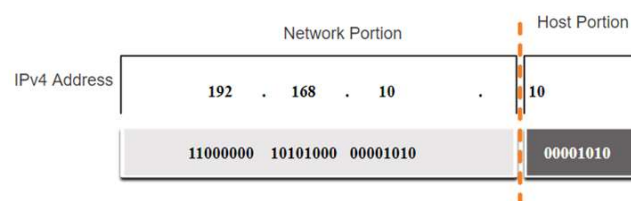


Computer Networks - Hoofdstuk 11 - IPv4 Addressing

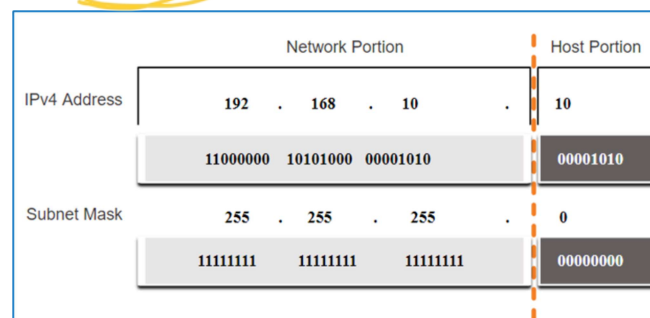
IPv4 Address Structure

- Een IPv4 adres is een 32-bit hiërarchisch adres dat bestaat uit een *netwerkgedeelte* en een *hostgedeelte*
- We gebruiken een *subnet mask* om het netwerkgedeelte en het hostgedeelte te bepalen van het adres.



The Subnet Mask

- Om de netwerk- en hostgedeelten van een IPv4 adres te bepalen vergelijken we de binaire waarde van het IPv4 adres en die van het subnet mask.
- We voeren hierop een *bitwis AND* op uit.



The Prefix Length

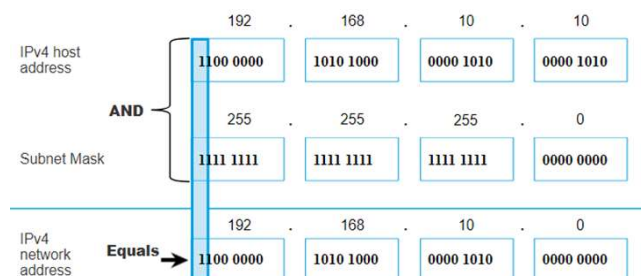
- Een prefix-lengte is een eenvoudigere manier om een subnet mask te identificeren.
- Deze prefix-lengte komt overeen met het aantal bits men op 1 een plaats voor het subnet mask.
- Meestal schrijven we deze in een "/"-notatie

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Determining the Network: Logical AND

We gebruiken een logische EN operator om het netwerk-adres te bepalen.

We voeren deze operatie uit tussen het host IPv4 adres en het subnet mask.



Network, Host, and Broadcast Addresses

Binnen elk netwerk zijn er drie type IP adressen:

- het netwerk adres
- het host adres
- het broadcast adres

	Network Portion			Host Portion	Host Bits
Subnet mask 255.255.255.0 or /24	255	255	255	0	
	11111111	11111111	11111111	00000000	
Network address 192.168.10.0 or /24	192	168	10	0	All 0s
	11000000	10100000	00001010	00000000	
First address 192.168.10.1 or /24	192	168	10	1	All 0s and a 1
	11000000	10100000	00001010	00000001	
Last address 192.168.10.254 or /24	192	168	10	254	All 1s and a 0
	11000000	10100000	00001010	11111110	
Broadcast address 192.168.10.255 or /24	192	168	10	255	All 1s
	11000000	10100000	00001010	11111111	

IPv4 Unicast, Broadcast and Multicast

- Bij **unicast** wordt er een pakket verstuurd naar één IP adres.
- Bij **broadcast** wordt een pakket naar alle IP adressen verstuurd
- Bij **multicast** wordt een pakker naar een multicast groep verstuurd.

Types of IPv4 Address

Zoals beschreven in RFC 1918, zijn publieke IPv4 adressen globaal geroute tussen de verschillende ISP (Internet Service Providers)

- Private IP adressen zijn veel voorkomende blokken IP adressen die vaak door organisaties gebruikt worden om IPv4 adressen te assigneren aan interne hosts.
- Private IPv4 adressen zijn niet uniek en kunnen intern binnen elk netwerk gebruikt worden.
- Private IPv4 adressen kunnen niet publiek geroute worden.

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.32.255.255
192.168.0.0/16	192.168.255.255

Routing to the Internet

- Network Address Translation (NAT)** vertaald private IPv4 adressen naar Public IPv4 adressen
- NAT is typische ingeschakeld op de randrouter die de verbinding met het internet maakt.

Special Use IPv4 Addresses

Loopback addresses

127.0.0.0/8 (127.0.0.1 tot 127.255.255.254)

- Vaak wordt er verwezen naar een loopback adres door 127.0.0.1 (localhost)
- Wordt gebruikt op een host om te testen of TCP/IP operationeel is

Link-Local addresses

169.254.0.0/16 (169.254.0.1 tot 169.254.255.254)

- Beter bekend als **Automatic Private IP Addressing (APIPA)** adressen of **self-assigned** adressen
- Gebruikt door Windows DHCP clients om zelf IP adressen in te stellen wanneer er geen DHCP servers beschikbaar zijn.

Legacy Classful Addressing

RFC 790 (1981) heeft de IPv4 adressen toegewezen in volgende klassen:

- Class A: 0.0.0.0/8 tot 127.0.0.0/8
- Class B: 128.0.0.0/8 tot 191.255.0.0./16
- Class C: 192.0.0.0/24 tot 223.255.255.0/24
- Class D: 224.0.0.0 tot 239.0.0.0
- Class E: 240.0.0.0 tot 255.0.0.0

Het grote nadeel van klassevol te adresseren is dat verschillende IPv4 adressen verloren gaan.

Important

Als antwoord op de nadelen van klassevol adressen werd deze vervangen met klasseloos adresseren, waarbij men geen rekening meer hield met de regels van de klasse A, B en C.

Assignment of IP Addresses

- Het **Internet Assigned Numbers Authority (IANA)** beheert en wijst de blokken IPv4 en IPv6 adressen toe aan vijf **Regional Internet Registries (RIR's)**

- RIR's zijn verantwoordelijk voor het toewijzen van IP adressen aan ISP's, die op hun beurt verantwoordelijk zijn voor het doorgeven van kleinere blokken IP adressen aan organisaties of kleinere ISP's.

Network Segmentation

Broadcast Domains and Segmentation

- Verschillende protocollen gebruiken broadcast of multicast (bv. ARP gebruikt broadcast om andere toestellen te localiseren, hosts versturen DHCP discover broadcast om een DHCP server terug te vinden.)
- Switches propageren uitzendingen naar alle interfaces behalve de interface waarop ze ontvangen werden
-  [!important] Het enige toestel dat een broadcast kan stopzetten is een router
- Routers verspreiden geen broadcasts
- Elke router interface verbind met een broadcast domein. (broadcasts worden enkel verspreid binnen dat domein)

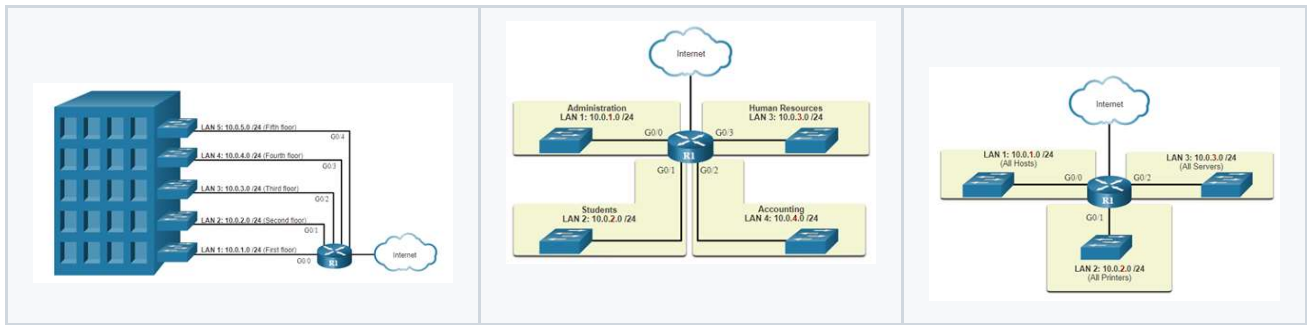
Problems with Large Broadcast Domains

- Hosts kunnen binnen een groot broadcast domein onnodige broadcasts genereren en zo een negatieve impact hebben op het netwerk.
- De oplossing om de grootte van het netwerk in te perken en zo kleiner broadcast domeinen aan te maken noemen we **subnetting**.

Reasons for Segmenting Networks

- Subnetten kan het totale netwerkverkeer verminderen en verbeterd de performantie van het netwerk.
- Het kan gebruikt worden om security policies te implementeren tussen de verschillende subnetten
- Subnetten verminderd het aantal toestellen die geïmpacteerd zijn door onnodig broadcast verkeer
- Subnetten worden onder andere gebruikt voor:

Location	Group of Function	Device Type
----------	-------------------	-------------



Subnet an IPv4 Network

Subnet on an Octet Boundary

- Netwerken worden meestal gesubnet op de octetgrens van /8, /16 en /24
- Merk op: het gebruik van langere prefix lengten betekend minder aantal hosts per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16 777 214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65 534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Subnetting voorbeelden

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

We kunnen duidelijk zien dat in het tweeded voorbeeld er meer subnetten aanwezig zijn elk met een minder aantal hosts in het netwerk.

Subnet within an Octet Boundary

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11111100	64	2

Subnet a Slash 16 and a Slash 8 Prefix

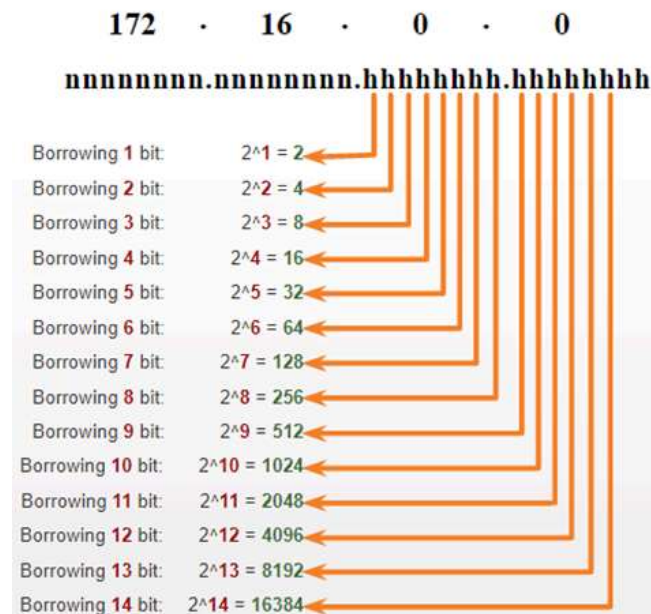
Onderstaande tabel toont alle mogelijkheden bij het subnetten van een /16 Prefix

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11111100	16384	2

Create 100 Subnets with a Slash 16 prefix

Een subnet kunnen we maken door bits te lenen uit het IP adres.

In onderstaand voorbeeld tonen we hoe we een netwerk met /16 kunnen verdelen in verschillende subnets. We kunnen tot 14 bits lenen.



Om te voldoen aan de vereisten (100 subnets) doen we de volgende berekening:

Nodig aantal bits = 2^x waar het resultaat $>$ of $=$ nodig aantal bits

Subnet to Meet Requirements

Subnet Private versus Public IPv4 Address Space

Bedrijven zullen meestal het volgende hebben:

- **Intranet:** een bedrijfs intern netwerk, meestal door gebruik te maken van private IPv4 adressen
- **DMZ (Demilitarized Zone):** De servers van een bedrijf die op het internet gericht zijn. Toestellen in de DMZ gebruiken publieke IPv4 adressen.
- Een bedrijf kan 10.0.0.0/8 gebruiken en subnetten naar /16 of /24

Minimize Unused Host IPv4 Addresses and Maximise Subnets

Er zijn twee zaken waarmee we moeten rekening houden wanneer we subnetten:

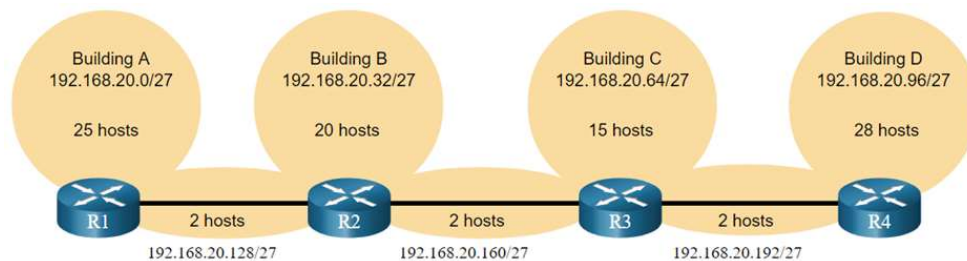
- Het aantal **host adressen** die nodig zijn voor het netwerk
- Het aantal **individuele subnets** die nodig zijn

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhnnnnnn 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11111100	64	2

VLSM

IPv4 Address Conservation

Stel de volgende infrastructuur voor: 7 subnets zijn nodig (4 LAN's en 3 WAN's) en het grootst aantal host is in gebouw D met 28 hosts.

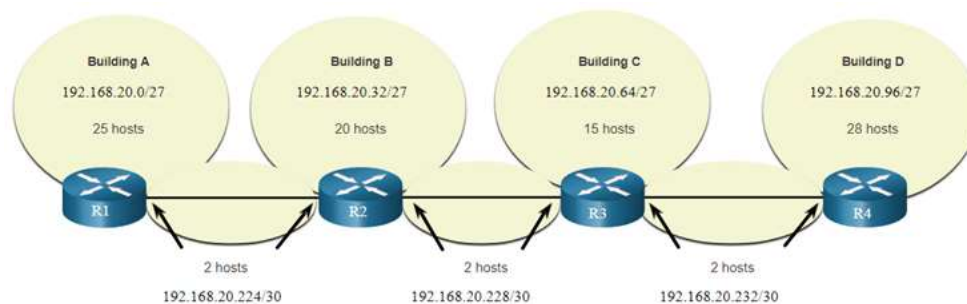


Hier zo een /27 mask 8 subnetten voorzien van 30 hosts en dus de infrastructuur ondersteunen. Echter hebben de point-to-point WAN links maar 2 adressen nodig en verliezen we daarom 28 adressen, voor een totaal van 84 ongebruikte adressen.

Een traditioneel subnetting schema toepassen op deze infrastructuur is niet efficiënt

VLSM werd ontwikkeld om het verliezen van IP adressen tegen te gaan door het subnetten van een subnet mogelijk te maken.

Wanner we gebruik maken van VLSM, beginnen we best steeds met het voldoen aan de hostvereisten van het grootste subnet. Hierna subnetten we verder tot we voldoen aan de vereisten van het kleinste subnet.



Structured Design

IPv4 Network Address Planning

IP netwerkplanning is nodig om een schaalbaar oplossing te voorzien voor een bedrijfsnetwerk.

- Om een IPv4 netwerk adresserings-schema te ontwikkelen moeten we volgende zaken weten:
 - hoeveel subnets zijn nodig
 - hoeveel hosts heeft een specifiek subnet nodig
 - welke toestellen maken onderdeel van een subnet
 - welke delen van het netwerk maken gebruik van private IP-adressen
 - welke delen van het netwerk maken gebruik van public IP-adressen

Onderzoek de netwerkbehoeften van een organisatie en hoe de subnetten gestructureerd moeten zijn.

- Voer een netwerkvereisten studie uit door te kijken naar het volledige netwerk en te bepalen hoe elk deel opgesplitst wordt.
- Bepaal hoeveel subnetten nodig zijn en hoeveel hosts elk van deze subnetten zal hebben
- Bepaal de DHCP adress pools en de Laag 2 VLAN pools

Device Address Assignment

Binnen een netwerk zijn er verschillende type toestellen die adressen nodig hebben:

- **End user clients:** De meeste maken gebruik van DHCP om fouten te beperken en de netwerkteams te ontlasten. IPv6 clients kunnen hun adres krijgen door gebruik te maken van DHCPv6 of SLAAC
- **Servers and peripherals:** Deze zouden best een voorspelbaar statisch IP adres hebben
- **Servers that are accessible from the internet:** Servers moeten een public IPv4 adres hebben, meestal toegankelijk door NAT.
- **Intermediary devices:** Toestellen worden adressen toegewezen voor netwerkbeheer, monitoring en beveiliging.
- **Gateway:** Routers en firewall toestellen zijn gateways voor de hosts in dat netwerk.

Wanneer je een IP adresserings schema ontwikkeld is het best practise om een verschillende patronen te hebben voor hoe je verschillende toestellen een adres geeft.