Access (WPA)
Implements the improved RC4-based encryption Temporal Key Integrity Protocol (TKIP) which can operate on WEP-capable hardware

IEEE 802.11i (WPA2)
IEEE standard developed to replace WPA; requires a new generation of hardware to implement significantly stronger AES-based CCMP encryption

Quality of Service Markings

WMM	802.11e	802.1p
Platinum	7/6	6/5
Gold	5/4	4/3
Silver	3/0	0
Bronze	2/1	2/1

Wi-Fi Multimedia (WMM)
A Wi-Fi Alliance certification for QoS; a subset of 802.11e QoS

IEEE 802.11e
Official IEEE WLAN QoS standard ratified in 2005; replaces WMM

IEEE 802.1p
QoS markings in the 802.1Q header on wired Ethernet

Client Authentication

Open · No authentication is used

Pre-shared Encryption Keys
Keys are manually distributed among clients and APs

Lightweight EAP (LEAP)
Cisco-proprietary EAP method introduced to provide dynamic keying for WEP (deprecated)

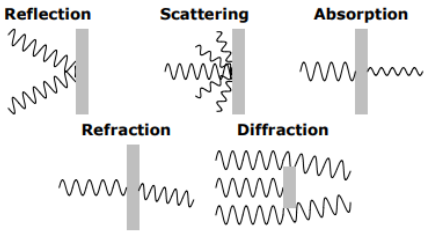
EAP-TLS
Employs Transport Layer Security (TLS); PKI certificates are required on the AP and clients

EAP-TTLS
Clients authenticate the AP via PKI, then form a secure tunnel inside which the client authentication takes place (clients do not need PKI certificates)

Protected EAP (PEAP)
A proposal by Cisco, Microsoft, and RSA which employs a secure tunnel for client authentication like EAP-TTLS

EAP-FAST
Developed by Cisco to replace LEAP; establishes a secure tunnel using a Protected Access Credential (PAC) in the absence of PKI certificates

RF Signal Interference



Antenna Types

Directional · Radiates power in one focused direction

Omnidirectional
Radiates power uniformly across a plane

Isotropic
A theoretical antenna referenced when measuring effective radiated power

by Jeremy Stretch

v2.2

IOS IPv4 Access Lists

packetlife.net

Standard ACL Syntax

```
! Legacy syntax
access-list <number> {permit | deny} <source> [log]

! Modern syntax
ip access-list standard {<number> | <name>}
 [<sequence>] {permit | deny} <source> [log]
```

Actions

permit	Allow matched packets
deny	Deny matched packets
remark	Record a configuration comment
evaluate	Evaluate a reflexive ACL

Extended ACL Syntax

```
! Legacy syntax
access-list <number> {permit | deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]

! Modern syntax
ip access-list extended {<number> | <name>}
 [<sequence>] {permit | deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]
```

ACL Numbers

1-99 **1300-1999**	IP standard
100-199 **2000-2699**	IP extended
200-299	Protocol
300-399	DECnet
400-499	XNS
500-599	Extended XNS
600-699	Appletalk
700-799	Ethernet MAC
800-899	IPX standard
900-999	IPX extended
1000-1099	IPX SAP
1100-1199	MAC extended
1200-1299	IPX summary

TCP Options

ack	Match ACK flag
fin	Match FIN flag
psh	Match PSH flag
rst	Match RST flag
syn	Match SYN flag
urg	Match URG flag
established	Match packets in an established session

Logging Options

log	Log ACL entry matches
log-input	Log matches including ingress interface and source MAC address

Source/Destination Definitions

any	Any address
host <address>	A single address
<network> <mask>	Any address matched by the wildcard mask

IP Options

dscp <DSCP>	Match the specified IP DSCP
fragments	Check non-initial fragments
option <option>	Match the specified IP option
precedence {0-7}	Match the specified IP precedence
ttl <count>	Match the specified IP time to live (TTL)

TCP/UDP Port Definitions

eq <port>	Equal to	**neq <port>**	Not equal to
lt <port>	Less than	**gt <port>**	Greater than
range <port> <port>	Matches a range of port numbers		

Miscellaneous Options

reflect <name>	Create a reflexive ACL entry
time-range <name>	Enable rule only during the given time range

Applying ACLs to Restrict Traffic

```
interface FastEthernet0/0
 ip access-group {<number> | <name>} {in | out}
```

Troubleshooting

```
show access-lists [<number> | <name>]
show ip access-lists [<number> | <name>]
show ip access-lists interface <interface>
show ip access-lists dynamic
show ip interface [<interface>]
show time-range [<name>]
```

by Jeremy Stretch v2.0

IOS ZONE-BASED FIREWALL

packetlife.net

Terminology

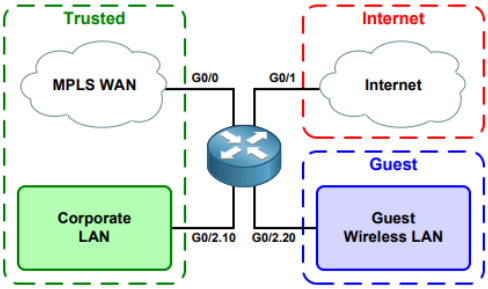
Security Zone
A group of interfaces which share a common level of security

Zone Pair
A unidirectional pairing of source and destination zones to which a security policy is applied

Inspection Policy
An inspect-type policy map used to statefully filter traffic by matching one or more inspect-type class maps

Parameter Map
An optional configuration of protocol-specific parameters referenced by an inspection policy

Security Zones




```
! Defining security zones
zone security Trusted
zone security Guest
zone security Internet

! Assigning interfaces to security zones
interface GigabitEthernet0/0
 zone-member security Trusted
!
interface GigabitEthernet0/1
 zone-member security Internet
!
interface GigabitEthernet0/2.10
 zone-member security Trusted
!
interface GigabitEthernet0/2.20
 zone-member security Guest
```

Inspection Class Configuration

```
! Match by protocol
class-map type inspect match-any ByProtocol
 match protocol tcp
 match protocol udp
 match protocol icmp

! Match by access list
ip access-list extended MyACL
 permit ip 10.0.0.0 255.255.0.0 any
!
class-map type inspect match-all ByAccessList
 match access-group name MyACL
```

Parameter Map Configuration

```
parameter-map type inspect MyParameterMap
 alert on
 audit-trail off
 dns-timeout 5
 max-incomplete low 20000
 max-incomplete high 25000
 icmp idle-time 3
 tcp synwait-time 3
```

Inspection Policy Actions

Drop	Traffic is prevented from passing
Pass	Traffic is permitted to pass without stateful inspection
Inspect	Traffic is subjected to stateful inspection; legitimate return traffic is permitted in the opposite direction

Inspection Policy Configuration

```
policy-map type inspect MyInspectionPolicy
 ! Pass permitted stateless traffic
 class VPN-Tunnel
  pass
 ! Inspect permitted stateful traffic
 class Allowed-Traffic1
  inspect
 ! Stateful inspection with a parameter map
 class Allowed-Traffic2
  inspect MyParameterMap
 ! Drop and log unpermitted traffic
 class class-default
  drop log
```

Zone Pair Configuration

```
! Service policies are applied to zone pairs
zone-pair security T2I source Trusted destination Internet
 service-policy type inspect Trusted2Internet

zone-pair security G2I source Guest destination Internet
 service-policy type inspect Guest2Internet

zone-pair security I2T source Internet destination Trusted
 service-policy type inspect Internet2Trusted
```

Troubleshooting

```
show zone security
show zone-pair security
show policy-map type inspect
show class-map type inspect
show parameter-map type inspect
debug zone security events
```

by Jeremy Stretch

v1.0

IPSEC

packetlife.net

Protocols

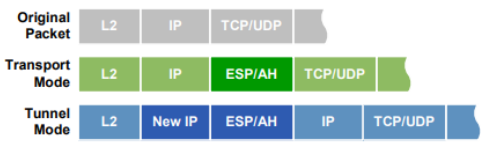
Internet Security Association and Key Management Protocol (ISAKMP)
A framework for the negotiation and management of security associations between peers (traverses UDP/500)

Internet Key Exchange (IKE)
Responsible for key agreement using asymmetric cryptography

Encapsulating Security Payload (ESP)
Provides data encryption, data integrity, and peer authentication; IP protocol 50

Authentication Header (AH)
Provides data integrity and peer authentication, but not data encryption; IP protocol 51

IPsec Modes



Transport Mode
The ESP or AH header is inserted behind the IP header; the IP header can be authenticated but not encrypted

Tunnel Mode
A new IP header is created in place of the original; this allows for encryption of the entire original packet

Configuration

ISAKMP Policy

```
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 2
 lifetime 3600
```

ISAKMP Pre-Shared Key

```
crypto isakmp key 1 MySecretKey address 10.0.0.2
```

IPsec Transform Set

```
crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac
 mode tunnel
```

IPsec Profile

```
crypto ipsec profile MyProfile
 set transform-set MyTS
```

Virtual Tunnel Interface

```
interface Tunnel0
 ip address 172.16.0.1 255.255.255.252
 tunnel source 10.0.0.1
 tunnel destination 10.0.0.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile MyProfile
```

Encryption Algorithms

	Type	Key Length (Bits)	Strength
DES	Symmetric	56	Weak
3DES	Symmetric	168	Medium
AES	Symmetric	128/192/256	Strong
RSA	Asymmetric	1024+	Strong

Hashing Algorithms

	Length (Bits)	Strength
MD5	128	Medium
SHA-1	160	Strong

IKE Phases

Phase 1
A bidirectional ISAKMP SA is established between peers to provide a secure management channel (IKE in main or aggressive mode)

Phase 1.5 (optional)
Xauth can optionally be implemented to enforce user authentication

Phase 2
Two unidirectional IPsec SAs are established for data transfer using separate keys (IKE quick mode)

Terminology

Data Integrity
Secure hashing (HMAC) is used to ensure data has not been altered in transit

Data Confidentiality
Encryption is used to ensure data cannot be intercepted by a third party

Data Origin Authentication
Authentication of the SA peer

Anti-replay
Sequence numbers are used to detect and discard duplicate packets

Hash Message Authentication Code (HMAC)
A hash of the data and secret key used to provide message authenticity

Diffie-Hellman Exchange
A shared secret key is established over an insecure path using public and private keys

Troubleshooting

```
show crypto isakmp sa
show crypto isakmp policy
show crypto ipsec sa
show crypto ipsec transform-set
debug crypto {isakmp | ipsec}
```

by Jeremy Stretch

v2.0

IPv4 Multicast

packetlife.net

Layer 2 Addressing

239.142.57.6

11101111 10001110 00111001 00000110

01-00-5E-0E-39-06

00000001 00000000 01011110 00001110 00111001 00000110

Terminology

Reverse Path Forwarding (RPF)
Verifies that multicast traffic travels in the reverse direction of unicast traffic, away from the tree root

Cisco Group Management Protocol (CGMP)
A proprietary protocol used by switches to obtain multicast membership information for end hosts (deprecated)

Internet Group Management Protocol (IGMP)
Hosts send IGMP requests to local routers to join multicast groups

IGMP Configuration

IGMP Support `Router(config-if)# ip igmp [version <#>]`

IGMP Snooping `Switch(config)# ip igmp snooping`

Protocol Independent Multicast (PIM)

Dense Mode
The initial tree encompasses all multicast routers; after a period of time, routers without IGMP members prune back branches

Sparse Mode
The tree is grown from a central rendezvous point out to the multicast source and recipients

Sparse-Dense Mode
Allows a PIM-enabled interface to function in either sparse or dense mode per group

PIMv1
Provides automatic RP discovery with Auto-RP (Cisco proprietary)

PIMv2
Automatic RP discovery is accomplished by the bootstrap router (BSR) method (standard)

PIM Configuration

```
ip multicast-routing
!
interface FastEthernet0/0
 ip pim {sparse-mode | dense-mode | sparse-dense-mode}
 ip pim version {1 | 2}
```

Group Ranges

224.0.0.0/24	Local network control
224.0.1.0/24	Internetwork control
232.0.0.0/8	Source-specific
233.0.0.0/8	GLOP (RFC 3180)
239.0.0.0/8	Admin-scoped

Common Groups

224.0.0.1	All hosts
224.0.0.2	All routers
224.0.1.39	Cisco RP Announce
224.0.1.40	Cisco RP Discovery

Distribution Trees

Shared
A common set of links which carry all multicast traffic; statically configured

Source-Rooted
Provides the shortest paths from the source to receivers

IGMP

IGMPv1
Original IGMP specification

IGMPv2
Adds support for dynamic leave requests and querier election to original IGMP

IGMPv3
Adds multicast source filtering to v2

IGMP Snooping
A switch passively inspects IGMP requests to determine which hosts should receive multicast traffic

IGMP Troubleshooting

```
show ip igmp
show ip igmp group
show ip igmp interface
show ip igmp snooping
ip igmp join-group
```

RP Configuration

Manual	`ip pim rp-address <IP>`
Auto-RP Mapping Agent	`ip pim send-rp-discovery scope <TTL>`
Auto-RP Candidate	`ip pim send-rp-announce <interface>`
BSR Candidate	`ip pim bsr-candidate <interface>`
BSR RP Candidate	`ip pim rp-candidate <interface>`

PIM Troubleshooting

```
show ip mroute
show ip pim interface
show ip pim neighbor
show ip pim rp [mapping]
show ip rpf <IP>
```

by Jeremy Stretch v2.0

IPv4 Subnetting

packetlife.net

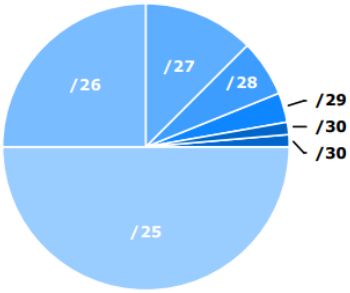
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

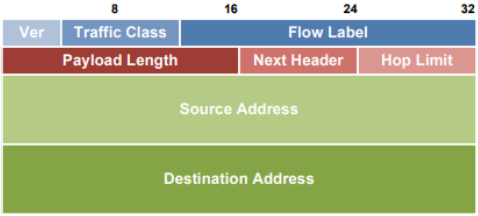
VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

by Jeremy Stretch v2.0

IPv6

packetlife.net

Protocol Header



Version (4 bits) · Always set to 6
Traffic Class (8 bits) · A DSCP value for QoS
Flow Label (20 bits) · Identifies unique flows (optional)
Payload Length (16 bits) · Length of the payload in bytes
Next Header (8 bits) · Header or protocol which follows
Hop Limit (8 bits) · Similar to IPv4's time to live field
Source Address (128 bits) · Source IP address
Destination Address (128 bits) · Destination IP address

Address Types

Unicast · One-to-one communication
Multicast · One-to-many communication
Anycast · An address configured in multiple locations

Address Notation

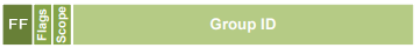
· Eliminate leading zeros from all two-byte sets
· Replace up to one string of consecutive zeros with a double-colon (::)

Address Formats

Global unicast

Link-local unicast

Multicast



EUI-64 Formation

· Insert 0xfffe between the two halves of the MAC
· Flip the seventh bit (universal/local flag) to 1

Multicast Scopes

1 Interface-local	**5** Site-local
2 Link-local	**8** Org-local
4 Admin-local	**E** Global

Special-Use Ranges

::/0	Default route
::/128	Unspecified
::1/128	Loopback
::/96	IPv4-compatible*
::FFFF:0:0/96	IPv4-mapped
2001::/32	Teredo
2001:DB8::/32	Documentation
2002::/16	6to4
FC00::/7	Unique local
FE80::/10	Link-local unicast
FEC0::/10	Site-local unicast*
FF00::/8	Multicast

* Deprecated

Extension Headers

Hop-by-hop Options (0)
Carries additional information which must be examined by every router in the path

Routing (43)
Provides source routing functionality

Fragment (44)
Included when a packet has been fragmented by its source

Encapsulating Security Payload (50)
Provides payload encryption (IPsec)

Authentication Header (51)
Provides packet authentication (IPsec)

Destination Options (60)
Carries additional information which pertains only to the recipient

Transition Mechanisms

Dual Stack
Transporting IPv4 and IPv6 across an infrastructure simultaneously

Tunneling
IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

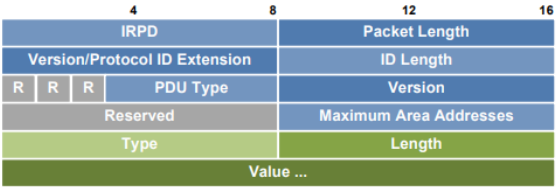
Translation
Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses

by Jeremy Stretch v2.0

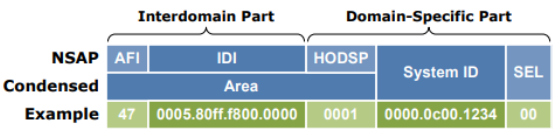
IS-IS · PART 1

packetlife.net

Protocol Header



NSAP Addressing



Interdomain Part (IDP)
Portion of the address used in routing between autonomous systems; assigned by ISO

Domain-Specific Part (DSP)
Portion of the address relevant only within the local AS

Authority and Format Identifier (AFI)
Identifies the authority which dictates the format of the address

Initial Domain Identifier (IDI)
An organization belonging to the AFI

High Order DSP (HODSP)
The area within the AS

System ID
Unique router identifier; 48 bits for Cisco devices (often taken from a MAC address)

NSAP Selector (SEL)
Identifies a network layer service; always 0x00 in a NET address

Network Types

	Broadcast	Point-to-Point
DIS Elected	Yes	No
Neighbor Discovery	Yes	Yes
Hello/Dead Timers	10/30	10/30

Troubleshooting

`show ip route`	`show isis spf-log`
`show ip protocols`	`debug isis spf-events`
`show [clns|isis] neighbor`	`debug isis adjacencies-packets`
`show [clns|isis] interface`	`debug isis spf-statistics`
`show isis database`	`debug isis update-packets`

Attributes

Type	Link-State
Algorithm	Dijkstra
Metric	Default (10)
AD	115
Standard	ISO 10589
Protocols	IP, CLNS
Transport	Layer 2
Authentication	Plaintext, MD5

Routing Levels

Level 0	Used to locate end systems
Level 1	Routing within an area
Level 2	Backbone between areas
Level 3	Inter-AS routing

Terminology

Type-Length-Value (TLV)
Variable-length modular datasets

Link State PDU (LSP)
Carry TLVs encompassing link state information

Sequence Number Packet (SNP)
Used to request and advertise LSPs; can be complete (CSNP) or partial (PSNP)

Hello Packet
Establishes and maintains neighbor adjacencies

Designated Intermediate System
A pseudonode responsible for emulating point-to-point links across a multi-access segment

Adjacency Requirements

- Interface MTUs must match
- Levels must match
- Areas must match (if level 1)
- System IDs must be unique
- Authentication must succeed

DIS Election

- Highest-priority interface elected
- Highest SNPA (MAC/DLCI) breaks tie
- Highest system ID breaks SNPA tie
- Default interface priority is 64
- Current DIS may be preempted

by Jeremy Stretch

v2.0

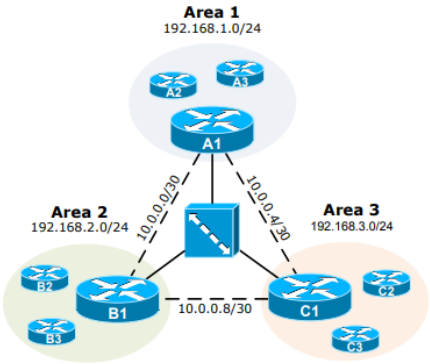
IS-IS · PART 2

packetlife.net

TLV Types

	Name	Use		Name	Use		Name	Use
1	Area Addresses	Hello, LSP	**6**	IS Neighbors	Hello, L2 LSP	**128**	IP Internal Reach.	LSP
2	IS Neighbors	LSP	**8**	Padding	Hello	**129**	Protocols Supported	Hello, LSP
3	ES Neighbors	L1 LSP	**9**	LSP Entries	SNP	**131**	IDRPI	SNP, L2 LSP
5	Prefix Neighbors	L2 LSP	**10**	Authentication	All	**132**	IP Interface Address	Hello, LSP

Configuration Example



Router A2

```
interface FastEthernet0/0
 description Area 1
 ip address 192.168.1.2 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
router isis
 net 49.0001.0000.0000.00a2.00
```

Router B2

```
interface FastEthernet0/0
 description Area 2
 ip address 192.168.2.2 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
router isis
 net 49.0002.0000.0000.00b2.00
```

Router A1

```
interface FastEthernet0/0
 description Area 1
 ip address 192.168.1.1 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
!
interface Serial1/0.1 point-to-point
 description To Area 2
 ip address 10.0.0.1 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
! MD5 authentication (keychain not shown)
 isis authentication mode md5
 isis authentication key-chain <keychain>
 frame-relay interface-dlci 101
!
interface Serial1/0.2 point-to-point
 description To Area 3
 ip address 10.0.0.5 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
 frame-relay interface-dlci 102
!
router isis
 net 49.0001.0000.0000.00a1.00
```

Router B1

```
interface FastEthernet0/0
 description Area 2
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
!
interface Serial1/0.1 point-to-point
 description To Area 1
 ip address 10.0.0.2 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
! MD5 authentication (keychain not shown)
 isis authentication mode md5
 isis authentication key-chain <keychain>
 frame-relay interface-dlci 101
!
interface Serial1/0.2 point-to-point
 description To Area 3
 ip address 10.0.0.9 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
 frame-relay interface-dlci 103
!
router isis
 net 49.0002.0000.0000.00b1.00
```

by Jeremy Stretch v2.0

MARKDOWN

packetlife.net

Headers

`# Text`	`<h1>Text</h1>`
`## Text`	`<h2>Text</h2>`
`### Text`	`<h3>Text</h3>`
`#### Text`	`<h4>Text</h4>`
`##### Text`	`<h5>Text</h5>`
`###### Text`	`<h6>Text</h6>`

Lists

```
* Sizes
* Shapes
* Colors
    * Blue
    * Green
```

```
<ul>
  <li>Sizes</li>
  <li>Shapes</li>
  <li>Colors
  <ul>
    <li>Blue</li>
    <li>Green</li>
  </ul></li>
</ul>
```

```
1. First
2. Second
3. Third
    1. Alpha
    2. Bravo
```

```
<ol>
  <li>First</li>
  <li>Second</li>
  <li>Third
  <ol>
    <li>Alpha</li>
    <li>Bravo</li>
  </ol></li>
</ol>
```

Blockquotes

```
> Lorem ipsum
> dolor sit amet
```

```
<blockquote>
<p>Lorem ipsum dolor sit amet</p>
</blockquote>
```

```
> Lorem ipsum dolor
sit amet
```

```
<blockquote>
<p>Lorem ipsum dolor sit amet</p>
</blockquote>
```

```
> Level one
>
> > Level two
> >
> > > Level three
```

```
<blockquote><p>Level one</p>
  <blockquote><p>Level two</p>
    <blockquote><p>Level three</p>
    </blockquote>
  </blockquote>
</blockquote>
```

Inline Code

`Use ` ` tags`	`Use <code>&lt;div&gt;</code> tags`
``` ``echo `uname -a`` ```	`<code>echo `uname -a`</code>`

Code Blocks

```
Normal text

    #include <stdio.h>
```

```
<p>Normal text</p>
<pre><code>
#include &lt;stdio.h&gt;
</code></pre>
```

Horizontal Rules

`* * *`	`<hr />`	`- - -`	`<hr />`
`***`	`<hr />`	`---`	`<hr />`

Emphasis

`*Emphasis*`	`<em>Emphasis</em>`
`_Emphasis_`	`<em>Emphasis</em>`
`**Strong**`	`<strong>Strong</strong>`
`__Strong__`	`<strong>Strong</strong>`
`*Super*emphasis`	`<em>Super</em>emphasis`
`**Super**strong`	`<strong>Super</strong>strong`

Escapable Characters

`\`	Backslash	`( )`	Parantheses
`` ` ``	Backtick	`#`	Hash mark
`*`	Asterisk	`+`	Plus sign
`_`	Underscore	`-`	Hyphen
`{ }`	Curly braces	`.`	Period
`[ ]`	Square brackets	`!`	Exclamation

Links

`[Google](http://google.com/)`	`<a href="http://google.com/">Google</a>`
`[Google](http://google.com/ "Search")`	`<a href="http://google.com/" title="Search">Google</a>`
`[google]: http://google.com/ "Search"` `[Google][google]`	`<a href="http://google.com/" title="Search">Google</a>`
`<http://google.com>`	`<a href="http://google.com/">http://google.com</a>`

Images

`![Alt text](/path/to/img.jpg)`	`<img src="/path/to/img.jpg" alt="Alt text"/>`
`![Alt text](/path/to/img.jpg "Title")`	`<img src="/path/to/img.jpg" alt="Alt text" title="Title"/>`
`[img1]: /path/to/img.jpg "Title"` `![Alt text][img1]`	`<img src="/path/to/img.jpg" alt="Alt text" title="Title"/>`

Markdown is available at http://daringfireball.net/projects/markdown/

by Jeremy Stretch v2.0

MediaWiki

packetlife.net

Headers

`=Text=`	`<h1>Text</h1>`
`==Text==`	`<h2>Text</h2>`
`===Text===`	`<h3>Text</h3>`
`====Text====`	`<h4>Text</h4>`
`=====Text=====`	`<h5>Text</h5>`
`======Text======`	`<h6>Text</h6>`

Code

`<code>Text</code>`	`<code>Text</code>`
`<code><pre>Text</pre></code>`	`<code><pre>Text</pre></code>`

Miscellaneous

`<nowiki>Suppress [[wiki]] '''markup'''</nowiki>`	`Suppress [[wiki]] '''markup'''`
`<!-- a comment -->`	`<!-- a comment -->`

Lists

```
* Sizes
* Shapes
* Colors
** Blue
** Green
```

```
<ul>
  <li>Sizes</li>
  <li>Shapes</li>
  <li>Colors
  <ul>
    <li>Blue</li>
    <li>Green</li>
  </ul></li>
</ul>
```

```
# First
# Second
# Third
```

```
<ol>
  <li>First</li>
  <li>Second</li>
  <li>Third</li>
</ol>
```

```
; Term 1 : Foo
; Term 2 : Bar
; Term 3 : Baz
```

```
<dl>
 <dt>Term 1</dt>
  <dd>Foo</dd>
 <dt>Item 2</dt>
  <dd>Bar</dd>
 <dt>Item 3</dt>
  <dd>Baz</dd>
</dl>
```

Formatting

`''Text''`	`<i>Text</i>`
`'''Text'''`	`<b>Text</b>`
`'''''Text'''''`	`<i><b>Text</b></i>`
`<ins>Text</ins>`	`<ins>Text</ins>`
`<del>Text</del>`	`<del>Text</del>`
`<tt>Text</tt>`	`<tt>Text</tt>`

Templates

Unnamed variables	`Books by {{{1}}}`
Invoking the template	`{{Author|Palahniuk}}`
Named variables	`Books by {{{name}}}`
Invoking the template	`{{Author|name=Palahniuk}}`

Categories

Assign object to a category	`[[Category:Humor]]`
Link to a category	`[[:Category:Humor]]`

Links

`[[packet switching]]`	`<a href="Packet_switching">packet switching</a>`
`[[packet switching|packet switched]]`	`<a href="Packet_switching">packet switched</a>`
`IP [[network]]ing`	`IP <a href="Network">networking</a>`
`IEEE [[802.3 (Ethernet)|]]`	`IEEE <a href="802.3_(Ethernet)">802.3</a>`
`[http://google.com/]`	`<a href="http://google.com/">http://google.com/</a>`
`[http://google.com/ Google]`	`<a href="http://google.com/">Google</a>`

Images

`[[Image:photo.png]]`	`<a href="Image:photo.png"><img src="photo.png" /></a>`
`[[Image:photo.png|Alt text]]`	`<a href="Image:photo.png"><img src="photo.png" alt="Alt text" /></a>`
`[[Image:photo.png|30 px]]`	`<a href="Image:photo.png"><img src="30px-photo.png" /></a>`
`[[:Image:photo.png|A photo]]`	`<a href="Image:photo.png">A photo</a>`

Tables

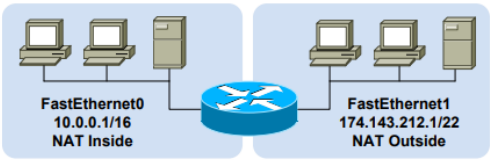
`{|`	Starts a table	`!`	Table header
`|+`	Table caption (optional; one per table)	`|`	Table cell
`|-`	Begin a new row	`|}`	Table end

by Jeremy Stretch v2.1

NETWORK ADDRESS TRANSLATION

packetlife.net

Example Topology



Address Classification

Inside Local	An actual address assigned to an inside host
Inside Global	An inside address seen from the outside
Outside Global	An actual address assigned to an outside host
Outside Local	An outside address seen from the inside

NAT Boundary Configuration

```
interface FastEthernet0
 ip address 10.0.0.1 255.255.0.0
 ip nat inside
!
interface FastEthernet1
 ip address 174.143.212.1 255.255.252.0
 ip nat outside
```

		Perspective	
		Local	Global
Location	Inside	Inside Local	Inside Global
	Outside	Outside Local	Outside Global

Static Source Translation

```
! One line per static translation
ip nat inside source static 10.0.0.19 192.0.2.1
ip nat inside source static 10.0.1.47 192.0.2.2
ip nat outside source static 174.143.212.133 10.0.0.47
ip nat outside source static 174.143.213.240 10.0.2.181
```

Dynamic Source Translation

```
! Create an access list to match inside local addresses
access-list 10 permit 10.0.0.0 0.0.255.255
!
! Create NAT pool of inside global addresses
ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24
!
! Combine them with a translation rule
ip nat inside source list 10 pool MyPool
!
! Dynamic translations can be combined with static entries
ip nat inside source static 10.0.0.42 192.0.2.42
```

Port Address Translation (PAT)

```
! Static layer four port translations
ip nat inside source static tcp 10.0.0.3 8080 192.0.2.1 80
ip nat inside source static udp 10.0.0.14 53 192.0.2.2 53
ip nat outside source static tcp 174.143.212.4 23 10.0.0.8 23
!
! Dynamic port translation with a pool
ip nat inside source list 11 pool MyPool overload
!
! Dynamic translation with interface overloading
ip nat inside source list 11 interface FastEthernet1 overload
```

Terminology

NAT Pool
A pool of IP addresses to be used as inside global or outside local addresses in translations

Port Address Translation (PAT)
An extension to NAT that translates information at layer four and above, such as TCP and UDP port numbers; dynamic PAT configurations include the **overload** keyword

Extendable Translation
The **extendable** keyword must be appended when multiple overlapping static translations are configured

Special NAT Pool Types

Rotary	Used for load balancing
Match-Host	Preserves the host portion of the address after translation

Troubleshooting

```
show ip nat translations [verbose]
show ip nat statistics
clear ip nat translations
```

NAT Translations Tuning

```
ip nat translation tcp-timeout <seconds>
ip nat translation udp-timeout <seconds>
ip nat translation max-entries <number>
```

Inside Destination Translation

```
! Create a rotary NAT pool
ip nat pool LoadBalServers 10.0.99.200 10.0.99.203 prefix-length 24 type rotary
!
! Enable load balancing across inside hosts for incoming traffic
ip nat inside destination list 12 pool LoadBalServers
```

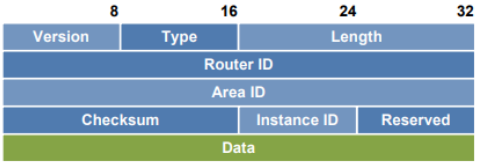
by Jeremy Stretch

v1.0

OSPF · PART 1

packetlife.net

Protocol Header



Link State Advertisements

Router Link (Type 1)
Lists neighboring routers and the cost to each; flooded within an area

Network Link (Type 2)
Generated by a DR; lists all routers on an adjacent segment; flooded within an area

Network Summary (Type 3)
Generated by an ABR and advertised among areas

ASBR Summary (Type 4)
Injected by an ABR into the backbone to advertise the presence of an ASBR within an area

External Link (Type 5)
Generated by an ASBR and flooded throughout the AS to advertise a route external to OSPF

NSSA External Link (Type 7)
Generated by an ASBR in a not-so-stubby area; converted into a type 5 LSA by the ABR when leaving the area

Router Types

Internal Router
All interfaces reside within the same area

Backbone Router
A router with an interface in area 0 (the backbone)

Area Border Router (ABR)
Connects two or more areas

AS Boundary Router (ASBR)
Connects to additional routing domains; typically located in the backbone

Area Types

Standard Area
Default OSPF area type

Stub Area
External link (type 5) LSAs are replaced with a default route

Totally Stubby Area
Type 3, 4, and 5 LSAs are replaced with a default route

Not So Stubby Area (NSSA)
A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area

External Route Types

E1 · Cost to the advertising ASBR plus the external cost of the route

E2 (Default) · Cost of the route as seen by the ASBR

Troubleshooting

`show ip [route | protocols]`	`show ip ospf border-routers`
`show ip ospf interface`	`show ip ospf virtual-links`
`show ip ospf neighbor`	`debug ip ospf […]`

Attributes

Type	Link-State
Algorithm	Dijkstra
Metric	Cost (Bandwidth)
AD	110
Standard	RFC 2328, 2740
Protocols	IP
Transport	IP/89
Authentication	Plaintext, MD5
AllSPF Address	224.0.0.5
AllDR Address	224.0.0.6

Metric Formula

$$\text{cost} = \frac{100{,}000\ \text{Kbps}^*}{\textbf{link speed}}$$

* modifiable with `ospf auto-cost reference-bandwidth`

Adjacency States

1	Down	**5**	Exstart
2	Attempt	**6**	Exchange
3	Init	**7**	Loading
4	2-Way	**8**	Full

DR/BDR Election

· The DR serves as a common point for all adjacencies on a multiaccess segment

· The BDR also maintains adjacencies with all routers in case the DR fails

· Election does not occur on point-to-point or multipoint links

· Default priority (0-255) is 1; highest priority wins; 0 cannot be elected

· DR preemption will not occur unless the current DR is reset

Virtual Links

· Tunnel formed to join two areas across an intermediate

· Both end routers must share a common area

· At least one end must reside in area 0

· Cannot traverse stub areas

by Jeremy Stretch

v2.1

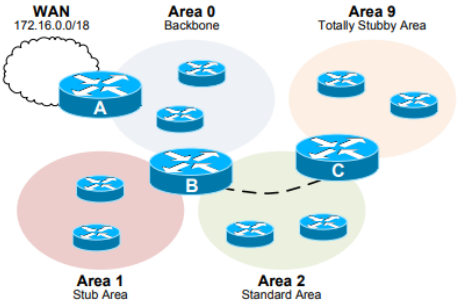
OSPF · PART 2

packetlife.net

Network Types

	Nonbroadcast (NBMA)	Multipoint Broadcast	Multipoint Nonbroadcast	Broadcast	Point-to-Point
DR/BDR Elected	Yes	No	No	Yes	No
Neighbor Discovery	No	Yes	No	Yes	Yes
Hello/Dead Timers	30/120	30/120	30/120	10/40	10/40
Defined By	RFC 2328	RFC 2328	Cisco	Cisco	Cisco
Supported Topology	Full Mesh	Any	Any	Full Mesh	Point-to-Point

Configuration Example



Router A

```
interface Serial0/0
 description WAN Link
 ip address 172.16.34.2 255.255.255.252
!
interface FastEthernet0/0
 description Area 0
 ip address 192.168.0.1 255.255.255.0
!
interface Loopback0
 ! Used as router ID
 ip address 10.0.34.1 255.255.255.0
!
router ospf 100
 ! Advertising the WAN cloud to OSPF
 redistribute static subnets
 network 192.168.0.0 0.0.0.255 area 0
!
 ! Static route to the WAN cloud
ip route 172.16.0.0 255.255.192.0 172.16.34.1
```

Router B

```
interface Ethernet0/0
 description Area 0
 ip address 192.168.0.2 255.255.255.0
 ip ospf 100 area 0
!
interface Ethernet0/1
 description Area 2
 ip address 192.168.2.1 255.255.255.0
 ip ospf 100 area 2
 ! Optional MD5 authentication configured
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 FooBar
 ! Give B priority in DR election
 ip ospf priority 100
!
interface Ethernet0/2
 description Area 1
 ip address 192.168.1.1 255.255.255.0
 ip ospf 100 area 1
!
interface Loopback0
 ip address 10.0.34.2 255.255.255.0
!
router ospf 100
 ! Define area 1 as a stub area
 area 1 stub
 ! Virtual link from area 0 to area 9
 area 2 virtual-link 10.0.34.3
```

Router C

```
interface Ethernet0/0
 description Area 9
 ip address 192.168.9.1 255.255.255.0
 ip ospf 100 area 9
!
interface Ethernet0/1
 description Area 2
 ip address 192.168.2.2 255.255.255.0
 ip ospf 100 area 2
 ! Optional MD5 authentication configured
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 FooBar
 ! Give C second priority (BDR) in election
 ip ospf priority 50
!
!
!
!
!
!
interface Loopback0
 ip address 10.0.34.3 255.255.255.0
!
router ospf 100
 ! Define area 9 as a totally stubby area
 area 9 stub no-summary
 ! Virtual link from area 9 to area 0
 area 2 virtual-link 10.0.34.2
```

by Jeremy Stretch v2.1

PHYSICAL TERMINATIONS

packetlife.net

Optical Terminations

ST (Straight Tip)

SC (Subscriber Connector)

LC (Local Connector)

MT-RJ

Wireless Antennas

RP-TNC

RP-SMA

Copper Terminations

RJ-45

RJ-11

RJ-21 (25-pair)

DE-9 (Female)

DB-25 (Male)

DB-60 (Male)

GBICs

1000Base-SX/LX

1000Base-T

Cisco GigaStack

1000Base-SX/LX SFP

1000Base-T SFP

X2 (10Gig)

by Jeremy Stretch

v1.1

POINT-TO-POINT PROTOCOL

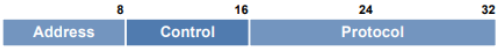
packetlife.net

PPP Components

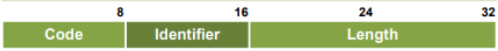
Link Control Protocol (LCP)
Provides for the establishment, configuration, and maintenance of a PPP link. Protocol-independent options are negotiated by LCP.

Network Control Protocol (NCP)
A separate NCP is used to negotiate the configuration of each network layer protocol (such as IP) carried by PPP.

PPP Header



LCP Header



Authentication Protocols

Plaintext Authentication Protocol (PAP)
Original, obsolete authentication protocol which relies on the exchange of a plaintext key to authenticate peers (RFC 1334).

Challenge Handshake Authentication Protocol (CHAP)
Authenticates peers using the MD5 checksum of a pre-shared secret key (RFC 1994).

Extensible Authentication Protocol (EAP)
Provides MD5-based authentication similar to CHAP (RFC 3748). Could be expanded to support other EAP mechanisms as well.

General PPP Configuration

```
! Configure a peer account if authentication will be used
username peer-hostname password password

! Configure a local IP address pool if needed
ip pool name first-IP last-IP

interface Serial0/0
 ! Enable PPP encapsulation
 encapsulation ppp
 ! Enable CHAP and/or PAP for authentication
 ppp authentication { chap | pap } [ chap | pap ]
 ! Enable compression
 compress { predictor | stac }
 ! Enable peer IP address assignment (server side)
 peer default ip address { pool name | IP-address }
 ! Enable IP address negotiation (client side)
 ip address negotiated
```

Multilink PPP Configuration

```
! Create the multilink interface
interface Multilink1
 ip address IP-address subnet-mask
 ppp multilink group group

! Assign physical interfaces to the multilink group
interface Serial0/0
 encapsulation ppp
 ppp multilink group group
```

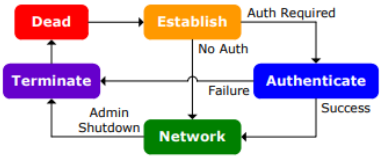
PPP Summary

Standard	RFC 1661
Interfaces	Asynchronous serial, synchronous serial, ISDN, HSSI

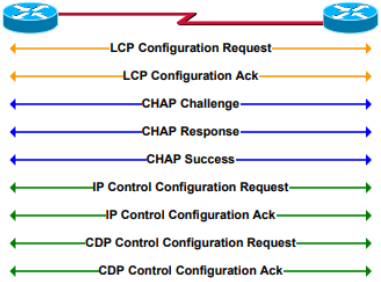
PPP Features

Protocol Multiplexing · Multiple NCPs
Optional Authentication · PAP/CHAP
Optional Compression · Stacker/predictor
Loopback Detection · Provided by LCP
Load Balancing · Multilink PPP

Connection Phase Flowchart



PPP Connection Example



PPP Compression Algorithms

Stacker
Replaces repetitive data with symbols from a dynamic dictionary (more processor-intensive)

Predictor
Attempts to predict sequential data (more memory-intensive)

Troubleshooting

```
show ppp multilink
debug ppp authentication
debug ppp { negotiation | packet }
```

by Jeremy Stretch

QUALITY OF SERVICE · PART 1

packetlife.net

Quality of Service Models

Best Effort · No QoS policies are implemented

Integrated Services (IntServ)
Resource Reservation Protocol (RSVP) is used to reserve bandwidth per-flow across all nodes in a path

Differentiated Services (DiffServ)
Packets are individually classified and marked; policy decisions are made independently by each node in a path

Layer 2 QoS Markings

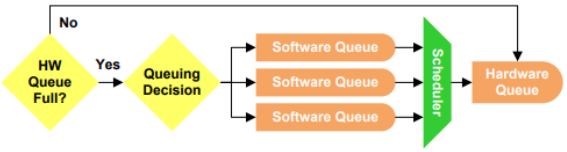
Medium	Name	Type
Ethernet	Class of Service (CoS)	3-bit 802.1p field in 802.1Q header
Frame Relay	Discard Eligibility (DE)	1-bit drop eligibility flag
ATM	Cell Loss Priority (CLP)	1-bit drop eligibility flag
MPLS	Traffic Class (TC)	3-bit field compatible with 802.1p

IP QoS Markings

IP Precedence
The first three bits of the IP TOS field; limited to 8 traffic classes

Differentiated Services Code Point (DSCP)
The first six bits of the IP TOS are evaluated to provide more granular classification; backward-compatible with IP Precedence

QoS Flowchart



Terminology

Per-Hop Behavior (PHB)
The individual QoS action performed at each independent DiffServ node

Trust Boundary · Beyond this, inbound QoS markings are not trusted

Tail Drop · Occurs when a packet is dropped because a queue is full

Policing
Imposes an artificial ceiling on the amount of bandwidth that may be consumed; traffic exceeding the policer rate is reclassified or dropped

Shaping
Similar to policing but buffers excess traffic for delayed transmission; makes more efficient use of bandwidth but introduces a delay

TCP Synchronization
Flows adjust TCP window sizes in synch, making inefficient use of a link

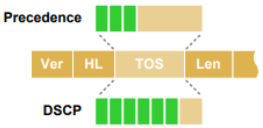
DSCP Per-Hop Behaviors

Class Selector (CS) · Backward-compatible with IP Precedence values

Assured Forwarding (AF) · Four classes with variable drop preferences

Expedited Forwarding (EF) · Priority queuing for delay-sensitive traffic

IP Type of Service (TOS)



Precedence/DSCP

	Binary	DSCP	Prec.
56	111000	Reserved	7
48	110000	Reserved	6
46	101110	EF	5
32	100000	CS4	4
34	100010	AF41	
36	100100	AF42	
38	100110	AF43	
24	011000	CS3	3
26	011010	AF31	
28	011100	AF32	
30	011110	AF33	
16	010000	CS2	2
18	010010	AF21	
20	010100	AF22	
22	010110	AF23	
8	001000	CS1	1
10	001010	AF11	
12	001100	AF12	
14	001110	AF13	
0	000000	BE	0

Congestion Avoidance

Random Early Detection (RED)
Packets are randomly dropped before a queue is full to prevent tail drop; mitigates TCP synchronization

Weighted RED (WRED)
RED with the added capability of recognizing prioritized traffic based on its marking

Class-Based WRED (CBWRED)
WRED employed inside a class-based WFQ (CBWFQ) queue

by Jeremy Stretch

v2.0

QUALITY OF SERVICE · PART 2

packetlife.net

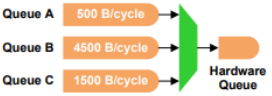
Queuing Comparison

	FIFO	PQ	CQ	WFQ	CBWFQ	LLQ
Default on Interfaces	>2 Mbps	No	No	<=2 Mbps	No	No
Number of Queues	1	4	Configured	Dynamic	Configured	Configured
Configurable Classes	No	Yes	Yes	No	Yes	Yes
Bandwidth Allocation	Automatic	Automatic	Configured	Automatic	Configured	Configured
Provides for Minimal Delay	No	Yes	No	No	No	Yes
Modern Implementation	Yes	No	No	No	Yes	Yes

First In First Out (FIFO)

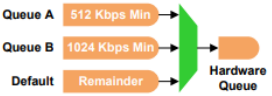
- Packets are transmitted in the order they are processed
- No prioritization is provided
- Default queuing method on high-speed (>2 Mbps) interfaces
- Configurable with the **tx-ring-limit** interface config command

Custom Queuing (CQ)



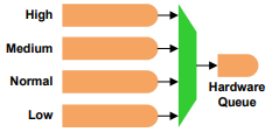
- Rotates through queues using Weighted Round Robin (WRR)
- Processes a configurable number of bytes from each queue per turn
- Prevents queue starvation but does not provide for delay-sensitive traffic

Class-Based WFQ (CBWFQ)



- WFQ with administratively configured queues
- Each queue is allocated an amount/percentage of bandwidth
- No support for delay-sensitive traffic

Priority Queuing (PQ)

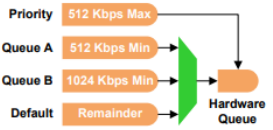


- Provides four static queues which cannot be reconfigured
- Higher-priority queues are always emptied before lower-priority queues
- Lower-priority queues are at risk of bandwidth starvation

Weighted Fair Queuing (WFQ)

- Queues are dynamically created per flow to ensure fair processing
- Statistically drops packets from aggressive flows more often
- No support for delay-sensitive traffic

Low Latency Queuing (LLQ)



- CBWFQ with the addition of a policed strict-priority queue
- Highly configurable while still supporting delay-sensitive traffic

LLQ Config Example

Class Definitions

```
! Match packets by DSCP value
class-map match-all Voice
 match dscp ef
!
class-map match-all Call-Signaling
 match dscp cs3
!
class-map match-any Critical-Apps
 match dscp af21 af22
!
! Match packets by access list
class-map match-all Scavenger
 match access-group name Other
```

Policy Creation

```
policy-map Foo
 class Voice
  ! Priority queue policed to 33%
  priority percent 33
 class Call-Signaling
  ! Allocate 5% of bandwidth
  bandwidth percent 5
 class Critical-Apps
  bandwidth percent 20
  ! Extend queue size to 96 packets
  queue-limit 96
 class Scavenger
  ! Police to 64 kbps
  police cir 64000
   conform-action transmit
   exceed-action drop
 class class-default
  ! Enable WFQ
  fair-queue
  ! Enable WRED
  random-detect
```

Policy Application

```
interface Serial0
 ! Apply the policy in or out
 service-policy output Foo
```

LLQ Config Example

```
show policy-map [interface]
Show interface
show queue <interface>
Show mls qos
```

by Jeremy Stretch

v2.0

RIP

packetlife.net

RIP Implementations

RIPv1
Original RIP implementation, limited to classful routing (obsolete)

RIPv2
Introduced support for classless routing, authentication, triggered updates, and multicast announcements (RFC 2453)

RIPng (RIP Next Generation)
Extends RIPv2 to support IPv6 routing (RFC 2080); functions very similarly to RIPv2 and is subsequently as limited

Protocols Comparison

	RIPv1	RIPv2	RIPng
IP	IPv4	IPv4	IPv6
Admin Distance	120	120	120
UDP Port	520	520	521
Classless	No	Yes	Yes
Adv. Address	Broadcast	224.0.0.9	FF02::9
Authentication	None	Plain, MD5	None

RIPv2 Configuration

```
! Enable RIPv2 IPv4 routing
router rip
 version 2

 ! Disable RIPv2 automatic summarization
 no auto-summary

 ! Designate RIPv2 interfaces by network
 network network

 ! Identify unicast-only neighbors
 neighbor IP-address

 ! Originate a default route
 default-information originate

 ! Designate passive interfaces
 passive-interface {interface | default}

 ! Modify timers
 timers basic update invalid hold flush
```

RIPng Configuration

```
! Enable IPv6 routing
ipv6 unicast-routing

! Enable RIPng IPv6 routing
ipv6 router rip name

 ! Toggle split-horizon and poison-reverse
 [no] split-horizon
 [no] poison-reverse

 ! Modify timers
 timers basic update invalid hold flush
```

Attributes

Type	Distance Vector
Algorithm	Bellman-Ford
Admin Distance	120
Metric	Hop count (max 15)
Standard	RFCs 2080, 2453
Protocols	IPv4, IPv6
Transport	UDP
Authentication	Plaintext, MD5
Multicast IP	224.0.0.9/FF02::9

Terminology

Split Horizon
A rule that states a router may not advertise a route back to the neighbor from which it was learned

Route Poisoning
When a network becomes unreachable, an update with an infinite metric is generated to explicitly advertise the route as unreachable

Poison Reverse
A router advertises a network as unreachable through the interface on which it was learned

Timer Defaults

Update	30 sec	**Flush**	240 sec
Invalid	180 sec	**Hold-down**	180 sec

RIPv2 Interface Configuration

```
! Configure manual route summarization
ip summary-address rip network mask

! Enable MD5 authentication (RIPv2 only)
ip rip authentication mode md5
ip rip authentication key-chain key-chain
```

RIPng Interface Configuration

```
! Enable RIPng on the interface
ipv6 rip name enable

! Configure manual route summarization
ipv6 rip name summary-address prefix
```

Troubleshooting

```
show ip[v6] protocols
show ip[v6] rip database
show ip[v6] route rip
debug ip rip { database | events }
debug ipv6 rip [interface]
```

by Jeremy Stretch v1.1

SCAPY

packetlife.net

Basic Commands

ls()
List all available protocols and protocol options

lsc()
List all available scapy command functions

conf
Show/set scapy configuration parameters

Constructing Packets

```
# Setting protocol fields
>>> ip=IP(src="10.0.0.1")
>>> ip.dst="10.0.0.2"

# Combining layers
>>> l3=IP()/TCP()
>>> l2=Ether()/l3

# Splitting layers apart
>>> l2.getlayer(1)
<IP  frag=0 proto=tcp |<TCP  |>>
>>> l2.getlayer(2)
<TCP  |>
```

Displaying Packets

```
# Show an entire packet
>>> (Ether()/IPv6()).show()
###[ Ethernet ]###
  dst= ff:ff:ff:ff:ff:ff
  src= 00:00:00:00:00:00
  type= 0x86dd
###[ IPv6 ]###
     version= 6
     tc= 0
     fl= 0
     plen= None
     nh= No Next Header
     hlim= 64
     src= ::1
     dst= ::1

# Show field types with default values
>>> ls(UDP())
sport   : ShortEnumField = 1025 (53)
dport   : ShortEnumField = 53   (53)
len     : ShortField     = None (None)
chksum  : XShortField    = None (None)
```

Fuzzing

```
# Randomize fields where applicable
>>> fuzz(ICMP()).show()
###[ ICMP ]###
  type= <RandByte>
  code= 227
  chksum= None
  unused= <RandInt>
```

Specifying Addresses and Values

```
# Explicit IP address (use quotation marks)
>>> IP(dst="192.0.2.1")

# DNS name to be resolved at time of transmission
>>> IP(dst="example.com")

# IP network (results in a packet template)
>>> IP(dst="192.0.2.0/24")

# Random addresses with RandIP() and RandMAC()
>>> IP(dst=RandIP())
>>> Ether(dst=RandMAC())

# Set a range of numbers to be used (template)
>>> IP(ttl=(1,30))

# Random numbers with RandInt() and RandLong()
>>> IP(id=RandInt())
```

Sending Packets

send(pkt, inter=0, loop=0, count=1, iface=N)
Send one or more packets at layer three

sendp(pkt, inter=0, loop=0, count=1, iface=N)
Send one or more packets at layer two

sendpfast(pkt, pps=N, mbps=N, loop=0, iface=N)
Send packets much faster at layer two using tcpreplay

```
>>> send(IP(dst="192.0.2.1")/UDP(dport=53))
.
Sent 1 packets.
>>> sendp(Ether()/IP(dst="192.0.2.1")/UDP(dport=53))
.
Sent 1 packets.
```

Sending and Receiving Packets

sr(pkt, filter=N, iface=N), srp(...)
Send packets and receive replies

sr1(pkt, inter=0, loop=0, count=1, iface=N), srp1(...)
Send packets and return only the first reply

srloop(pkt, timeout=N, count=N), srploop(...)
Send packets in a loop and print each reply

```
>>> srloop(IP(dst="packetlife.net")/ICMP(), count=3)
RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140
RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140
RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140
```

Sniffing Packets

sniff(count=0, store=1, timeout=N)
Record packets off the wire; returns a list of packets when stopped

```
# Capture up to 100 packets (or stop with ctrl-c)
>>> pkts=sniff(count=100, iface="eth0")
>>> pkts
<Sniffed: TCP:92 UDP:7 ICMP:1 Other:0>
```

by Jeremy Stretch

v1.0

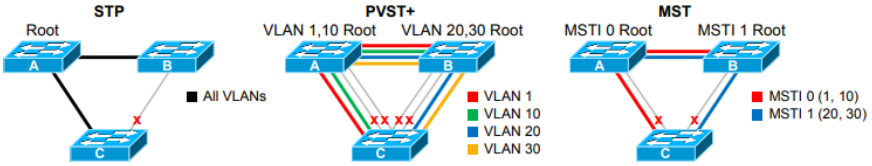
SPANNING TREE · PART 1

packetlife.net

Spanning Tree Protocols

	Legacy STP	PVST	PVST+	RSTP	RPVST+	MST
Algorithm	Legacy ST	Legacy ST	Legacy ST	Rapid ST	Rapid ST	Rapid ST
Defined By	802.1D-1998	Cisco	Cisco	802.1w, 802.1D-2004	Cisco	802.1s, 802.1Q-2003
Instances	1	Per VLAN	Per VLAN	1	Per VLAN	Configurable
Trunking	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL	802.1Q, ISL

Spanning Tree Instance Comparison



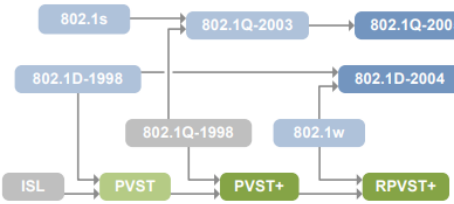
BPDU Format

Field	Bits
Protocol ID	16
Version	8
BPDU Type	8
Flags	8
Root ID	64
Root Path Cost	32
Bridge ID	64
Port ID	16
Message Age	16
Max Age	16
Hello Time	16
Forward Delay	16

Default Timers

Hello	2s
Forward Delay	15s
Max Age	20s

Spanning Tree Specifications



IEEE

- **IEEE 802.1D-1998** · Deprecated legacy STP standard
- **IEEE 802.1w** · Introduced RSTP
- **IEEE 802.1D-2004** · Replaced legacy STP with RSTP
- **IEEE 802.1s** · Introduced MST
- **IEEE 802.1Q-2003** · Added MST to 802.1Q
- **IEEE 802.1Q-2005** · Most recent 802.1Q revision

Cisco

- **PVST** · Per-VLAN implementation of legacy STP
- **PVST+** · Added 802.1Q trunking to PVST
- **RPVST+** · Per-VLAN implementation of RSTP

Link Costs

Bandwidth	Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2
20+ Gbps	1

Port States

Legacy ST	Rapid ST
Disabled	Discarding
Blocking	
Listening	
Learning	Learning
Forwarding	Forwarding

Port Roles

Legacy ST	Rapid ST
Root	Root
Designated	Designated
Blocking	Alternate
	Backup

Spanning Tree Operation

1. **Determine root bridge**
   The bridge advertising the lowest bridge ID becomes the root bridge
2. **Select root port**
   Each bridge selects its primary port facing the root
3. **Select designated ports**
   One designated port is selected per segment
4. **Block ports with loops**
   All non-root and non-desginated ports are blocked

by Jeremy Stretch

v3.0

SPANNING TREE · PART 2

packetlife.net

PVST+ and RPVST+ Configuration

```
spanning-tree mode {pvst | rapid-pvst}

! Bridge priority
spanning-tree vlan 1-4094 priority 32768

! Timers, in seconds
spanning-tree vlan 1-4094 hello-time 2
spanning-tree vlan 1-4094 forward-time 15
spanning-tree vlan 1-4094 max-age 20

! PVST+ Enhancements
spanning-tree backbonefast
spanning-tree uplinkfast

! Interface attributes
interface FastEthernet0/1
 spanning-tree [vlan 1-4094] port-priority 128
 spanning-tree [vlan 1-4094] cost 19

 ! Manual link type specification
 spanning-tree link-type {point-to-point | shared}

 ! Enables PortFast if running PVST+, or
 ! designates an edge port under RPVST+
 spanning-tree portfast

 ! Spanning tree protection
 spanning-tree guard {loop | root | none}

 ! Per-interface toggling
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
```

MST Configuration

```
spanning-tree mode mst

! MST Configuration
spanning-tree mst configuration
 name MyTree
 revision 1

 ! Map VLANs to instances
 instance 1 vlan 20, 30
 instance 2 vlan 40, 50

! Bridge priority (per instance)
spanning-tree mst 1 priority 32768

! Timers, in seconds
spanning-tree mst hello-time 2
spanning-tree mst forward-time 15
spanning-tree mst max-age 20

! Maximum hops for BPDUs
spanning-tree mst max-hops 20

! Interface attributes
interface FastEthernet0/1
 spanning-tree mst 1 port-priority 128
 spanning-tree mst 1 cost 19
```

Bridge ID Format

Priority
4-bit bridge priority (configurable from 0 to 61440 in increments of 4096)

System ID Extension
12-bit value taken from VLAN number (IEEE 802.1t)

MAC Address
48-bit unique identifier

Path Selection

1. Bridge with lowest root ID becomes the root
2. Prefer the neighbor with the lowest cost to root
3. Prefer the neighbor with the lowest bridge ID
4. Prefer the lowest sender port ID

Optional PVST+ Ehancements

PortFast
Enables immediate transition into the forwarding state (designates edge ports under MST)

UplinkFast
Enables switches to maintain backup paths to root

BackboneFast
Enables immediate expiration of the Max Age timer in the event of an indirect link failure

Spanning Tree Protection

Root Guard
Prevents a port from becoming the root port

BPDU Guard
Error-disables a port if a BPDU is received

Loop Guard
Prevents a blocked port from transitioning to listening after the Max Age timer has expired

BPDU Filter
Blocks BPDUs on an interface (disables STP)

RSTP Link Types

Point-to-Point
Connects to exactly one other bridge (full duplex)

Shared
Potentially connects to multiple bridges (half duplex)

Edge
Connects to a single host; designated by PortFast

Troubleshooting

```
show spanning-tree [summary | detail | root]
show spanning-tree [interface | vlan]
show spanning-tree mst […]
```

by Jeremy Stretch

v3.0

TCPDUMP

packetlife.net

Command Line Options			
`-A`	Print frame payload in ASCII	`-q`	Quick output
`-c <count>`	Exit after capturing **count** packets	`-r <file>`	Read packets from **file**
`-D`	List available interfaces	`-s <len>`	Capture up to **len** bytes per packet
`-e`	Print link-level headers	`-S`	Print absolute TCP sequence numbers
`-F <file>`	Use **file** as the filter expression	`-t`	Don't print timestamps
`-G <n>`	Rotate the dump file every n seconds	`-v[v[v]]`	Print more verbose output
`-i <iface>`	Specifies the capture interface	`-w <file>`	Write captured packets to **file**
`-K`	Don't verify TCP checksums	`-x`	Print frame payload in hex
`-L`	List data link types for the interface	`-X`	Print frame payload in hex and ASCII
`-n`	Don't convert addresses to names	`-y <type>`	Specify the data link type
`-p`	Don't capture in promiscuous mode	`-Z <user>`	Drop privileges from root to **user**

Capture Filter Primitives	
`[src|dst] host <host>`	Matches a host as the IP source, destination, or either
`ether [src|dst] host <ehost>`	Matches a host as the Ethernet source, destination, or either
`gateway host <host>`	Matches packets which used **host** as a gateway
`[src|dst] net <network>/<len>`	Matches packets to or from an endpoint residing in **network**
`[tcp|udp] [src|dst] port <port>`	Matches TCP or UDP packets sent to/from **port**
`[tcp|udp] [src|dst] portrange <p1>-<p2>`	Matches TCP or UDP packets to/from a port in the given range
`less <length>`	Matches packets less than or equal to **length**
`greater <length>`	Matches packets greater than or equal to **length**
`(ether|ip|ip6) proto <protocol>`	Matches an Ethernet, IPv4, or IPv6 protocol
`(ether|ip) broadcast`	Matches Ethernet or IPv4 broadcasts
`(ether|ip|ip6) multicast`	Matches Ethernet, IPv4, or IPv6 multicasts
`type (mgt|ctl|data) [subtype <subtype>]`	Matches 802.11 frames based on type and optional subtype
`vlan [<vlan>]`	Matches 802.1Q frames, optionally with a VLAN ID of **vlan**
`mpls [<label>]`	Matches MPLS packets, optionally with a label of **label**
`<expr> <relop> <expr>`	Matches packets by an arbitrary expression

Protocols		
`arp`	`ip6`	`slip`
`ether`	`link`	`tcp`
`fddi`	`ppp`	`tr`
`icmp`	`radio`	`udp`
`ip`	`rarp`	`wlan`

TCP Flags	
`tcp-urg`	`tcp-rst`
`tcp-ack`	`tcp-syn`
`tcp-psh`	`tcp-fin`

Modifiers	
`!` or `not`	
`&&` or `and`	
`||` or `or`	

Examples	
`udp dst port not 53`	UDP not bound for port 53
`host 10.0.0.1 && host 10.0.0.2`	Traffic between these hosts
`tcp dst port 80 or 8080`	Packets to either TCP port

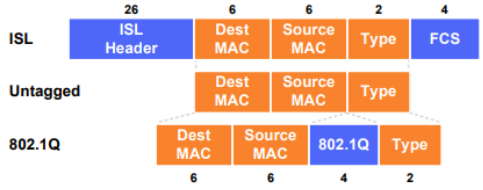
ICMP Types		
`icmp-echoreply`	`icmp-routeradvert`	`icmp-tstampreply`
`icmp-unreach`	`icmp-routersolicit`	`icmp-ireq`
`icmp-sourcequench`	`icmp-timxceed`	`icmp-ireqreply`
`icmp-redirect`	`icmp-paramprob`	`icmp-maskreq`
`icmp-echo`	`icmp-tstamp`	`icmp-maskreply`

by Jeremy Stretch v2.0

VLANs

packetlife.net

Trunk Encapsulation



VLAN Creation

```
Switch(config)# vlan 100
Switch(config-vlan)# name Engineering
```

Access Port Configuration

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 150
```

Trunk Port Configuration

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk allowed vlan 10,20-30
Switch(config-if)# switchport trunk native vlan 10
```

SVI Configuration

```
Switch(config)# interface vlan100
Switch(config-if)# ip address 192.168.100.1 255.255.255.0
```

VLAN Trunking Protocol (VTP)

Domain
Common to all switches participating in VTP

Server Mode
Generates and propagates VTP advertisements to clients; default mode on unconfigured switches

Client Mode
Receives and forwards advertisements from servers; VLANs cannot be manually configured on switches in client mode

Transparent Mode
Forwards advertisements but does not participate in VTP; VLANs must be configured manually

Pruning
VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic

VTP Configuration

```
Switch(config)# vtp mode {server | client | transparent}
Switch(config)# vtp domain <name>
Switch(config)# vtp password <passsword>
Switch(config)# vtp version {1 | 2}
Switch(config)# vtp pruning
```

Trunk Types

	802.1Q	ISL
Header Size	4 bytes	26 bytes
Trailer Size	N/A	4 bytes
Standard	IEEE	Cisco
Maximum VLANs	4094	1000

VLAN Numbers

0	Reserved	**1004**	fdnet
1	default	**1005**	trnet
1002	fddi-default	**1006-4094**	Extended
1003	tr	**4095**	Reserved

Terminology

Trunking
Carrying multiple VLANs over the same physical connection

Native VLAN
By default, frames in this VLAN are untagged when sent across a trunk

Access VLAN
The VLAN to which an access port is assigned

Voice VLAN
If configured, enables minimal trunking to support voice traffic in addition to data traffic on an access port

Dynamic Trunking Protocol (DTP)
Can be used to automatically establish trunks between capable ports (insecure)

Switched Virtual Interface (SVI)
A virtual interface which provides a routed gateway into and out of a VLAN

Switch Port Modes

`trunk`
Forms an unconditional trunk

`dynamic desirable`
Attempts to negotiate a trunk with the far end

`dynamic auto`
Forms a trunk only if requested by the far end

`access`
Will never form a trunk

Troubleshooting

```
show vlan
show interface [status | switchport]
show interface trunk
show vtp status
show vtp password
```

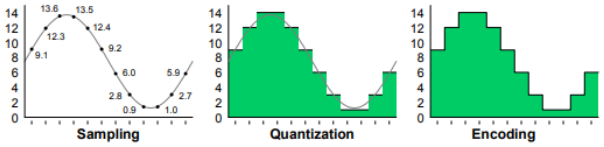
by Jeremy Stretch

v2.0

VOIP BASICS

packetlife.net

Pulse Code Modulation (PCM)



Sampling
8000 discrete signal measurements are taken at equal intervals every second

Quantization
The level of each sample is rounded to the nearest expressible value

Encoding
Digital values are encoded as binary numbers for encapsulation

Compression (Optional)
The digital signal is compressed in real time to consume less bandwidth

Power Over Ethernet (PoE)

Cisco Inline Power (ILP)
Pre-standard; employs a 340 kHz tone to detect devices; power needs communicated via CDP

IEEE 802.3af
Detects power requirements of PoE device by the line resistance present

IEEE 802.3at
Uses LLDP to negotiate delivery of up to 25 watts in .10 W intervals

IEEE 802.3af Classes

0	15.4 W	**3**	15.4 W
1	4 W	**4**	Reserved
2	7 W		

Voice Codecs

	MOS	Bandwidth	Complexity	Free
G.722 SB-ADPCM	4.13	48-64 kbps	Medium	Yes
G.711 PCM	4.1	64 kbps	Low	Yes
iLBC	4.1	15.2 kbps	High	Yes
G.729 CS-ACELP	3.92	8 kbps	High	No
G.726 ADPCM	3.85	32 kbps	Medium	Yes
G.729a CS-ACELP	3.7	8 kbps	Medium	No
G.728 LD-CELP	3.61	16 kbps	High	No

Signaling Protocols

ITU-T H.323
Originally designed for multimedia transmission over ISDN; mature and widely supported; peer-to-peer call control

Session Initiation Protocol (SIP)
Text-based, similar in nature to HTTP; defined in RFC 3261; peer-to-peer call control

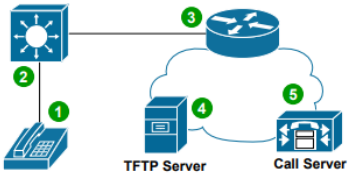
Media Gateway Control Protocol (MGCP)
Employs centralized call control; defined in RFC 3661

Skinny Client Control Protocol (SCCP)
Cisco-proprietary; limited support on gateways; centralized control

Calculating Required Bandwidth

G.711/Ethernet Example			
Codec Payload (Bitrate × Sample Size)	64 Kbps × 20 msec		160 B
L2 Overhead	Ethernet (18) + 802.1Q (4)	+	22 B
L3 Overhead	IP (20)	+	20 B
L4 Overhead	UDP (8) + RTP (12)	+	20 B
Packets per Second	1000 msec / 20 msec		× 50 pps
Total Bandwidth			88.8 Kbps

IP Phone Boot Process



1. Power Over Ethernet (Optional)
Power is supplied via IEEE 802.3af/at or Cisco ILP

2. VLANs Learned via CDP or LLDP
Voice and data VLANs communicated via CDP/LLDP

3. IP Assignment via DHCP
The phone sends a DHCP request in the voice VLAN; the response includes an IP and DHCP option 150

4. Configuration Retrieved via TFTP
The phone retrieves its configuration from one of the TFTP servers specified in the DHCP option

5. Registration
The phone registers with the call server(s) specified in its configuration

Access Switch Port Configuration

```
interface FastEthernet0/1

 ! Configure data and voice access VLANs
 switchport access vlan <VLAN>
 switchport voice vlan <VLAN>

 ! Trust ingress QoS markings
 mls qos trust cos

 ! Optionally pre-allocate power for the port
 power inline static [max <wattage>]
```

by Jeremy Stretch

v1.0

Wireshark Display Filters · Part 1

packetlife.net

Ethernet

eth.addr	eth.len	eth.src
eth.dst	eth.lg	eth.trailer
eth.ig	eth.multicast	eth.type

IEEE 802.1Q

vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer

IPv4

ip.addr	ip.fragment.overlap.conflict
ip.checksum	ip.fragment.toolongfragment
ip.checksum_bad	ip.fragments
ip.checksum_good	ip.hdr_len
ip.dsfield	ip.host
ip.dsfield.ce	ip.id
ip.dsfield.dscp	ip.len
ip.dsfield.ect	ip.proto
ip.dst	ip.reassembled_in
ip.dst_host	ip.src
ip.flags	ip.src_host
ip.flags.df	ip.tos
ip.flags.mf	ip.tos.cost
ip.flags.rb	ip.tos.delay
ip.frag_offset	ip.tos.precedence
ip.fragment	ip.tos.reliability
ip.fragment.error	ip.tos.throughput
ip.fragment.multipletails	ip.ttl
ip.fragment.overlap	ip.version

IPv6

ipv6.addr	ipv6.hop_opt
ipv6.class	ipv6.host
ipv6.dst	ipv6.mipv6_home_address
ipv6.dst_host	ipv6.mipv6_length
ipv6.dst_opt	ipv6.mipv6_type
ipv6.flow	ipv6.nxt
ipv6.fragment	ipv6.opt.pad1
ipv6.fragment.error	ipv6.opt.padn
ipv6.fragment.more	ipv6.plen
ipv6.fragment.multipletails	ipv6.reassembled_in
ipv6.fragment.offset	ipv6.routing_hdr
ipv6.fragment.overlap	ipv6.routing_hdr.addr
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type
ipv6.fragments	ipv6.src
ipv6.fragment.id	ipv6.src_host
ipv6.hlim	ipv6.version

ARP

arp.dst.hw_mac	arp.proto.size
arp.dst.proto_ipv4	arp.proto.type
arp.hw.size	arp.src.hw_mac
arp.hw.type	arp.src.proto_ipv4
arp.opcode	

TCP

tcp.ack	tcp.options.qs
tcp.checksum	tcp.options.sack
tcp.checksum_bad	tcp.options.sack_le
tcp.checksum_good	tcp.options.sack_perm
tcp.continuation_to	tcp.options.sack_re
tcp.dstport	tcp.options.time_stamp
tcp.flags	tcp.options.wscale
tcp.flags.ack	tcp.options.wscale_val
tcp.flags.cwr	tcp.pdu.last_frame
tcp.flags.ecn	tcp.pdu.size
tcp.flags.fin	tcp.pdu.time
tcp.flags.push	tcp.port
tcp.flags.reset	tcp.reassembled_in
tcp.flags.syn	tcp.segment
tcp.flags.urg	tcp.segment.error
tcp.hdr_len	tcp.segment.multipletails
tcp.len	tcp.segment.overlap
tcp.nxtseq	tcp.segment.overlap.conflict
tcp.options	tcp.segment.toolongfragment
tcp.options.cc	tcp.segments
tcp.options.ccecho	tcp.seq
tcp.options.ccnew	tcp.srcport
tcp.options.echo	tcp.time_delta
tcp.options.echo_reply	tcp.time_relative
tcp.options.md5	tcp.urgent_pointer
tcp.options.mss	tcp.window_size
tcp.options.mss_val	

UDP

udp.checksum	udp.dstport	udp.srcport
udp.checksum_bad	udp.length	
udp.checksum_good	udp.port	

Operators

eq or ==	
ne or !=	
gt or >	
lt or <	
ge or >=	
le or <=	

Logic

and or &&	Logical AND
or or ||	Logical OR
xor or ^^	Logical XOR
not or !	Logical NOT
[n] […]	Substring operator

by Jeremy Stretch v2.0

WIRESHARK DISPLAY FILTERS · PART 2

packetlife.net

Frame Relay

fr.becn	fr.de
fr.chdlctype	fr.dlci
fr.control	fr.dlcore_control
fr.control.f	fr.ea
fr.control.ftype	fr.fecn
fr.control.n_r	fr.lower_dlci
fr.control.n_s	fr.nlpid
fr.control.p	fr.second_dlci
fr.control.s_ftype	fr.snap.oui
fr.control.u_modifier_cmd	fr.snap.pid
fr.control.u_modifier_resp	fr.snaptype
fr.cr	fr.third_dlci
fr.dc	fr.upper_dlci

PPP

ppp.address	ppp.direction
ppp.control	ppp.protocol

MPLS

mpls.bottom	mpls.oam.defect_location
mpls.cw.control	mpls.oam.defect_type
mpls.cw.res	mpls.oam.frequency
mpls.exp	mpls.oam.function_type
mpls.label	mpls.oam.ttsi
mpls.oam.bip16	mpls.ttl

ICMP

icmp.checksum	icmp.ident	icmp.seq
icmp.checksum_bad	icmp.mtu	icmp.type
icmp.code	icmp.redir_gw	

DTP

dtp.neighbor	dtp.tlv_type	vtp.neighbor
dtp.tlv_len	dtp.version	

VTP

vtp.code	vtp.vlan_info.802_10_index
vtp.conf_rev_num	vtp.vlan_info.isl_vlan_id
vtp.followers	vtp.vlan_info.len
vtp.md	vtp.vlan_info.mtu_size
vtp.md5_digest	vtp.vlan_info.status.vlan_susp
vtp.md_len	vtp.vlan_info.tlv_len
vtp.seq_num	vtp.vlan_info.tlv_type
vtp.start_value	vtp.vlan_info.vlan_name
vtp.upd_id	vtp.vlan_info.vlan_name_len
vtp.upd_ts	vtp.vlan_info.vlan_type
vtp.version	

ICMPv6

icmpv6.all_comp	icmpv6.option.name_type.fqdn
icmpv6.checksum	icmpv6.option.name_x501
icmpv6.checksum_bad	icmpv6.option.rsa.key_hash
icmpv6.code	icmpv6.option.type
icmpv6.comp	icmpv6.ra.cur_hop_limit
icmpv6.haad.ha_addrs	icmpv6.ra.reachable_time
icmpv6.identifier	icmpv6.ra.retrans_timer
icmpv6.option	icmpv6.ra.router_lifetime
icmpv6.option.cga	icmpv6.recursive_dns_serv
icmpv6.option.length	icmpv6.type
icmpv6.option.name_type	

RIP

rip.auth.passwd	rip.ip	rip.route_tag
rip.auth.type	rip.metric	rip.routing_domain
rip.command	rip.netmask	rip.version
rip.family	rip.next_hop	

BGP

bgp.aggregator_as	bgp.mp_reach_nlri_ipv4_prefix
bgp.aggregator_origin	bgp.mp_unreach_nlri_ipv4_prefix
bgp.as_path	bgp.multi_exit_disc
bgp.cluster_identifier	bgp.next_hop
bgp.cluster_list	bgp.nlri_prefix
bgp.community_as	bgp.origin
bgp.community_value	bgp.originator_id
bgp.local_pref	bgp.type
bgp.mp_nlri_tnl_id	bgp.withdrawn_prefix

HTTP

http.accept	http.proxy_authorization
http.accept_encoding	http.proxy_connect_host
http.accept_language	http.proxy_connect_port
http.authbasic	http.referer
http.authorization	http.request
http.cache_control	http.request.method
http.connection	http.request.uri
http.content_encoding	http.request.version
http.content_length	http.response
http.content_type	http.response.code
http.cookie	http.server
http.date	http.set_cookie
http.host	http.transfer_encoding
http.last_modified	http.user_agent
http.location	http.www_authenticate
http.notification	http.x_forwarded_for
http.proxy_authenticate	

by Jeremy Stretch v2.0

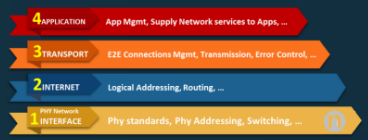
TCP/IP Model – Cheat Sheet (Network Walks) – Part-1 v1.2

What is TCP/IP Model ???

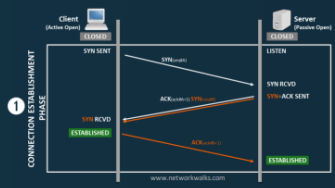
"TCP/IP Model is a standardised Reference Framework for conceptualising data communications between networks"

- ✓ Relevant RFC: RFC1122
- ✓ Also called 'Internet Model' or 'DoD Model'

TCP/IP Model Layers & their Functions



TCP 3-way Handshake Process



OSI Model Vs TCP/IP Model

OSI Model	TCP/IP Model
Mostly used for reference purposes only	Practical Model in use today
Released in 1984 by ISO	Released in 1970s by DARPA
Each layer participates in Error Handling	Only Transport Layer handles Errors
Not so simple Model (7 Layers)	Simple Model (4Layers only)
Session Layer does Connection Management	Transport Layer does Connection Mgmt
Data Formatting is done by Present. Layer	Data Formatting is done by Application Layer
Uses Horizontal Approach	Uses Vertical Approach
--- www.networkwalks.com	Trans Layer uses 3WHS + Sliding Windows
Transport Layer is Connection Oriented	Trans Layer can be Connection Oriented or not
Netw Layer can be Connection Oriented or not	Network Layer is always Connectionless
Services & protocols are clearly defined	Services & protocols are not clearly separated
A protocol independent Model	A Protocol dependent Model
Hosts do not handle network operations	Hosts participate in most network protocols

Transport Layer Ports

Category	Range	Comments
Well Known	0 - 1023	Used by system processes e.g. FTP(21)
Registered	1024 - 49151	For specific services e.g. Port 8080
Private	49152 – 65535	For Private purposes

Important Ports on Transport Layer

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
23	TCP	SSH
22	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (HTML)
110	TCP	POP3
161	UDP	SNMP

Protocols at each TCP/IP Layer

4	APPLICATION	DNS, DHCP, FTP, PDU, Telnet, POP3/IMAP, ...
3	TRANSPORT	TCP, UDP
2	INTERNET	IPv4, IPv6, OSPF, RIP, BGP, ICMP,...
1	PHY NETWORK INTERFACE	WiFi, USB, BT, RJ45, SDH, MW/RF, Ethernet, PPP, FR,...

www.networkwalks.com

Encapsulation:

"Preparing & passing the data by any Upper layer to the layer below it, is called Encapsulation"

(Means, going from the application layer all the way down to the physical layer)

Decapsulation:

"Decoding data while going Upwards from the physical layer till application layer is called decapsulation"

TCP/IP Model	OSI Model
APPLICATION	APPLICATION
	PRESENTATION
	SESSION
TRANSPORT	TRANSPORT
InterNETWORK / INTERNET	NETWORK
NETWORK INTERFACE (Subnet Layer)	DATA LINK
	PHYSICAL

www.networkwalks.com

Devices at each TCP/IP Layer

4	APPLICATION	End Devices (PC, Server, Phones), Firewalls, IDS, ...
3	TRANSPORT	Firewalls (Some), Load Balancers, ...
2	INTERNET	Routers, L3 Switches, ...
1	PHY NETWORK INTERFACE	Hubs/Rep, Modems, L2 Switches, Bridges, ...

www.networkwalks.com

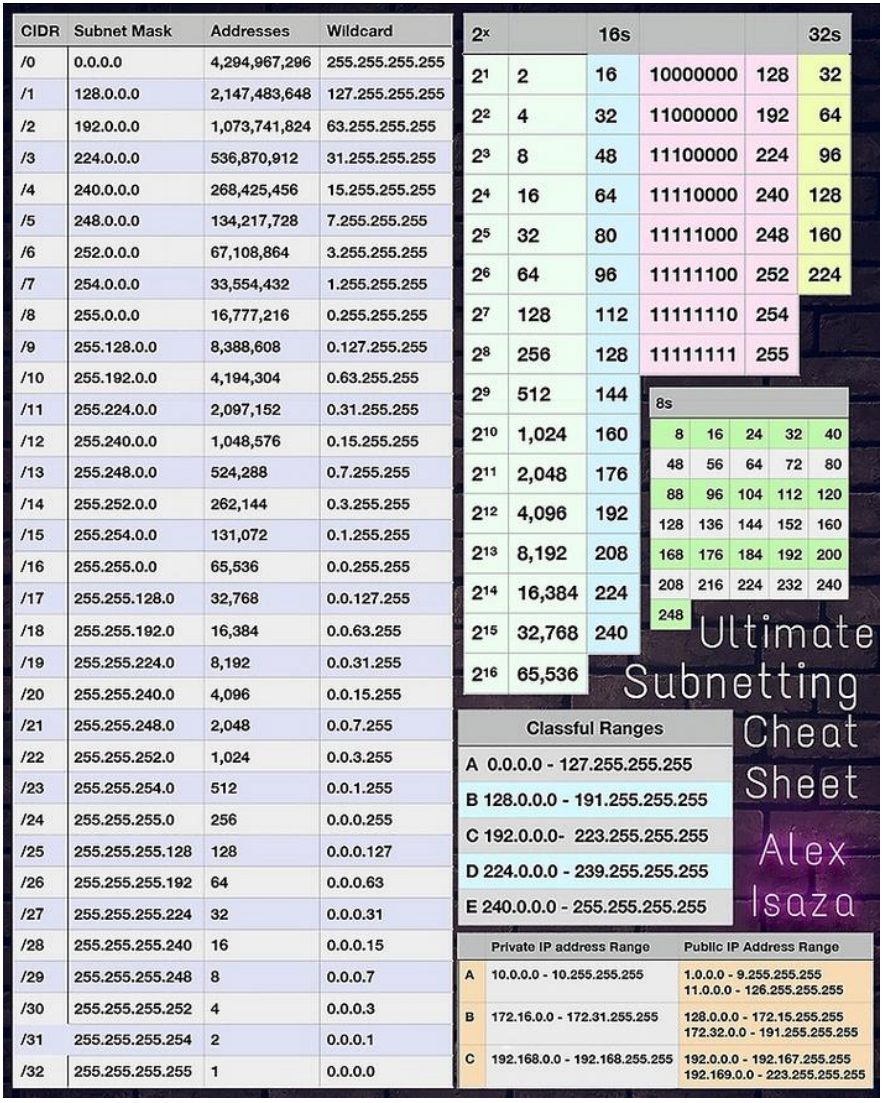
/Network Walks /NetworkWalks /company/networkwalks

Your Feedback, Comments are always Welcomed: info@networkwalks.com

New batch of Cisco CCNA is starting.
Enrol today with us for quality training: info@networkwalks.com
Visit our website & YouTube Channel for more FREE resources like:

- ✓ Cheatsheets, Interview Questions & Answers, Quiz, VCE exams & much more
- ✓ Labs & workbooks (Packet Tracer, GNS3, EVE-NG, ...)

Network Walks Training Academy (www.networkwalks.com)



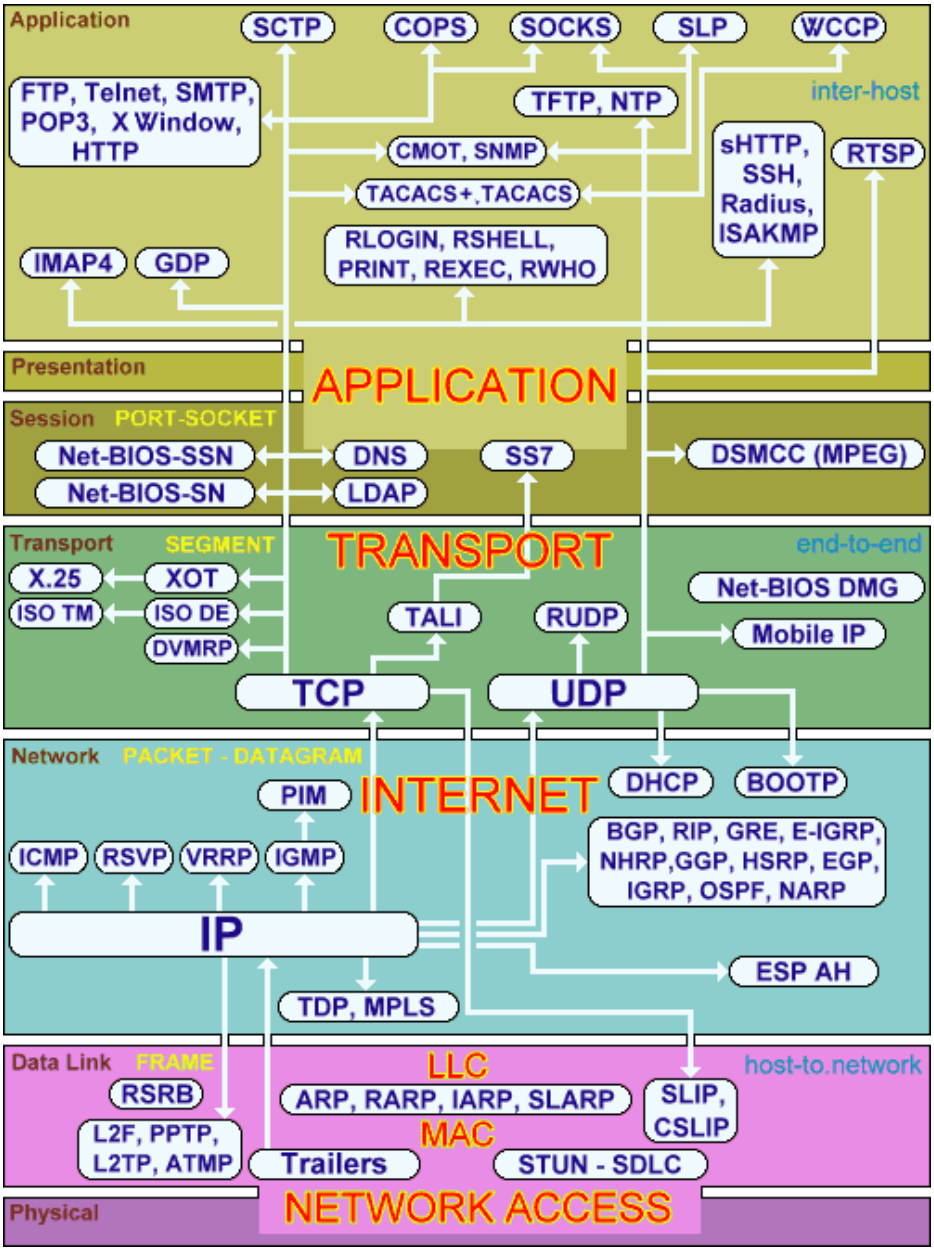
CIDR	Subnet Mask	Addresses	Wildcard
/0	0.0.0.0	4,294,967,296	255.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/4	240.0.0.0	268,425,456	15.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/13	255.248.0.0	524,288	0.7.255.255
/14	255.252.0.0	262,144	0.3.255.255
/15	255.254.0.0	131,072	0.1.255.255
/16	255.255.0.0	65,536	0.0.255.255
/17	255.255.128.0	32,768	0.0.127.255
/18	255.255.192.0	16,384	0.0.63.255
/19	255.255.224.0	8,192	0.0.31.255
/20	255.255.240.0	4,096	0.0.15.255
/21	255.255.248.0	2,048	0.0.7.255
/22	255.255.252.0	1,024	0.0.3.255
/23	255.255.254.0	512	0.0.1.255
/24	255.255.255.0	256	0.0.0.255
/25	255.255.255.128	128	0.0.0.127
/26	255.255.255.192	64	0.0.0.63
/27	255.255.255.224	32	0.0.0.31
/28	255.255.255.240	16	0.0.0.15
/29	255.255.255.248	8	0.0.0.7
/30	255.255.255.252	4	0.0.0.3
/31	255.255.255.254	2	0.0.0.1
/32	255.255.255.255	1	0.0.0.0

2^x		16s			32s
2^1	2	16	10000000	128	32
2^2	4	32	11000000	192	64
2^3	8	48	11100000	224	96
2^4	16	64	11110000	240	128
2^5	32	80	11111000	248	160
2^6	64	96	11111100	252	224
2^7	128	112	11111110	254	
2^8	256	128	11111111	255	
2^9	512	144			
2^{10}	1,024	160			
2^{11}	2,048	176			
2^{12}	4,096	192			
2^{13}	8,192	208			
2^{14}	16,384	224			
2^{15}	32,768	240			
2^{16}	65,536				

8s				
8	16	24	32	40
48	56	64	72	80
88	96	104	112	120
128	136	144	152	160
168	176	184	192	200
208	216	224	232	240
248				

Classful Ranges
A 0.0.0.0 - 127.255.255.255
B 128.0.0.0 - 191.255.255.255
C 192.0.0.0- 223.255.255.255
D 224.0.0.0 - 239.255.255.255
E 240.0.0.0 - 255.255.255.255

	Private IP address Range	Public IP Address Range
A	10.0.0.0 - 10.255.255.255	1.0.0.0 - 9.255.255.255 11.0.0.0 - 126.255.255.255
B	172.16.0.0 - 172.31.255.255	128.0.0.0 - 172.15.255.255 172.32.0.0 - 191.255.255.255
C	192.168.0.0 - 192.168.255.255	192.0.0.0 - 192.167.255.255 192.169.0.0 - 223.255.255.255


Application
SCTP
COPS
SOCKS
SLP
WCCP
FTP, Telnet, SMTP, POP3, X Window, HTTP
TFTP, NTP
inter-host
CMOT, SNMP
sHTTP, SSH, Radius, ISAKMP
RTSP
TACACS+,TACACS
RLOGIN, RSHELL, PRINT, REXEC, RWHO
IMAP4
GDP
Presentation
APPLICATION
Session
PORT-SOCKET
Net-BIOS-SSN
DNS
SS7
DSMCC (MPEG)
Net-BIOS-SN
LDAP
Transport
SEGMENT
TRANSPORT
end-to-end
X.25
XOT
Net-BIOS DMG
ISO TM
ISO DE
TALI
RUDP
Mobile IP
DVMRP
TCP
UDP
Network
PACKET - DATAGRAM
INTERNET
PIM
DHCP
BOOTP
BGP, RIP, GRE, E-IGRP, NHRP,GGP, HSRP, EGP, IGRP, OSPF, NARP
ICMP
RSVP
VRRP
IGMP
IP
ESP AH
TDP, MPLS
Data Link
FRAME
LLC
host-to.network
RSRB
ARP, RARP, IARP, SLARP
SLIP, CSLIP
L2F, PPTP, L2TP, ATMP
MAC
Trailers
STUN - SDLC
Physical
NETWORK ACCESS