

Class full(A,B,C,D,E)

Class less (CIDR , slash notation)

دسته بندی IP های class full

- A = 0 → 127 . X . X . X
- B = 128 → 191 . X . X . X
- C = 192 → 223 . X . X . X
- D = 224 → 239 . X . X . X → multicast
- E = 240 → 255 . X . X . X

IP های بدون کلاس

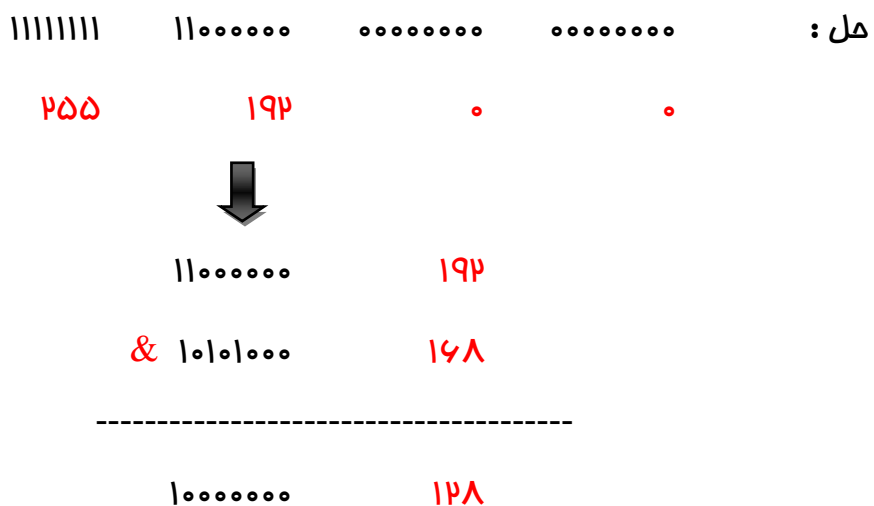
/8 → ۲۵۵.۰.۰.۰

/14 → ۲۵۵.۲۵۵.۰.۰

/۲۴ → ۲۵۵.۲۵۵.۲۵۵.۰

بدست آوردن subnet mask

مثال: ۱۹۲.۱۴۸.۲۱۹.۴۰ / ۱۰



۱۹۲.۱۴۸.۲۱۹.۴۰

& ۲۵۵.۱۹۲.۰.۰

۱۹۲.۱۲۸.۰.۰

Sub netting

مثال : فرض کنید یک شبکه با آدرس IP ۱۶ / ۱۷۲.۱۹.۰.۰ وجود دارد . می‌فواهیم این فضای IP را به چهار شبکه مساوی تقسیم کنیم . network address هر شبکه ، subnet mask ، IP های قابل استفاده و آدرس پخش همگانی هر زیر شبکه را پیدا کنید ؟

حل : ۲۵۵.۲۵۵.۰.۰ → ۱۶

۱۷۲.۱۹.۰.۰

& ۲۵۵.۲۵۵.۰.۰

۱۷۲.۱۹.۲۵۵.۲۵۵

Network address = ۱۷۲.۱۹.۰.۰

۱۷۲.۱۹.۰.۱ → ۱۷۲.۱۹.۲۵۵.۲۵۴

Br(broadcast) = ۱۷۲.۱۹.۲۵۵.۲۵۵

تعداد کل IP ها = $۲^{۱۶}$

تعداد IP های قابل استفاده = $۲^{۱۶} - ۲$

تعداد شبکه‌ها (۱۴) پس : $(۲^{۱۶} \div ۱۴) = (۲^{۱۶} \div ۲^۲) = ۲^{۱۴}$

شبکه اول :

Network address = ۱۷۲.۱۹.۰.۰

۱۷۲.۱۹.۰.۱ → ۱۷۲.۱۹.۶۳.۲۵۴

Br = ۱۷۲.۱۹.۶۳.۲۵۵

شبکه دوم :

Network address = ۱۷۲.۱۹.۶۴.۰

۱۷۲.۱۹.۶۴.۱ → ۱۷۲.۱۹.۱۲۷.۲۵۴

Br = ۱۷۲.۱۹.۱۲۷.۲۵۵

شبکه سوم :

Network address = ۱۷۲.۱۹.۱۲۸.۰

۱۷۲.۱۹.۱۲۸.۱ → ۱۷۲.۱۹.۱۹۱.۲۵۴

Br = ۱۷۲.۱۹.۱۹۱.۲۵۵

شبکه چهارم :

Network address = ۱۷۲.۱۹.۱۹۲.۰

۱۷۲.۱۹.۱۹۲.۱ → ۱۷۲.۱۹.۲۵۵.۲۵۴

Br = ۱۷۲.۱۹.۲۵۵.۲۵۵

برای بدست آوردن subnet mask فرمول زیر بکار می‌رود :

Subnet mask = mask + عدد توان ۲ بدست آمده subnet ها

سپس IP های باقی مانده (سمت راست تقسیم بندی) را معکوس می‌کنیم (۰ را به ۱ و یک را به ۰ تبدیل می‌کنیم) و حاصل را مناسبه می‌کنیم.

subnet mask = (۱۴ = ۲^۳) ۲ + ۱۶ = ۱۸ در مثال قبل :

	۱۷۲	۱۹	۰۰ ^{۱۸}].....	شبکه اول :
	۱۷۲	۱۹	۰۰ ^{۱۸}] ۱۱۱۱۱۱	۱۱۱۱۱۱۱۱	

	۱۷۲	۱۹	۶۳ (۲۵۵ - ۱۹۲)	۲۵۵	
	۱۷۲	۱۹	۰۱ ^{۱۸}].....	شبکه دوم :
	۱۷۲	۱۹	۰۱ ^{۱۸}] ۱۱۱۱۱۱	۱۱۱۱۱۱۱۱	

	۱۷۲	۱۹	۱۲۷ (۲۵۵ - ۱۲۸)	۲۵۵	
	۱۷۲	۱۹	۱۰ ^{۱۸}].....	شبکه سوم :
	۱۷۲	۱۹	۱۰ ^{۱۸}] ۱۱۱۱۱۱	۱۱۱۱۱۱۱۱	

	۱۷۲	۱۹	۱۹۱ (۲۵۵ - ۶۴)	۲۵۵	

شبکه چهارم :]۱۱^{۱۸} ۱۹ ۱۷۲

.....]۱۱^{۱۸} ۱۹ ۱۷۲

۲۵۵ (۲۵۵-۰) ۱۹ ۱۷۲ ۲۵۵

پروتکل ARP (تبدیل IP به آدرس فیزیکی)

ARP table = حافظه موقتی که جهت ذخیره سازی موارد جستجو مورد استفاده قرار می‌گیرد .

pending = p result = r free = f

پروتکل RARP (تبدیل آدرس فیزیکی به IP)

دستورات config نرم افزار cisco packet tracer

en → ورود به ترمینال روتر

conf t → ورود به کانفیگ روتر

int → نام پورت مربوطه

ip add → آیدی منتصب به پورت سابنت مسک آیدی

no shut → دستور فعال سازی پورت (هتماً بعد از آدرس آیدی باید وارد شود)

clock rate → یک عدد (مثلاً ۲۵۰۰۰۰) برای پورت‌های سریال دارای کلاک

دستور دادن static IP

router(config)# ip route آیدی شبکه سابنت مسک آیدی بعدی

دستور دادن DHCP IP

router(config)# ip DHCP pool یک نام

net آیدی شبکه سابنت مسک

default-router **آی پی دروازه عبور (گیت وی)**

DNS-server **آی پی دی ان اس**

دستور جهت ذخیره سازی IP ها در DHCP

router(config)# ip DHCP excluded-address **آی پی ابتدایی** **آی پی انتهایی**

دستور RIP

router(config)# router rip

network **آی پی های متصل به روتر جهت تبلیغ**

دستور access list (برای درک بهتر دستورات را به همراه چند مثال بیان می کنم)

نکته : wildcard mask معکوس subnet mask است مثلاً

subnet mask ۲۵۵.۰.۰.۰ ۱۹۲.۱۲۷.۰.۰

wildcard mask ۰.۲۵۵.۲۵۵.۲۵۵ ۶۳.۱۲۸.۲۵۵.۲۵۵ (۲۵۵-۱۲۷=۱۲۸ ...)

(deny) (permit) اجازه دسترسی نداشته باشد)

host در زمان افضصاص داده یک آی پی خاص مورد استفاده قرار می گیرد

eq یا echo در زمان فراخوانی پورت های خاص مانند ping و ... مورد استفاده قرار می گیرد

۱- می خواهیم شبکه ۱۰.۰.۰.۰ اجازه دسترسی به شبکه ۱۳.۰.۰.۰ را نداشته باشد .

```
access-list 70 deny 10.0.0.0 0.255.255.255
```

```
access-list 70 permit any
```

```
int f0/0
```

```
ip access-group 70 out
```

۲- می خواهیم IP ۱۰.۰.۰.۴۱ اجازه دسترسی به شبکه ۱۳.۰.۰.۰ را نداشته باشد .

```
access-list 50 deny host 10.0.0.41
```

```
access-list 50 permit any
```

```
int f0/0
```

```
ip access-group 50 out
```

۳- دسترسی IP ۱۰.۰.۰.۴۱ به IP ۱۳.۰.۰.۴ مسدود گردد .

```
access-list 100 deny ip host 10.0.0.41 host 13.0.0.4
access-list 100 permit ip any any
int f0/0
ip access-group 100 out
```

۴- اجازه ping گرفتن فقط به ip ۱۰.۰.۰.۴۱ از سرور ۱۳.۰.۰.۴ داده شود .

```
access-list 109 permit icmp host 10.0.0.41 host 13.0.0.4 echo
access-list 109 deny icmp any any
int f0/0
ip access-group 109 out
```

۵- سرور ۱۰.۰.۰.۴ بتواند با IP یا نام به وب سرور ۱۳.۰.۰.۳ و DNS سرور ۱۳.۰.۰.۴ دسترسی داشته باشد

```
access-list 179 permit tcp host 10.0.0.4 host 13.0.0.3 eq 80
access-list 179 permit udp host 10.0.0.4 host 13.0.0.4
access-list 179 deny tcp any any
access-list 179 deny udp any any
int f0/0
ip access-group 179 out
```

تکنیک nating (تبدیل چند IP نامعتبر به یک IP معتبر در شبکه)

نکته :

```
A class = ۱۰.۰.۰.۰ → ۱۰.۲۵۵.۲۵۵.۲۵۵
B class = ۱۷۲.۱۶.۰.۰ → ۱۷۲.۳۱.۲۵۵.۲۵۵
C class = ۱۹۲.۱۶۸.۰.۰ → ۱۹۲.۱۶۸.۲۵۵.۲۵۵
```

دستور

```
router(config)# ip route (آی پی بعدی) سابنت مسک (۰.۰.۰.۰) آی پی شبکه (۰.۰.۰.۰)
int f0/0 (پورت شبکه داخلی)
Router(config-if)# ip nat outside
int f0/1 (پورت شبکه خارجی)
```

Router(config-if)# ip nat inside

ex

router(config)# ip nat inside source static **آی پی بعدی** **آی پی سیستم** **برای یک کامپیوتر**

router(config)# access-list 50 permit **آی پی شبکه** **وایدکار مسک** **برای یک شبکه**

ip nat inside source list 50 int **پورت متصل به اینترنت**

دستور passive

router(config)# router rip

passive-interface **پورت متصل به شبکه داخلی**

net **آی پی**

دستور eigrp

router(config)# eigrp **یک عدد**

net **آی پی های متصل به روتر** **وایدکار مسک**