Fungsi Dasar Network (OSI Layer 3)

S1 Teknik Telekomunikasi
Fakultas Teknik Elektro
Telkom University

Outline

- Overview
- Basic Operation Network Layer Protocol
- Internet Protocol Versi 4 (IPv4)
- Subnetting IPv4

Overview

Network layer

Overview

- Network Layer → OSI Layer 3
- Menyediakan layanan untuk memungkinkan antar perangkat untuk saling bertukar data di lintas jaringan
- Protocol yang paling popular pada layer network ini adalah Internet Protocol Versi 4 (IPv4) dan Internet Protocol Versi 6 (IPv6)
- Protocol lainnya termasuk Routing Protocol seperti Open Shortest Path First (OSPF) dan messaging protocol seperti Internet Control Message Protocol (ICMP)

Basic Operation Network Layer Protocol

Basic Operation Network Layer Protocol

Untuk mencapai terjadinya komunikasi end to end melintasi batas-batas jaringan, protokol lapisan jaringan melakukan empat operasi dasar:

- Addressing end devices
- Enkapsulasi
- Routing
- De-enkapsulasi

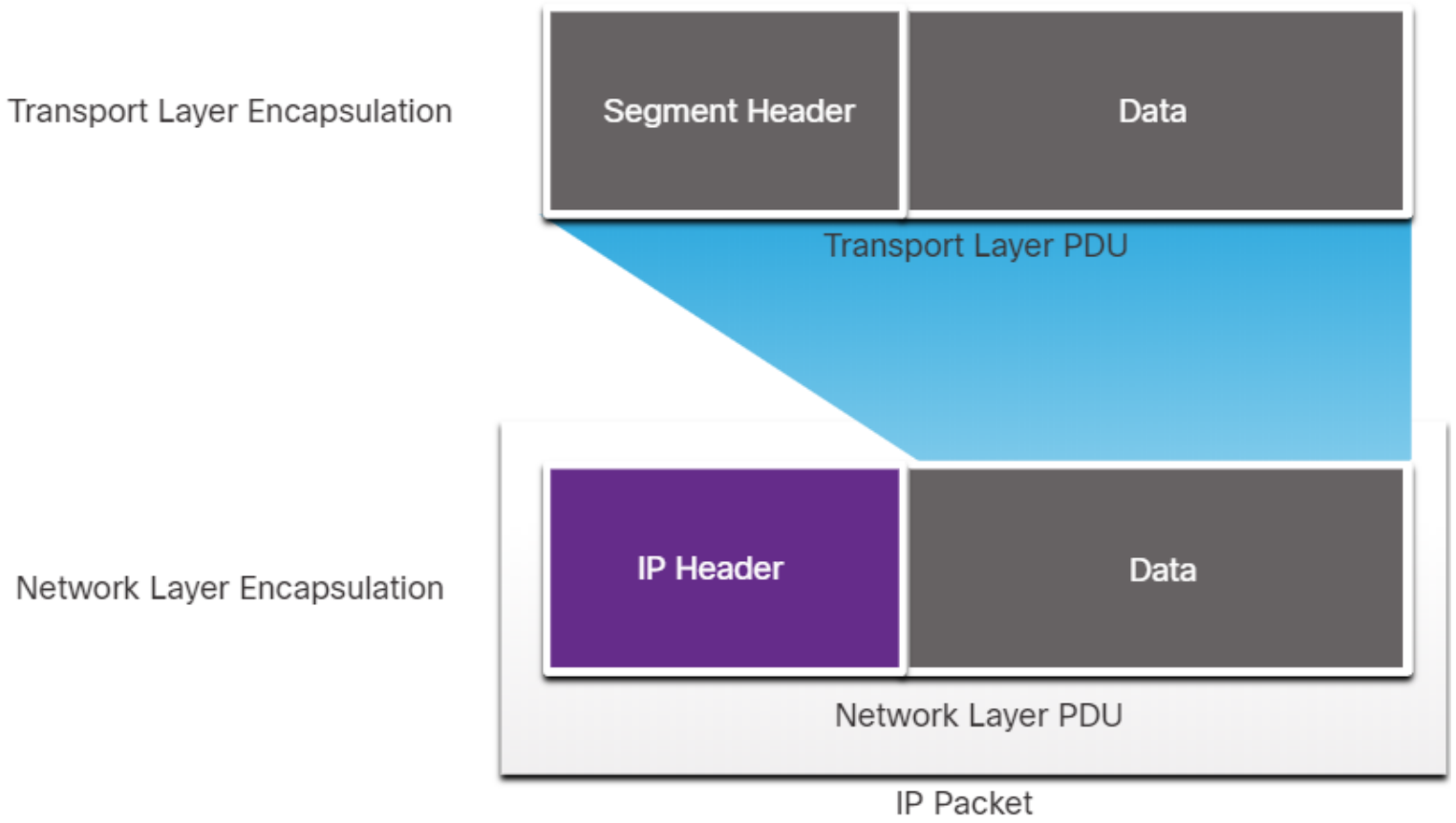
Addressing end devices

End devices harus dikonfigurasikan dengan alamat IP yang unik agar dapat diidentifikasi di jaringan

Enkapsulasi

- Network Layer merangkum Protocol Data Unit (PDU) dari transport layer ke dalam sebuah paket.
- Proses enkapsulasi yang dilakukan pada network layer yaitu menambahkan informasi header IP, seperti alamat IP dari host sumber (pengirim) dan tujuan (penerima).
- Proses enkapsulasi dilakukan oleh sumber paket IP.

Enkapsulasi PDU Layer Transport



Routing

- Network layer menyediakan layanan untuk mengarahkan paket ke host tujuan di jaringan lain.
- Untuk melakukan perjalanan ke jaringan lain, paket harus diproses oleh router.
- Peran router adalah memilih jalur terbaik dan mengarahkan paket ke host tujuan dalam proses yang dikenal sebagai routing.
- Suatu paket dapat melintasi banyak router sebelum mencapai host tujuan.
- Setiap router yang dilewati paket untuk mencapai host tujuan disebut hop.

De - Enkapsulasi

- Ketika paket tiba di network layer host tujuan, host akan memeriksa header IP paket
- Jika alamat IP tujuan dalam header cocok dengan alamat IP-nya sendiri, maka header IP akan dihapus dari paket
- Setelah paket didekapsulasi oleh network layer, Layer 4 PDU yang dihasilkan diteruskan ke layanan yang sesuai pada transport layer
- Proses de-enkapsulasi dilakukan oleh host tujuan dari paket IP.

Karakteristik Internet Protocol (IP)

- IP dirancang sebagai protokol dengan overhead rendah.
- Protokol Ini hanya menyediakan fungsi-fungsi yang diperlukan untuk mengirimkan paket dari sumber ke tujuan melalui sistem jaringan yang saling berhubungan.
- Protokol ini tidak dirancang untuk melacak dan mengelola aliran paket.

Karakteristik Internet Protocol (IP)

- **Connectionless** - Tidak ada pembangunan koneksi dengan tujuan yang dibuat terlebih dahulu sebelum mengirimkan paket data.
- **Best Effort** - IP secara inheren tidak dapat diandalkan karena pengiriman paket tidak dijamin.
- **Media Independent** - Pengoperasian tidak tergantung pada medium (mis., Tembaga, serat optik, atau nirkabel) yang membawa data.

Internet Protocol Versi 4

IPv4

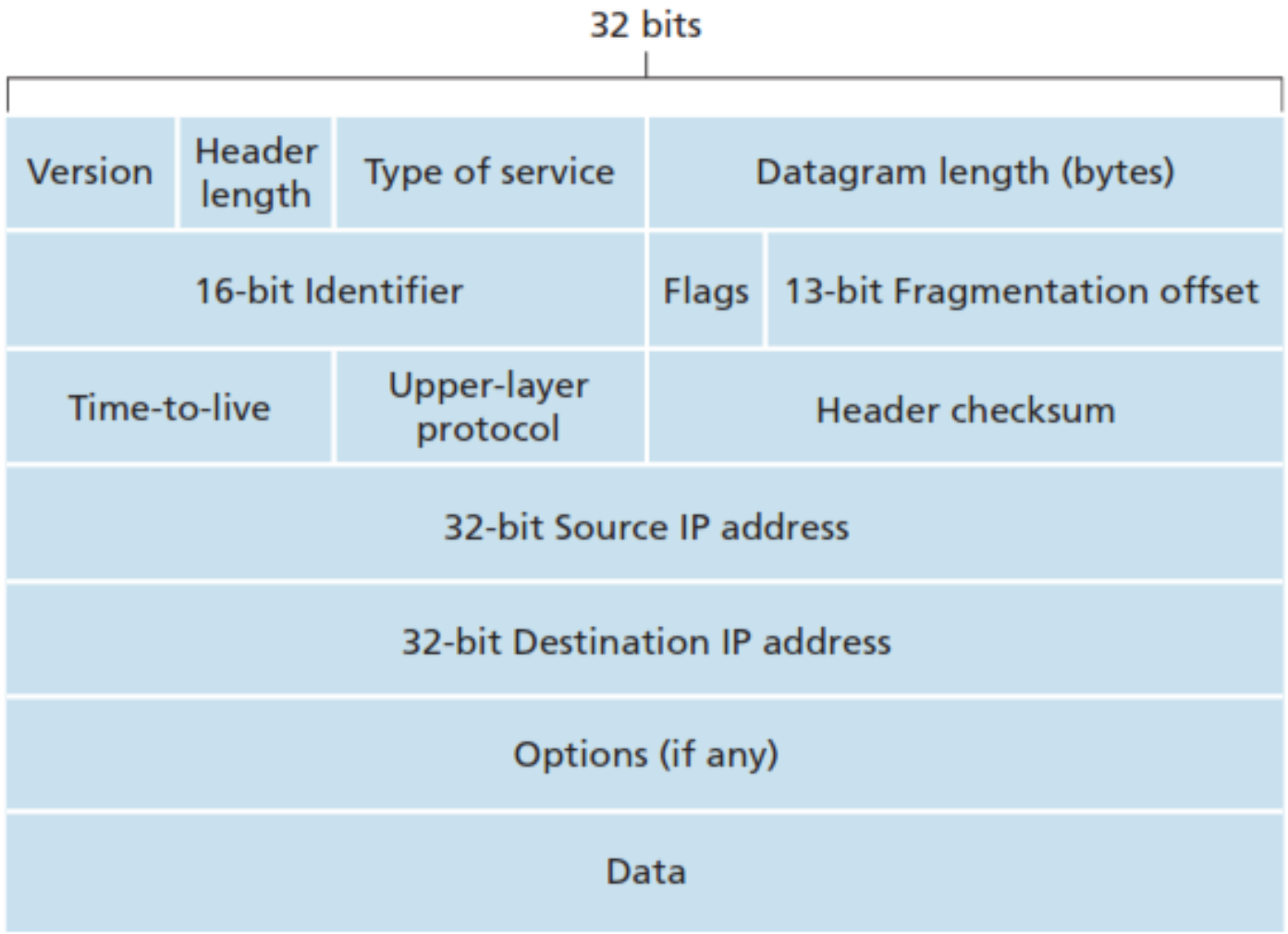
Internet Protocol Versi 4 (IPv4)

- IPv4 adalah salah satu protokol komunikasi network layer yang utama.
- Header paket IPv4 digunakan untuk memastikan bahwa paket ini dikirim ke pemberhentian berikutnya dalam perjalanan ke perangkat akhir tujuan.
- Header paket IPv4 terdiri dari field yang berisi informasi penting tentang paket. Field-field ini berisi angka-angka biner yang diperiksa oleh proses Layer 3.

Field Penting di Header Packet IPv4 (1)

- Version - Berisi nilai biner 4-bit yang diatur ke 0100 yang mengidentifikasi ini sebagai paket IPv4.
- Type of Service - Terdiri dari DS, DSCP dan ECN. Differentiated Services atau DiffServ (DS), Field DS adalah field 8-bit yang digunakan untuk menentukan prioritas setiap paket. Enam bit paling signifikan dari bidang DiffServ adalah differentiated services code point (DSCP) dan dua bit terakhir adalah bit explicit congestion notification (ECN).
- Header Checksum - Field ini digunakan untuk mendeteksi korupsi di header IPv4.
- Time to Live (TTL) - TTL berisi nilai biner 8-bit yang digunakan untuk membatasi masa pakai suatu paket. Perangkat source paket IPv4 menetapkan nilai TTL awal. Nilai TTL ini berkurang satu setiap kali paket diproses oleh router. Jika field TTL menurun ke nol, router membuang paket dan mengirim pesan ICMP yang melebihi waktu ke alamat IP source. Karena router menurunkan TTL dari setiap paket, router juga harus menghitung ulang Header Checksum.

IPv4 Header Packet



Field Penting di Header Packet IPv4 (2)

- Protocol - Field ini digunakan untuk mengidentifikasi protokol tingkat berikutnya. Nilai biner 8-bit ini menunjukkan tipe payload data yang dibawa paket, yang memungkinkan lapisan jaringan untuk meneruskan data ke protokol lapisan atas yang sesuai. Nilai yang paling umum muncul pada field ini adalah ICMP (1), TCP (6), dan UDP (17).
- Source IPv4 Address - Field ini berisi nilai biner 32-bit yang mewakili alamat IPv4 asal paket. Source IPv4 address memiliki alamat unicast.
- Destination IPv4 Address - Field ini berisi nilai biner 32-bit yang mewakili alamat IPv4 tujuan paket. Destination IPv4 address dapat berupa alamat unicast, multicast, maupuna broadcast.

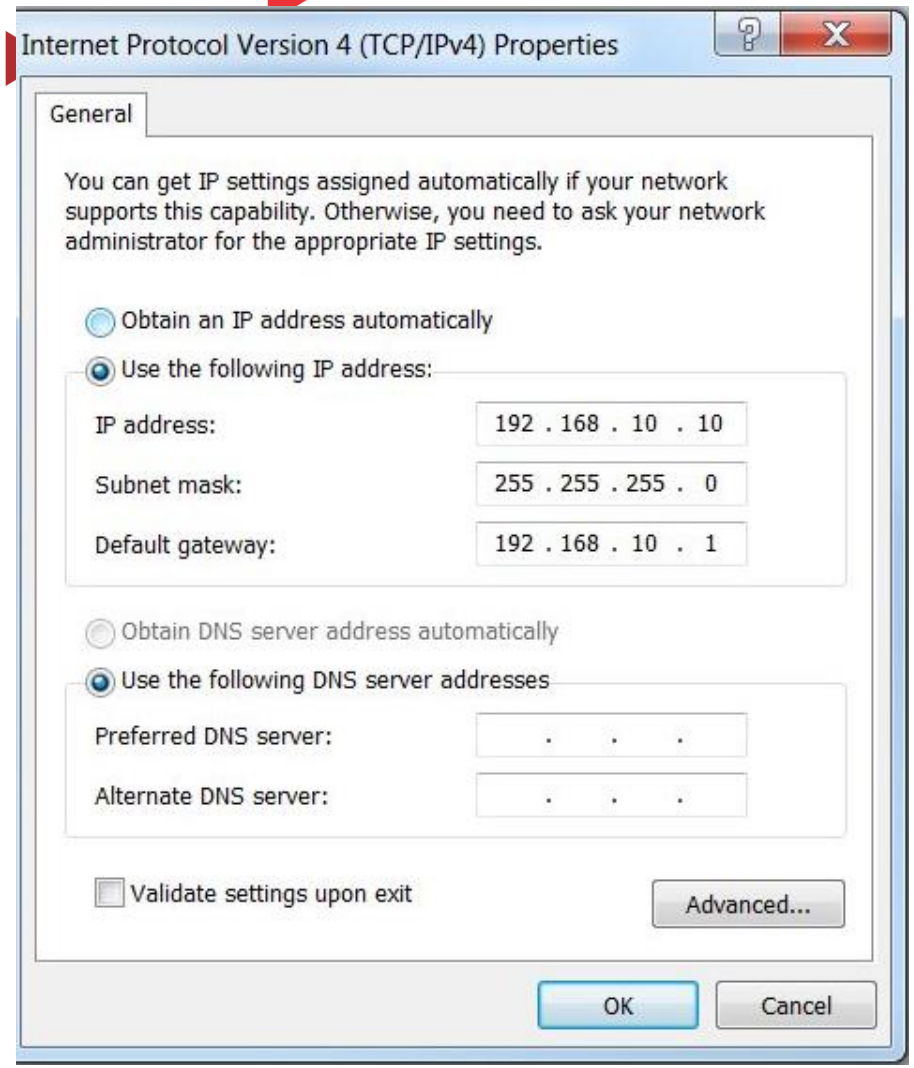
Field Penting di Header Packet IPv4 (3)

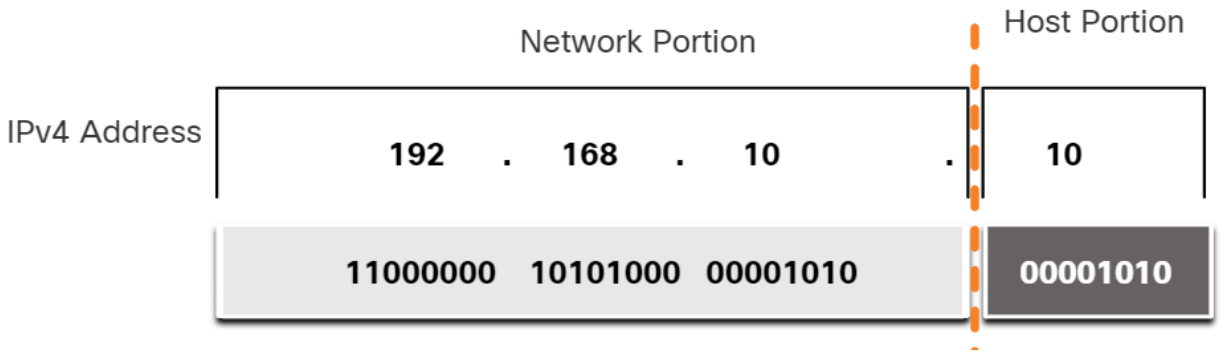
- Dua field yang paling sering dirujuk adalah sumber dan alamat IP tujuan. Field ini mengidentifikasi dari mana paket itu berasal dan ke mana ia pergi. Alamat-alamat ini tidak akan berubah saat bepergian dari sumber ke tujuan.
- Field Internet Header Length (IHL), Total Length, dan Header Checksum digunakan untuk mengidentifikasi dan memvalidasi paket.
- Field lain digunakan untuk menyusun ulang paket yang terfragmentasi. Secara khusus, paket IPv4 menggunakan field Identification, Flags, dan Fragmen Offset untuk melacak fragmen.
- Router akan memecah-mecah paket IPv4 saat meneruskannya dari satu medium ke medium lain dengan MTU yang lebih kecil.

IPv4 Adressing

- Alamat IPv4 adalah alamat hierarki berukuran 32-bit yang terdiri dari bagian network dan bagian host
- Bit yang berada di bagian network harus identik (memiliki pola bit yang sama) untuk semua perangkat yang berada di jaringan yang sama
- Bit yang berada di bagian host harus unik untuk mengidentifikasi host tertentu dalam suatu jaringan
- Tetapi bagaimana host tahu bagian mana dari 32-bit yang mengidentifikasi network dan yang mengidentifikasi host? Itulah peran subnet mask

Contoh konfigurasi alamat IPv4 di windows





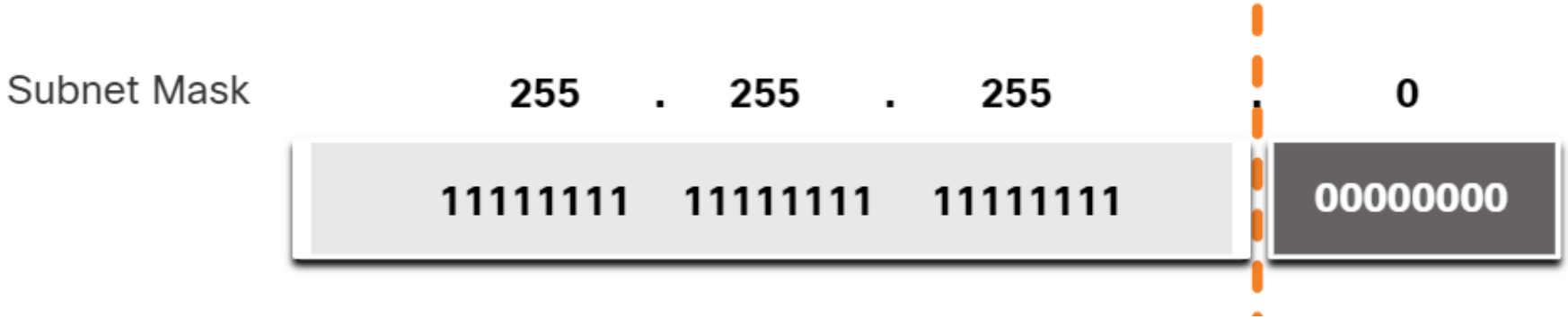
IPv4 address - Alamat unik IPv4 dari suatu host.
Subnet mask- Digunakan untuk mengidentifikasi bagian network/host dari alamat IPv4

Catatan:
Alamat IPv4 gateway default diperlukan untuk mencapai jaringan lain (contoh misal public internet) dan alamat IPv4 server DNS diperlukan untuk menerjemahkan nama domain ke alamat IPv4

Subnet mask IPv4

- Subnet mask IPv4 digunakan untuk membedakan bagian network dan bagian host dari suatu alamat IPv4.
- Ketika alamat IPv4 ditetapkan ke perangkat, subnet mask digunakan untuk menentukan alamat jaringan / Network Address perangkat.
- Network Address mewakili semua perangkat di jaringan yang sama.

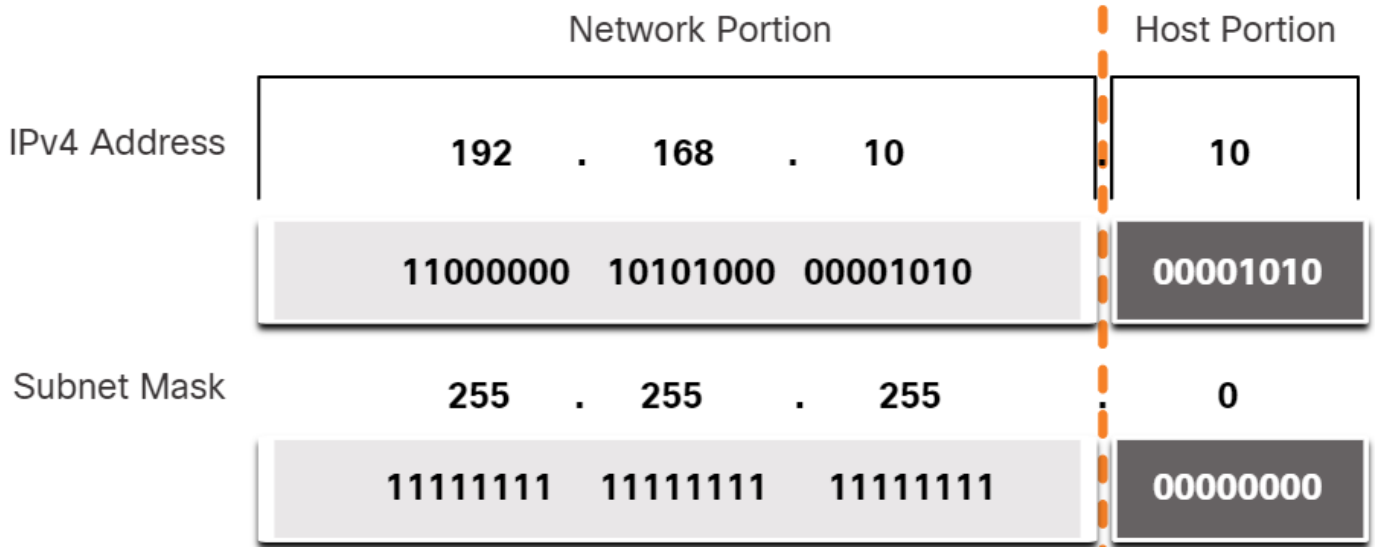
Format Subnet mask IPv4



Perhatikan bagaimana subnet mask adalah urutan 1 bit berturut-turut diikuti oleh urutan 0 bit berturut-turut.

Asosiasi IPv4 dengan subnet mask nya

Untuk mengidentifikasi bagian-bagian network dan host dari alamat IPv4, subnet mask harus dibandingkan bit per bit alamat IPv4, dari kiri ke kanan seperti yang ditunjukkan pada gambar di bawah



Prefix Length Subnet Mask

- Mengekspresikan alamat network dan alamat host dengan alamat subnet mask desimal bertitik dapat menjadi rumit.
- Untungnya, ada metode alternatif untuk mengidentifikasi subnet mask, metode yang disebut prefix length.
- Prefix length adalah jumlah bit yang diset menjadi angka 1 di subnet mask.
- Penulisanya dalam "notasi slash", yang dicatat oleh garis miring (/) diikuti dengan jumlah bit yang diatur ke 1.

Tabel Representasi Prefix length

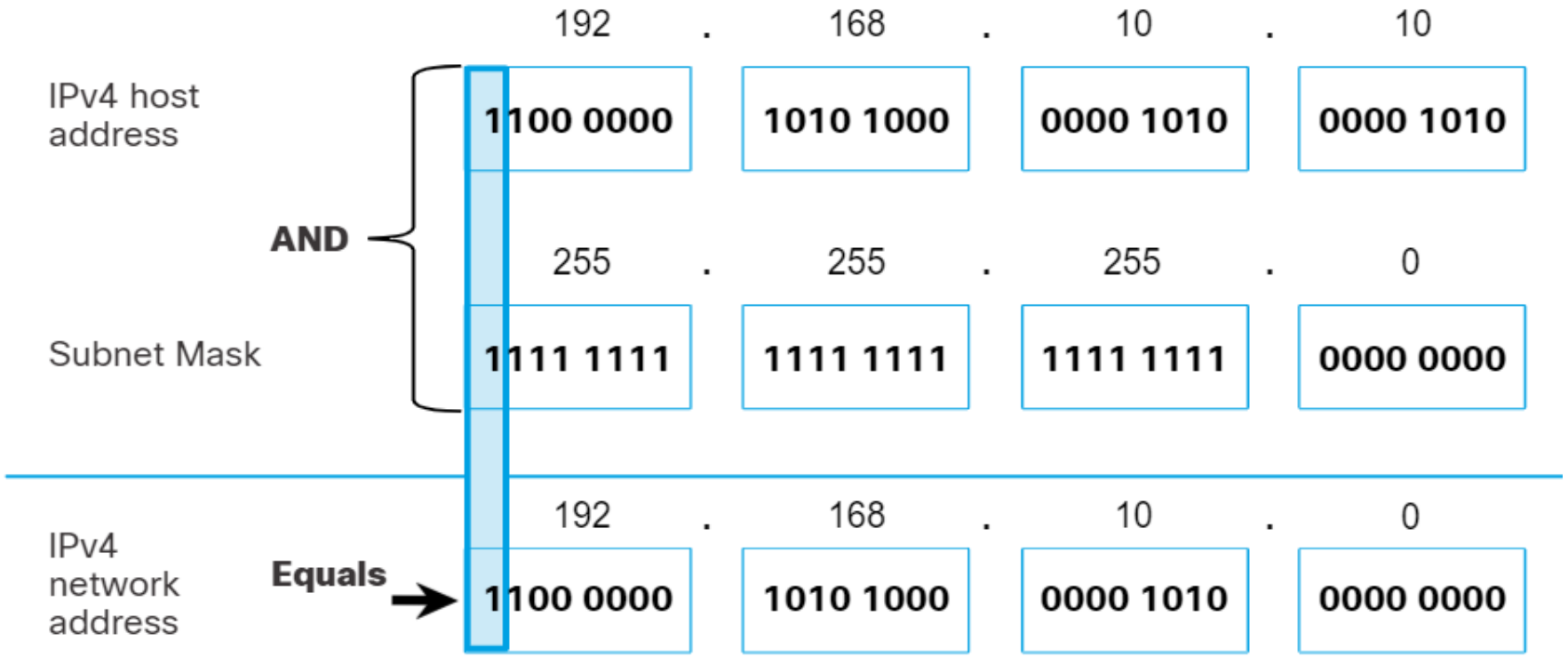
Cara penulisan prefix length ini berada di belakang alamat IPv4 tanpa spasi

Misalnya, alamat 192.168.10.10, dengan subnet mask 255.255.255.0 dapat ditulis sebagai 192.168.10.10/24.

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

Cara mencari network address IPv4 dari host address IPv4 dan subnet mask nya

Jika terdapat beberapa host yang memiliki network address yang sama, berarti host-host tersebut berada pada satu jaringan (atau biasa disebut satu subnet jaringan)



Network, Host, dan Broadcast Address

- Kita telah mengenal apa itu network dan host address pada slide sebelumnya
- Sebagai contoh host 192.168.10.10/24 memiliki network address 192.168.10.0
- Kemudian apa itu broadcast address?

Network, Host, dan Broadcast Address

	Network Portion			Host Portion	Host Bits
Subnet mask **255.255.255.**0 or **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Network address **192.168.10.**0 or **/24**	192 11000000	168 10100000	10 00001010	0 00000000	All 0s
First address **192.168.10.**1 or **/24**	192 11000000	168 10100000	10 00001010	1 00000001	All 0s and a 1
Last address **192.168.10.**254 or **/24**	192 11000000	168 10100000	10 00001010	254 11111110	All 1s and a 0
Broadcast address **192.168.10.**255 or **/24**	192 11000000	168 10100000	10 00001010	255 11111111	All 1s

Pada subnet mask /24,

Network address memiliki bit 0 semua di bagian bit host

Host address dapat menggunakan bit antara first address (bit 1) s.d last address (bit 254)

Broadcast address akan memiliki bit 1 semua di bagian bit host nya

Broadcast address adalah alamat yang digunakan saat diperlukan untuk menjangkau semua perangkat di jaringan IPv4. Seperti yang ditunjukkan dalam tabel, broadcast address jaringan memiliki semua 1 bit di bagian host, seperti yang ditentukan oleh subnet mask. Dalam contoh ini, alamat jaringan adalah 192.168.10.255/24. Broadcast address tidak dapat ditetapkan ke perangkat.

Menghitung Jumlah Host

- Masih pusing menentukan first address, last address, dan broadcast address dari suatu subnet mask?
- Cara mudah menentukan jumlah host dari suatu subnet mask adalah menghitung bit 0 nya.
- Misal prefix length /24, berarti terdapat 8 buah bit 0. Sehingga kita bisa menentukan jumlah host pada prefix length tersebut dengan rumus : $2^n - 2$ dimana n adalah jumlah bit 0

Menghitung Jumlah Host

- Sehingga total host pada prefix /24 adalah $2^8 - 2 = 256 - 2 = 254$
- Jadi, jika diketahui Network address suatu jaringan adalah 192.168.10.0/24, maka terdapat 254 alamat yang bisa dipasang pada host yaitu alamat **192.168.10.1** s.d **192.168.10.254**
- Kemudian untuk broadcast address, kita tinggal menambahkan satu angka di belakang alamat terakhir dari host yaitu **192.168.10.255**

Classfull Adressing IPv4

Pada tahun 1981, alamat IPv4 ditugaskan menggunakan pengalamatan classful sebagaimana didefinisikan dalam RFC 790 (ht tps: //tools.ietf.org/html/rfc790)

- **Kelas A (0.0.0.0/8 hingga 127.0.0.0/8)** - Dirancang untuk mendukung jaringan yang sangat besar dengan lebih dari 16 juta alamat host. Kelas A menggunakan awalan tetap / 8 dengan oktet pertama untuk menunjukkan alamat network dan tiga oktet lainnya untuk alamat host (lebih dari 16 juta alamat host per jaringan).
- **Kelas B (128.0.0.0 / 16 - 191.255.0.0 / 16)** - Dirancang untuk mendukung kebutuhan jaringan ukuran sedang hingga besar dengan sekitar 65.000 alamat host. Kelas B menggunakan awalan tetap / 16 dengan dua oktet tingkat tinggi untuk menunjukkan alamat network dan dua oktet lainnya untuk alamat host (lebih dari 65.000 alamat host per jaringan).
- **Kelas C (192.0.0.0 / 24 - 223.255.255.0 / 24)** - Dirancang untuk mendukung jaringan kecil dengan maksimum 254 host. Kelas C menggunakan awalan tetap / 24 dengan tiga oktet pertama untuk menunjukkan network dan oktet yang tersisa untuk alamat host (hanya 254 alamat host per jaringan).

Catatan: Ada juga blok multicast Kelas D yang terdiri dari 224.0.0.0 hingga 239.0.0.0 dan blok alamat eksperimen Kelas E yang terdiri dari 240.0.0.0 - 255.0.0.0.

Classless Adressing IPv4

- Pada pertengahan 1990-an, dengan diperkenalkannya World Wide Web (WWW), pengalamatan classfull tidak digunakan lagi untuk mengalokasikan ruang alamat IPv4 terbatas secara lebih efisien
- Alokasi alamat classful diganti dengan pengalamatan classless, yang digunakan hari ini
- Mengatasi tanpa kelas dengan mengabaikan aturan kelas (A, B, C)
- Alamat jaringan IPv4 publik (alamat jaringan dan subnet mask) dialokasikan berdasarkan jumlah alamat yang dapat dijustifikasi

Jenis alamat IPv4

- Terdapat 2 buah jenis alamat IPv4 yang dipakai di jaringan computer. Yaitu Public IPv4 dan Private IPv4.
- Alamat Public IPv4 diperuntukkan untuk pengalamatan di jaringan yang terhubung langsung dengan internet (WAN network)
- Sedangkan Alamat Private IPv4 diperuntukkan untuk pengalamatan di jaringan local (LAN/WLAN) . Range alokasi ini berdasarkan table di samping) →

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 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Routing Private IPv4 ke Internet

- Jaringan Lokal (LAN/WLAN) menggunakan private IPv4, sedangkan untuk bisa berkomunikasi dengan internet, host harus dikenali menggunakan public IPv4
- Metode untuk mentranslasikan private IPv4 ke Public IPv4 (dan sebaliknya) ini dikenal dengan metode NAT (Network Address Translation)

Subnetting IPv4

Subnetting IPv4

Konsep Subnetting merupakan konsep memecah suatu jaringan menjadi beberapa buah segment jaringan yang berbeda

Subnet Masks on Octet Boundaries

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 IPv4 (1)

- Pada slide pembahasan sebelumnya kita telah membahas mengenai bagaimana cara menentukan jumlah host dari suatu subnet mask yang diberikan pada suatu network addres.
- Pada contoh berikut ini kita ingin memecah jaringan kelas C 192.168.10.0/24 menjadi 4 buah subnet
- Membuat subnet, berarti dengan kata lain kita akan mengubah nilai dari subnet mask nya atau prefix length nya

Subnetting IPv4 (2)

- 192.168.10.0/24 ingin dipecah menjadi 4 buah subnet

Subnet = 2^x dimana x adalah jumlah bit 1 di bagian bit host

Dengan kata lain, jika /24 atau dalam decimal : 255.255.255.0 atau dalam bentuk biner :

11111111.11111111.11111111.**00000000** → memiliki 1 buah subnet karena jumlah bit 1 = 0 di bagian bit host (ditandai dengan font bold)

Jika ingin memecah menjadi 4 buah subnet, berarti kita akan meminjam 2 bit 1 di bagian bit host, karena $2^2 = 4$ sehingga bentuk binernya menjadi 11111111.11111111.11111111.**11000000** atau dalam bentuk decimal 255.255.255.192 atau bisa dalam bentuk prefix length /26

Subnetting IPv4 (3)

- Pernah kita bahas bahwa untuk menentukan jumlah host, pada saat diketahui network address dan prefix length nya dapat dicari dengan menggunakan rumus $2^n - 2$ dimana n adalah jumlah bit 0 di bagian bit host
- Sehingga, dari hasil sebelumnya jika diketahui network address 192.168.10.0 berubah prefixnya dari /24 ke /26 maka range host juga akan berubah
- Maka dengan rumus $2^n - 2$, kita dapat menentukan jumlah host di setiap subnet nya. Dikarenakan prefix length sudah berubah menjadi /26, maka jumlah bit 0 di bagian bit host juga berubah menjadi 6 buah (ingat bentuk biner /26 adalah 11111111.11111111.11111111.11**000000**)

- Maka jumlah host pada saat prefix length /26 adalah :

$2^6 - 2 = 62$, dengan kata lain network address 192.168.10.0/26, pada subnet ke 1 dimulai dengan host 192.168.10.1/26 s.d 192.168.10.62/26 dan broadcast address 192.168.10.63/26

- Penentuan subnet selanjutnya tinggal ditambahkan network address sebagai alamat setelah broadcast address subnet ke 1

Sehingga bisa dituliskan semua subnet sebagai berikut :

Subnet 1 : Network address 192.168.10.0/26, start address 192.168.10.1/26, end address 192.168.10.62/26, broadcast address 192.168.10.63/26

Subnet 2 : Network address 192.168.10.64/26, start address 192.168.10.65/26, end address 192.168.10.126/26, broadcast address 192.168.10.127/26

Subnet 3 : Network address 192.168.10.128/26, start address 192.168.10.129/26, end address 192.168.10.190/26, broadcast address 192.168.10.191/26

Subnet 4 : Network address 192.168.10.192/26, start address 192.168.10.193/26, end address 192.168.10.254/26, broadcast address 192.168.10.255/26