

Campus Networks
Layer 3

IP address planning & Inter-VLAN routing

Author:
Sami Ait Ali Oulahcen

Nouakchott, Mauritania
17-22 February 2025

Internet Protocol addresses

IPv4 and IPv6 addresses quick review

Internet Protocol

- Devices on the Internet communicate using Internet Protocol addresses
- Currently 2 types of Internet Protocol (IP) addresses:
    - IPv4: legacy Internet Protocol
    - IPv6: current Internet Protocol
- When we use both types on a network, it is called **dual stack**

IPv4 addresses

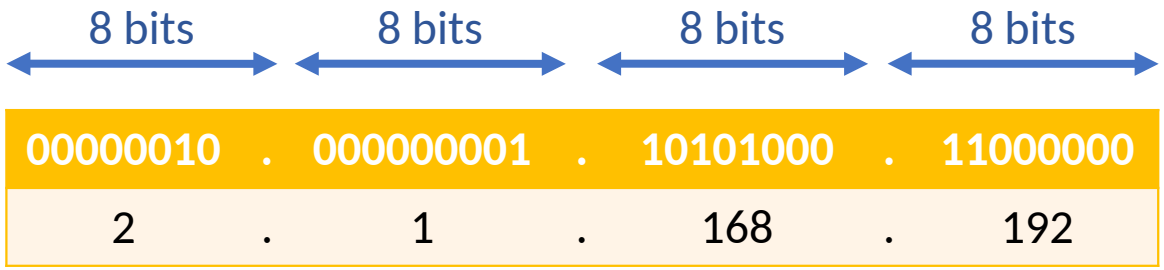
- 32-bits binary numbers
- Written as 4 decimals of 8 bits separated by dots (.)

00000010	.	000000001	.	10101000	.	11000000
2	.	1	.	168	.	192

- Total number of IPv4 addresses is 2^{32} = 4,294,967,296
- But in reality, about 3,702,258,432 available after removing:
  - 0.0.0.0/8 Current network RFC 6890 and 127.0.0.0/8 Loopback
  - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 Private network RFC 1918
  - 224.0.0.0/4 IP multicast RFC 5771 and some others.

IPv4 addresses binary to decimals

- Let’s do some algebra

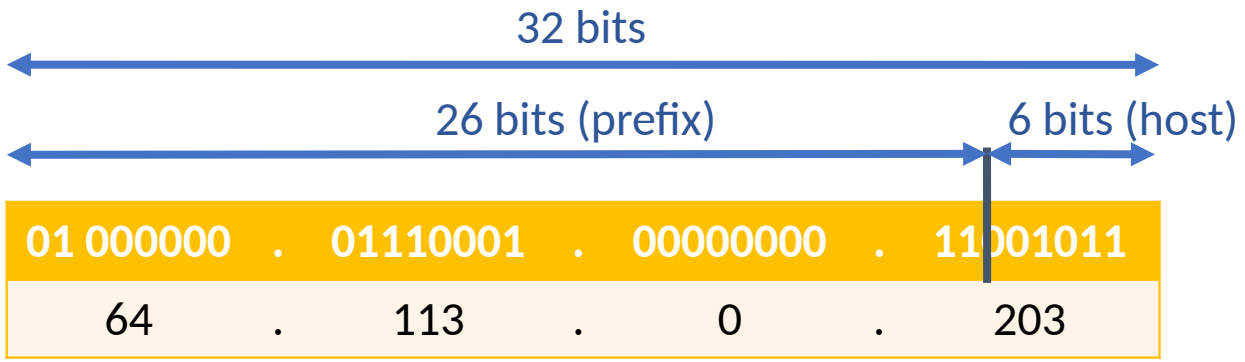


- Why is 10101000 = 168 ?
- $1x2^7 + 0x2^6 + 1x2^5 + 0x2^4 + 1x2^3 + 0x2^2 + 0x2^1 + 0x2^0 = 128 + 32 + 8 = 168$

IPv4 prefixes

- A group of contiguous IP addresses can be represented as a subnet

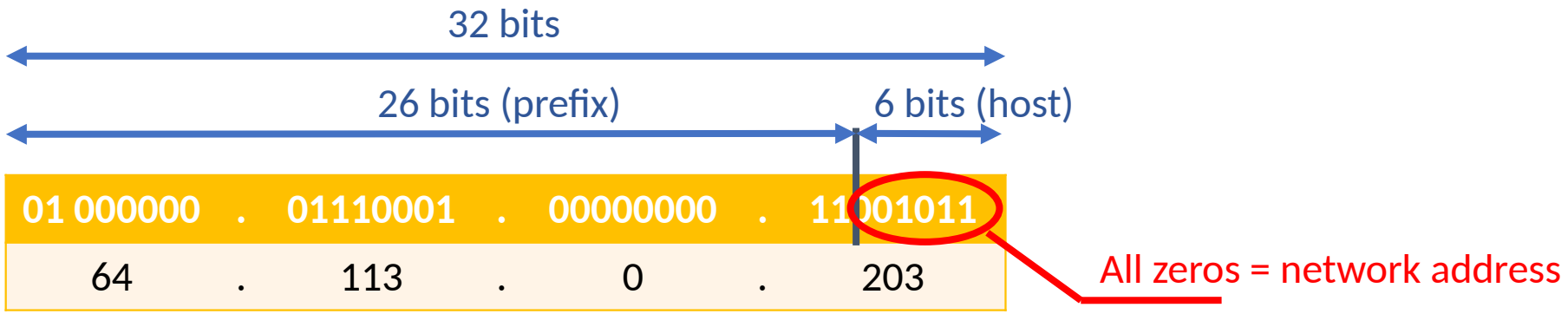
203.0.113.64/26



IPv4 prefixes

- A group of contiguous IP addresses can be represented as a subnet

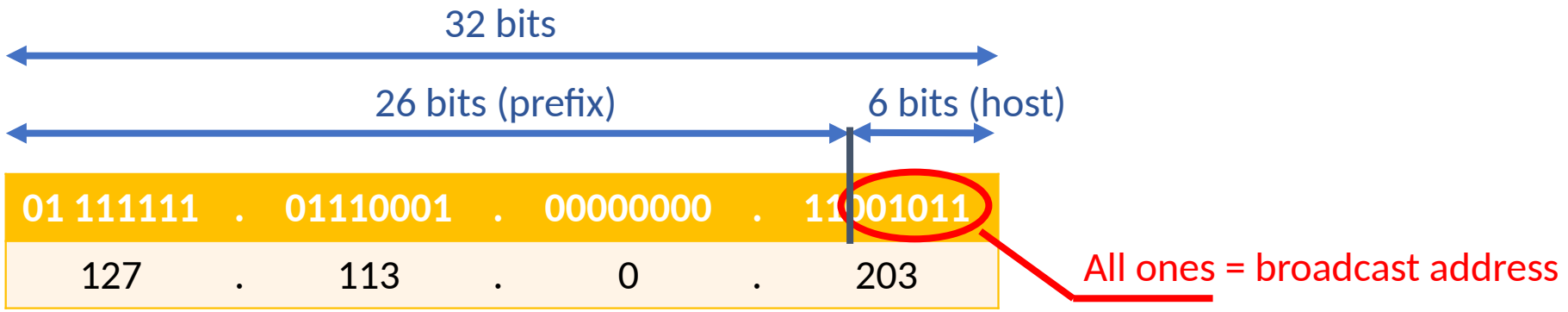
203.0.113.64/26



IPv4 prefixes

- A group of contiguous IP addresses can be represented as a subnet

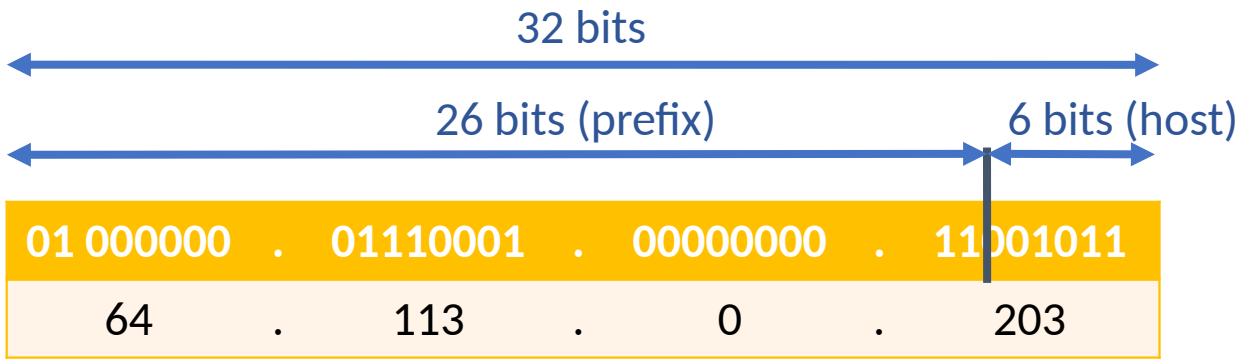
203.0.113.64/26



IPv4 prefixes

- A group of contiguous IP addresses can be represented as a subnet

  203.0.113.64/26



- Number of usable addresses is $2^6 - 2 = 62$

IPv4 rules

- Devices on the same layer 2 network should have the same prefix
- Devices on the same prefix, must have different host IDs
- The first and last addresses of a subnet are reserved (*)

(*) The only exceptions are point-to-point links i.e. /31s

IPv6 addresses

- 128-bits binary numbers
- Written as hexadecimal **words** of 16 bits separated by **colons** (:)

0000 0000 0001 0101	:	0000 0000 0000 0000	:	0000 0000 0000 0000	:	0000 0000 0000 0000	:	1010 0110 0000 1110	:	0000 0000 0000 0000	:	0000 1101 1011 1000	:	0010 0000 0000 0001
0015	:	0000	:	0000	:	0000	:	A60E	:	0000	:	0DB8	:	2001

- Total number of IPv6 addresses: 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456
- In reality the only routable addresses currently are in 2001::/3

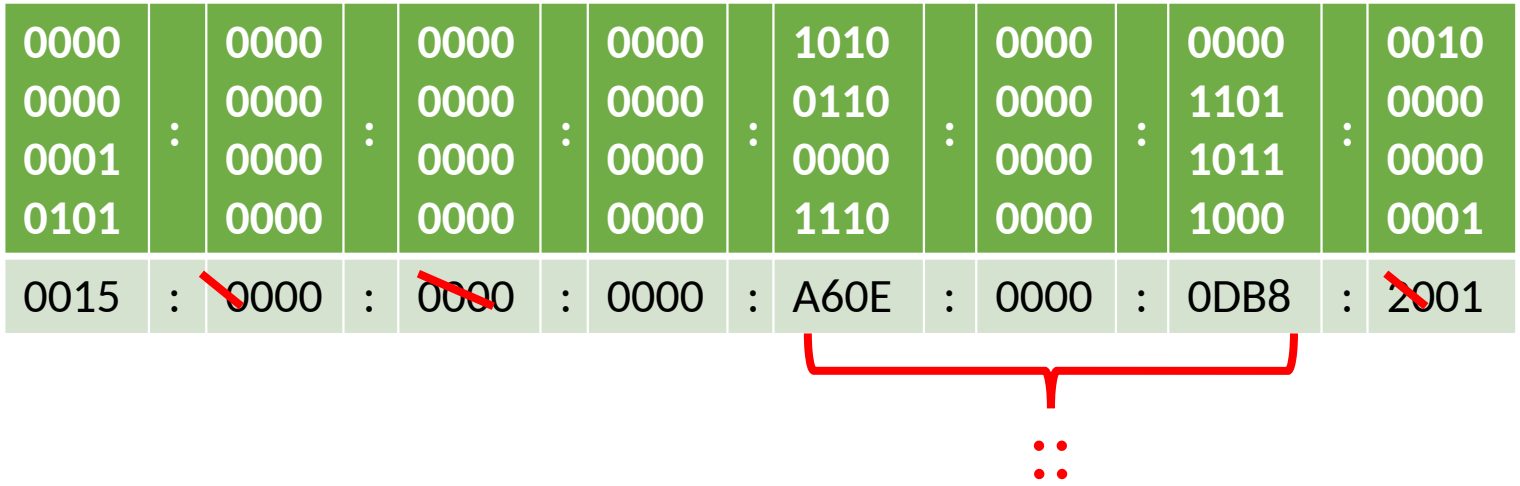
IPv6 address conventions

- Leading zeros can be dropped

0000 0000 0001 0101	:	0000 0000 0000 0000	:	0000 0000 0000 0000	:	0000 0000 0000 0000	:	1010 0110 0000 1110	:	0000 0000 0000 0000	:	0000 1101 1011 1000	:	0010 0000 0000 0001
0015	:	~~0~~000	:	~~0000~~	:	0000	:	A60E	:	0000	:	0DB8	:	~~2~~001

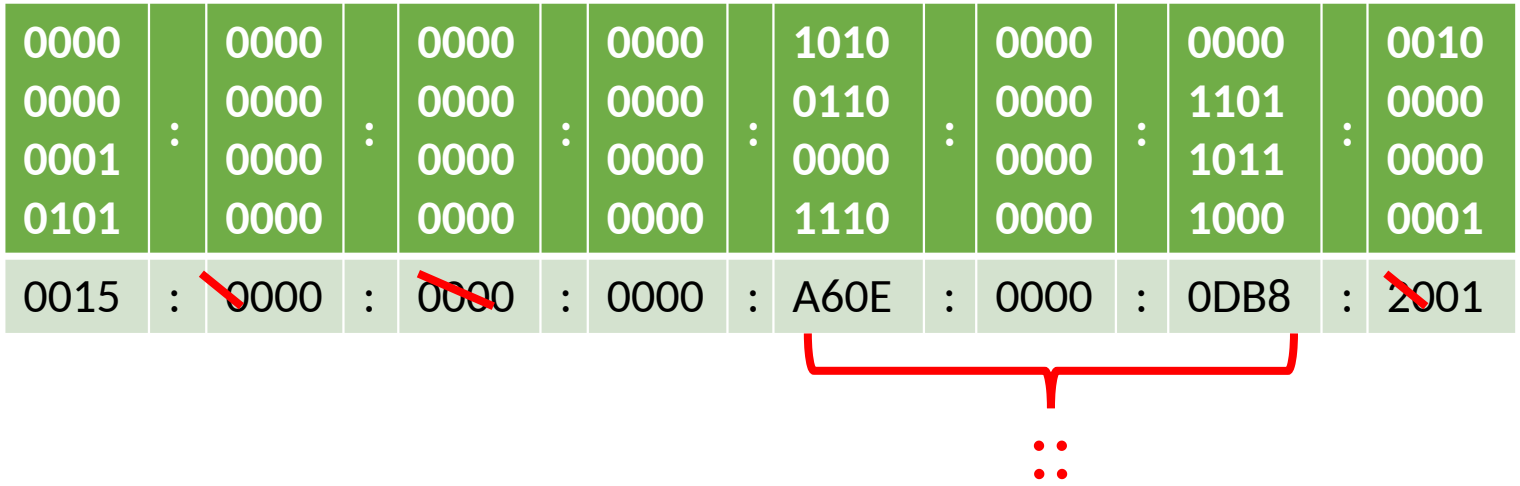
IPv6 address conventions

- Leading zeros can be dropped
- Largest number of all-zero words can be replaced by double colons (::)



IPv6 address conventions

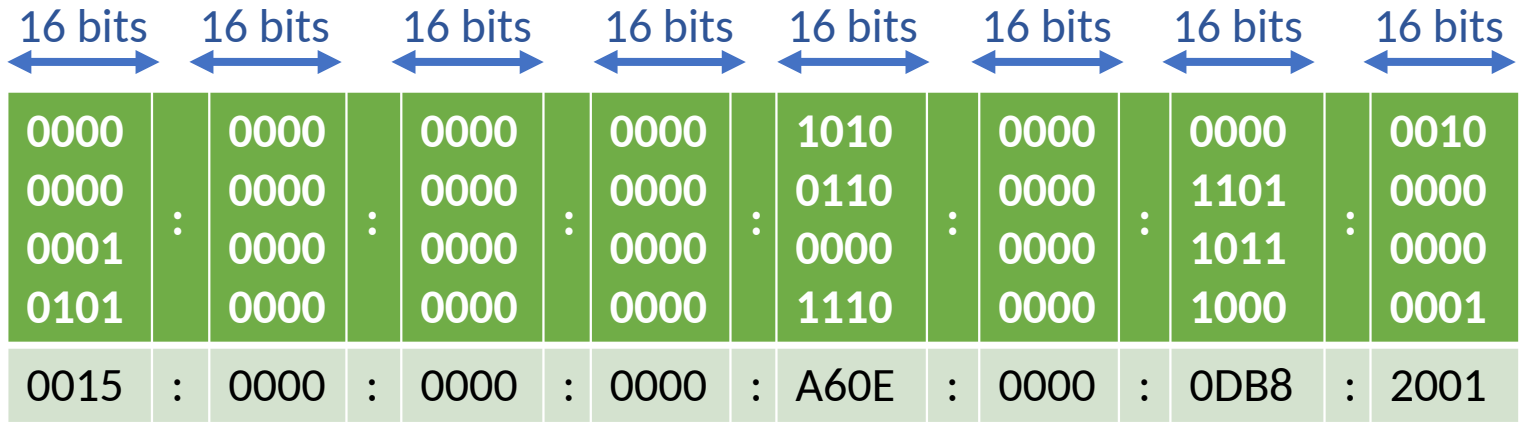
- Leading zeros can be dropped
- Largest number of all-zero words can be replaced by double colons (::)



- The result would be **2001:DB8:0:A60E::15**

IPv6 binary to hexadecimal

- Let's do some algebra

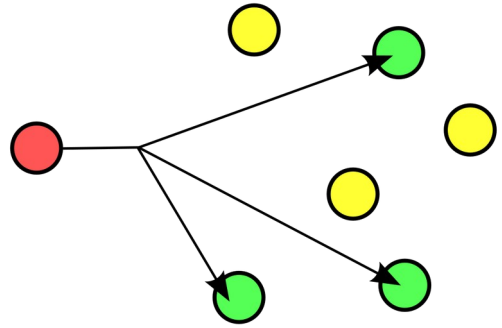


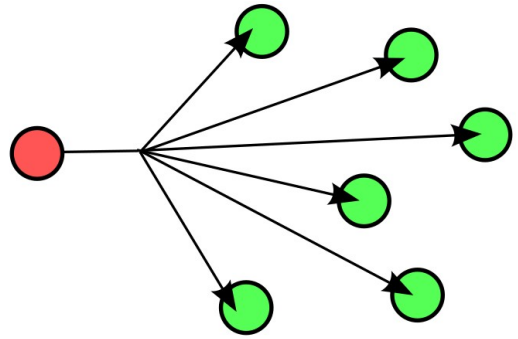
A = 10
B = 11
C = 12
D = 13
E = 14
F = 15

- Why is 1010 0110 0000 1110 = A60E ?
- $1x2^3+0x2^2+1x2^1+0x2^0$=**10** similarly 0110=**6**, 0000=**0**, and 1110=**14**
- Refer to table on the right for decimals above 10, and you get **A 6 0 E**

IPv6 multicast

- In IPv6, there is no **broadcast,** only multicast
- **Examples:**
- **fe00::0 ip6-localnet**
- **ff00::0 ip6-mcastprefix**
- **ff02::1 ip6-allnodes (where RAs are sent)**
- **ff02::2 ip6-allrouters (for router discovery)**
- **ff02::3 ip6-allhosts**
- **:: all-interfaces**





IPv6 rules

- Every subnet is a /64 (*)
- Devices on the same prefix, must have different host IDs
- First (all zeros) address is reserved (*)

- (*) The only exceptions are point-to-point links i.e. /127s

How to obtain IP addresses

- From your REN or ISP

RIMER



- Directly from the RIR



IP address planning

How to establish an IPv4/IPv6 address plan and corresponding VLANs

Establish an address plan

- The typical allocation for an end-site campus is:
    - /24 to /22 in ipv4
    - /48 to /44 in ipv6
- Usable VLAN numbers from 2 to 4096
- Numbering your buildings helps in assigning VLAN numbers:
    - Administration : Building 1
    - Engineering : Building 2
    - Arts : Building 3

Establish an address plan

- The typical allocation for an end-site campus is:
  - /24 to /22 in ipv4 => 2^8 to 2^{10} => 256 to 1024 addresses
  - /48 to /44 in ipv6 => 2^{16} to 2^{20} => 65,536 to 1,048,576 subnets
- Identify the need for IP addresses in each part of the campus

Number of devices	Campus location
100	Network Core
1000	Building 1
2500	Building 2
340	Building 3
450	Building 4

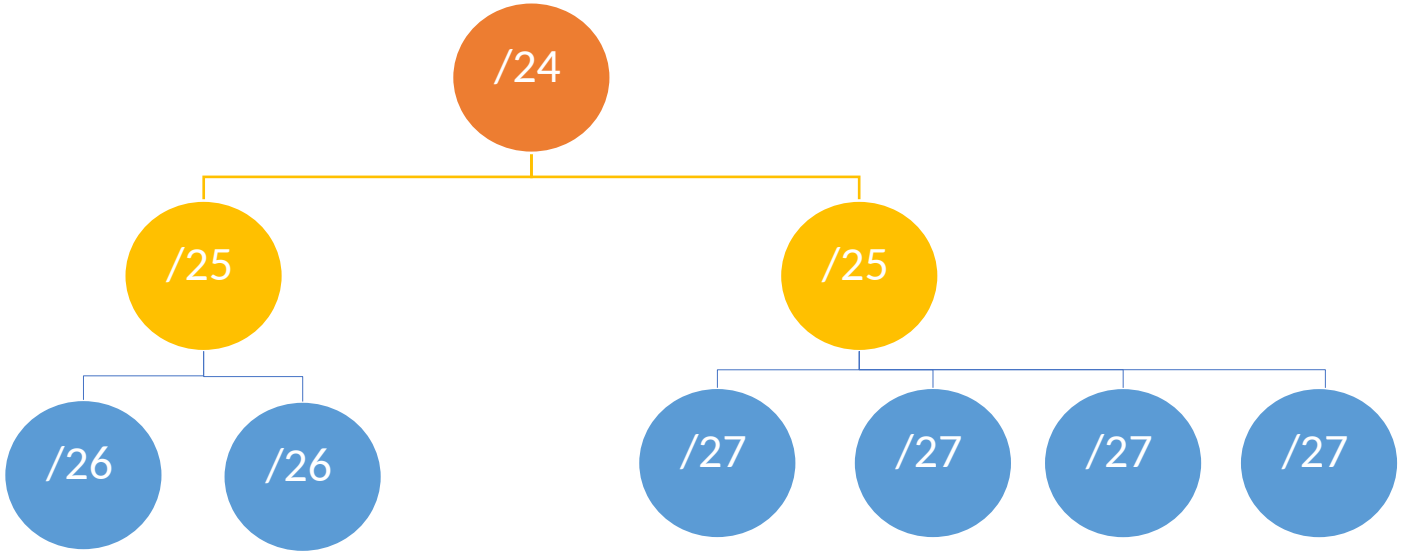
Establish an address plan

- The typical allocation for an end-site campus is:
  - /24 to /22 in ipv4 => 2^8 to 2^{10} => 256 to 1024 addresses
  - /48 to /44 in ipv6 => 2^{16} to 2^{20} => 65,536 to 1048576 subnets
- Identify the need for IP addresses in each part of the campus
- Address plan should be future-proof to avoid renumbering

  => When subnetting, allow sufficient space for expansion

Subnetting

- When subnetting in ipv4, half your /24 will probably go to NAT
- For a healthy NAT, one IP for each 10-24 users
- We will use 203.0.113.0/24 and 10.0.0.0/8 for IPv4
- And 2001:db8:d1::/48 for IPv6



Address plan example for IPv4

Usage	Subnets
Public IPv4 allocation	203.0.113.0/24
Private IPv4 Address space (RFC 1918)	10.0.0.0/8

Usage	Subnets
Public servers	203.0.113.0/26
P2P links and future use	203.0.113.64/26
NAT	203.0.113.128/25
Core network	10.0.0.0/16
Building X	10.X.0.0/16
Management	10.250.0.0/16
IP cameras	10.240.0.0/16
IP phones	10.230.0.0/16

Address plan example for IPv4

Usage	Subnets
Public IPv4 allocation	203.0.113.0/24
Private IPv4 Address space (RFC 1918)	10.0.0.0/8

Usage	Subnets
Public servers	203.0.113.0/26
P2P links and future use	203.0.113.64/26
NAT	
NOC	
Building X	
Management	
IP cameras	
IP phones	10.230.0.0/16

VLAN	Usage	Subnets
X11	Classrooms	10.X.11.0/24
X13	Offices	10.X.13.0/24
X16	Labs	10.X.16.0/24
X32	Wifi	10.X.32.0/24

Address plan example for IPv4

Usage	Subnets
Public IPv4 allocation	203.0.113.0/24
Private IPv4 Address space (RFC 1918)	10.0.0.0/8

Usage	Subnets
Public servers	203.0.113.0/26
P2P links and future use	203.0.113.64/26
NAT	203.0.113.128/25
NOC	
Building X	
Management	
IP cameras	
IP phones	

VLAN	Usage	Subnets
2501	Management for Building 1	10.250.1.0/24
2502	Management for Building 2	10.250.2.0/24
…	..	…
250Y	Management for Building Y	10.250.Y.0/24

Address plan example for IPv4

Usage	Subnets
Public IPv4 allocation	203.0.113.0/24
Private IPv4 Address space (RFC 1918)	10.0.0.0/8

Usage	Subnets
Public servers	203.0.113.0/26
P2P links and future use	203.0.113.64/26
NAT	203.0.113.128/25
NOC	
Building X	
Management	
IP cameras	
IP phones	

VLAN	Usage	Subnets
2401	IP Cameras for Building 1	10.240.1.0/24
2402	IP Cameras for Building 2	10.240.2.0/24
…	..	…
240Y	IP Cameras for Building Y	10.240.Y.0/24

Address plan example for IPv6

Usage	Subnets
Public IPv6 allocation	2001:db8:d1::/48

Usage	Subnets
Public servers	2001:db8:d1:A203::/64
P2P links	2001:db8:d1:B203::/64
NAT	N/A
Core network	2001:db8:d1::/56
Building X	2001:db8:d1:X00::/56
Management	2001:db8:d1:FA00::/56
IP cameras	2001:db8:d1:F000::/56
IP phones	2001:db8:d1:E600::/56

Address plan example for IPv6

Usage	Subnets
Public IPv6 allocation	2001:db8:d1::/48

Usage	Subnets
Public servers	2001:db8:d1:A203::/64
P2P links	2001:db8:d1:B203::/64
NAT	
Core network	
Building X	
Management	
IP cameras	
IP phones	2001:db8:d1:E600::/56

VLAN	Usage	Subnets
X11	Classrooms	2001:db8:d1:X11::/64
X13	Offices	2001:db8:d1:X13::/64
X16	Labs	2001:db8:d1:X16::/64
X32	Wifi	2001:db8:d1:X32::/64

Address plan example for IPv6

Usage	Subnets
Public IPv6 allocation	2001:db8:d1::/48

Usage	Subnets
Public servers	2001:db8:d1:A203::/64
P2P links	2001:db8:d1:B203::/64
NAT	N/A
Core network	
Building X	
Management	
IP cameras	
IP phones	

VLAN	Usage	Subnets
2501	Management for Building 1	2001:db8:d1:FA01::/64
2502	Management for Building 2	2001:db8:d1:FA02::/64
…	..	…
250Y	Management for Building Y	2001:db8:d1:FA0Y::/64

Address plan example for IPv6

Usage	Subnets
Public IPv6 allocation	2001:db8:d1::/48

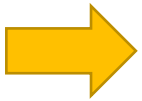
Usage	Subnets
Public servers	2001:db8:d1:A203::/64
P2P links	2001:db8:d1:B203::/64
NAT	N/A
Core network	2001:db8:d1::/56
Building X	
Management	
IP cameras	
IP phones	

VLAN	Usage	Subnets
2401	IP Cameras for Building 1	2001:db8:d1:F001::/64
2402	IP Cameras for Building 2	2001:db8:d1:F002::/64
…	..	…
240Y	IP Cameras for Building Y	2001:db8:d1:F00Y::/64

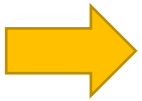
Static IP addressing on Debian

Modify the network interfaces file:

```
sudo vi /etc/network/interfaces
```



```
source /etc/network/interfaces.d/*
auto lo
iface lo inet loopback
allow-hotplug ens18
iface ens18 inet6 static
        address 2001:db8:f1:d::230
        netmask 64
        gateway 2001:db8:f1:d::129
        dns-nameservers
2001:db8:f1:d::53 2001:db8:f1:e::53
iface ens18 inet static
        address 203.0.113.230
        netmask 25
        gateway 203.0.113.129
```

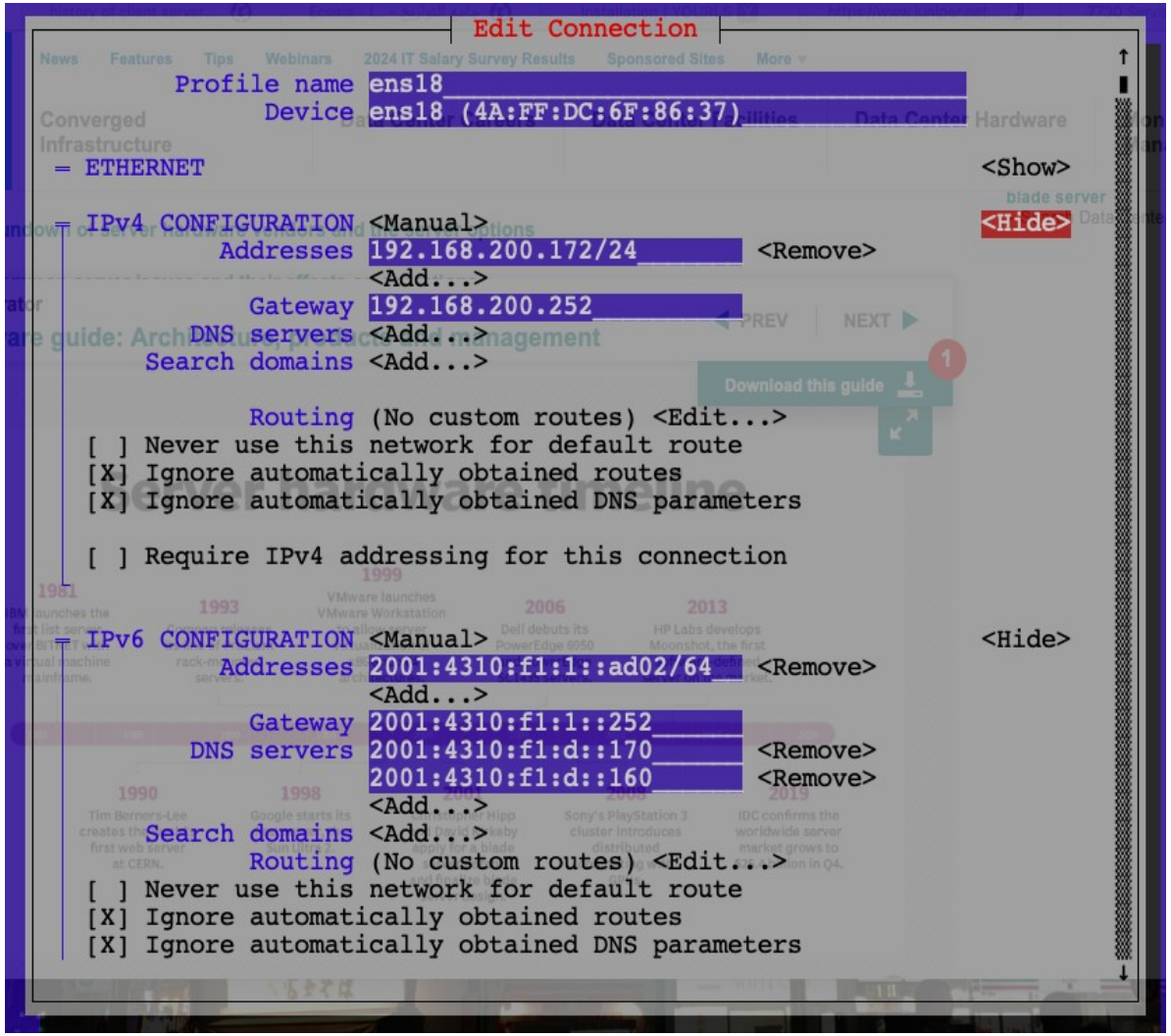


Then restart the networking daemon:

```
sudo systemctl restart networking
```

Static IP addressing on RHEL / Rocky / Alma

- Type “`nmtui`”, then choose “Edit a connection”, and choose the interface you want to set up (in our case “ens18”)



- To apply changes you have 2 options:

- If you are connected via console, you can Deactivate / Activate the interface in nmtui

- If you are connected via SSH, you can “`systemctl restart NetworkManager`”

Inter-VLAN routing

Routing traffic between VLANs at the core

Core switch

- Why it’s always best to route inter-vlan traffic at the core:
  - Closer to your STP root
  - Can isolate infected VLANs
  - Easier for applying filters: who can see management network…
- Equipment needed is a router/firewall (router on a stick) or a layer 3 switch

Routed VLAN interfaces

- IP addresses on VLAN interfaces or sub.interfaces

```
interface ge11
    no switchport
interface ge11.213
    encapsulation dot1q 213
    ip address 10.2.13.1/24
    ipv6 address 2001:db8:d1:213::1/64
```

```
interface ge11
    switchport mode trunk
    switchport trunk allowed 213
interface vlan 213
    ip address 10.2.13.1/24
    ipv6 address 2001:db8:d1:213::1/64
```

- Used as a default gateway on all interfaces connected to the VLAN
- Routing datagrams according to:
    - static routes
    - routing protocol (IS-IS or OSPF)

Useful ACLs on your core switch

For outgoing connections, deny known problematic ports:

deny tcp any any eq 25 --- mail not trough our mx

deny tcp any any range 135 139 --- netbios

deny udp any any range 135 139 --- netbios

deny tcp any any eq 445 --- SMB

Deny all traffic to management VLAN except from IT team

allow ip 10.0.0.0/24 10.250.0.0/16

deny ip any 10.250.0.0/16

Questions ?