Network Fundamental

Network Fundamental

Daftar Isi

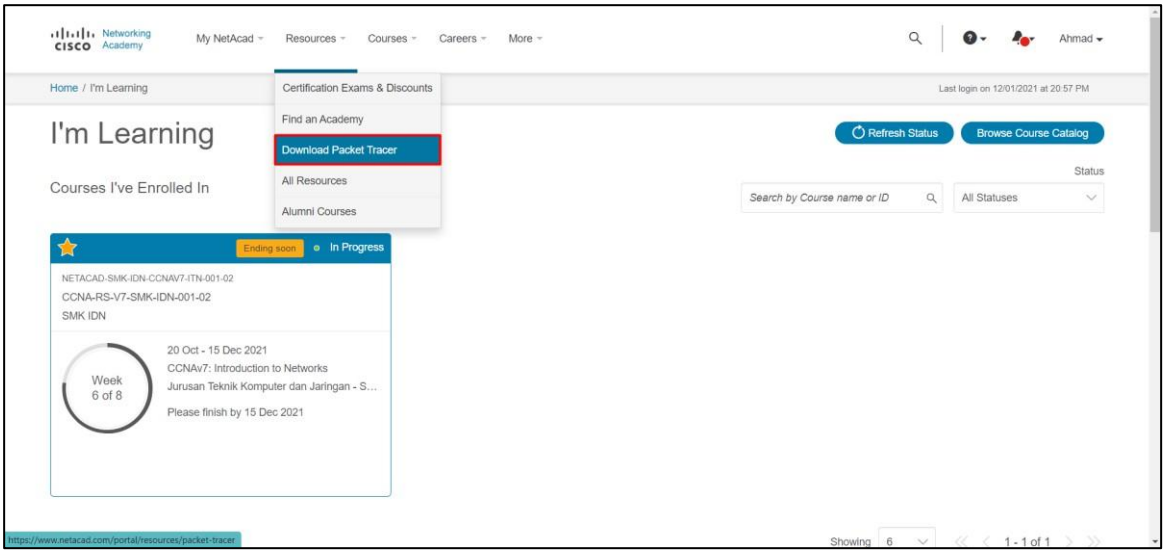
PREPARATION

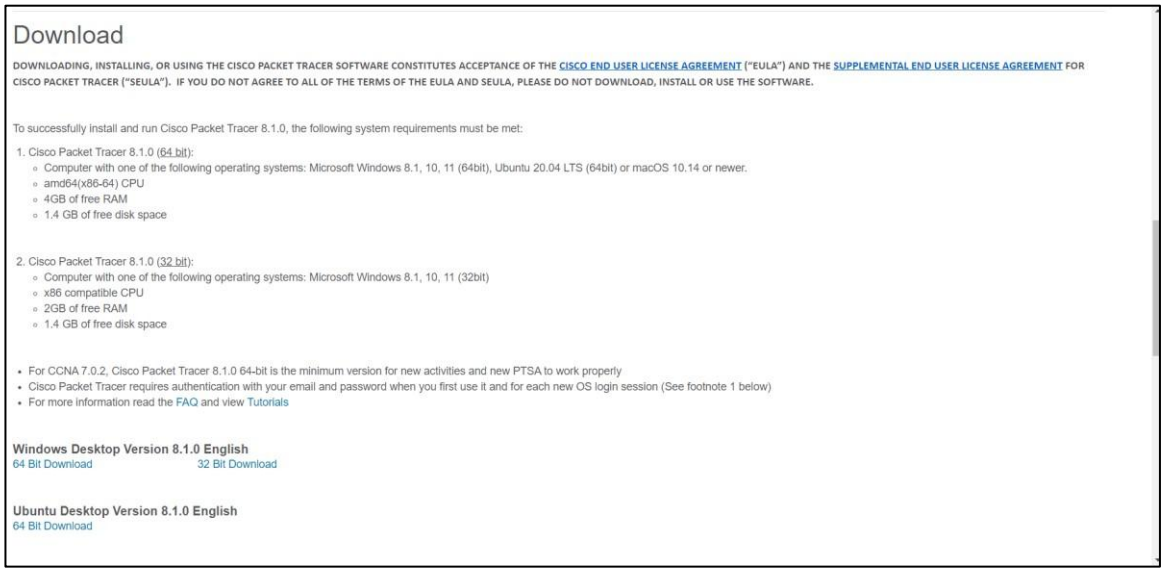
Ibarat mengawali sebuah pembangunan, pasti kita membutuhkan perlengkapannya terlebih dahulu sebagai awalan. Jika sudah, tinggal kita menunggu proses, apakah akhirnya bangunan yang dibangun kokoh atau tidak, indah atau tidak. Itu tergantung usaha dan pemahaman kita. Maka dari itu, untuk mengawali Materi CCNA kali ini, maka disarankan untuk menggunakan perlengkapan berikut, agar kita bisa lebih memahami.

Download Cisco Packet Tracer:

- Pertama-tama, kita daftar netacad terlebih dahulu, agar kita bisa menggunakan dan mengunduh CPT.
- Klik https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer
- Lalu klik ‘Sign up Today!’ dan klik ‘English’ untuk bahasa inggris.

- Selanjutnya kita isi formulir dan verifikasi e-mail.
- Jika kita sudah, masuk ke homepage netacad.





Download

DOWNLOADING, INSTALLING, OR USING THE CISCO PACKET TRACER SOFTWARE CONSTITUTES ACCEPTANCE OF THE CISCO END USER LICENSE AGREEMENT ("EULA") AND THE SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO PACKET TRACER ("SEULA"). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE EULA AND SEULA, PLEASE DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE.

To successfully install and run Cisco Packet Tracer 8.1.0, the following system requirements must be met:

1. Cisco Packet Tracer 8.1.0 (64 bit):
   - Computer with one of the following operating systems: Microsoft Windows 8.1, 10, 11 (64bit), Ubuntu 20.04 LTS (64bit) or macOS 10.14 or newer.
   - amd64(x86-64) CPU
   - 4GB of free RAM
   - 1.4 GB of free disk space

2. Cisco Packet Tracer 8.1.0 (32 bit):
   - Computer with one of the following operating systems: Microsoft Windows 8.1, 10, 11 (32bit)
   - x86 compatible CPU
   - 2GB of free RAM
   - 1.4 GB of free disk space

- For CCNA 7.0.2, Cisco Packet Tracer 8.1.0 64-bit is the minimum version for new activities and new PTSA to work properly
- Cisco Packet Tracer requires authentication with your email and password when you first use it and for each new OS login session (See footnote 1 below)
- For more information read the FAQ and view Tutorials

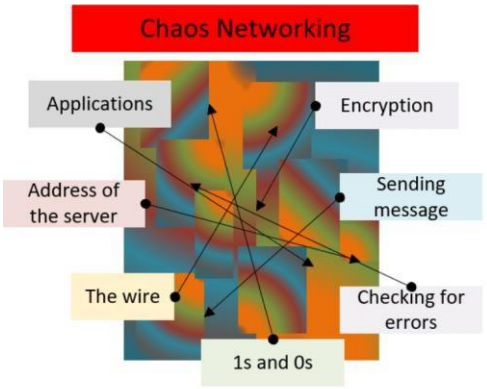
Windows Desktop Version 8.1.0 English
64 Bit Download 32 Bit Download

Ubuntu Desktop Version 8.1.0 English
64 Bit Download

- Lalu klik ‘Resources’ pada tab atas kemudian klik ‘Download Packet Tracer’.
- Disitu ada beberapa jenis Packet Tracer, unduhlah sesuai dengan OS atau system yang sedang digunakan.

OSI & TCP/IP LAYER

Apakah kamu tau?, bahwa jika ketika kita akan mengakses internet, ada suatu proses yang sangat panjang hingga akhirnya ktia bisa mengakses email, menonton youtube dll. Semua hal tersebut dapat kita akses dengan mudah karena kemajuan teknologi. Bayangkan pada zaman dahulu, untuk internet sangat susah sekali, hal ini dikarenakan terjadinya Chaos Networking. Yaitu sebuah proses dimana semua proses saling bertabrakan, tidak termodel.



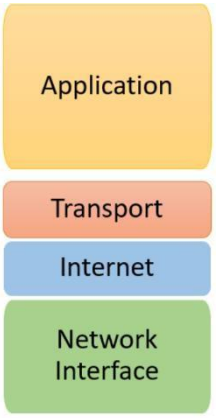
This network would be dificult to understand and implement

Dan susah untuk berkomunikasi. Hal ini juga dikarenakan tiap vendor pada networking memiliki protokol komunikasi yang berbeda-beda. Hal ini mengakibatkan antara vendor satu dan yang lain tidak bisa saling berkomunikasi.

Maka dari itu, pada tahun 1970-an DARPA membuat sebuah model protokol komunikasi yang disebut TCP/IP yang dapat digunakan oleh semua vendor networking sehingga dapat saling berkomunikasi. Ini merupakan kemajuan teknologi. TCP/IP sendiri merupakan singkatan dari Transmission Control Protocol/ Internet Protocol.

TCP/IP terdiri dari 4 layer :

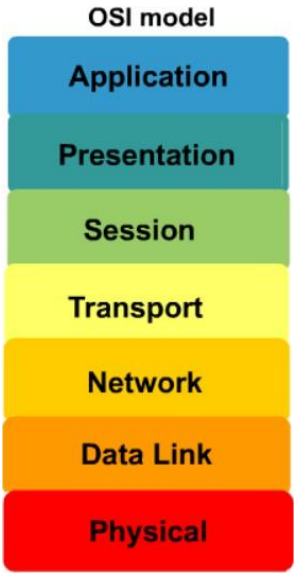
1. Network Interface
2. Internet
3. Transport
4. Application



OSI Layer

Sementara itu, 10 tahun kemudian, pada tahun 1980-an. ISO atau Organisasi Standar Internasional membuat protocol komunikasi lain yang lebih kompleks dan jelas fungsinya dari TCP/IP. Protokol komunikasi itu disebut juga dengan OSI Layer. OSI Layer merupakan singkatan dari Open System Interconnection.

OSI Layer terdiri dari 7 layer :



1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Lalu apa perbedaan dari TCP/IP dan OSI Layer?

Perbedaanya terletak pada layer-nya. Jika pada TCP/IP terdapat 4 Layer, maka pada OSI terdapat 7 layer. OSI layer, memecah satu layer pada TCP/IP menjadi beberapa layer. Secara fungsi pada tiap layer masing-masing protocol tidak ada perbedaan, hanya saja pada OSI Layer. Fungsi-fungsi nya dibuat menjadi lebih kompleks dan lebih mudah dimengerti. Sehingga untuk secara keunggulan masih bagus OSI layer. Hanya saja, protocol yang kita

OSI Model	TCP/IP Model
Application Layer	Application layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data link layer	Link Layer
Physical layer	

gunakan dari dulu sampai sekarang adalah TCP/IP. Hal ini dikarenakan TCP/IP dulu lah yang pertama keluar dan langsung digunakan oleh hampir semua vendor jaringan yang ada didunia.

Fungsi tiap layer pada OSI

1. **Physical**
   Pada layer ini, kita mengirimkan data dari unsur terluar atau unsur fisik seperti kabel, antenna. Yang menghubungkan antar penyedia layanan internet (ISP) data yang dikirim berupa bit dan pengalamatannya menggunakan bit (101010101).

2. **Data Link**
   Setelah data (bit) tadi dikirim lewat kabel, setelah itu akan naik lagi ke layer 2. Pada layer 2, data diproses oleh hardware yang bernama switch, data yang dikirim berupa frame dan pengalamatannya berupa MAC Address.

3. **Network**
   Jika data tadi sudah diproses switch, maka selanjutnya akan diproses oleh router. Data yang dikirim berupa Packet dan pengalamatannya menggunakan IP address.

4. **Transport**
   Sebelum packet ini dikirim oleh router, maka akan dipilih packetnya berdasarkan protocol apa, ada TCP dan juga UDP .

5. **Session,Presentation, Application**
   Setelah packet itu dikirim ke IP Adress tujuan, selanjutnya akan diproses oleh software yang akan menghasilkan protocol baru, seperti DHCP (UDP no 67-68) atau telnet (TCP no 23) dan masih banyak lagi.

   Atau lebih ringkasnya dapat dilihat di tabel berikut :

Layer	Nama	Perangkat	Data Unit	Pengalamatan
Layer 1	Physical	Hub	Bit	0111001110
Layer 2	Data Link	Switch	Frame	MAC Address
Layer 3	Network	Router	Paket	IP Address

Tabel 3 . 1 Daftar Pengalamatan

Apabila 7 OSI Layer susah untuk dihafal, maka sebagai seorang network engineer hafal Layer 1, 2 dan 3 adalah suatu keharusan, karena dapat menunjukkan bedanya antara Hub, Switch dan Router dimana ketiganya berada di layer yang berbeda sehingga memiliki cara kerja yang berbeda tentunya.

Perangkat	Layer	Konektivitas	Pengiriman Data	Memory
Hub	Layer 1	Antar network yang sama	Broadcast ke semua port	Tidak Punya
Switch	Layer 2	Antar network yang sama	Berdasar MAC Address Tujuan	MAC Address Tabel
Router	Layer 3	Antar network yang berbeda	Berdasar IP Address Tujuan	Routing Tabel

Tabel 3 . 2 Daftar Konektivitas

Berdasarkan tabel diatas dapat kita simpulkan bahwa pada layer 1 dan 2 bekerja pada network yang sama alias masih pada satu jaringan. Jika kita analogikan, layer 1 dan 2 ini masih bekerja di satu desa, sementara layer 3, dia bekerja di perbatasan desa. Jadi layer 3 ini, nanti fungsinya mengenalkan desa (network) nya kepada desa-desa lain (network lain).

TCP & UDP

Fungsi dari layer 4 adalah untuk menerima data dari session layer, lalu dibagi menjadi segmen-segmen yang lebih kecil untuk diteruskan ke network layer. Transport layer juga memastikan setiap bit yang diterima adalah bit yang sama dengan bit yang dikirim tanpa ada modifikasi ataupun loss.

Jika terjadi error, maka transport layer harus memperbaiki error tersebut. Cara memperbaikinya, bisa dengan mengirim ulang data yang corrupt atau dengan mengirim semua data dari awal.

Berikut tabel perbandingan TCP & UDP :

No	TCP	UDP
1.	Beroperasi berdasarkan konsep koneksi.	Tidak berdasarkan konsep koneksi, jadi harus membuat kode sendiri.
2.	Jaminan pengiriman-penerimaan data akan reliable dan teratur.	Tidak ada jaminan bahwa pengiriman dan penerimaan data akan reliable dan teratur, sehingga paket data mungkin dapat kurang, terduplikat, atau bahkan tidak sampai sama sekali.
3.	Secara otomatis memecah data ke dalam paket-paket.	Pemecahan ke dalam paket-paket dan proses pengirimannya dilakukan secara manual.
4.	Tidak akan mengirimkan data terlalu cepat sehingga memberikan jaminan koneksi internet dapat menanganinya.	Harus membuat kepastian mengenai proses transfer data agar tidak terlalu cepat sehingga internet masih dapat menanganinya.
5.	Mudah untuk digunakan, transfer paket data seperti menulis dan membaca file.	Jika paket ada yang hilang, perlu dipikirkan di mana letak kesalahan yang terjadi dan mengirim ulang data yang diperlukan.

Mudahnya, jika kita analogikan dalam jaringan :

TCP :

Misalkan kita sebagai klien, mengirimkan 10 paket kepada server, jika waktu dijalan paketnya hilang 5 (drop) dan sampai di server hanya 5. Maka klien akan mengirim 5 paket susulan agar 10 paket sempurna sampai di server atau mengoreksi paketnya kembali. Ini disebut juga dengan Reliable atau seimbang. Selain itu TCP justru lebih lambat daripada UDP dikarenakan adanya koreksi paket tersebut dan ukuran paket TCP juga lebih berat daripada UDP yaitu 20 bytes.

UDP :

Pada UDP, jika kita sebagai klien dan mengirim 10 data kepada server, jika waktu dijalan paketnya hilang 5 (drop) dan sampai di server hanya 5. Maka klien tidak akan mengirim ulang karena dianggap urusan pengiriman paket itu sudah selesai. Ini disebut juga dengan non-

reliable atau tidak seimbang. Namun, UDP jauh lebih cepat pengiriman paketnya daripada TCP dikarenakan UDP sekali kirim dan ukuran paketnya jauh lebih kecil dari TCP yaitu 8 bytes.

Port Numbers

Sementara itu, Port adalah nomor 16-bit yang digunakan untuk mengidentifikasi aplikasi dan layanan tertentu. TCP dan UDP menentukan nomor port sumber dan tujuan di header paket mereka dan informasi itu, bersama dengan alamat IP sumber dan tujuan dan protokol transport (TCP atau UDP), memungkinkan aplikasi yang berjalan pada host di jaringan TCP / IP untuk berkomunikasi. T

Terdapat 3 port number range :

• Well known port (0 - 1023): Untuk core services.

• Registered port number (1024 – 49151) : Untuk keperluan industri aplikasi dan process.

• Dynamic port number (49152 – 65535) : Digunakan untuk keperluan temporary untuk sebuah komunikasi yang spesifik.

Contoh dari TCP dan UDP

TCP :

Contohnya pada browser (HTTP & HTTPS). Pada saat kita berselancar di internet, saat kita mengakses situs, jika misalkan ada gambar/bagian dari situs itu yang kurang lengkap atau hilang, kita tinggal melakukan refresh agar gambar tersebut bisa muncul. Hal ini sama seperti protocol TCP yang mengirim ulang packet nya.

UDP :

Contohnya ketika kita bertelpon menggunakan VOIP (Voice Over Internet Protocol). Pada saat kita menggunakan VOIP, pasti pernah kita merasakan suara lawan bicara kita putus-putus dikarenakan jaringan alias packet yang terkirim tidak sampai. Itu karena UDP hanya sekali mengirimkan packet. Jika VOIP menggunakan TCP, jika saat kita mengirimkan paket suara namun tidak sampai, maka suara tersebut akan dikirim ulang ke penerima dan terjadilah keterlambatan. Maka dari itu VOIP menggunakan UDP agar tidak terjadi keaneahan dan keterlambatan dalam bertelpon, lebih baik suara terputus daripada suara dikirim ulang disaat yang tidak tepat.

Common Ports

packetlife.net

TCP/UDP Port Numbers

7	Echo	**554**	RTSP	**2745**	Bagle.H	**6891-6901**	Windows Live
19	Chargen	**546-547**	DHCPv6	**2967**	Symantec AV	**6970**	Quicktime
20-21	FTP	**560**	rmonitor	**3050**	Interbase DB	**7212**	GhostSurf
22	SSH/SCP	**563**	NNTP over SSL	**3074**	XBOX Live	**7648-7649**	CU-SeeMe
23	Telnet	**587**	SMTP	**3124**	HTTP Proxy	**8000**	Internet Radio
25	SMTP	**591**	FileMaker	**3127**	MyDoom	**8080**	HTTP Proxy
42	WINS Replication	**593**	Microsoft DCOM	**3128**	HTTP Proxy	**8086-8087**	Kaspersky AV
43	WHOIS	**631**	Internet Printing	**3222**	GLBP	**8118**	Privoxy
49	TACACS	**636**	LDAP over SSL	**3260**	iSCSI Target	**8200**	VMware Server
53	DNS	**639**	MSDP (PIM)	**3306**	MySQL	**8500**	Adobe ColdFusion
67-68	DHCP/BOOTP	**646**	LDP (MPLS)	**3389**	Terminal Server	**8767**	TeamSpeak
69	TFTP	**691**	MS Exchange	**3689**	iTunes	**8866**	Bagle.B
70	Gopher	**860**	iSCSI	**3690**	Subversion	**9100**	HP JetDirect
79	Finger	**873**	rsync	**3724**	World of Warcraft	**9101-9103**	Bacula
80	HTTP	**902**	VMware Server	**3784-3785**	Ventrilo	**9119**	MXit
88	Kerberos	**989-990**	FTP over SSL	**4333**	mSQL	**9800**	WebDAV
102	MS Exchange	**993**	IMAP4 over SSL	**4444**	Blaster	**9898**	Dabber
110	POP3	**995**	POP3 over SSL	**4664**	Google Desktop	**9988**	Rbot/Spybot
113	Ident	**1025**	Microsoft RPC	**4672**	eMule	**9999**	Urchin
119	NNTP (Usenet)	**1026-1029**	Windows Messenger	**4899**	Radmin	**10000**	Webmin
123	NTP	**1080**	SOCKS Proxy	**5000**	UPnP	**10000**	BackupExec
135	Microsoft RPC	**1080**	MyDoom	**5001**	Slingbox	**10113-10116**	NetIQ
137-139	NetBIOS	**1194**	OpenVPN	**5001**	iperf	**11371**	OpenPGP
143	IMAP4	**1214**	Kazaa	**5004-5005**	RTP	**12035-12036**	Second Life
161-162	SNMP	**1241**	Nessus	**5050**	Yahoo! Messenger	**12345**	NetBus
177	XDMCP	**1311**	Dell OpenManage	**5060**	SIP	**13720-13721**	NetBackup
179	BGP	**1337**	WASTE	**5190**	AIM/ICQ	**14567**	Battlefield
201	AppleTalk	**1433-1434**	Microsoft SQL	**5222-5223**	XMPP/Jabber	**15118**	Dipnet/Oddbob
264	BGMP	**1512**	WINS	**5432**	PostgreSQL	**19226**	AdminSecure
318	TSP	**1589**	Cisco VQP	**5500**	VNC Server	**19638**	Ensim
381-383	HP Openview	**1701**	L2TP	**5554**	Sasser	**20000**	Usermin
389	LDAP	**1723**	MS PPTP	**5631-5632**	pcAnywhere	**24800**	Synergy
411-412	Direct Connect	**1725**	Steam	**5800**	VNC over HTTP	**25999**	Xfire
443	HTTP over SSL	**1741**	CiscoWorks 2000	**5900+**	VNC Server	**27015**	Half-Life
445	Microsoft DS	**1755**	MS Media Server	**6000-6001**	X11	**27374**	Sub7
464	Kerberos	**1812-1813**	RADIUS	**6112**	Battle.net	**28960**	Call of Duty
465	SMTP over SSL	**1863**	MSN	**6129**	DameWare	**31337**	Back Orifice
497	Retrospect	**1985**	Cisco HSRP	**6257**	WinMX	**33434+**	traceroute
500	ISAKMP	**2000**	Cisco SCCP	**6346-6347**	Gnutella		
512	rexec	**2002**	Cisco ACS	**6500**	GameSpy Arcade		
513	rlogin	**2049**	NFS	**6566**	SANE		
514	syslog	**2082-2083**	cPanel	**6588**	AnalogX		
515	LPD/LPR	**2100**	Oracle XDB	**6665-6669**	IRC		
520	RIP	**2222**	DirectAdmin	**6679/6697**	IRC over SSL		
521	RIPng (IPv6)	**2302**	Halo	**6699**	Napster		
540	UUCP	**2483-2484**	Oracle DB	**6881-6999**	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

by Jeremy Stretch

v1.1

NETWORK PROTOCOL

Dalam dunia jaringan, terdapat banyak jenis komunikasi yang berbeda-beda, namun itu semua sudah tertata rapi sesuai dengan protocol yang digunakan. Seperti ketika kita browsing di internet, kita menggunakan protocol HTTP dan HTTPS, lalu saat kita akan meremote router atau switch, kita menggunakan telnet maupun SSH.

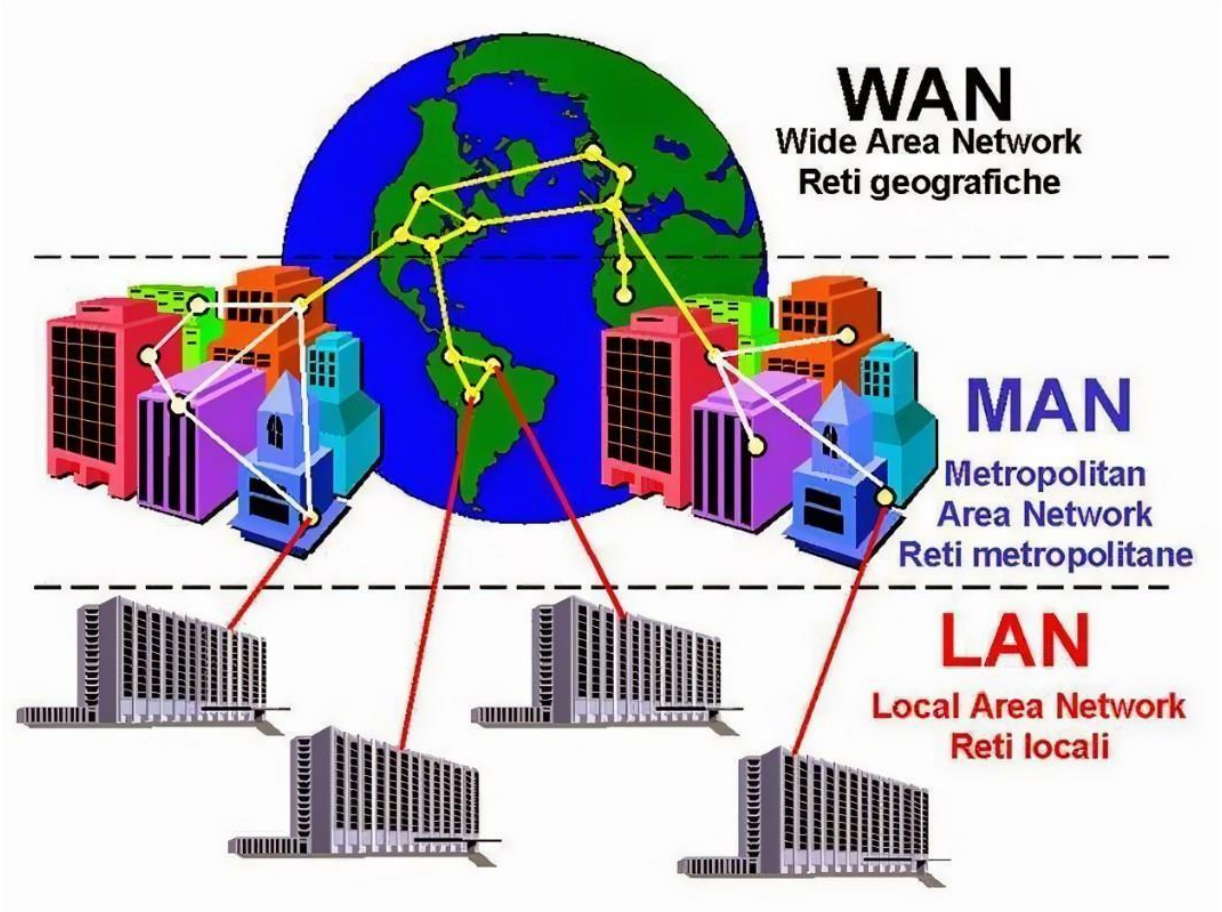
Jadi, fungsi dari Network Protocol, ialah mengatur jalannya komunikasi pada jaringan dengan protokol-protokol agar berjalan dengan lancer.

Contoh Network Protocol

Berikut beberapa network protocol yang harus kita pahami :

Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 UDP 161,162
TELNET	Telnet Terminal	TCP 23
FTP	File Transfer Protocol	TCP 20,21
SSH	Secure Shell (terminal)	TCP 22
AFP IP	Apple File Protocol/IP	TCP 447, 548

INFRASTRUKTUR JARINGAN



Dalam implementasinya, infrastruktur jaringan dibagi menjadi 2 :

1. LAN (Local Area Network)- Merupakan jaringan skala kecil yang terdiri dari sekumpulan perangkat yang saling terhubung yang masih dalam ruang lingkup yang belum luas. Seperti jaringan pada Sekolah, Rumah, Warnet.

2. WAN (Wide Area Network)- Merupakan jaringan skala besar yang terdiri dari kumpulan LAN yang saling terhubung satu sama lain. Contohnya Internet.

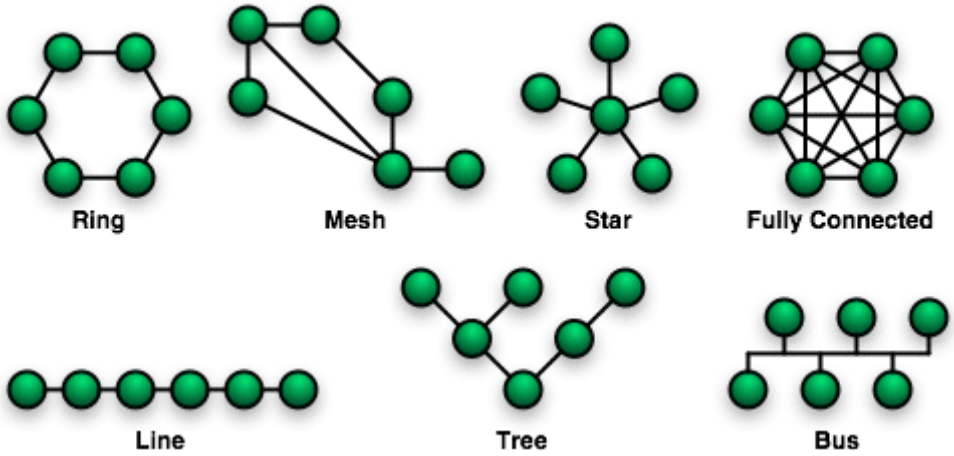
Adapun beberapa istilah jaringan lain yang berkaitan :

1. WLAN (Wireless Local Area Network)- Merupakan jaringan skala kecil, sama seperti LAN. Namun dalam konektivitasnya menggunakan jaringan wireless (tanpa kabel).

2. MAN (Metropolitan Area Network)- Merupakan jaringan skala menengah, diantara WAN dan LAN. MAN ini sendiri merupakan kumpulan dari LAN dan diimplementasikan pada jaringan seperti kota.

Topologi Jaringan

Dalam membangun sebuah jaringan, ada sebuah aspek penting yang harus diperhatikan, yaitu topologi. Topologi adalah sebuah cara bagaimana perangkat-perangkat jaringan ini dapat saling berkomunikasi, baik lewat menggunakan kabel maupun nirkabel. Tujuannya untuk mempermudah perangkat-perangkat tersebut saling bertukar informasi.



selain itu, efisien dalam memilih topologi yang digunakan juga dapat menghemat sumber daya perangkat dan juga pastinya lebih hemat dana.

Berikut ini penjelasan singkat beberapa topologi :

1. **Topologi Ring**
   Ini adalah metode topologi jaringan yang banyak digunakan di perusahaan. Sesuai dengan namanya, metode ini menghubungkan antarkomputer dengan cara membentuk rangkaian sepertisebuah lingkaran.

2. **Topologi Mesh/Fully Connected**
   Topologi jaringan mesh atau jala adalah sistem topologi di mana koneksi antar komputer saling terhubung secara langsung satu sama lain. Koneksi antarkomputer secara langsung seperti ini disebut dedicated link

3. **Topologi Star**
   Topologi jaringan berbentuk star atau bintang adalah jaringan dari beberapa komputer yang memiliki koneksi dengan node yang berada di jaringan pusat. Jadi, masing-masing perangkat memiliki koneksi dengan node yang berada di tengah sistem jaringan.

4. **Topologi Point to Point/Line**
   Jenis topologi linear sebenarnya merupakan perluasan dari jenis topologi bus, yang mana kabel utama di dalam jaringan harus dihubungkan dengan setiap titik-titik yang ada di komputer dengan T-Connector. Seperti yang dijelaskan sebelumnya, jaringan linear merupakan topologi jaringan yang memiliki layout cukup umum.

5. **Topologi Tree**
   Topologi jaringan berbentuk tree (pohon) merupakan bentuk gabungan dari sistem topologi bus dan star, di mana jaringan topologi bus menjadi konektor utama beberapa topologi star. Jika diibaratkan dengan bentuk seperti pohon, topologi bus adalah batang utama yang menghubungkan beberapa topologi starsebagai rantingnya.

6. **Topologi Bus**
   Topologi yang merupakan cara dalam jaringan komputer dalam menghubungkan suatu jaringan satu dengan yang lainnya menggunakan kabel tunggal yang menghubungkan ke client dan server. Metode topologi bus ini digunakan pada jaringan dengan skala

kecil yang semua perangkatnya saling terhubung dan membentuk sebuah bus, oleh karena itu disebut topologi bus.

NETWORK DEVICE

Sebelum kita dapat mengakses internet, terdapat sebuah proses panjang yang terjadi sehingga kita dapat menggunakan internet. Proses itu terjadi pada perangkatperangkat jaringan berjalan disekitar kita. Perangkat-perangkat tersebut saling terhubung hingga seluruh perangkat yang ada di bumi. Sehingga terciptalah internet. Maka dari itu, perangkat jaringan ini merupakan komponen penting dalam terbentuknya internet yang tersebar diseluruh negara.

Contoh Network Device dibawah ini :

1. **Router**
   Router termasuk kedalam perangkat WAN. Router sendiri merupakan perangkat Layer 3 – Network, yang bekerja berdasarkan IP Address. Data unit di perangkat router adalah Packet. Fungsi utamanya adalah untuk menghubungkan jaringanjaringan yang berbeda. Dan juga sebagai penghubung antara jaringan LAN dan WAN.

2. **Switch**
   Switch, pada dasarnya merupakan perangkat Layer 2 – Datalink, yang bekerja berdasarkan MAC Address. Data unit perangkat Switch adalah Frame. Switch digunakan untuk menghubungkan beberapa komputer dalam 1 broadcast domain / 1 jaringan.

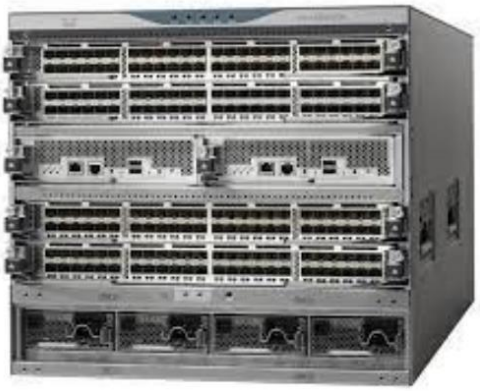
3. **Access-Point**
   Access Point merupakan perangkat jaringan yang bekerja menggunakan teknologi wireless, sehingga memungkinkan kita untuk mengkoneksikan perangkat kita ke Access Point tersebut tanpa harus menggunakan kabel.

4. Server

Server merupakan sebuah komputer atau perangkat yang menyediakan layanan atau fungsi untuk sebuah program atau perangkat lain yang biasa disebut klien. Tujuan dari server adalah untuk berbagi data serta sumber daya serta mendistribusikannya kepada klien yang ingin menggunakan data atau sumber daya tersebut.

5. MLS

MLS adalah salah satu jenis switch yang bekerja pada 2 layer yaitu : Data Link dan Network, switch ini berfungsi sebagai layer-3 ketika mengaktifkan fungsi routernya yaitu ***ip routing*** dan MLS bisa memasang IP Address dengan mengaktifkan command ***no switchport***.



PYHSICAL INTERFACE AND CABLE TYPE

Ethernet

Ethernet merupakan jenis perkabelan dan pemrosesan sinyal untuk data jaringan komputer. Ethernet merupakan sebuah teknologi yang sudah dikenal oleh masyarakat luas sebagai interface yang digunakan untuk konektivitas perangkat komputer maupun laptop, hampir di setiap jaringan LAN (Local Area Network) di seluruh dunia. Ethernet menggunakan standar IEEE 802.3. Ethernet ini bisa menggunakan kabel twisted pair ataupun fiber optic.

IEEE Ethernet

Standards ethernet didefinisikan dalam standar IEEE 802.3 Standar ini menentukan spesifikasi layer fisik dan data-link untuk Ethernet. Berfungsi sebagai standar LAN paling populer untuk framing dan menyiapkan data untuk transmisi ke media jaringan.

Standar 802.3 yang paling penting untuk diketahui diantaranya :

1. **10Base-T (IEEE 802.3)** -10 Mbps dengan kabel cat 3 UTP. Jangkauan hingga 100 meter.

2. **100Base-TX (IEEE 802.3u)** -dikenal juga sebagai Fast Ethernet, menggunakan kabel cat 5, 5E, atau cat 6 dengan jangkauan 100 meter.

3. **100Base-FX (IEEE 802.3u)** -versi Fast Ethernet yang menggunakan kabel fiber optic dengan jangkauan hingga 412 meter.

4. **100Base-CX (80002.3z)** -menggunakan kabel twisted-pair dengan jangkaun 25 meter.

5. **100Base-T (IEEE 802.3ab)** -Gigabit Ethernet yang menggunakan Kabel cat 5 UTP dengan jangkauan 100 meter.

6. **100Base-SX (IEEE 802.3z)** -1 Gigabit Ethernet yang berjalan menggunakan multimode kabel fiberoptic.

7. **100Base-LX (IEEE 802.3z)** -1 Gigabit Ethernet yang berjalan single-mode kabel fiber optic.

8. **100Base-T (802.an)** -Koneksi dengan kecepatan 10 Gbps dengan kategori cat 5e, 6, 7 kabel UTP.

Jika kita perhatikan nomor pertama dari standar tersebut mewakilkan kecepatan dengan satuan megabits per detik. Bagian terakhir dari standard tersebut mengacu pada jenis kabel yang digunakan untuk membawa sinyal. Sebagai contoh, 1000Base-T berarti bahwa kecepatan jaringan up to 1000 Mbps, menggunakan sinyal baseband, dan menggunakan kabel twisted-pair (T sendiri melambangkan dari Twisted-pair).

Ada tiga jenis kabel yang biasa digunakan untuk pemasangan kabel Ethernet :

• **coaxial** (biasa digunakan untuk tv kabel)

• **twisted pair** (biasa digunakan untuk LAN)

• **fiber optic** (digunakan untuk jaringan yang dituntut berkinerja tinggi)

Fiber Optic

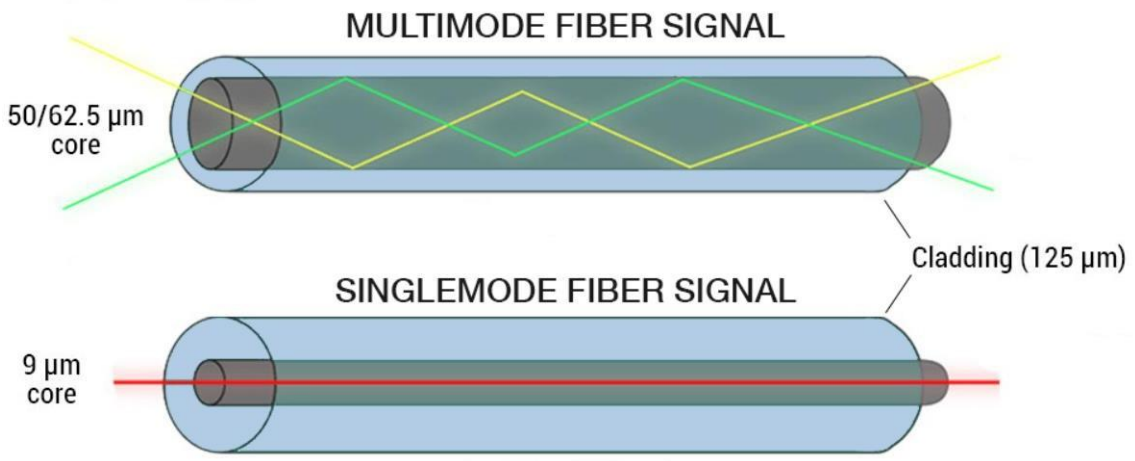
Berbeda dengan kabel twisted-pair, kabel fiber menggunakan cahaya untuk transmisi data dan dengan alasan inilah Fiber Optic bekerja lebih baik dibandingkan twisted-pair yang menggunakan gelombang elektromagnetik untuk transmisi data.

Kelebihan dari Fiber Optic dibanding temannya twisted-pair ialah :

1. Jangkauan lebih jauh
2. Bandwidth lebih besar
3. Bebas gangguan interferensi gelombang elektromagnetik.

Namun walau begitu, menggunakan fiber optic tentunya ada kekurangannya juga. Biaya pemasangan yang tidak murah, pemasangan yang memerlukan keahlian khusus, dll.

Fiber Optic dibagi menjadi 2 jenis yaitu :



PoE

Power Over Ethernet (PoE) adalah teknologi yang berfungsi untuk memberi daya pada perangkat melalui kabel jaringan Ethernet biasa. Kelebihan utama menggunakan PoE ialah flexibility, karena kita bisa menyimpan perangkat kita dimana saja, tanpa harus memikirkan electrical outlet. Namun tentu saja ada kekurangan menggunakan PoE, salah satu kendala utamanya ialah suhu perangkat yang tinggi.

Device yang menggunakan PoE diantaranya :

• VoIP phones

• IP cameras

• Wireless access points

• IoT devices

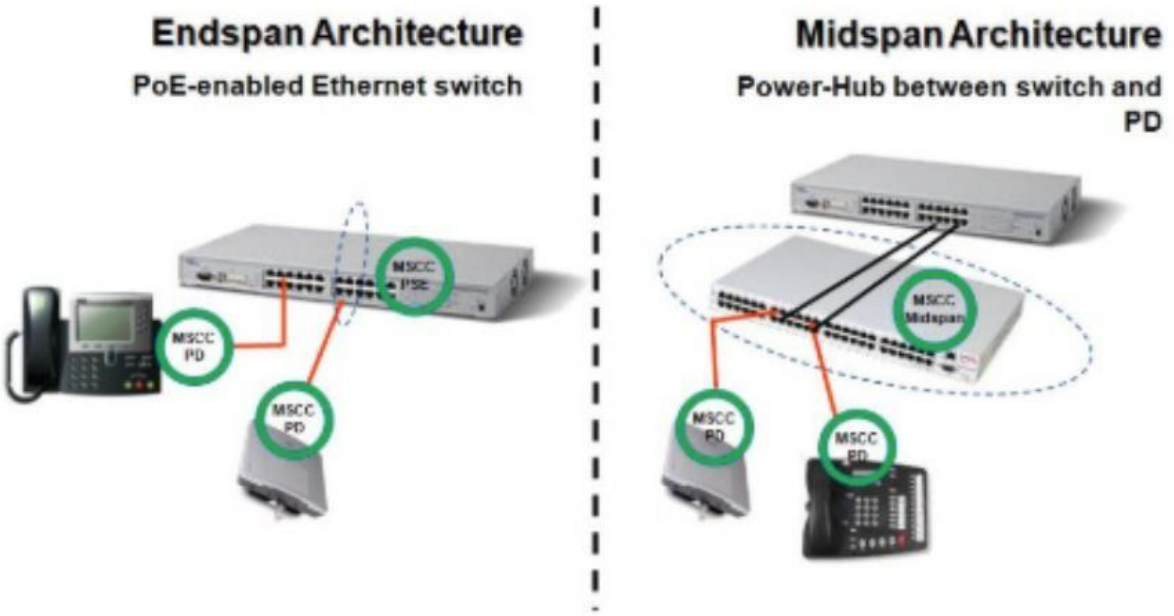
• Small routers and switches

Device yang diberi power oleh PoE disebut **Powered Device (PD).**

Ada dua jenis penggunaan PoE, yaitu **endspan** dan **midspan**.

Endspan, artinya pada perangkat (switch, router, atau sejenisnya) sudah tersedia fitur PoE, sehingga perangkat bisa memberikan power (PoE out).

Midspan, artinya perangkat tidak bisa memberikan power. Di antara perangkat utama dengan perangkat tujuan dihubungkan dengan PoE injector (perangkat penengah) sebagai midspan.



How to choose?

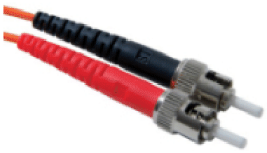
- Midspan memerlukan dua device untuk di manage. Memerlukan extra space di rack.
- Kalo switch-nya baru beli, dan ga support PoE mending pilih yang midspan. Ganti switch cuman buat.

PoE adalah solusi yang mahal

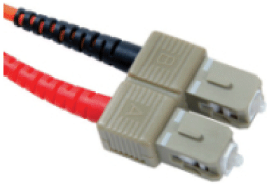
- Endspan walau keliatannya mantap, tapi tentu saja ada kekurangannya. Power yang tersedia terbatas, sehingga bisa saja setiap port tidak mendapat power yang maximum.

PHYSICAL TERMINATIONS

Optical Terminations



ST (Straight Tip)



SC (Subscriber Connector)

LC (Local Connector)

MT-RJ

Wireless Antennas

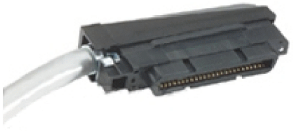
RP-TNC

RP-SMA

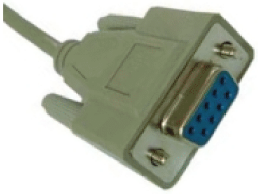
Copper Terminations

RJ-45

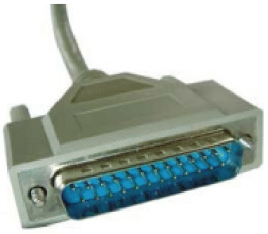
RJ-11



RJ-21 (25-pair)



DE-9 (Female)



DB-25 (Male)

DB-60 (Male)

GBICs

1000Base-SX/LX

1000Base-T

Cisco GigaStack

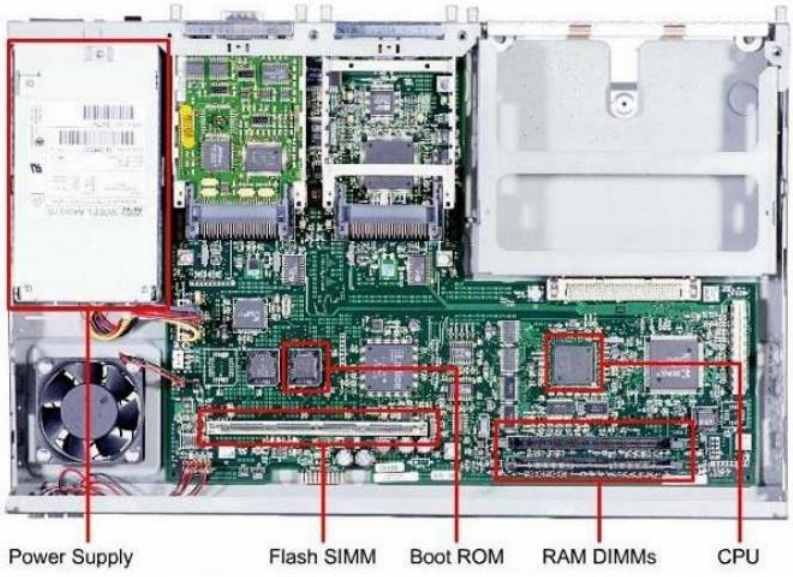
1000Base-SX/LX SFP

1000Base-T SFP

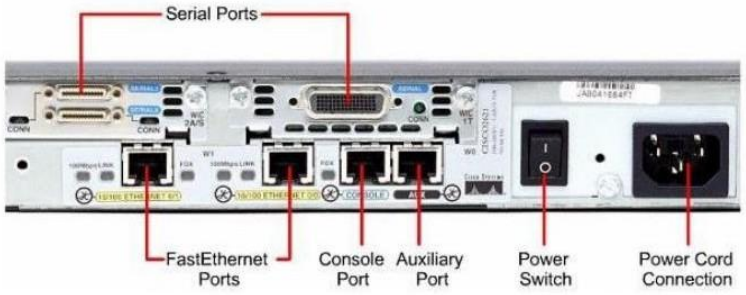
X2 (10Gig)

PENGENALAN CISCO ROUTER DAN SWITCH

Cisco ini, terkenal dengan produk Router dan Switchnya, dan kita akan mempelajari bentuk dan komponen-komponen penyusun dari router. Berikut gambarnya :



Gambar 1 . 12 Komponen internal Cisco router 2600



Gambar 1 . 13 Komponen External Cisco router 2600

Bagian utama router :

1. **Power Supply**
   Power Supply, merupakan komponen yang memiliki tugas utama menyediakan sumber daya untuk pengoperasian komponen didalam router. Beberapa router memiliki beberapa power supply.

2. **CPU**
   Ini adalah bagian inti dari riuter, yang fungsinya sebagai otak si router dalam melakukan routing.

3. **RAM**
   Bagian ini berfungsi sebagai penyimpanan sementara dari routing tabel dan segala konfigurasi yang dijalankan di router.

4. **NVRAM**
   Merupakan tempat penyimpanan startup configuration yaitu penyimpanan konfigurasi yang di-save atau disimpan. Dan startup configuration berjalan ketika router pertama kali dinyalakan.

5. **FLASH**
   Flash merupakan tempat penyimpanan Os dari routernya yaitu Cisco IOS.

Perbedaan Hub, Switch dan Router

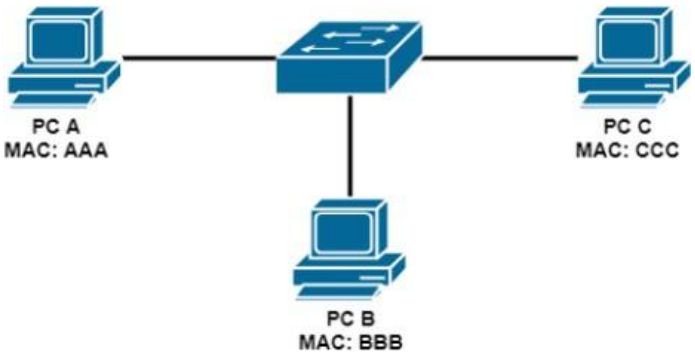
A. Hub

Hub tidak lebih dari physical repeater yang bekerja pada layer 1 dan tidak punya intelijensi. Cara kerja hub adalah dengan menerima sinyal electric dari satu interface dan mengirimkannya ke semua interface kecuali ke source interface, butuh atau tidak butuh. Karena bekerja pada layer physical dengan half-duplex (satu mengirim, yang lain menunggu), maka dapat terjadi tabrakan (collision) ketika ada packet yang dikirimkan dalam waktu yang bersamaan. Area dimana dapat terjadi collision disebut dengan collision domain.

B. **Switch**

Switch ini mirip dengan bridge, namun memiliki banyak kelebihan. Terdapat banyak port dan bermacam jenis.

Cara kerja switch



• Switch mempunyai tabel MAC Address yang menyimpan MAC Address dari PC yang tersambung ke port-port pada switch. Misal ketika pertama kali ketika PC disambungkan ke switch, PC A ingin mengirimkan data ke C.

• Maka PC A membuat Ethernet frame berisi IP address, MAC address dan tujuannya dan mengirimkannya ke switch.

• Switch lalu membroadcastnya ke semua port kecuali source. Sampai sini, switch telah menyimpan MAC address A.

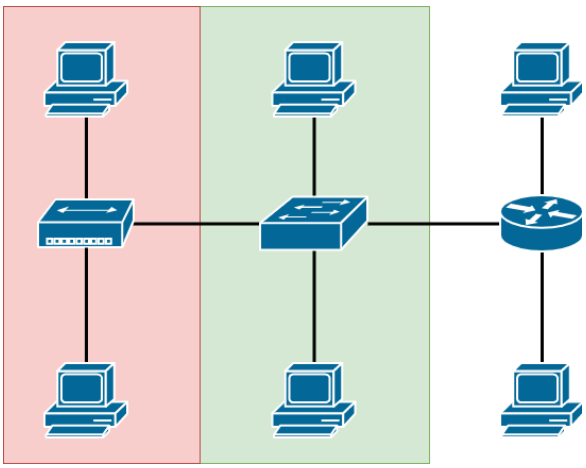
• Setelah dibroadcast, PC C akan mengirim reply berisi MAC addressnya dan ketika lewat switch, switch akan menyimpan MAC address C.
Catatan : Switch melakukan broadcast hanya ketika ada packet data yang destination MAC addressnya tidak terdapat pada tabel MAC address switch.

C. **Router**

Jika switch dan hub hanya dapat menghubungkan pada satu jaringan saja. Maka router, adalah perangkat jaringan yang tugasnya menghubungkan antar jaringan yang berbeda.

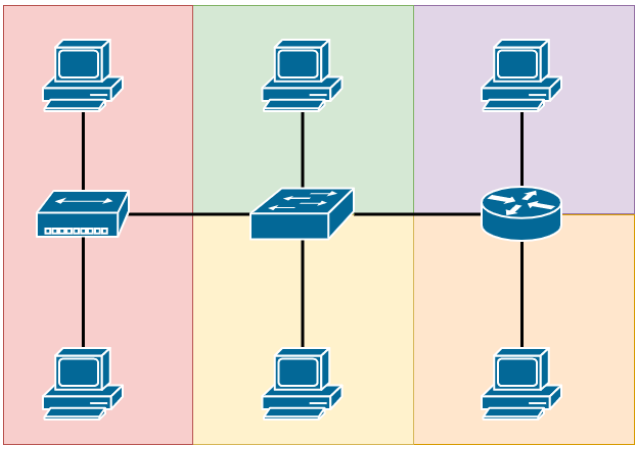
BROADCAST DOMAIN & COLLISION DOMAIN

Broadcast Domain



Broadcast domain, adalah sebuah area pada suatu network, dimana ketika ada packet yang lewat, maka packet tersebut akan di broadcast (disebarkan) ke semua port. Hub dan Switch memiliki Broadcast domain yang sama, karena sama-sama membroadcast packet tersebut keseluruh port yang dimilikinya, Sementara router tidak.

Collision Domain



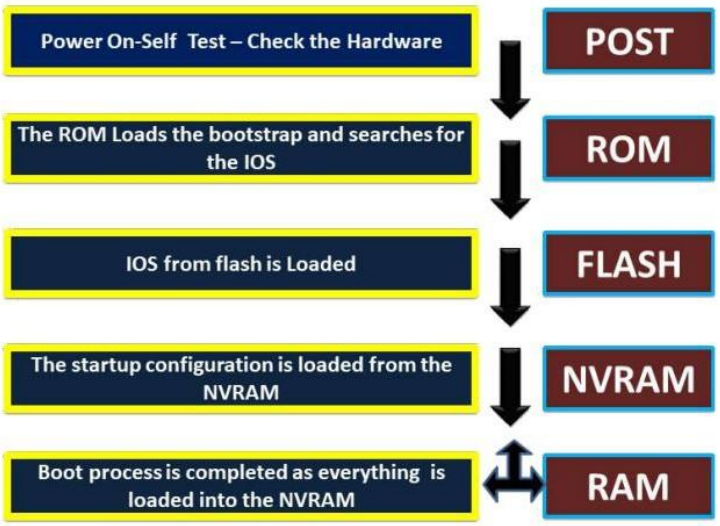
Collision domain, adalah sebuah area pada suatu network, dimana packet yang dikirimkan dapat mengalami tabrakan (collision) dikarenakan dikirim dalam waktu yang bersamaan. Hub memiliki collision domain 1 (besar) karena sifat hub half-duplex, sehingga dapat mengakibatkan terjadinya collision. Sementara itu, pada switch dan router, collision domain hanya terjadi pada tiap interface saja.

Half Duplex : Sebuah cara pengiriman data dengan cara menunggu satu data terkirim terlebih dahulu, barulah data yang lain bisa dikirim. Metode ini memungkinkan besanya terjadi tabrakan (collision). Contoh: Hub

Full Duplex : Sebuah cara pengiriman data dengan data bebas dikirim kemana saja, karena tiap data memiliki jalurnya masing-masing. Metode ini keci kemungkinannya terjadi tabrakan (collision). Contoh: Switch.

BOOTING PROCESS

Router akan mengalami beberapa process booting sebelum dapat digunakan, berikut penjelasannya.



- **POST (Power on Self-Test)**
  Power on Self-Test (POST) merupakan proses yang biasa dilakukan hampir disemua komputer, khususnya saat menjalankan prosedur bootup. Proses POST dilakukan untuk memeriksa perangkat keras (hardware) yang terdapat pada sebuah router. Ketika router dinyalakan, perangkat lunak (software) pada chip ROM melakukan POST.

- **ROM Bootstrap**
  Setelah proses POST, program bootstrap akan di-copy dari ROM ke RAM. Setelah program bootstrap berada didalam RAM, processor akan menjalankan instruksi yang terdapat pada program bootstrap tersebut. Fungsi utama program bootsrap adalah mencari lokasi keberadaan dari Cisco IOS (operating system) dan kemudian memuat IOS tersebut kedalam RAM.

- **IOS Load**
  Biasanya Internetwork Operating System (IOS) disimpan didalam “flash memory”, tetapi dapat juga disimpan pada media lainnya, contohnya pada TFTP server (Trivial File Transfer Protocol).

- **Configuration Load NVRAM**
  Setelah IOS di-copy dari flash memory ke RAM, program bootstrap akan mencari file “startup configuration” atau biasanya disebut “startup-config”. Pada file ini terdapat perintah-perintah konfigurasi.

- **Running Config RAM**
  Jika IOS menemukan startup-config pada NVRAM, selanjutnya IOS akan memuat startup-config kedalam RAM. Setelah dimuat ke dalam RAM, startup-config akan disebut sebagai running-config.

IPv4 & SUBNETTING

Secara dasar, dalam sebuah jaringan kita pasti membutuhkan sebuah alamat atau address agar semuanya bisa saling berkomunikasi atau terhubung. Atau bisa disebut juga, kita membutuhkan destinasi/tujuan kemana packet-packet yang kita kirimkan akan sampai. Hal seperti itu pasti membutuhkan yang namanya Sender/Pengirim dan Receiver/Penerima. Dan jangan lupa, IP Address ini merupakan pengalamatan yang bekerja di layer 3 atau layer network pada OSI Layer.

Karakteristik IP (Internet Protocol) :

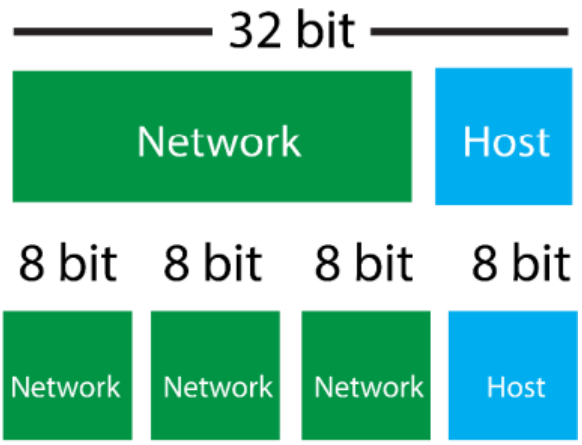
1. Beroperasi pada Layer Network di OSI Model.

2. Connectionless protocol: IP tidak meng-setup sebuah koneksi, sehingga untuk mengirim data kita memerlukan “transport” layer dan menggunakan TCP dan UDP.

3. Hierarkis : IP address memiliki aturan penyusunannya sendiri, pembahasannya akan dibahas pada pembahasan subnetting dan subnet mask IPv4 Address total bit-nya adalah 32-bit dan terdiri dari 2 bagian, Network dan Host.

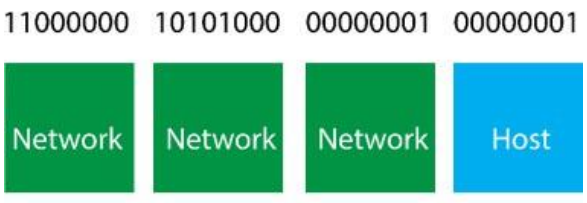
Penulisan IPv4

Namun, dalam penulisannya, IPv4 dibagi menjadi 8 blok, yang masing-masing blok itu berjumlah 8 bit, bit ini yang sering juga dicebut dengan byte. Jadi 8x4= 32 bit.



Gambar 1 . 3 Total bit IPv4

Maksud dari 8 bit ini, pada tiap blok memiliki 8 bilangan biner (0/1) Seperti gambar dibawah ini.



Gambar 1 . 4 Biner pada 4 blok IPv4

Konversi Binary ke Desimal

Agar IPv4 bisa digunakan pada perangkat, maka kita harus mengonversi IPv4 ini menjadi bilangan desimal terlebih dahulu. Cara mengonversinya jika tidak menggunakan kalkulator, dapat menggunakan tabel dibawah ini.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Pada tabel diatas terdapat 8 kolom yang diisi oleh 8 angka biner. Sementara angka yang berada diatasnya merupakan hasil pembagian dari 2^8.

Cara menggunakannya, tinggal mengisi angka 8-bit tadi secara urut dari kiri kekanan. Lalu jumlahkan angka yang berada diatas angka biner 1, angka 0 tidak usah.

Menurut tabel diatas, kita jumlahkan 128 + 64 = 192.

Berarti angka decimal dari biner 110000000 adalah 192.

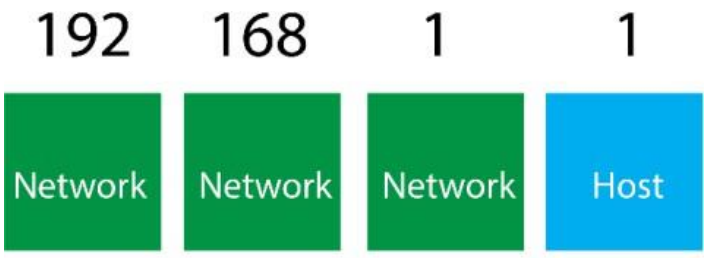
Kita lanjut dari ke blok selanjutnya dengan biner **10101000**. Caranya masih sama jika menggunakan tabel.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Berdasarkan tabel diatas, kita tinggal menjumlahkan 128 + 32 + 8/ angka diatas biner 1. Maka hasilnya adalah **168**.

Berarti decimal dari **10101000** adalah **168.**



Gambar 1 . 4 Desimal pada 4 blok subnet

Dan untuk 2 blok terakhir, karena binernya sama maka kita tinggal menghitung

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Sudah terlihat hasilnya, berarti decimal dari **00000001** adalah **1**. Hasilnya jika angka biner dari 4 blok diatas kita susun dalam bentuk decimal, maka akan diperoleh IP Address: **192.168.1.1** Begitulah cara konversi IPv4 dari biner ke decimal.

Konversi Desimal ke Binary

Setelah kita mengetahui bagaimana mengonversi binary ke decimal, kita juga harus mengetahui bagaimana caranya mengonversi Desimal ke Binary/biner. Misalkan mengonversi decimal 105, berapakah binernya?

Cara Pertama

Caranya adalah dengan membagi 2 tiap bilangan, jika bisa dibagi alias genap maka kita tandai dengan angka 0, jika tidak bisa dibagi alias ganjil, kita tandai dengan angka satu dan kita kurangi 1 pada angka ganjil tersebut, sehingga dapat dibagi. Terus dibagi hingga angka tersebut habis. Jika sudah kita urutkan tanda (0/1) yang telah kita tandai dari tiap pembagian. Kita urutkan dari bawah, maka disitu sudah terlihat angka binernya.

Caranya bisa dilihat pada gambar berikut

Gambar 1 . 5 Cara konversi decimal ke binary

Jika dijabarkan, seperti ini :

1. 105/2 :karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1 Maka (105-1)/2, hasilnya adalah 52 .

2. 52/2 : karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 26.

3. 26/2 : karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 13.

4. 13/2 : karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka (13-1)/2, hasilnya adalah 6.

5. 6/2 : karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 3

6. 3/2 : karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka (3-1)/2, hasilnya adalah 1

7. ½ : karena tidak bisa dibagi dan sudah habis, kita tandai saja dengan angka 1

8. Seperti yang kita lihat, pembagiannya sudah habis, sementara itu jumlah angka biner nya (0/1) belum mencapai 8 alias 8-bit. Maka dari itu, kita tambahkan saja angka 0 dibelakang hingga mencapai 8-bit.

9. Jika sudah, kita urutkan tanda biner yang telah kita buat dari bawah keatas, maka kita akan mendapatkan 1101001 + 0 (melengkapi 8-bit).

Kita coba satu contoh konversi lagi.

Kita konversi decimal 11, berapakah binernya?

1. 11/2: (11-1)/2 = 5 (1) -> tandanya
2. 5/2: (5-1)/2 = 2 (1) -> tandanya
3. 2/2= 1 (0) -> tandanya
4. 1/2: sudah habis dan tidak bisa dibagi (1) -> tandanya
5. Kita urutkan tandanya dari bawah keatas. Maka biner dari 11 adalah 1011 + 0000 (untuk melengkapi 8-bit).

Berdasarkan cara konversi diatas, mungkin akan timbul pertanyaan, Mengapa harus 8-bit?

Alasannya simpel. Kita kembali ke materi penulisan IPv4. Karena, setiap blok pada IPv4 (yang terdiri dari 4 blok) itu terdiri atas 8-bit angka biner, oleh karena itu kita hanya mencari 8-bit angka biner agar dapat kita masukkan dalam sebuah blok pada IPv4.

Cara kedua

Caranya adalah dengan menggunakan tabel yang kita gunakan untuk mengonversi dari biner ke decimal.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Untuk menggunakan tabel diatas, kita harus bisa menggunakan logika. Misalkan kita mencari biner dari **75**. Maka kita mencari, penjumlahan berapa tambah berapakah dengan bilangan diatas agar mendapatkan angka **75**.

Didapat : 75= 64 + 8 + 2 + 1. Maka binernya adalah: **01001011**

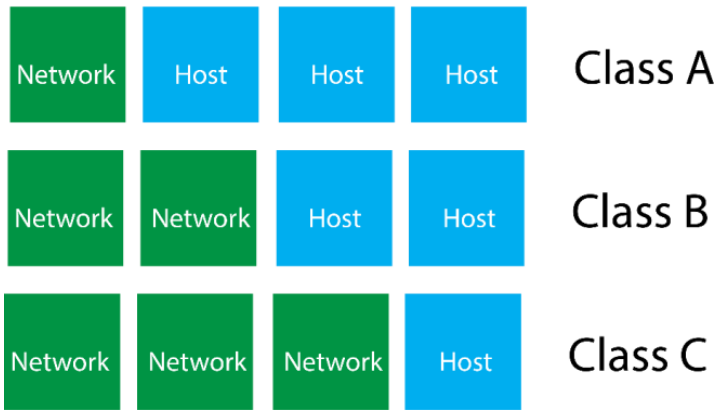
128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Begitulah cara konversi dari decimal ke biner, menurut kalian mudah yang mana? Cara pertama atau kedua?

Klasifikasi IPv4

IPv4 ini, dalam kegunaannya dibagi menjadi tiga kelas A, Kelas B, dan Kelas C.



Gambar 1 . 6 Pembagian kelas IPv4

Bagian pada IPv4

Bagian Network memberi tahu kita, ID dari Network yang kita gunakan. Bagian Host adalah angka unik yang berbeda di setiap perangkat yang mengidentifikasikan perangkat kita. Subnet mask berfungsi untuk memberi tahu komputer, mana bagian Network dan mana bagian Host.

- Kelas A, Kelas A bit pertamanya pasti 0.
- Kelas B, Kelas B 2-bit pertamanya pasti 10.
- Kelas C, Kelas C 3-bit pertamanya pasti 110.

Jika di konversi ke desimal maka kita dapat range IP Address :

- Kelas A = 0.0.0.0 - 126.255.255.255 <> USED FOR VERY LARGE NETWORK
- Kelas B = 128.0.0.0 - 191.255.255.255 <> USED FOR MEDIUM NETWORK
- Kelas C = 192.0.0.0 - 223.255.255.255 <> USER FOR SMALL NETWORKS

Ada pula kelas D dan E namun mereka tidak digunakan untuk penggunaan host :

- Kelas D = 224.0.0.0 - 239.255.255.255 <> USED FOR MULTICAST
- Kelas E = 240.0.0.0 - 247.255.255.255 <> USED FOR EXPERIMENTAL

Range IPv4 Private :

Kelas	Range IP	Subnet	Jumlah IP
A	10.0.0.0 – 10.255.255.255	255.0.0.0	16.777.212
B	172.16.0.0 – 172.16.31.255	255.255.0.0	8.190
C	192.168.0.0 – 192.168.255.255	255.255.255.0	65.354

Tabel 3 . 8 Daftar range IP Private IPv4

Ada juga range IP khusus yang digunakan untuk keperluan tertentu :

• 127.X.X.X = Digunakan untuk IP Loopback.

• 0.0.0.0 = Digunakan untuk routing seluruh network yang ada didunia (default route).

• 169.254.0.0/16 = Digunakan untuk Link Local Address(APIPA).

IPv4 Subnetting

packetlife.net

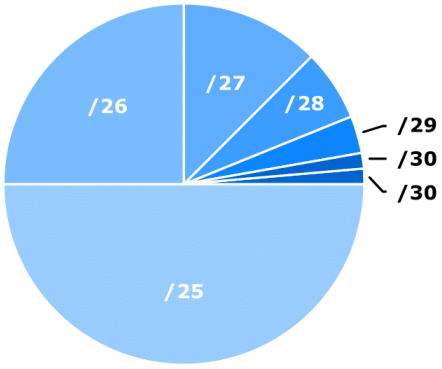
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes