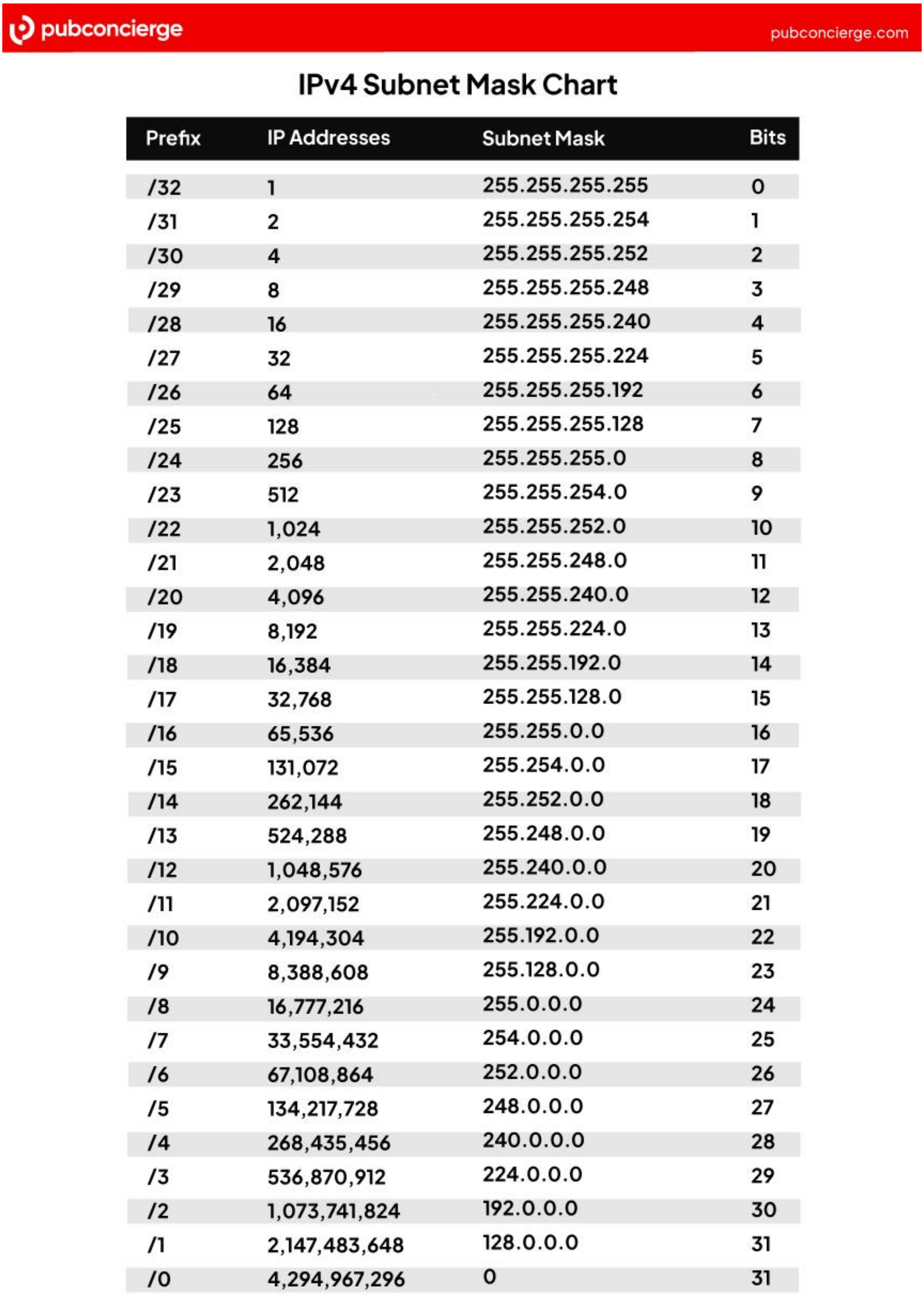
Cisco Packet Tracer: Commands

1. VLSM: Calculating IP Pools – Alhálózatok számítása



pubconcierge

pubconcierge.com

IPv4 Subnet Mask Chart

Prefix	IP Addresses	Subnet Mask	Bits
/32	1	255.255.255.255	0
/31	2	255.255.255.254	1
/30	4	255.255.255.252	2
/29	8	255.255.255.248	3
/28	16	255.255.255.240	4
/27	32	255.255.255.224	5
/26	64	255.255.255.192	6
/25	128	255.255.255.128	7
/24	256	255.255.255.0	8
/23	512	255.255.254.0	9
/22	1,024	255.255.252.0	10
/21	2,048	255.255.248.0	11
/20	4,096	255.255.240.0	12
/19	8,192	255.255.224.0	13
/18	16,384	255.255.192.0	14
/17	32,768	255.255.128.0	15
/16	65,536	255.255.0.0	16
/15	131,072	255.254.0.0	17
/14	262,144	255.252.0.0	18
/13	524,288	255.248.0.0	19
/12	1,048,576	255.240.0.0	20
/11	2,097,152	255.224.0.0	21
/10	4,194,304	255.192.0.0	22
/9	8,388,608	255.128.0.0	23
/8	16,777,216	255.0.0.0	24
/7	33,554,432	254.0.0.0	25
/6	67,108,864	252.0.0.0	26
/5	134,217,728	248.0.0.0	27
/4	268,435,456	240.0.0.0	28
/3	536,870,912	224.0.0.0	29
/2	1,073,741,824	192.0.0.0	30
/1	2,147,483,648	128.0.0.0	31
/0	4,294,967,296	0	31

2. Devices – Eszközök
   Router: 1941
   Switch: 2960
   WiFi: WRT300N
   ! Portokra odafigyelni !

3. Basic Configuration – Alap konfiguráció

```
banner motd "Unauthorized access is prohibited"

enable secret zipi-pass

no ip domain-lookup

ip domain-name zipi.net

hostname []

crypto key gen rsa

1024

ip ssh version 2

service password-encryption


line con 0

enable secret zipi-ssh


line vty 0 15

enable secret zipi-pass

line vty 0 15

login local

transport input ssh

exit
```

4. SSH
   ```
   username admin secret admin

   crypto key generate rsa
   1024

   line vty 0 4
   transport input ssh
   login local
   ```

5. VLAN létrehozása
   ```
   int g0/0.10
   encapsulation dot1q (vlan száma)
   ip cím – alhálózati maszk
   ip helper address 0.0.0.0
   ```

6. ETHERCHANNEL
   ```
   interface range ()
   channel-group (szám) mode active
   interface port-channel (szám)
   switchport mode trunk
   ```

7. VTP
   ```
   vtp domain (domain név)
   vtp mode server/client
   vtp password (jelszó)
   ```

8. ROUTING

   RIP, OSPF, EIGRP, BGP

   redistribute számok eigrp-nél: 1544 100 255 1 100

9. Statikus NAT

```
R2(config)# ip nat inside source static 192.168.10.2 195.1.1.3
R2(config)# interface g0/0
R2(config-if)# ip address 192.168.10.1 255.255.255.0
R2(config-if)# ip nat inside
R2(config-if)# interface g0/1
R2(config-if)# ip address 195.1.1.2 255.255.255.0
R2(config-if)# ip nat outside
```

Dinamikus NAT

```
R2(config)# ip nat pool NAT-POOL1 195.1.1.3 195.1.1.10 netmask
255.255.255.0
R2(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R2(config# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface g0/0
R2(config-if)# ip nat inside
R2(config)# interface g0/1
R2(config-if)# ip nat outside
```

10. Redistribute

OSPF

```
router ospf 25 redistribute eigrp 15 subnets redistribute rip subnets
```

EIGRP

```
router eigrp 15 redistribute ospf 25 metric 1544 100 255 1 100
redistribute rip metric 1544 100 255 1 100
```

RIP

```
router rip version 2
redistribute ospf 25 (metric 2)
redistribute eigrp 15 (metric 2)
```

11. ACL

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# interface g0/0
Router(config-if)# ip access-group 1 in
```

12. Extended ACL

```
Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 10.0.0.10 eq 80
Router(config)# interface g0/0
Router(config-if)# ip access-group 100 in
```

13. ACL Példa

```
ACL 100 - VLAN100 ne érje el az FTP szervert (port 21)
access-list 100 deny tcp 192.168.100.0 0.0.0.255 host 198.162.40.1 eq 21
access-list 100 permit ip any any


ACL 101 - VLAN101 ne érje el a HTTPS szervert (port 443)
access-list 101 deny tcp 172.101.0.0 0.0.255.255 host 198.162.40.1 eq 443
access-list 101 permit ip any any

ACL 110 - Tartomány 1 ne pingelje Tartomány 4-et
access-list 110 deny icmp 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 110 permit ip any any


ACL-ek alkalmazása interfészeken (példák)



! VLAN100 felől jövő forgalom (FTP tiltás)
interface g0/1
 ip access-group 100 in

! VLAN101 felől jövő forgalom (HTTPS tiltás)
interface g0/2
 ip access-group 101 in

! Tartomány 1 kijáratán
interface g0/0
 ip access-group 110 out

! Tartomány 6 kijáratán
interface g0/3
 ip access-group 111 out

! Tartomány 3 kijáratán
interface g0/4
 ip access-group 112 out
```

```
! Tartomány 4 és 5 belépő interfészein ROUTER0 előtt
interface g0/0
 ip access-group 113 in
```