

PERTEMUAN 1

KONSEP ROUTING

Definisi Routing

Routing merupakan sebuah proses yang digunakan untuk meneruskan paket-paket data didalam sebuah jaringan dari satu jaringan ke beberapa jaringan lainnya melalui internetworking.

Terdapat 2 jenis routing yang dikenal, yaitu:

1. Static Route
2. Dynamic Route

IP Routing

- IP Routing adalah perpindahan paket dari sebuah network ke network yang lainnya dan dilakukan oleh perangkat Layer 3.
- Perangkat Layer 3 disini adalah Router, atau Switch dengan kemampuan Layer 3 (Multilayer Switch – MLS).
- Kunci utama dari IP Routing adalah memahami cara kerja dari IP Address dan Subnetting

Jenis-Jenis Routing

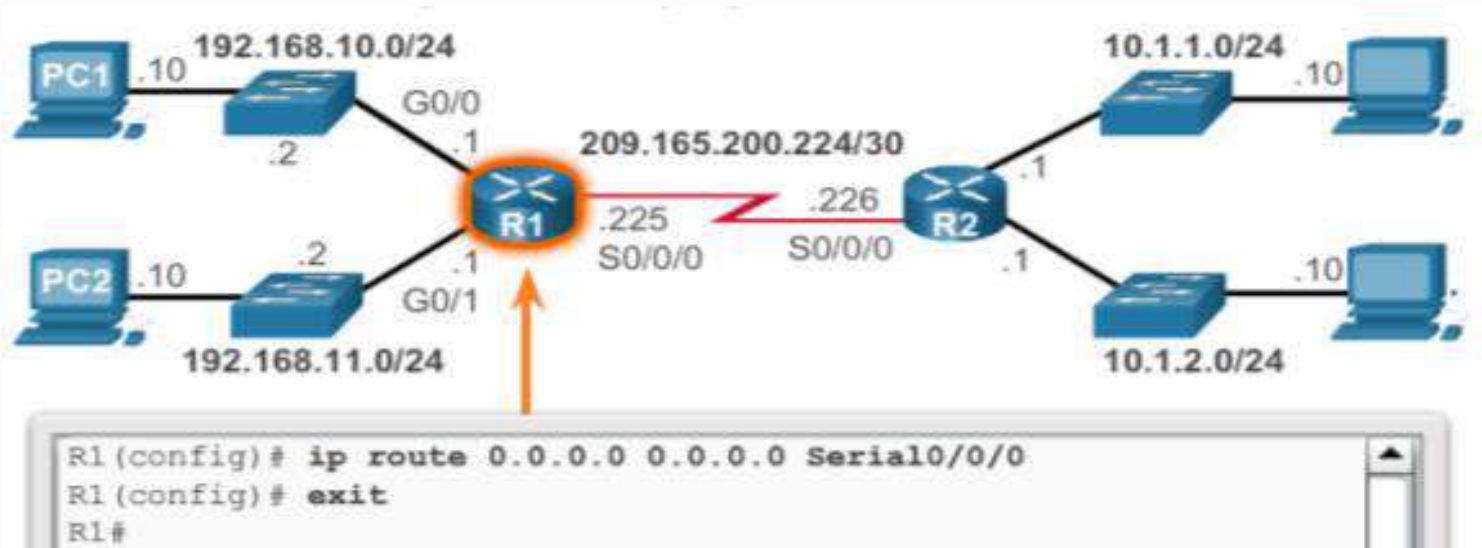
Static Routing

Routing statis merupakan routing yang dikonfigurasi secara manual oleh seorang network administrator dan mengaktifkan interface yang digunakan secara manual ketika ada penambahan tabel routing baru atau jika terjadi perubahan topologi baik menambahkan maupun menghapus

Karakteristik Static Routing

- Kesalahan dalam melakukan konfigurasi didalam routing static tidak dapat ditolerir
- Static Routing biasanya digunakan didalam jaringan yang hanya mempunyai beberapa router, umumnya tidak lebih dari 2 atau 3.

Contoh Konfigurasi Default Routing IPv4



Konfigurasi Default Routing dilakukan terhadap R1 dengan memasukkan network dan interface yang digunakan

Contoh Konfigurasi Static Routing IPv4



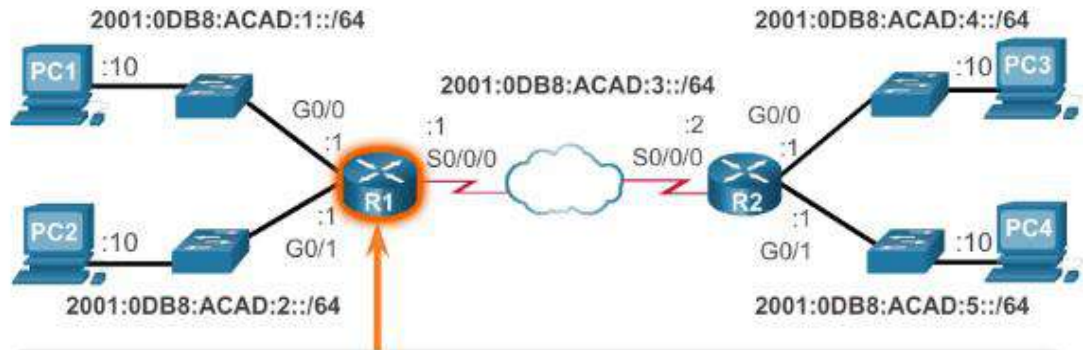
```

R2 (config)# ip route 192.168.10.0 255.255.255.0 s0/0/0
R2 (config)# ip route 192.168.11.0 255.255.255.0 209.165.200.225
R2 (config)# exit
R2#
R2# show ip route | begin Gateway
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C   10.1.1.0/24 is directly connected, GigabitEthernet0/0
L   10.1.1.1/32 is directly connected, GigabitEthernet0/0
C   10.1.2.0/24 is directly connected, GigabitEthernet0/1
L   10.1.2.1/32 is directly connected, GigabitEthernet0/1
S   192.168.10.0/24 is directly connected, Serial0/0/0
S   192.168.11.0/24 [1/0] via 209.165.200.225
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.224/30 is directly connected, Serial0/0/0
  
```

Contoh Konfigurasi Default Routing IPv6

Entering and Verifying an IPv6 Static Default Route

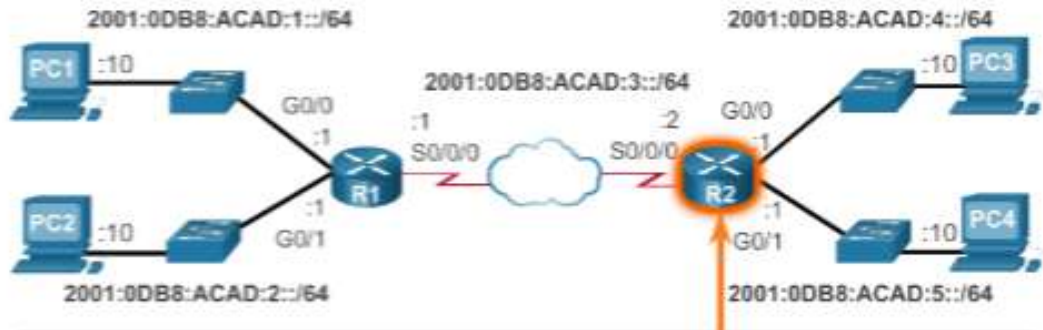


```
R1(config)# ipv6 route ::/0 s0/0/0
R1(config)# exit
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route
B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
D - EIGRP
EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
DCE - Destination
NDR - Redirect, O - OSPF Intra, OI - OSPF Inter,
OE1 - OSPF ext 1
OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S ::/0 [1/0]
  via Serial0/0/0, directly connected
C 2001:0DB8:ACAD:1::/64 [0/0]
  via GigabitEthernet0/0, directly connected
```

Contoh Konfigurasi Static Routing IPv6

Entering and Verifying IPv6 Static Routes



```
R2(config)# ipv6 route 2001:0DB8:ACAD:1::/64 2001:0DB8:ACAD:3::1
R2(config)# ipv6 route 2001:0DB8:ACAD:2::/64 s0/0/0
R2(config)# ^Z
R2#
```

```
R2# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static,
       U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
       D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
       DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter,
       OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    2001:0DB8:ACAD:1::/64 [1/0]
    via 2001:DB8:ACAD:3::1
S    2001:0DB8:ACAD:2::/64 [1/0]
    via Serial0/0/0, directly connected
```

Jenis-Jenis Routing

Dynamic Routing

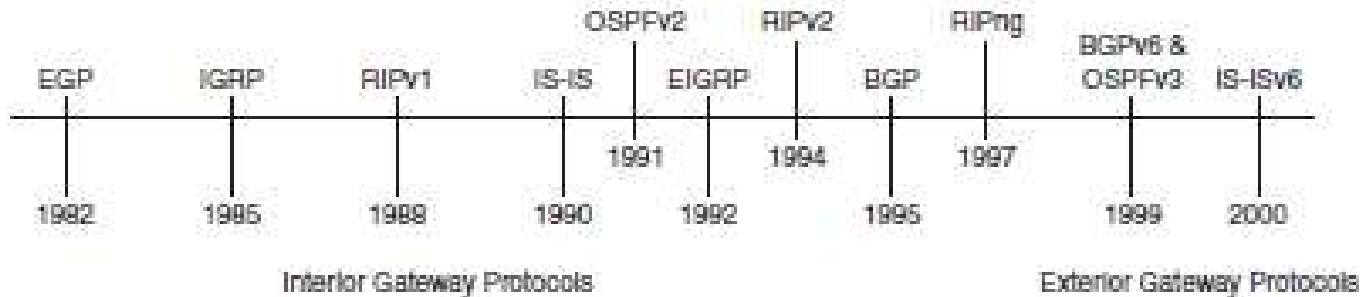
- Routing dinamis digunakan oleh router untuk berbagi informasi tentang reachability dan status jaringan jarak jauh,
- Digunakan untuk memelihara dan memperbaharui tabel routing secara otomatis.
- Routing dinamis dapat mempelajari rute secara otomatis untuk meneruskan paket data dari sebuah network ke network lainnya.

Karakteristik Dynamic Routing

- Tabel routing tidak diberikan secara manual lagi oleh seorang (administrator), melainkan menggunakan software
- Apabila salah satu jalur routing yang ada mengalami gangguan atau kerusakan peralatan, maka router akan secara otomatis mencari ganti dari jalur yang tidak dapat digunakan.
- Menangani jaringan yang lebih kompleks dan luas, atau jaringan yang konfigurasinya sering berubah-ubah

Jenis-Jenis Routing Dynamic Routing

Revolusi Dynamic Routing



	Distance Vector Routing Protocols	Link State Routing Protocols	Path Vector
Classful	RIP	IGRP	EGP
Classless	RIPv2	EIGRP, OSPFv2	BGPv4
IPv6	RIPng	EIGRP for IPv6, OSPFv3	BGPv4 for IPv6

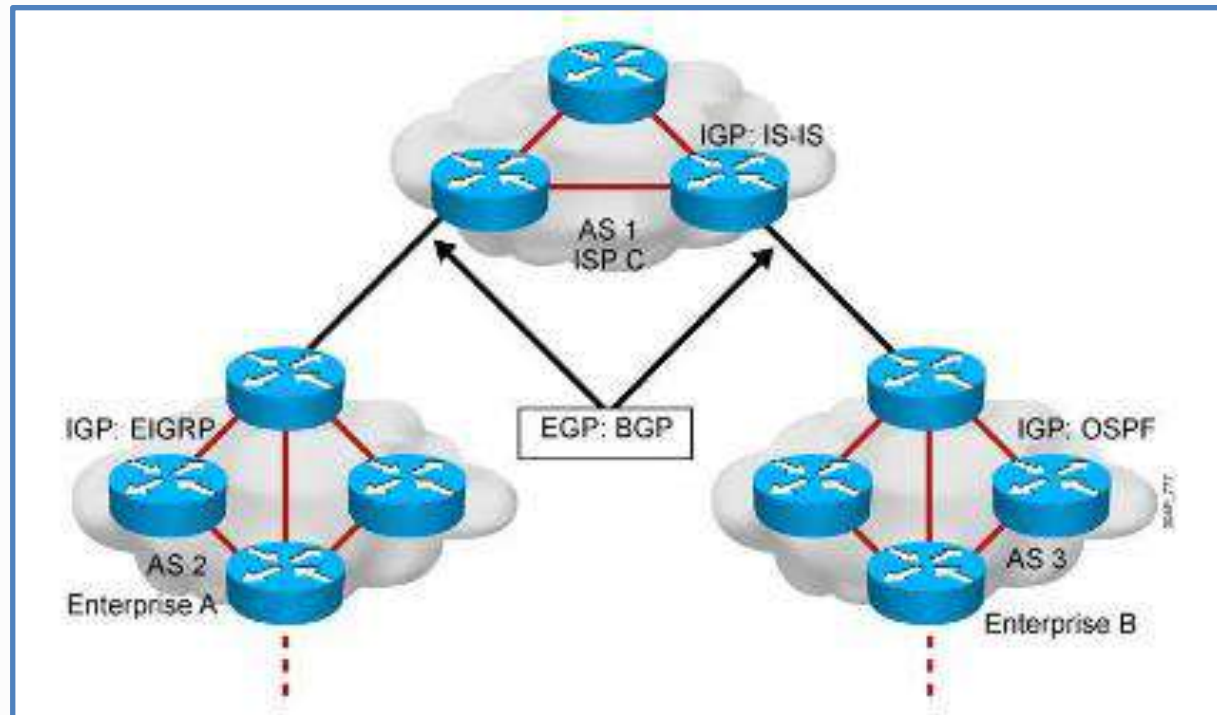
Routing Protocol

Interior Routing Protocol

Interior Routing Protocol biasanya digunakan pada jaringan yang bernama **Autonomous System**, yaitu sebuah jaringan yang berada hanya dalam satu kendali teknik yang terdiri dari beberapa subnetwork dan gateway yang saling berhubungan satu sama lain.

Routing Protocol

Exterior Routing Protocol



Exterior Routing Protocol, pada dasarnya terdiri dari beberapa **Autonomous System** yang saling berhubungan satu sama lainnya.

Routing Protocols

IPv4

EIGRP - Enhanced Interior Gateway Routing Protocol

OSPF - Open Shortest Path First

IS-IS - Intermediate System-to-Intermediate System

RIP - Routing Information Protocol

Routing Protocols

IPv6

RIPng (RIP generasi berikutnya)

OSPFv3

EIGRP untuk IPv6

Untuk mengaktifkan protocol routing IPv6 harus menggunakan perintah:

```
Router(config)#ipv6 unicast routing
```

Tabel Routing

Router akan memberi rekomendasi jalur mana yang paling tepat untuk melewati paket data yang dikirim ke alamat tertentu sesuai dengan informasi yang terdapat pada tabel routing sehingga pada saat paket data telah dikirimkan atau diarahkan maka router akan melakukan pemeriksaan yang terdapat pada tabel routing dan router akan menentukan jalur mana yang paling sesuai dengan informasi yang ada.

Perbandingan Static dan Dynamic Routing

Static Routing	Dynamic Routing
Hanya menggunakan IP Address	Menggunakan IP dan Routing Protocol (RIP/ OSPF/ EIGRP)
Router tidak saling bertukar informasi routing table mereka	Router yang bertetangga saling bertukar informasi routing table
Routing table diubah secara manual	Routing table berubah secara dinamis
Dipakai dalam jaringan skala kecil	Dipakai dalam jaringan skala besar

PERTEMUAN 2

STATIC ROUTING

Static Routing

- Static Routing merupakan routing yang dikonfigurasi secara manual oleh seorang network administrator.
- Static Routing dan Default Routing dapat digunakan setelah interface yang terkoneksi kedalam jaringan ditambahkan ke dalam tabel routing.

Fungsi Utama Static Routing

Routing static memiliki tiga fungsi utama, diantaranya:

- Menyediakan kemudahan dalam pemeliharaan tabel routing jaringan.
- Jaringan (neighbor) hanya diakses oleh satu rute, dan router tidak memiliki tetangga lainnya.
- Menggunakan rute default tunggal

Mengapa Menggunakan Static Routing?

Dikarenakan routing static memiliki beberapa **keunggulan** dibandingkan dengan routing dynamic, diantaranya:

- Routing static tidak melakukan broadcast jaringan, sehingga keamanan yang lebih baik.
- Static routing menggunakan bandwidth yang lebih kecil dibandingkan dengan protokol routing dynamic.
- Jalur yang digunakan untuk pengiriman paket data telah ditentukan.
- Menyediakan kemudahan dalam melakukan pemeliharaan tabel routing.
- Menggunakan Next Hop yang mampu untuk melakukan pencegahan terhadap terjadinya error didalam meneruskan paket data ke router tujuan.

Kelemahan Static Routing

- Rentan terhadap kesalahan dalam melakukan konfigurasi dan perawatan tabel routing.
- Administrator jaringan harus benar-benar memahami internetworking dan bagaimana setiap router dapat dihubungkan untuk dapat melakukan konfigurasi yang benar.
- Jika terdapat sebuah jaringan baru yang ditambahkan kedalam internetworking, administrator jaringan harus menambahkan sebuah route terhadap semua router secara manual.

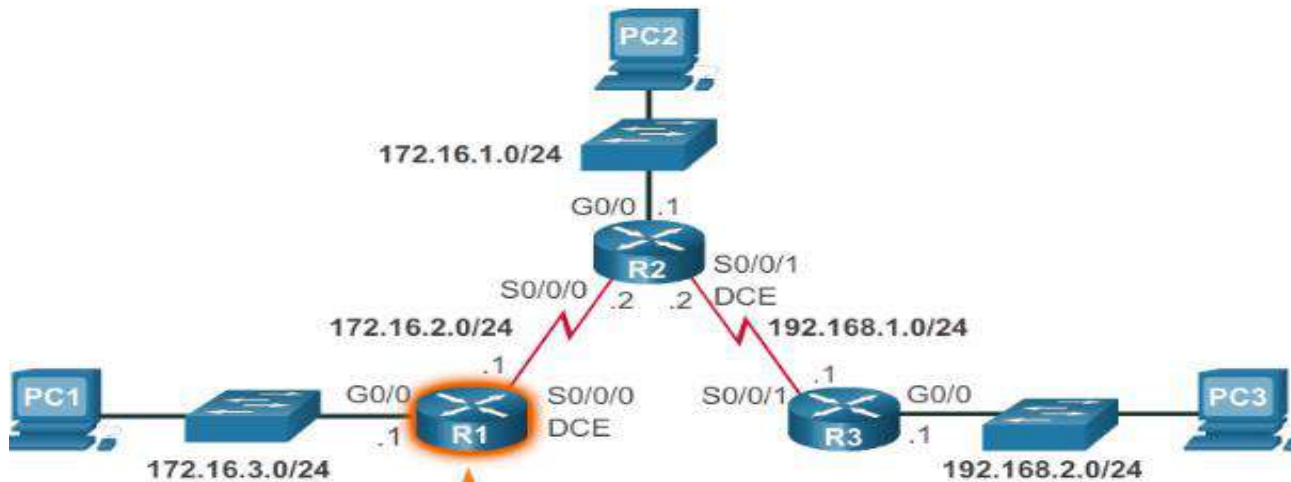
Perbedaan Konfigurasi Next Hop dengan Exit Interface

Model Konfigurasi	Kelebihan	Kekurangan
Penggunaan Next Hop	Dapat mencegah terjadinya error dalam meneruskan paket data ke router tujuan apabila router yang akan meneruskan paket memiliki link dengan banyak router.	Static routing yang menggunakan next hop akan mengalami multiple lookup atau lookup yg berulang.
Penggunaan exit interface	Proses lookup hanya akan terjadi satu kali saja (single lookup) karena router akan langsung meneruskan paket ke network tujuan melalui interface yang sesuai pada routing table	Kemungkinan akan terjadinya error jika router memiliki banyak link.

Perbedaan Konfigurasi Next Hop dengan Exit Interface

- Routing static dengan menggunakan next hop cocok digunakan untuk jaringan multi-access network atau point to multipoint.
- Sedangkan, untuk jaringan point to point cocok menggunakan exit interface dalam mengkonfigurasi static route.
- Recursive route lookup adalah proses yang terjadi pada routing tabel untuk menentukan exit interface mana yang akan digunakan ketika akan meneruskan paket ke tujuannya.

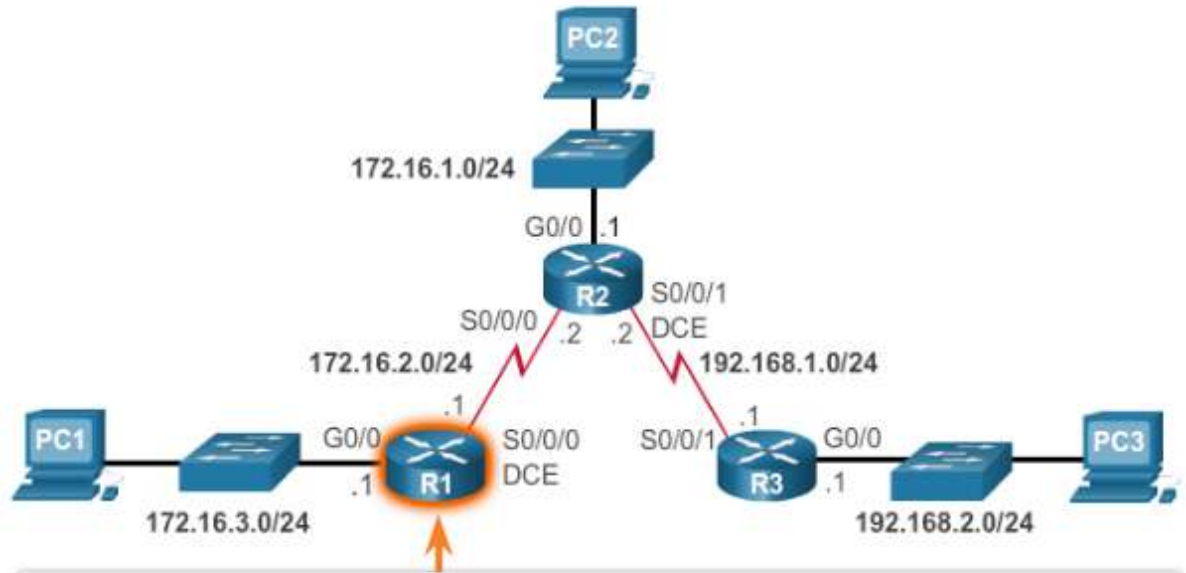
Konfigurasi Default Routing Static



```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2  
R1(config)#
```

Untuk melakukan konfigurasi default routing static dapat menggunakan perintah:
`ip route 0.0.0.0 0.0.0.0 {exit-interface | next-hop-ip}`

Konfigurasi Static Routing Next-Hop

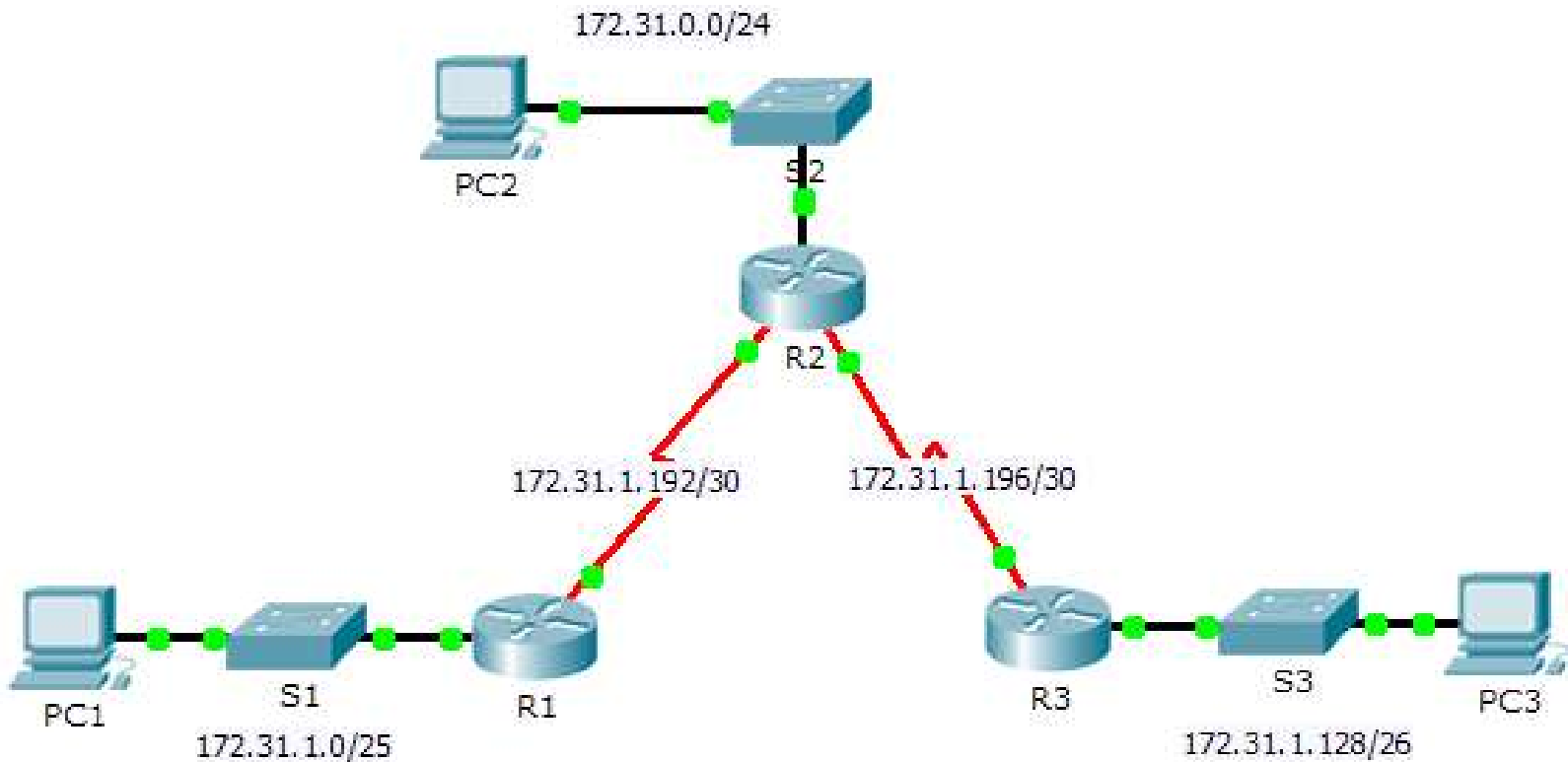


```
R1 (config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1 (config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1 (config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1 (config)#
```

Untuk melakukan konfigurasi routing static dapat menggunakan perintah:
`ip route network mask {next-hop-ip | exit-interface}`

DISKUSI

Configuring IPv4 Static and Default Router



Jalankan jaringan komputer dengan menggunakan PKA yang telah disediakan.

[Link: Configuring IPv4 Static and Default Router](#)

Diskusi

Configuring IPv4 Static Routing

Langkah 1: Konfigurasi yang dilakukan terhadap R1 adalah mendaftarkan alamat network yang digunakan pada R2 dan R3

```
R1(config)#ip route 172.31.0.0 255.255.255.0 172.31.1.193
```

```
R1(config)#ip route 172.31.1.196 255.255.255.252 172.31.1.193
```

```
R1(config)#ip route 172.31.1.128 255.255.255.192 172.31.1.193
```

Diskusi

Configuring IPv4 Static Routing

Langkah 2: Konfigurasi yang dilakukan terhadap R2 adalah mendaftarkan alamat network yang digunakan pada R1 dan R3

```
R2(config)#ip route 172.31.1.0 255.255.255.128 serial 0/0/0
```

```
R2(config)#ip route 172.31.1.128 255.255.255.192 serial 0/0/1
```

Diskusi

Configuring IPv4 Static Routing

Langkah 3: Konfigurasi yang dilakukan terhadap R3 adalah mendaftarkan alamat network yang digunakan pada R1 dan R2

```
R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
```

```
R3(config)#ip route 172.31.0.0 255.255.255.0 serial 0/0/1
```

```
R3(config)#ip route 172.31.1.192 255.255.255.252 serial 0/0/1
```

```
R3(config)#ip route 172.31.1.0 255.255.255.128 serial 0/0/1
```

Diskusi

Configuring IPv4 Static Routing

Langkah 4: Verifikasi routing terhadap R1, R2 dan R3 menggunakan perintah “R1#show ip route”

Langkah 5: Uji konektifitas jaringan untuk memastikan jaringan dapat berjalan sesuai kebutuhan

PERTEMUAN 3

Dynamic Routing

Routing Dynamic

- Protokol routing dynamic adalah sebuah proses routing yang dilakukan oleh sebuah router dengan cara melakukan update tabel routingnya secara otomatis.
- Protokol routing dynamic mampu mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi forwarding table, tergantung keadaan jaringannya.

Evolusi Protocol Routing Dinamis

- Protokol routing dinamis telah digunakan dalam jaringan sejak akhir 1980-an. Dan protokol routing Enhanced Interior Gateway Routing Protocol (EIGRP) merupakan protokol routing proprietari Cisco, yang artinya hanya bisa dijalankan oleh perangkat router Cisco saja.
- Versi protokol routing dinamis yang lebih baru mampu mendukung komunikasi berdasarkan IPv6.

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Routing Dinamis

IPv4 dan IPv6

Routing Dinamis IPv4:

- EIGRP
- OSPF
- IS-IS
- RIP

```
R1(config)# router ?
  bgp      Border Gateway Protocol (BGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis     ISO IS-IS
  iso-igrp IGRP for OSI networks
  mobile   Mobile routes
  odr      On Demand stub Routes
  ospf     Open Shortest Path First (OSPF)
  ospfv3   OSPFv3
  rip      Routing Information Protocol (RIP)

R1(config)# router
```

Routing Dinamis

IPv4 dan IPv6

Routing Dinamis IPv6:

- RIPng
- OSPFv3
- EIGRP for IPv6

```
R1(config)# ipv6 router ?  
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)  
  ospf     Open Shortest Path First (OSPF)  
  rip      IPv6 Routing Information Protocol (RIPv6)  
  
R1(config)# router
```

Tujuan Protokol Routing Dinamis

- Penemuan jaringan (neighbor) dengan jarak yang berjauhan.
- Mempertahankan up-to-date informasi pada tabel routing.
- Mampu memilih jalur terbaik dalam proses pengiriman paket data didalam jaringan.

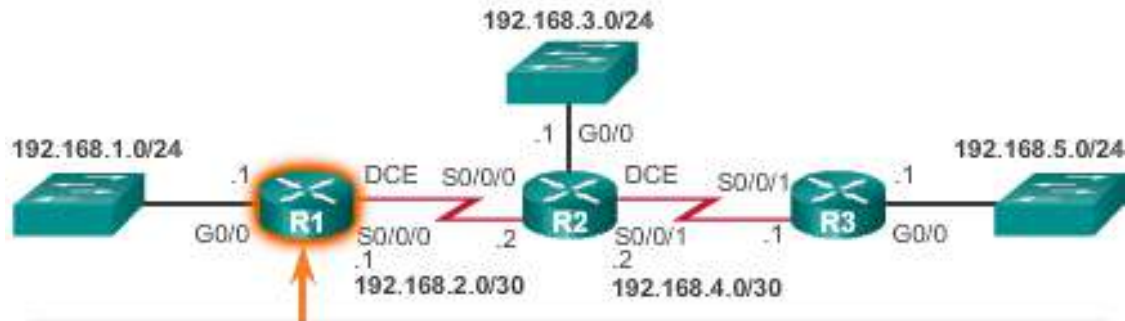
RIP

Routing Information Protocol

- Routing Information Protocol menggunakan algoritma *distance vector*, yaitu algoritma Bellman-Ford.
- RIP merupakan sebuah protokol routing dinamis yang digunakan dalam jaringan LAN dan WAN. Terdapat tiga versi dari Routing Information Protocol (RIP), yaitu:
 - RIPv1
 - RIPv2
 - RIPv6

RIPv1

- Dalam melakukan konfigurasi routing RIPv1, cukup memasukan network Address yang terhubung langsung dengan interface Router.
- RIPv1 bekerja menggunakan distance vektor untuk melakukan pencarian hop terpendek atau jalur terbaik.



```
R1 (config)#router rip
R1 (config-router)#network 192.168.1.0
R1 (config-router)#network 192.168.2.0
R1 (config-router)#
```

RIPv2

- RIPv2 merupakan perluasan dari RIPv1.
- RIPv2 sudah memiliki fitur konfigurasi menggunakan CIDR.
- Saat melakukan konfigurasi RIPv2 berisikan IP Address router berikutnya, sehingga dapat mencegah datagram dalam pengambilan rute yang tidak efisien.

Beberapa Kelebihan RIP

- RIP memiliki timer untuk mengetahui kapan router harus kembali untuk memberikan update informasi tabel routing.
- Jika terjadi perubahan pada jaringan, sementara timer belum habis, router tetap harus mengirimkan informasi routing karena dipicu oleh perubahan tersebut (triggered update).
- Mengimplementasikan routing menggunakan RIP tidaklah rumit dan penggunaan RIP mampu memberikan hasil yang cukup baik, terlebih jarang terjadi kegagalan pada penggunaan RIP didalam jaringan.

Beberapa Kekurangan RIP

- Terbatasnya jumlah Host yang dapat terkoneksi.
- RIP tidak memiliki informasi tentang subnet pada setiap route.
- RIP tidak mendukung penggunaan Variable Length Subnet Masking (VLSM).

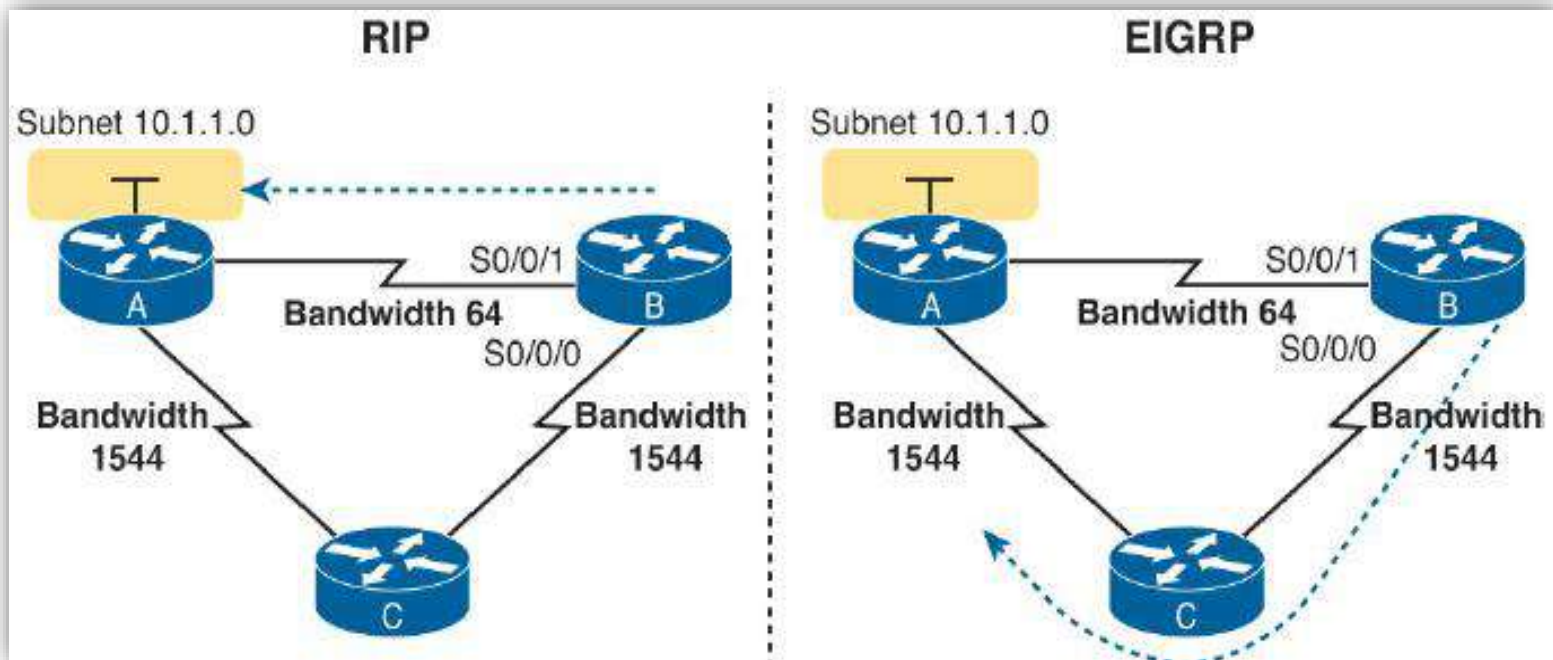
EIGRP

(Enhanced Interior Gateway Routing Protocol)

- EIGRP merupakan protokol routing lanjutan dari protokol IGRP.
- IGRP hanya mampu mendukung penggunaan /8 /16 /24. Sedangkan EIGRP mampu mendukung classless.
- EIGRP menggabungkan kemampuan dari **Link-State Protokol** dan **Distance Vector Protokol**, terlebih lagi EIGRP memuat beberapa protokol penting yang secara baik meningkatkan efisiensi penggunaannya dibandingkan dengan protokol lainnya.

EIGRP

Cara kerja protokol routing EIGRP



Fitur-fitur EIGRP

- Mampu mendukung penggunaan routing IPv4 dan IPv6.
- Support terhadap penggunaan VLSM/CIDR.
- Termasuk classless routing protocol.
- Update perubahan topologi secara dynamic dengan menggunakan Diffusing Update Algorithm (DUAL).
- Mendukung protocol IP, IPX, Apple Talk.
- Hello packet dikirimkan setiap 5 detik.

EIGRP

Konfigurasi Dasar

Mengaktifkan Routing EIGRP

```
“Router(config)#router eigrp[AS Number]”
```

Menentukan Router-id

```
“Router(config-router)#router eigrp-id [x.x.x.x]”
```

Nonaktifkan auto-summary

```
“Router(config-router)#no auto-summary”
```

Memasukan Network

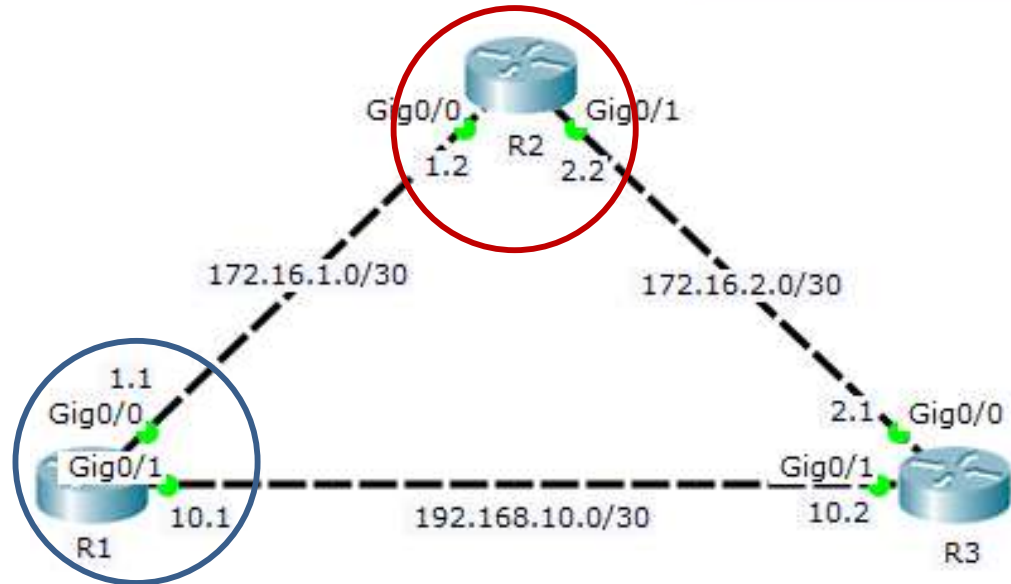
```
“Router(config-router)#network [n.n.n.n] [w.w.w.w]”
```

[n.n.n.n]: Alamat Network

[w.w.w.w]: Wildcard Mask atau kebalikan dari Subnet Mask

EIGRP

Konfigurasi Dasar



```
R1(config)# router eigrp 1
R1(config-router)#eigrp router-id 1.1.1.1
R1(config-router)#no auto-summary
R1(config-router)#network 172.16.1.0 0.0.0.3
R1(config-router)#network 192.168.10.0 0.0.0.3
```

```
R2(config)# router eigrp 1
R2(config-router)#eigrp router-id 1.1.1.1
R2(config-router)#no auto-summary
R2(config-router)#network 172.16.1.0 0.0.0.3
R2(config-router)#network 172.16.2.0 0.0.0.3
```

OSPF

(Open Shortest Path First)

- OSPF merupakan routing protokol standar yang bersifat terbuka yang telah diimplementasikan oleh beberapa vendor termasuk Cisco.
- OSPF lebih populer digunakan karena memilih jalur terpendek untuk melengkapi tabel routingnya.
- OPSF pun mampu mendukung untuk penggunaan IPv6.

OSPF

Fitur-fitur

Terdapat beberapa fitur-fitur dari OSPF diantaranya:

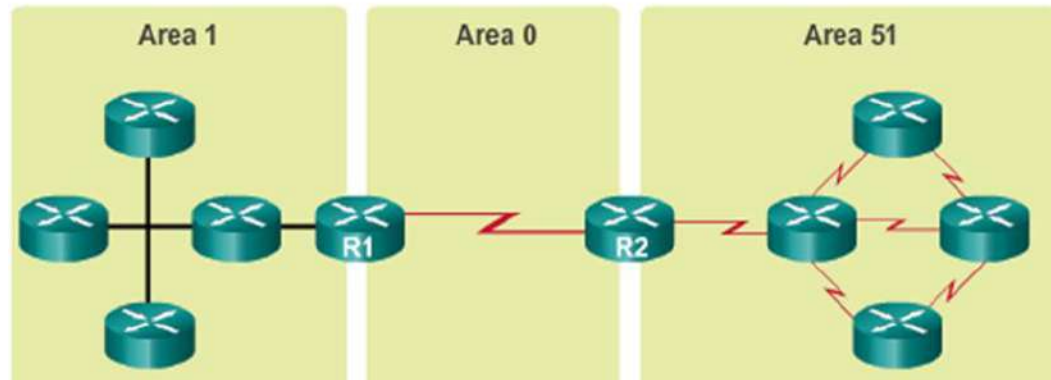
1. Memungkinkan untuk penciptaan area dan autonomous system.
2. Mampu meminimalkan lalu lintas routing.
3. Fleksibel, dan terukur.
4. Mendukung penggunaan VLSM/CIDR.

OSPF Area

Single-Area OSPF



Multiarea OSPF



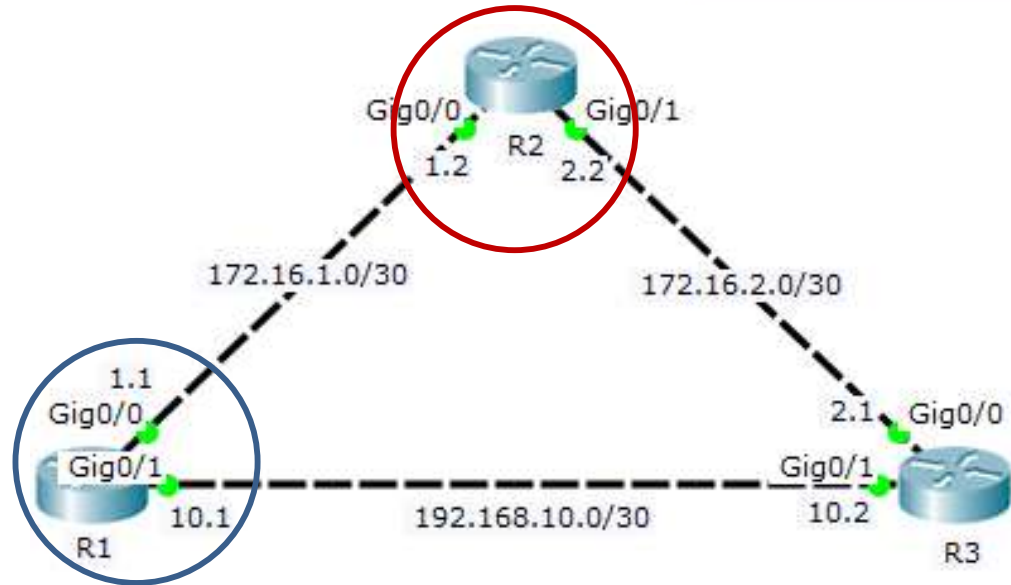
Cara Kerja OSPF

OSPF menggunakan logika Link-State (LS) yang mampu melakukan pemecahan dan pembuatan percabangan routingnya. Langkah demi langkah yang dilakukan pada Routing OSPF:

- **Langkah pertama** yang dilakukan oleh routing OSPF adalah menemukan Neighbor dari tabel routing.
- **Langkah kedua** yang dilakukan oleh routing OSPF adalah melakukan pertukaran database dari table routing yang didapatkan atau lebih sering disebut dengan Link-State Database (LSDB).

Cara Kerja OSPF

- **Langkah ketiga** yang dilakukan dari protokol routing OSPF adalah melakukan perhitungan berdasarkan rute untuk melakukan analisa secara independen agar mendapatkan rute terbaik.
- Secara khusus, algoritma yang digunakan pada OSPF adalah algoritma Shortest Path Firsts (SPF) yang digunakan untuk melakukan analisa data, jalur terbaik/jalur terpendek, dan netx-hop.
- Beberapa informasi yang didapatkan dari LSDB meliputi:
 - Keberadaan dan pengidentifikasi setiap ID router,
 - Mengetahui ip address, subnetmask yang digunakan pada interface router,
 - Membuat list interface router yang terjangkau/terhubung.



OSPF

Konfigurasi Dasar

```
R1(config)# router ospf 1
R1(config-router)#no auto-summary
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
```

```
R2(config)# router ospf 1
R2(config-router)#no auto-summary
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

Redistribute

EIGRP dan OSPF

Redistribute bertujuan untuk menyebarkan dan menggabungkan network dengan routing protokol yang berbeda. Atau bisa disebut dengan penghubung protokol routing EIGRP dengan protokol routing OSPF.

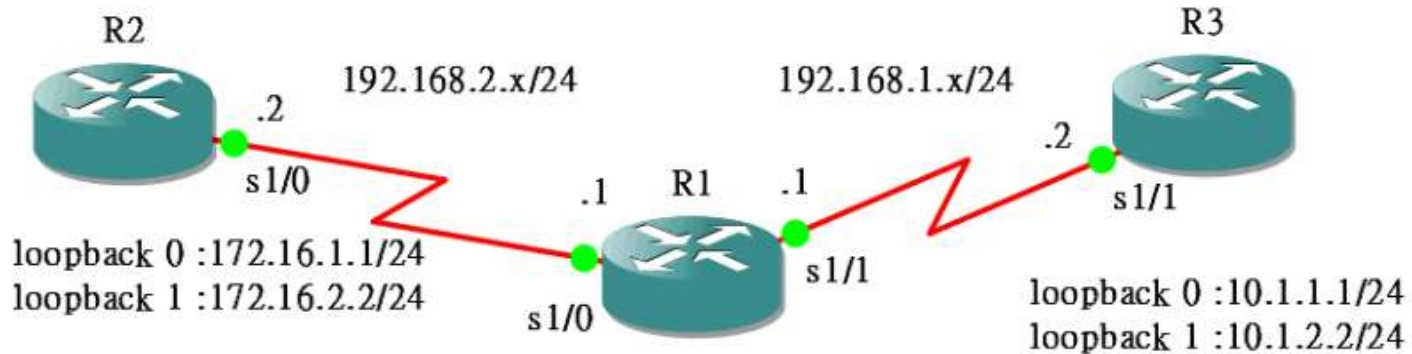
Redistribute terbagi menjadi beberapa macam, diantaranya:

1. Redistribute EIGRP
2. Redistribute OSPF
3. Redistribute RIP, dll

Redistribute EIGRP dan OSPF

EIGRP 10

OSPF 10 , Area 0.0.0.0



Konfigurasi Redistribute dilakukan pada R1 untuk menghubungkan Protokol Routing EIGRP dengan protokol Routing OSPF

PERTEMUAN 4

SWITCH NETWORK

Switch

- Switch merupakan salah satu Hardware yang digunakan didalam jaringan komputer yang berfungsi untuk menghubungkan beberapa komputer pada layer protokol jaringan.
- Switching dapat diartikan sebagai penguat sinyal pada jaringan komputer, sehingga dengan menggunakan perangkat Switch maka komputer akan dapat saling terhubung dengan komputer lain dengan jarak yang cukup jauh.

Switch

- Switch juga dapat digunakan sebagai perangkat untuk melakukan penyaringan (filtering) paket data didalam sebuah jaringan.
- Berdasarkan pada lapisan OSI, switch bekerja pada **layer data link (layer 2)** dan sebagian switch bekerja pada **layer Network (layer 3)**, sehingga dapat bekerja pada paket protokol apapun.

Type Switch

Secara umum switch terbagi menjadi dua jenis menurut OSI (Open System Interconnection):

- Switch Layer 2
 - Switch layer 2 dapat meneruskan paket dengan melihat alamat MAC tujuan, switch juga dapat menjalankan fungsi bridge antar segmen-segmen LAN (Local Area Network) sebab switch mengirimkan paket-paket data dengan cara melihat alamat yang akan ditujukan tanpa mengetahui protokol jaringan yang digunakan.

Type Switch

Secara umum switch terbagi menjadi dua jenis menurut OSI (Open System Interconnection):

- Switch Layer 3
 - Switch yang terletak di network layer yang berada di lapisan model OSI. Dimana switch dapat meneruskan paket data memakai IP Address. Switch layer 3 (tiga) biasa disebut dengan switch routing maupun switch multilayer.

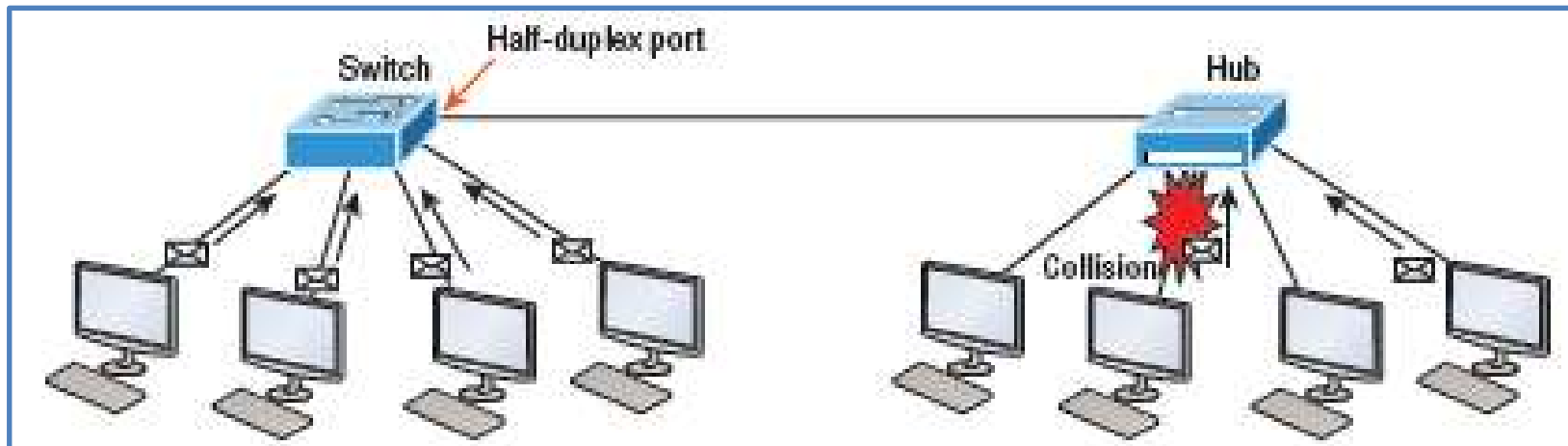
Type Switch

- Switch Unmanaged
 - Switch unmanaged sudah siap pakai (plug & play).
 - Switch unmanaged harganya lebih murah dibandingkan dengan switch managed.
- Switch Managed
 - Switch ini dapat dikonfigurasi sesuai dengan kebutuhan jaringan.

Switch vs HUB

Half and Full Duplex

Switch mampu memecah collision domain sedangkan HUB tidak. Dikarenakan, setiap port, setiap interface dan setiap koneksi memiliki bandwidth tersendiri.



Switch vs HUB

Half and Full Duplex

Cara kerja Switch adalah dengan menerima paket data dari suatu port lalu akan melihat MAC (Media Access Control) tujuannya dan juga membantun suatu koneksi logika dengan port yang telah terhubung dengan node maupun perangkat tujuan.

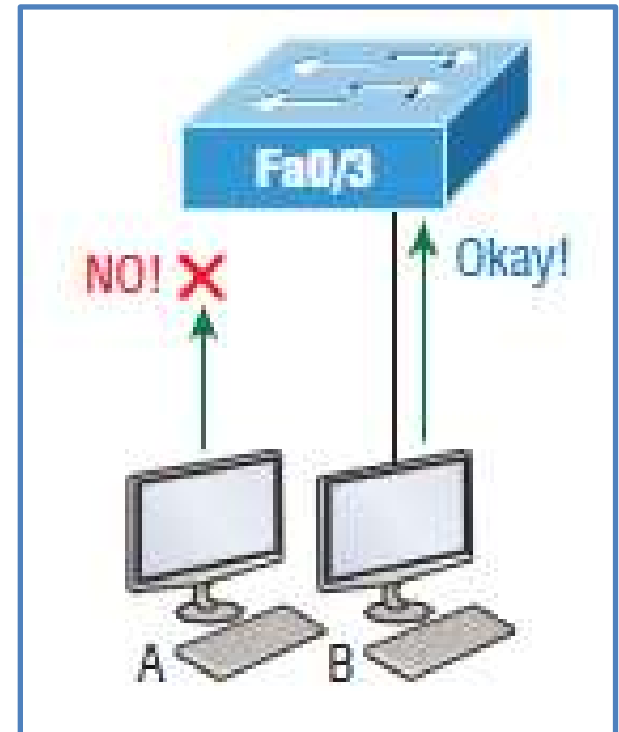
Sehingga selain port yang dituju tidak dapat menerima paket data yang dikirimkan dan akan mengurangi adanya tabrakan data atau dinamakan dengan collision.

Switch

Port Security

Dengan menggunakan port security, Interface FastEthernet 0/3 dikonfigurasi untuk mengamati dan mengizinkan alamat MAC Address tertentu untuk dihubungkan dengan port tertentu.

Jadi dalam contoh ini, Host A ditolak aksesnya, tetapi Host B diizinkan melakukan akses kedalam jaringan

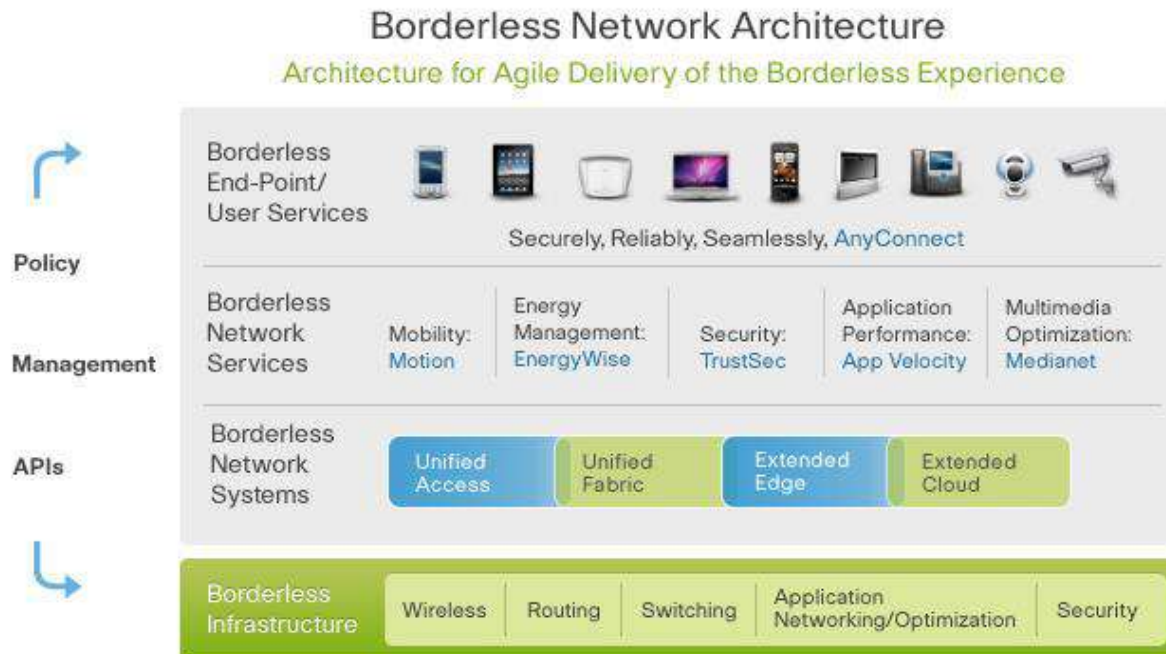


Cisco Borderless Networks

- Sebuah arsitektur jaringan yang memungkinkan sebuah organisasi untuk menghubungkan siapapun, dimanapun, kapanpun, dan pada perangkat apapun dengan aman, handal, dan mulus.
- Dirancang untuk mengatasi tantangan bisnis, seperti mendukung jaringan terkonvergensi dan mengubah pola kerja berbasis IT.

Cisco Borderless Networks

Cisco Borderless Networks bukanlah solusi statis pada dunia jaringan, tetapi solusi yang terus berkembang untuk membangun IT



Switch

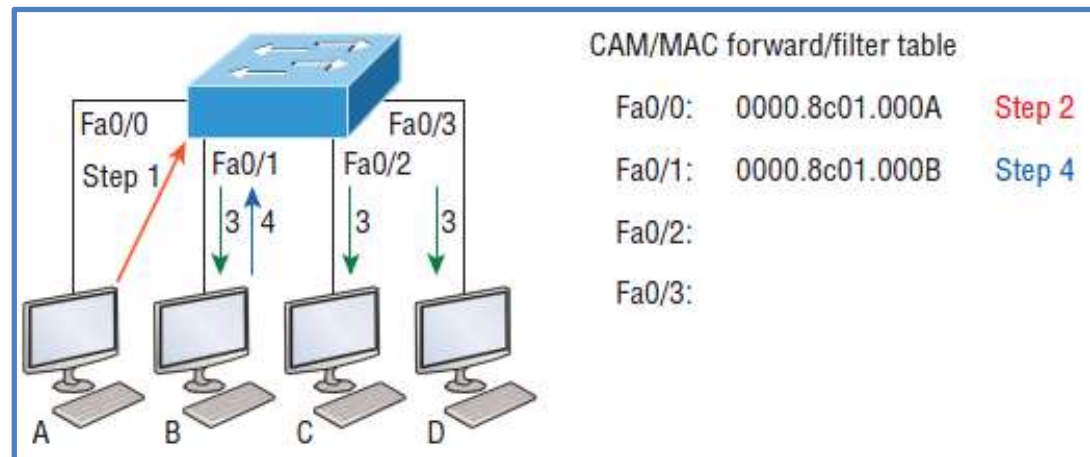
Frame Forwarding

- Sebuah switch membuat keputusan berdasarkan destination port.
- Sebuah switch menyimpan tabel MAC Address yang digunakan untuk menentukan bagaimana cara meneruskan lalu lintas melalui switch.
- Cisco switch melakukan forward frame Ethernet berdasarkan tujuan alamat MAC dari frame.

Switch

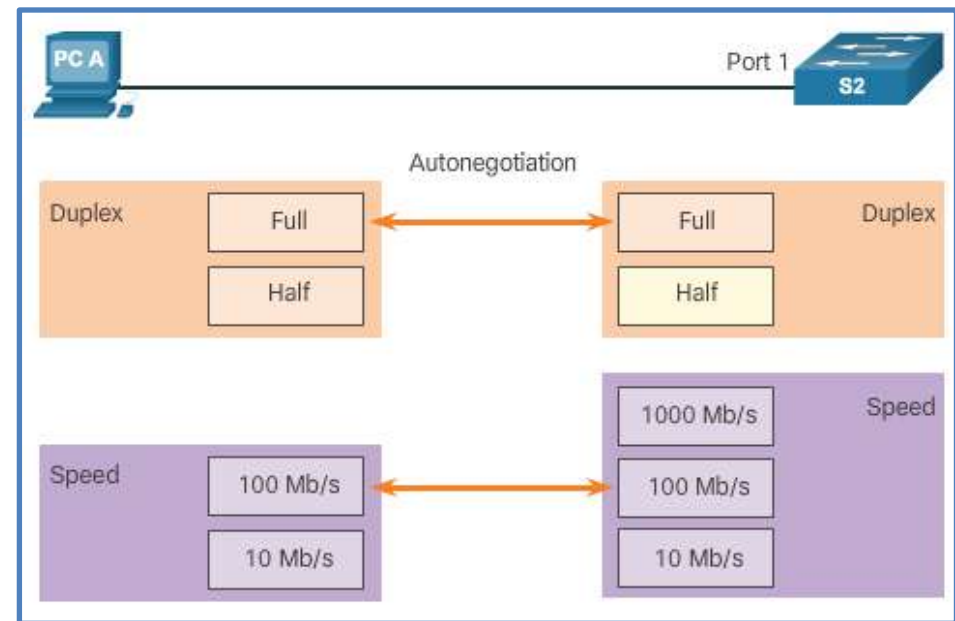
Frame Forwarding

- Switch membangun tabel yang disebut MAC address atau isi memori beralamat (CAM) tabel.
- CAM adalah tipe khusus dari memori yang digunakan dalam aplikasi pencarian kecepatan tinggi.
- Informasi dalam tabel MAC address digunakan untuk mengirim frame.



Switch Domain Collision Domain

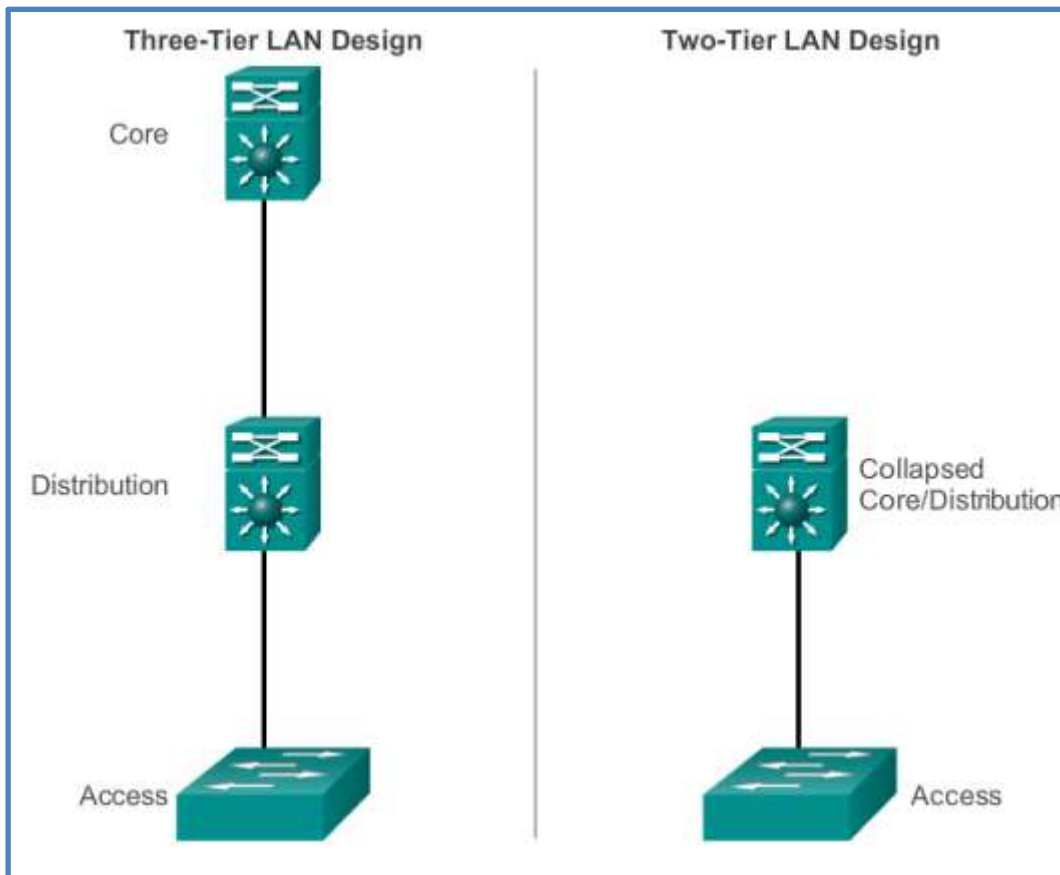
- Beroperasi di half duplex pada setiap segmen dalam collision domain sendiri.
- Beroperasi di full duplex untuk menghilangkan tabrakan.
- Secara default, akan otomatis bernegosiasi full duplex saat perangkat terhubung



Switch Domain Broadcast Domain

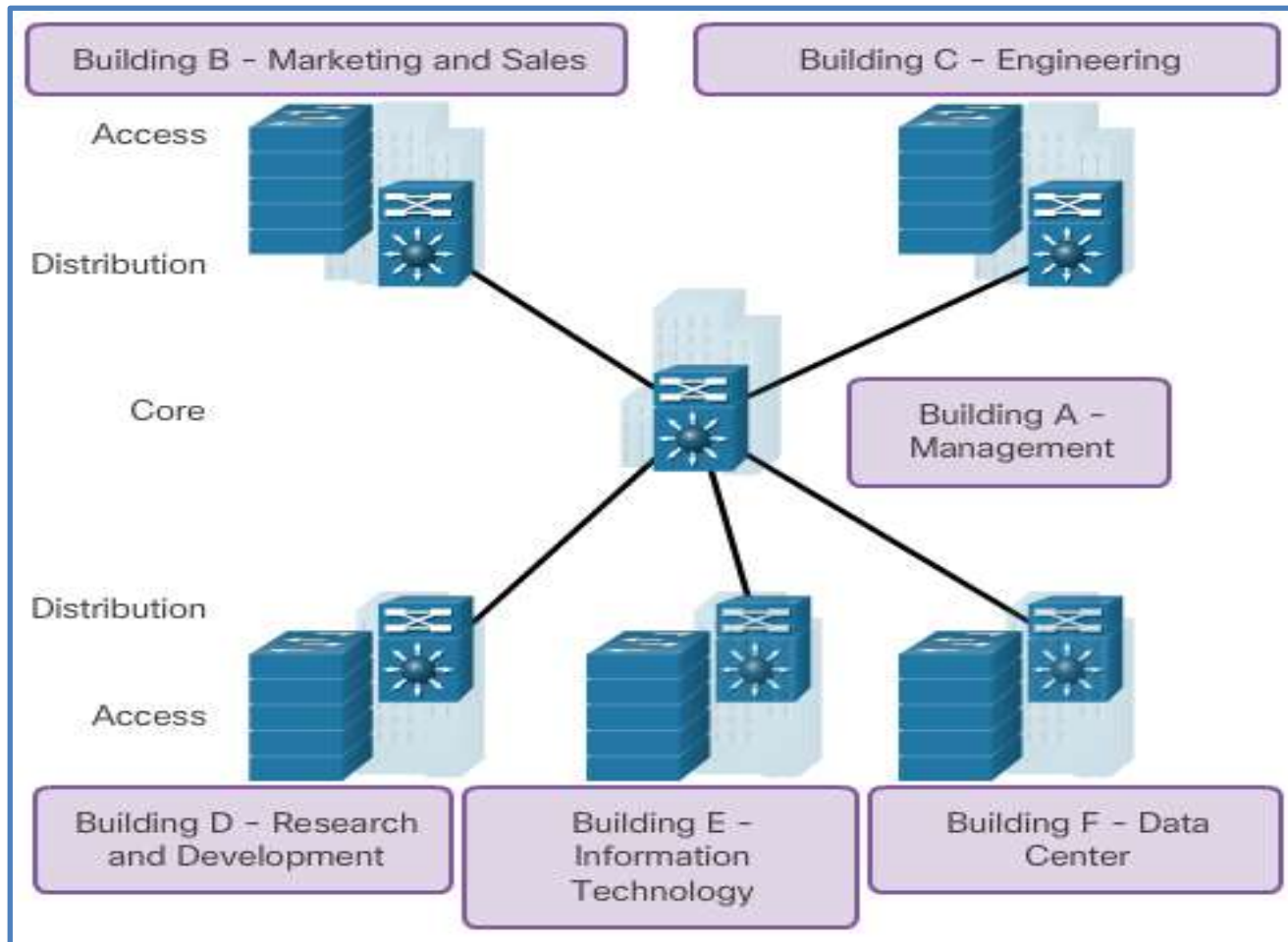
- Switch melakukan broadcast ke semua port yang digunakan. Oleh karena itu, switch tidak melanggar broadcast domain.
- Semua port pada switch dengan konfigurasi default memiliki domain broadcast yang sama.
- Jika dua atau lebih switch yang terhubung, broadcast akan diteruskan ke semua port dari semua switch, kecuali untuk port yang menyebarkan broadcast.

Hirarki Switch



Hirarki Switch

Access, Distributin, Core



Hirarki Switch

Keuntungan Jaringan Hirarki

1. Scalability: jaringan hierarki dapat diperluas/dikembangkan dengan lebih mudah
2. Redundancy: menjamin ketersediaan jalur pada level core dan distribution
3. Performance: performa switch pada layer core dan distribution lebih handal (link aggregation)

Hirarki Switch

Keuntungan Jaringan Hirarki

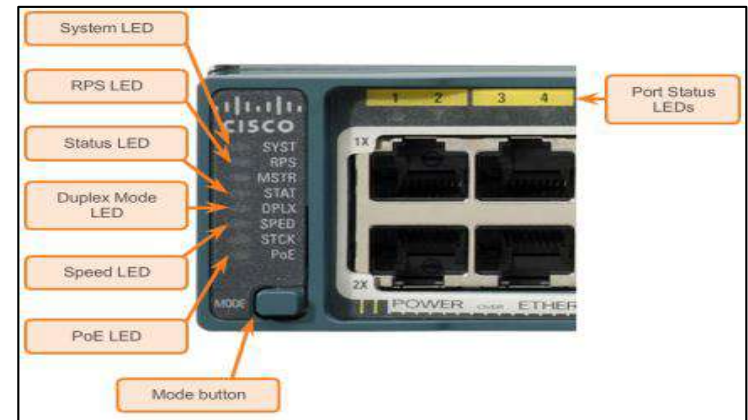
4. Security: port keamanan pada level access dan aturan pada level distribution membuat jaringan lebih aman
5. Manageability: konsistensi antar switch pada tiap level membuat manajemen menjadi lebih mudah
6. Maintainability: modularitas desain hirarki memungkinkan jaringan dibagi-bagi tanpa menambah kerumitan

PERTEMUAN 5

KONFIGURASI SWITCH

Indikator LED Switch

- Setiap port pada Switch Cisco memiliki LED untuk status indikator.
- Secara default LED mencerminkan aktivitas port, tetapi mereka juga dapat memberikan informasi lain tentang switch melalui tombol Mode.
- Modus berikut tersedia pada Cisco Catalyst 2960 switch:
 - Sistem LED
 - Redundant Power System (RPS) LED
 - Status Port LED
 - Port Duplex LED
 - Port Speed LED
 - Power over Ethernet (PoEMode) LED



Manajemen Dasar Switch

Cara untuk melakukan remote switch Cisco, yaitu:

- Menggunakan kabel consol untuk menghubungkan PC ke port consol pada switch untuk melakukan konfigurasi.
- Informasi IP meliputi (address, subnet mask, gateway) yang akan diberikan ke Switch Virtual Interface (SVI).

Konfigurasi Awal Switch

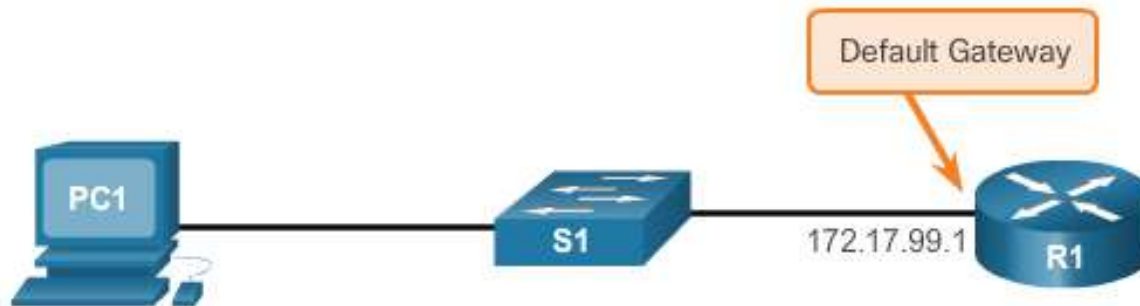
Cisco Switch IOS Commands

Enter global configuration mode.	<code>S1# configure terminal</code>
Enter interface configuration mode for the SVI.	<code>S1(config)# interface vlan 99</code>
Configure the management interface IP address.	<code>S1(config-if)# ip address 172.17.99.11 255.255.255.0</code>
Enable the management interface.	<code>S1(config-if)# no shutdown</code>
Return to the privileged EXEC mode.	<code>S1(config-if)# end</code>
Save the running config to the startup config.	<code>S1# copy running-config startup-config</code>

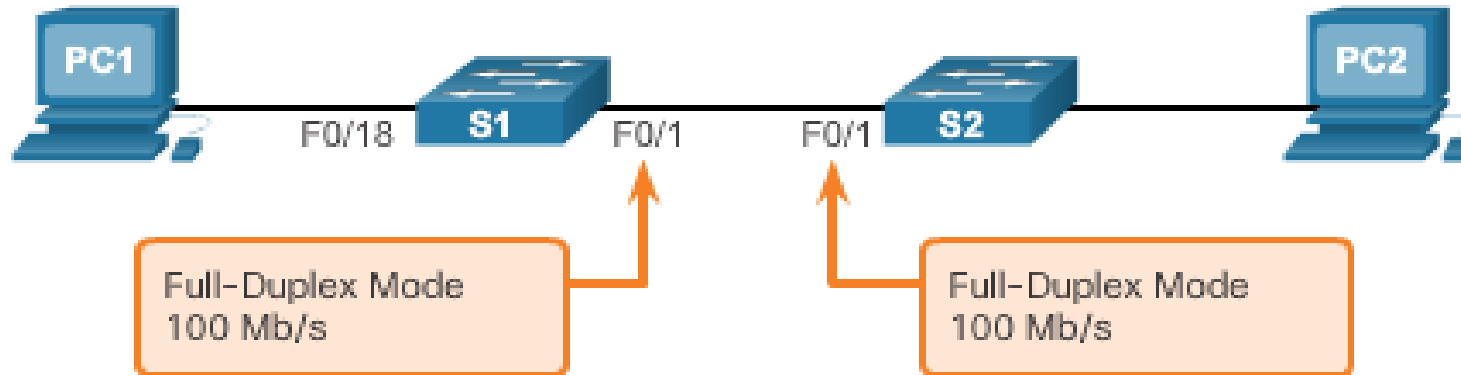
Konfigurasi Awal Switch

Cisco Switch IOS Commands

Enter global configuration mode.	<code>S1# configure terminal</code>
Configure the default gateway for the switch.	<code>S1(config)# ip default-gateway 172.17.99.1</code>
Return to the privileged EXEC mode.	<code>S1(config)# end</code>
Save the running config to the startup config.	<code>S1# copy running-config startup-config</code>



Konfigurasi Switch Port



Cisco Switch IOS Commands

Enter global configuration mode.	<code>S1# configure terminal</code>
Enter interface configuration mode.	<code>S1(config)# interface FastEthernet 0/1</code>
Configure the interface duplex.	<code>S1(config-if)# duplex full</code>
Configure the interface speed.	<code>S1(config-if)# speed 100</code>
Return to the privileged EXEC mode.	<code>S1(config-if)# end</code>
Save the running config to the startup config.	<code>S1# copy running-config startup-config</code>

Verifikasi Konfigurasi Switch

Cisco Switch IOS Commands

Display interface status and configuration.	S1# <code>show interfaces [interface-id]</code>
Display current startup configuration.	S1# <code>show startup-config</code>
Display current operating config.	S1# <code>show running-config</code>
Display information about flash file system.	S1# <code>show flash</code>
Display system hardware and software status.	S1# <code>show version</code>
Display history of commands entered.	S1# <code>show history</code>
Display IP information about an interface.	S1# <code>show ip [interface-id]</code>
Display the MAC address table.	S1# <code>show mac-address-table</code> OR S1# <code>show mac address-table</code>

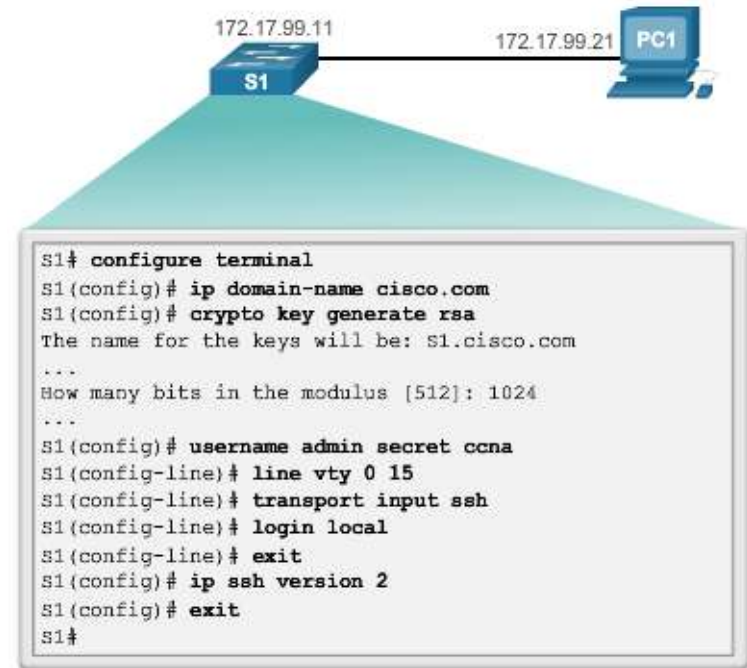
Secure Remote Access

SSH

- Secure Shell (SSH) adalah protokol yang menyediakan koneksi pada command-line.
- Karena fitur enkripsi yang kuat, SSH harus mengganti Telnet untuk koneksi manajemen.
- Secara default, SSH menggunakan TCP port 22.
- Telnet menggunakan TCP port 23.

Konfigurasi SSH

1. Verifikasi SHH menggunakan perintah **show ip ssh**
2. Konfigurasi domain IP.
3. Mengkonfigurasi otentikasi pengguna.
4. Konfigurasi vty line.
5. Mengaktifkan SSH versi 2.



Meverifikasi SSH



```
172.17.99.11 - PuTTY
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

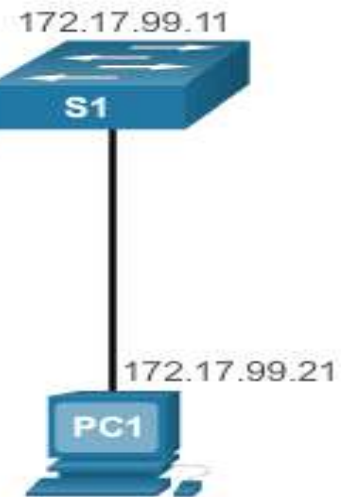
Switch Port Security

Secure Port

Disable Unused Ports

Disable unused ports using the **shutdown** command.

```
S1# show run
Building configuration...
...
version 15.0
hostname S1
...
interface FastEthernet0/4
 shutdown
 !
interface FastEthernet0/5
 shutdown
 !
interface FastEthernet0/6
 description web server
 !
interface FastEthernet0/7
 shutdown
 !
...
```



Switch Port Security

Secure Port

- Pengimplementasian Security MAC Address akan melakukan filtering terhadap perangkat yang diperbolehkan melakukan akses ke dalam jaringan, sedangkan MAC Address yang tidak terdaftar aksesnya akan ditolak.
- Security MAC Address dapat dikonfigurasi dengan beberapa cara, diantaranya:
 - Statis MAC Address - dikonfigurasi secara manual dan ditambahkan ke konfigurasi - **switchport port-security mac-address *alamat MAC***
 - Dinamis MAC Dynamic- dihapus ketika saklar restart
 - Sticky MAC Address - ditambahkan ke konfigurasi dan secara dinamis - **switchport port-security mac-address sticky**

Switch Port Security

Secure Port

- Switch akan menganggap terjadinya pelanggaran keamanan, jika terjadi:
 - Terdapatnya MAC Address yang mencoba melakukan akses kedalam jaringan dan MAC Address tersebut tidak terdaftar didalam MAC Address Tabel.
- Terdapat tiga tindakan yang dapat dilakukan untuk menangani kasus tersebut:
 - **protect** - tidak ada pemberitahuan yang diterima
 - **restrict** - pemberitahuan yang diterima dari pelanggaran keamanan
 - **shutdown**

Switch Port Security Konfigurasi

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

Configure Dynamic Port Security



Cisco IOS CLI Commands

Specify the interface to be configured for port security.	<code>S1(config)# interface fastethernet 0/18</code>
Set the interface mode to access.	<code>S1(config-if)# switchport mode access</code>
Enable port security on the interface.	<code>S1(config-if)# switchport port-security</code>

Configure Sticky Port Security

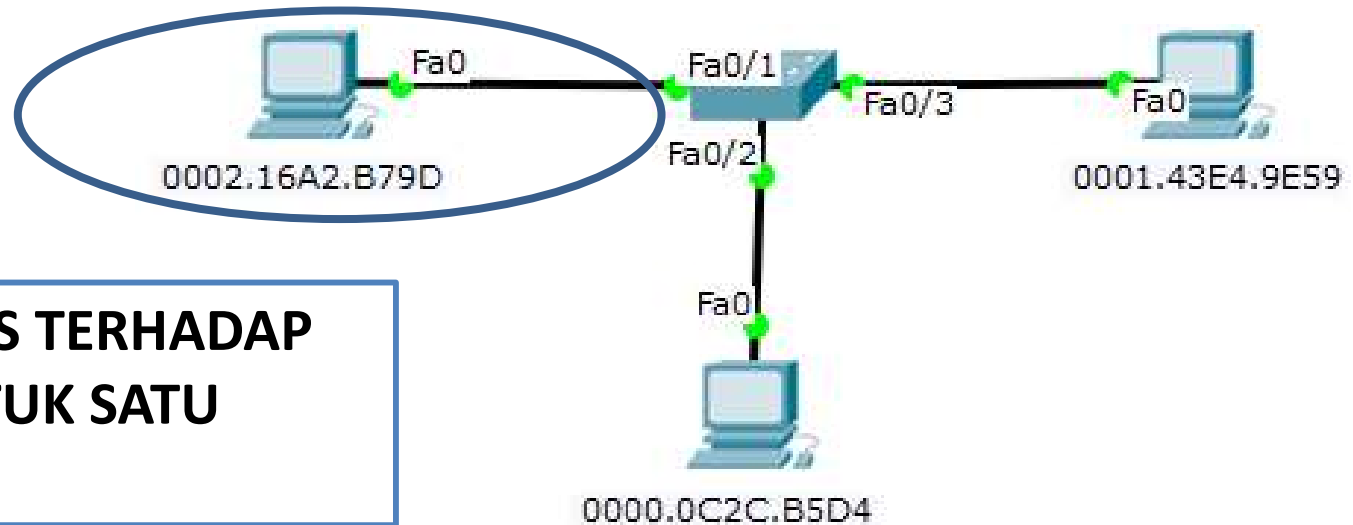


Cisco IOS CLI Commands

Specify the interface to be configured for port security.	<code>S1(config)# interface fastethernet 0/19</code>
Set the interface mode to access.	<code>S1(config-if)# switchport mode access</code>
Enable port security on the interface.	<code>S1(config-if)# switchport port-security</code>
Set the maximum number of secure addresses allowed on the port.	<code>S1(config-if)# switchport port-security maximum 10</code>
Enable sticky learning.	<code>S1(config-if)# switchport port-security mac-address sticky</code>

DISKUSI - Topologi Jaringan 1

Mengamankan FastEthernet Fa0/1



**MEMBATASI AKSES TERHADAP
Fa0/1 HANYA UNTUK SATU
0002.16A2.B79D**

```
Switch#configure terminal
```

```
Switch(config)#int fa0/1
```

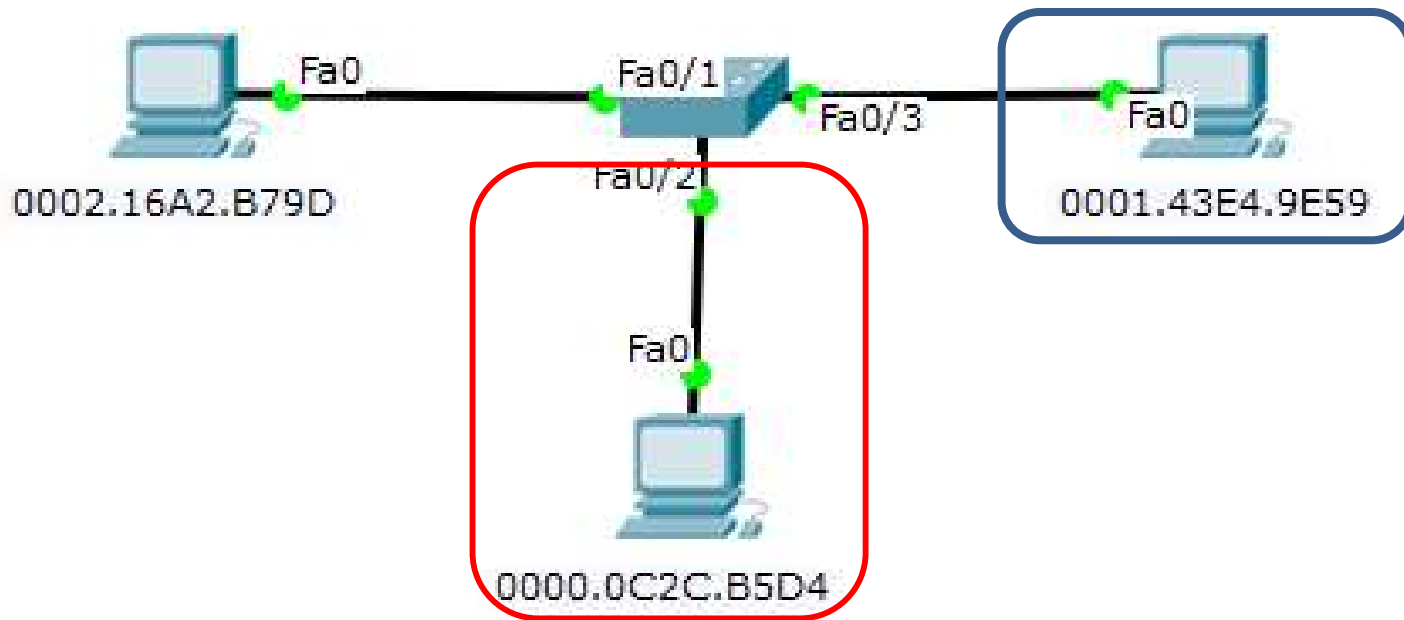
```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport port-security
```

```
Switch(config-if)#switchport port-security mac-address 0002.16A2.B79D
```

DISKUSI - Topologi Jaringan 1

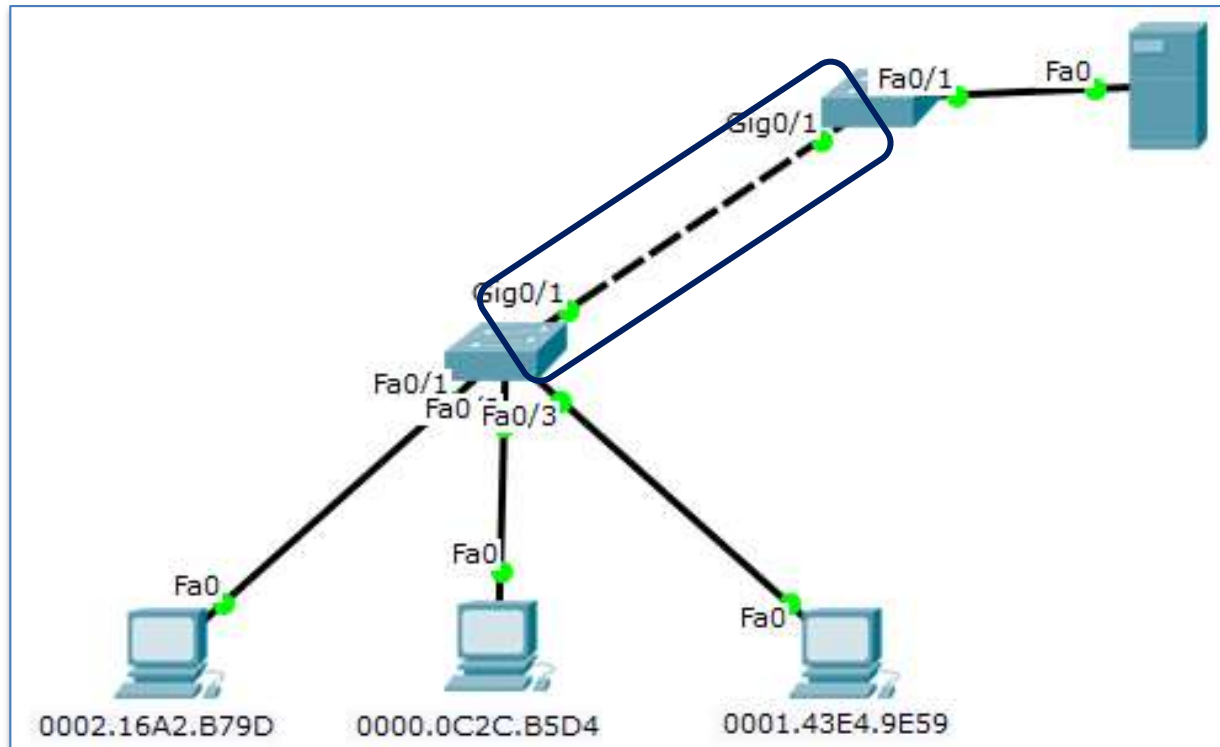
Mengamankan FastEthernet Fa0/2 dan Fa0/3



Lalu bagaimana cara mengamankan Interface Fast Ethernet 0/2 dan Interface Fast Ethernet 0/3 hanya untuk pengguna yang berhak saja?

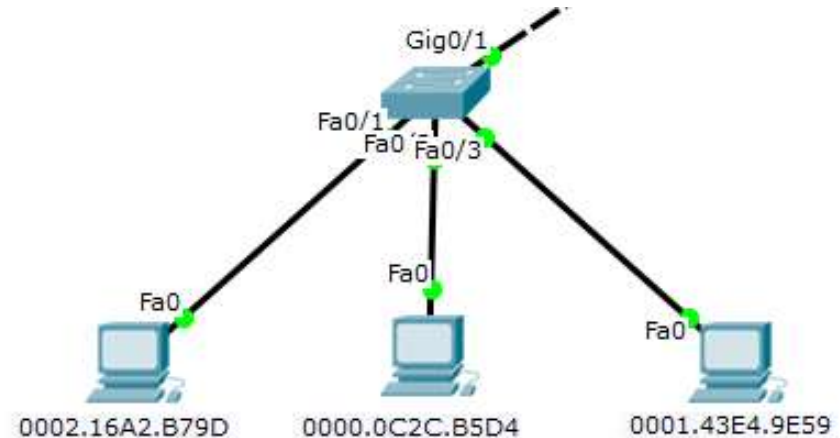
STUDI KASUS - Topologi Jaringan 2

Port Security G0/1



Filtering MAC Address hanya untuk pengguna yang telah didaftarkan pada Switch melalui port Interface G0/1

STUDI KASUS - Topologi Jaringan 2



```
Switch(config)#interface gigabitEthernet 0/1
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport port-security
```

```
Switch(config-if)#switchport port-security max 4
```

```
Switch(config-if)#switchport port-security mac-address 0002.16A2.B79D
```

```
Switch(config-if)#switchport port-security mac-address 0000.0C2C.B5D4
```

```
Switch(config-if)#switchport port-security mac-address 0001.43E4.9E59
```

```
Switch(config-if)#switchport port-security violation protect
```

STUDI KASUS - Topologi Jaringan 2

Verifikasi

Verifikasi MAC Address yang telah didaftarkan

```
Switch#sh mac-address-table
      Mac Address Table
-----
```

Vlan	Mac Address	Type	Ports
1	0000.0c2c.b5d4	STATIC	Gig0/1
1	0001.43e4.9e59	STATIC	Gig0/1
1	0001.630b.a219	STATIC	Gig0/1
1	0002.16a2.b79d	STATIC	Gig0/1

DAN, Tambahkan 1 user kembali sebagai uji coba untuk melihat apakah user yang tidak didaftarkan benar tidak dapat melakukan akses ke dalam jaringan

PERTEMUAN 6

PEMBUATAN JARINGAN ROUTING DAN PORT SECURITY

Configuring SSH Instruction

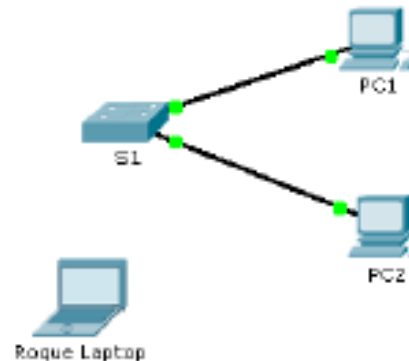


Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

1. Jalankanlah jaringan komputer dengan menggunakan PKA yang telah disediakan Link: [Configuring SSH Instruction](#)
2. Point penilaian tugas sesuai dengan Grade yang telah tersedia dari Link tersebut

Configuring Switch Port Security

Topology

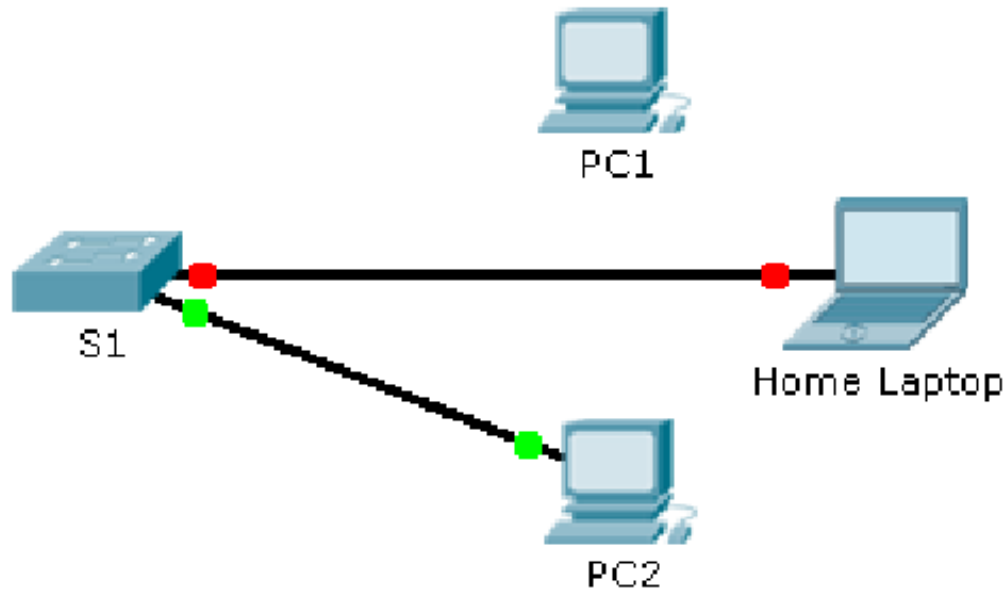


Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

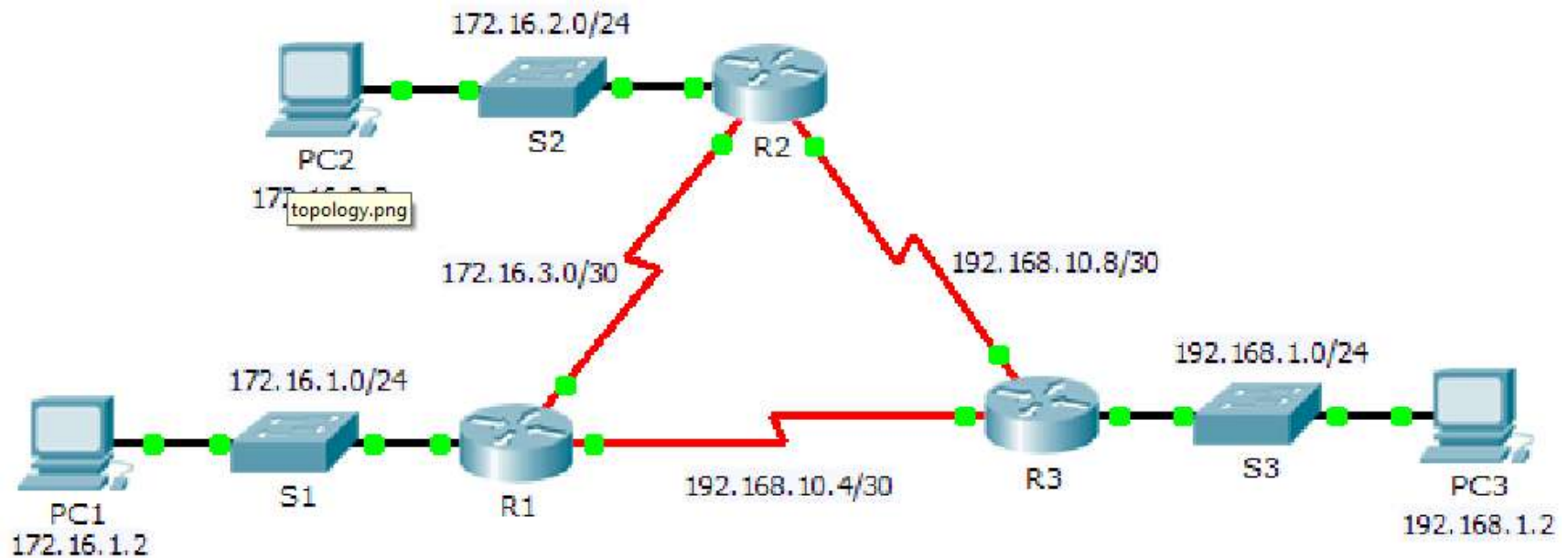
1. Jalankanlah jaringan komputer dengan menggunakan PKA yang telah disediakan Link: [Configuring Switch Port Security](#)
2. Point penilaian tugas sesuai dengan Grade yang telah tersedia dari Link tersebut

Troubleshooting Switch Port Security



1. Jalankanlah jaringan komputer dengan menggunakan PKA yang telah disediakan Link: [Troubleshooting Switch Port Security](#)
2. Point penilaian tugas sesuai dengan Grade yang telah tersedia dari Link tersebut

Configuring OSPFv2



1. Jalankanlah jaringan komputer dengan menggunakan PKA yang telah disediakan Link: [Configuring OSPFv2](#)
2. Point penilaian tugas sesuai dengan Grade yang telah tersedia dari Link tersebut

PERTEMUAN 9

VIRTUAL LOCAL AREA NETWORK (VLAN)

DEFINISI VLAN

- Virtual Local Area Network (VLAN) merupakan sebuah teknologi yang terdapat pada switch managed.
- VLAN biasanya digunakan untuk meningkatkan kinerja pada jaringan dengan memisahkan broadcast jaringan besar menjadi beberapa broadcast jaringan yang lebih kecil.
- VLAN menyediakan cara untuk menggabungkan beberapa buah VLAN agar dapat terkoneksi dengan satu buah VLAN, metode ini disebut dengan trunking

DEFINISI VLAN

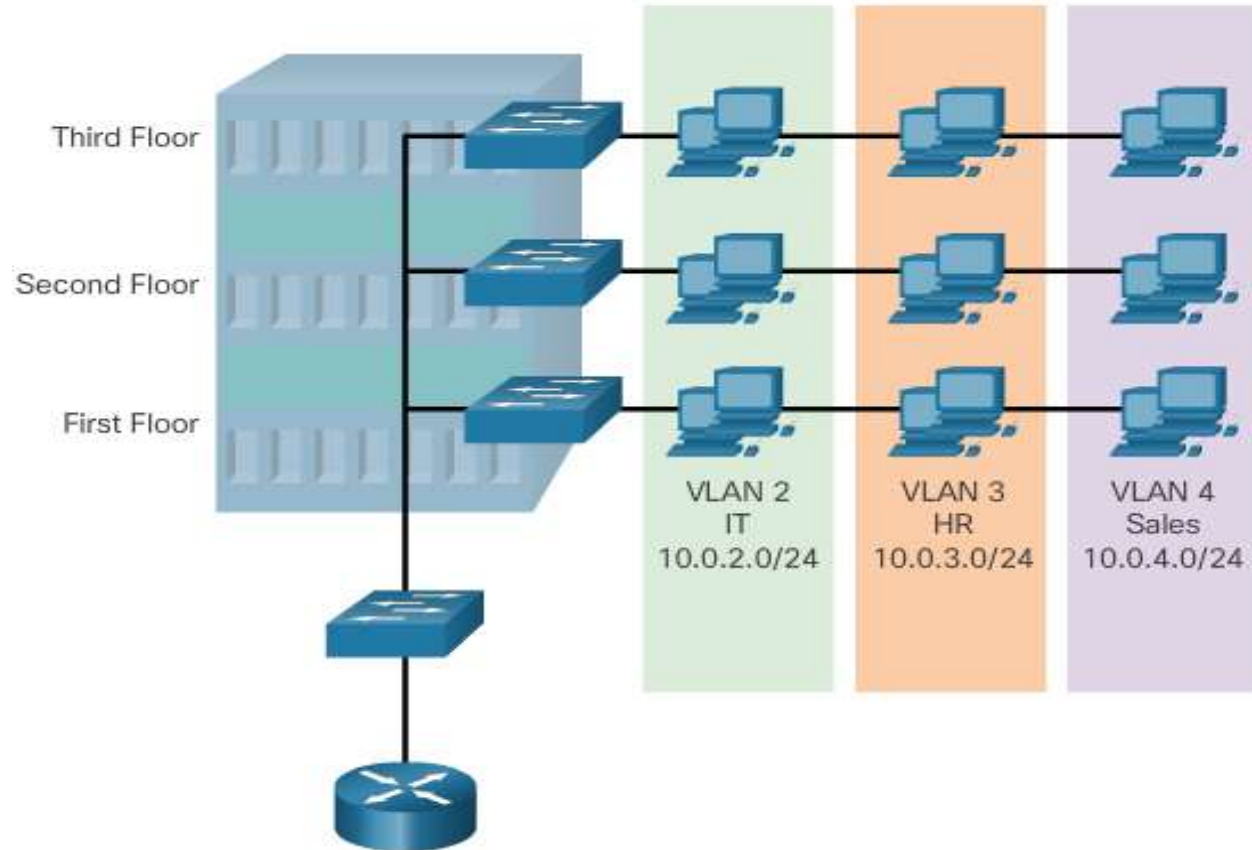
Pada dasarnya pada sebuah switch hanya terdapat satu buah VLAN saja, switch akan dikonfigurasi terlebih dahulu untuk memiliki dua atau lebih interface VLAN.

```
Switch# show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

MANFAAT VLAN

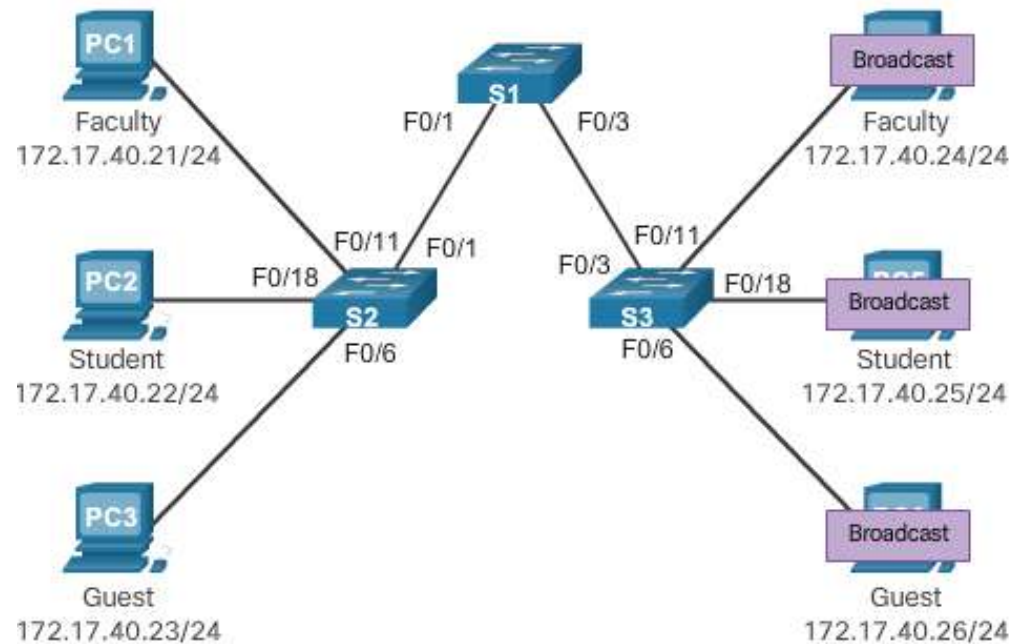
Defining VLAN Groups



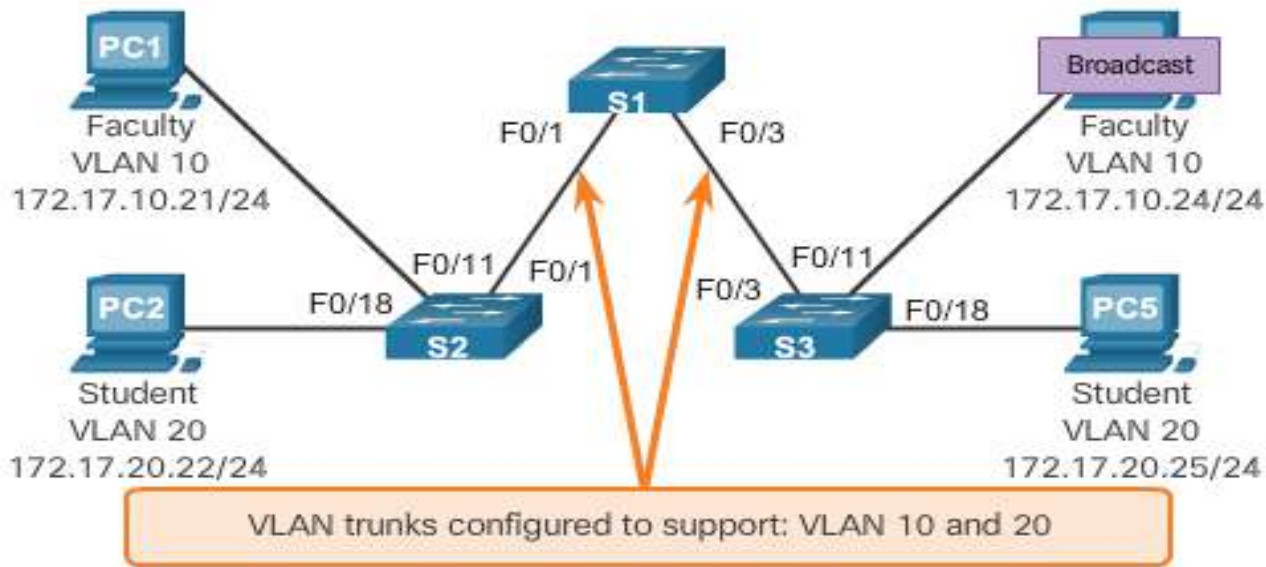
MANFAAT VLAN

Ketika jaringan komputer tidak menggunakan VLAN. PC1 ingin melakukan pengiriman paket data, maka semua client yang terhubung akan mendapatkan broadcast dari pengiriman paket data yang dilakukan oleh PC1.

Hal ini dikarenakan switch melakukan forward ke semua port.



MANFAAT VLAN



Ketika PC1 melakukan pengiriman paket data, maka paket tersebut hanya di broadcast terhadap VLAN yang sama (VLAN 10)

MANFAAT VLAN

- VLAN dapat digunakan untuk membatasi broadcast pada jaringan.
- VLAN menggunakan broadcast domain tersendiri.
- Sebuah frame broadcast yang dikirim oleh perangkat didalam VLAN tertentu hanya diteruskan dalam VLAN itu saja.
- VLAN mampu menjaga kinerja dari sebuah jaringan dengan menerapkan sistem keamanan.

Jenis-Jenis VLAN

- Data VLAN
- Default VLAN
- Native VLAN
- Management VLAN

IMPLEMENTASI VLAN

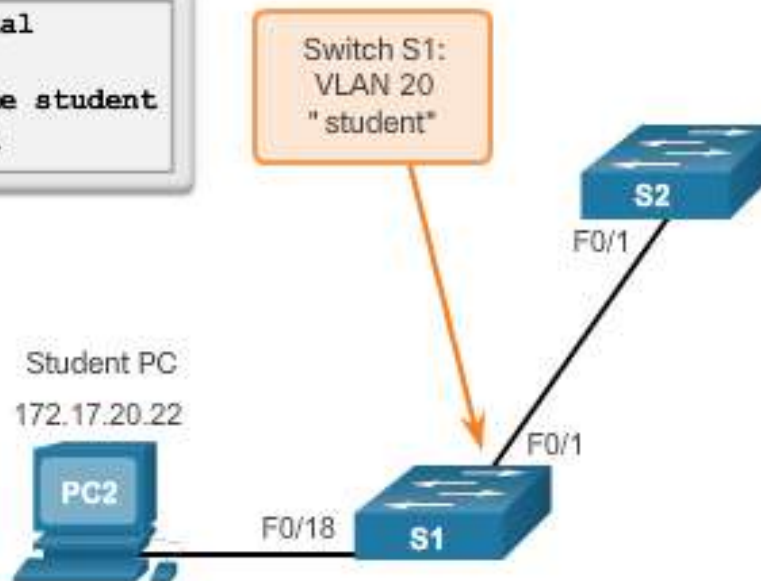
- Switch Cisco Catalyst 2960 dan 3560 mampu mendukung lebih dari 4.000 VLAN.
- VLAN dibagi menjadi dua kategori:
 - VLAN normal
 - Nomor VLAN 1 sampai 1005
 - Konfigurasi disimpan pada vlan.dat (dalam memori flash)
 - ID 1002 melalui 1005 dicadangkan untuk Token Ring dan Fiber Distributed Data Interface (FDDI) VLAN, otomatis dibuat dan tidak dapat dihapus
 - Extended Range VLAN
 - Nomor VLAN dari 1.006 ke 4.096
 - Konfigurasi disimpan dalam menjalankan konfigurasi (NVRAM)
 - VLAN trunking Protocol (VTP)

MEMBUAT VLAN

Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Create a VLAN with a valid id number.	S1(config)# vlan vlan-id
Specify a unique name to identify the VLAN.	S1(config-vlan)# name vlan-name
Return to the privileged EXEC mode.	S1(config-vlan)# end

```
S1# configure terminal  
S1(config)# vlan 20  
S1(config-vlan)# name student  
S1(config-vlan)# end
```



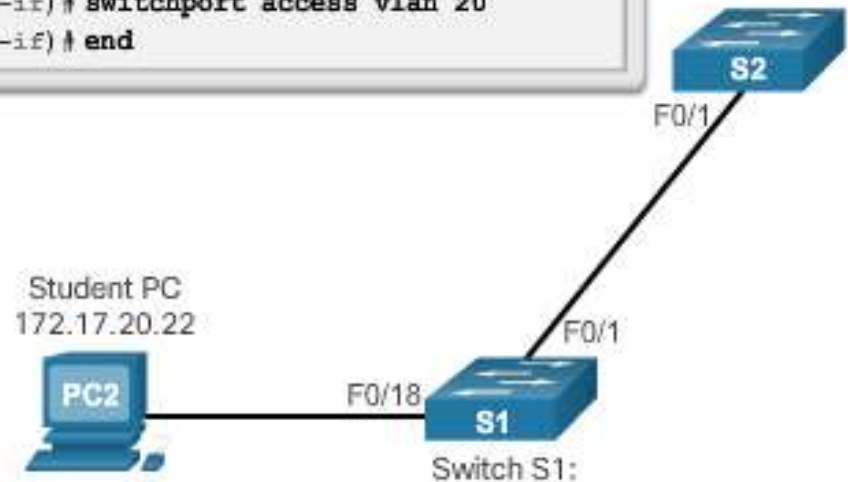
MENETAPKAN PORT VLAN

```

s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
    
```

Cisco Switch IOS Commands

Enter global configuration mode.	S1# <code>configure terminal</code>
Enter interface configuration mode.	S1(config)# <code>interface interface_id</code>
Set the port to access mode.	S1(config-if)# <code>switchport mode access</code>
Assign the port to a VLAN.	S1(config-if)# <code>switchport access vlan vlan_id</code>
Return to the privileged EXEC mode.	S1(config-if)# <code>end</code>



Menghapus VLAN

Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Remove the VLAN assignment from the port.	S1(config-if)# no switchport access vlan
Return to the privileged EXEC mode.	S1(config-if)# end

```

S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                           Gi0/2

1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
S1#

```

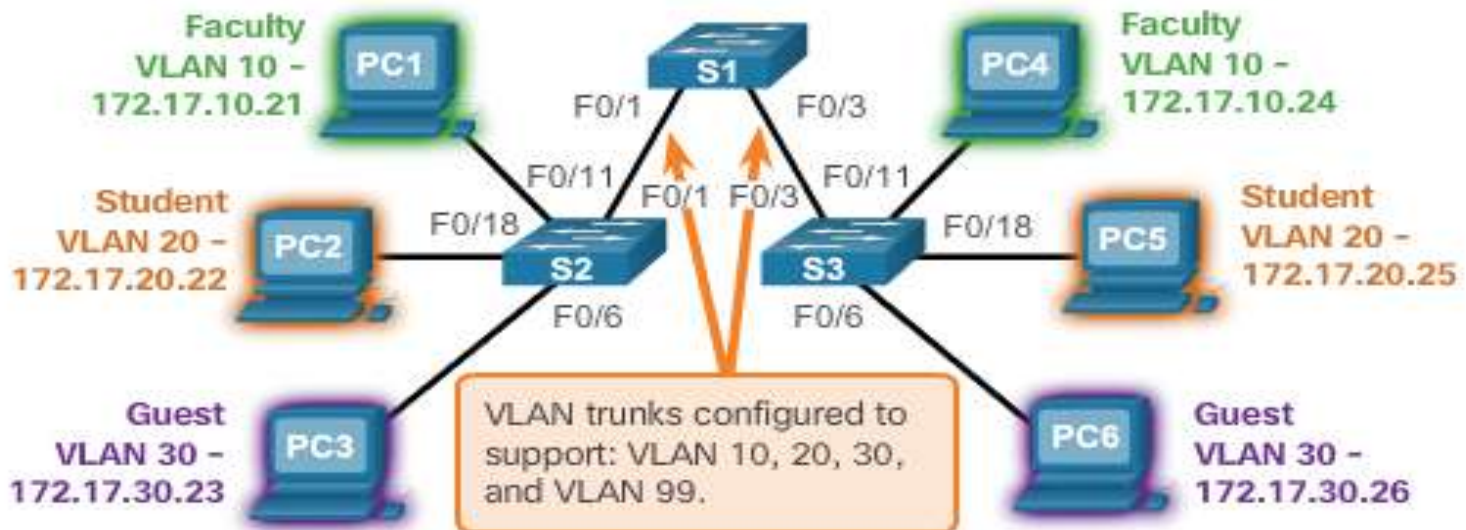
VLAN TRUNK

- VLAN Trunk merupakan sebuah VLAN yang memiliki link point to point yang mampu membawa lebih dari satu buah VLAN.
- VLAN Trunk biasanya dibentuk antara switch sehingga perangkat yang sama VLANnya dapat saling berkomunikasi, bahkan pada perangkat yang berbeda jika memiliki VLAN yang sama.
- Cisco IOS mendukung penggunaan protokol IEEE802.1Q yang merupakan protokol VLAN paling favorit.

VLAN TRUNK

VLAN 10 Faculty/Staff - 172.17.10.0/24
 VLAN 20 Students - 172.17.20.0/24
 VLAN 30 Guest - 172.17.30.0/24
 VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
 F0/11-17 are in VLAN 10.
 F0/18-24 are in VLAN 20.
 F0/6-10 are in VLAN 30.



Konfigurasi Trunk Link IEEE 802.1Q

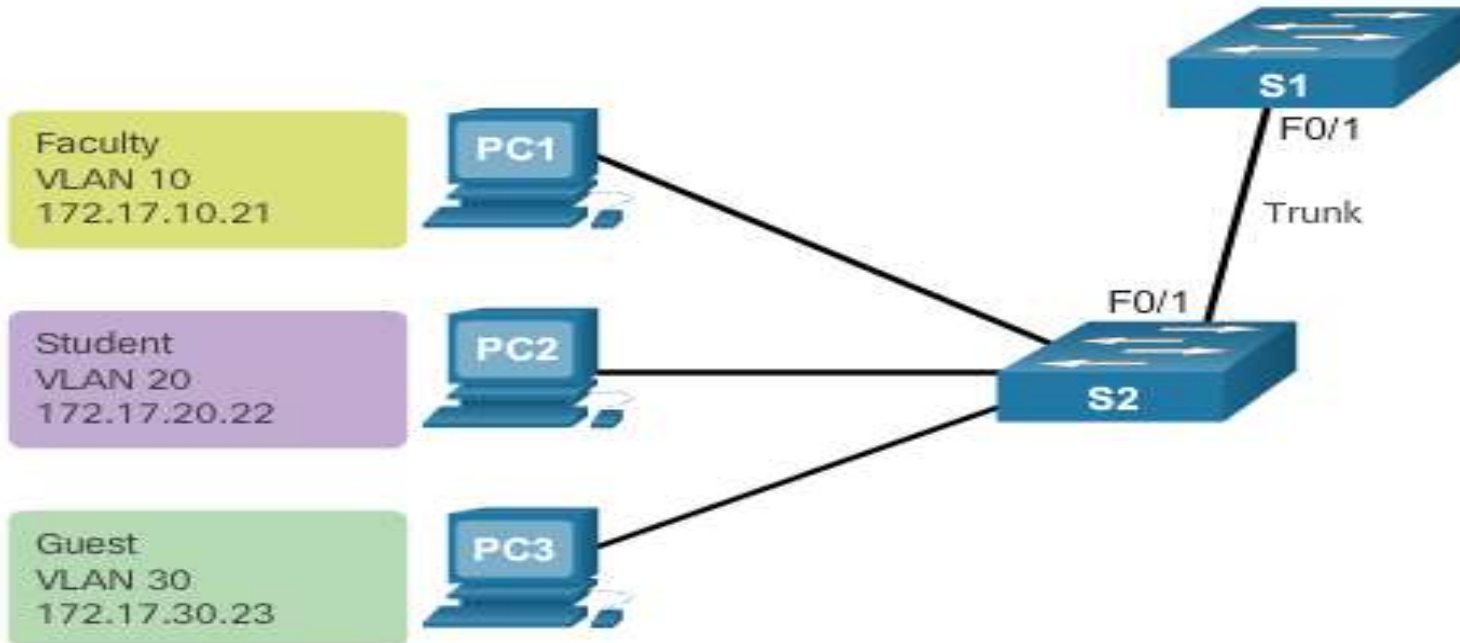
Cisco Switch IOS Commands

Enter global configuration mode.	<code>S1# configure terminal</code>
Enter interface configuration mode.	<code>S1(config)# interface interface_id</code>
Force the link to be a trunk link.	<code>S1(config-if)# switchport mode trunk</code>
Specify a native VLAN for untagged frames.	<code>S1(config-if)# switchport trunk native vlan vlan_id</code>
Specify the list of VLANs to be allowed on the trunk link.	<code>S1(config-if)# switchport trunk allowed vlan vlan-list</code>
Return to the privileged EXEC mode.	<code>S1(config-if)# end</code>

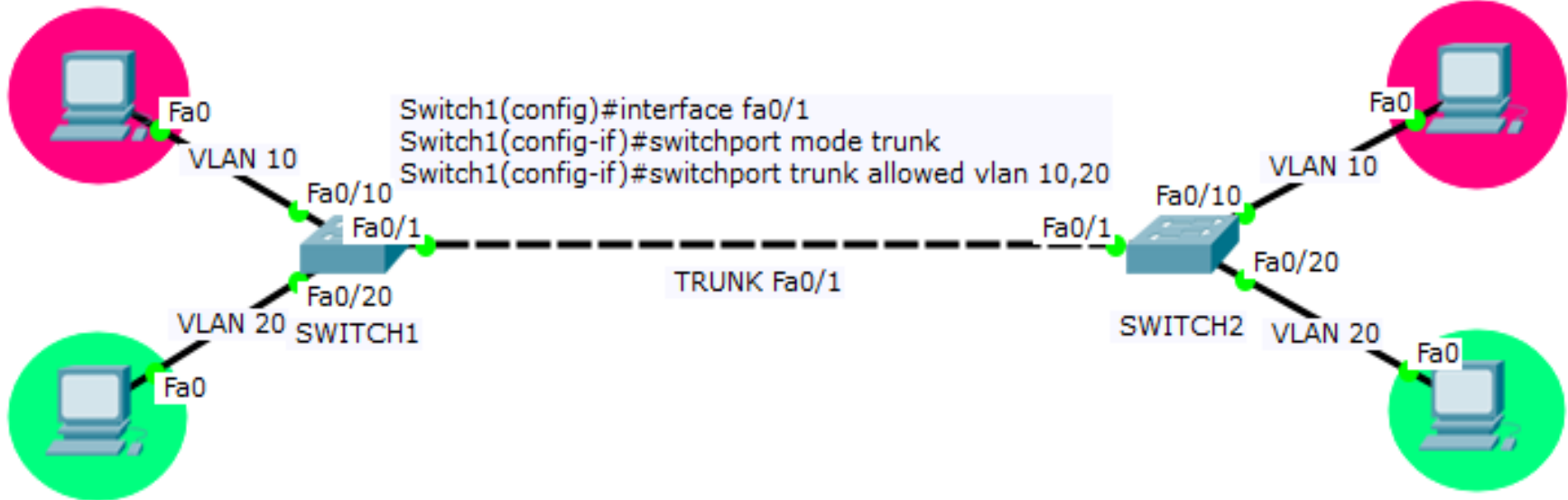
```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Konfigurasi Trunk Link IEEE 802.1Q

```
VLAN 10 - Faculty/Staff - 172.17.10.0/24  
VLAN 20 - Students - 172.17.20.0/24  
VLAN 30 - Guest - 172.17.30.0/24  
VLAN 99 - Native - 172.17.99.0/24
```



Konfigurasi Trunk



```
Switch1(config)#interface fa0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan 10,20
```

TRUNK Fa0/1

```
Switch1(config)#interface vlan 10
Switch1(config-if)#interface fa0/10
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
```

```
Switch1(config)#interface vlan 20
Switch1(config-if)#interface fa0/20
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
```

Verifikasi VLAN

```
Switch1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10 VLAN0010	active	Fa0/10
20 VLAN0020	active	Fa0/20
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Trunking Protocol

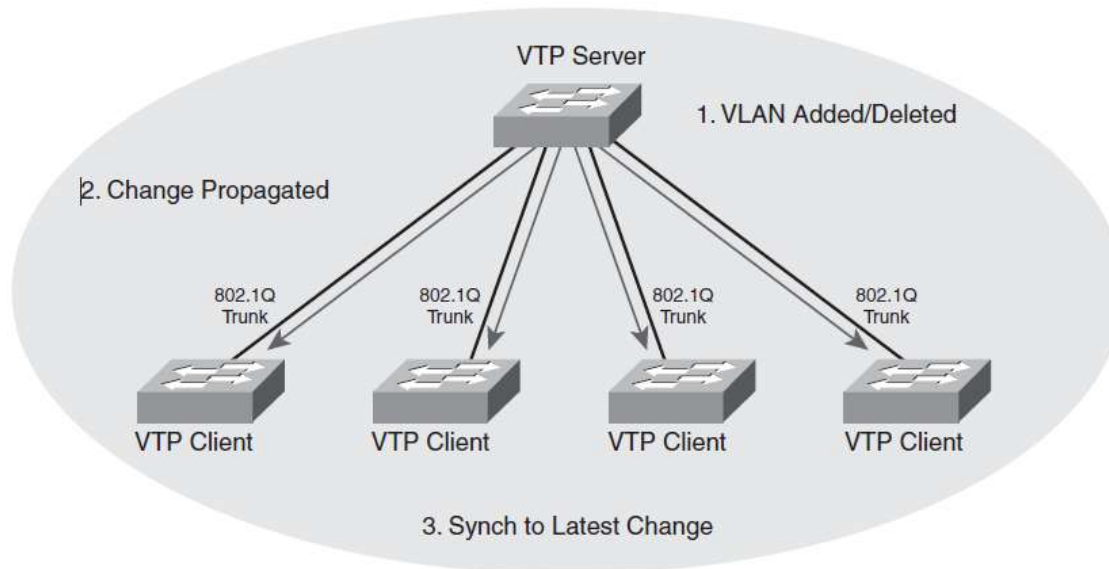
VLAN Trunking Protocol (VTP) menggunakan frame tagged untuk menandai suatu frame dari VLAN. Pada dasarnya trunking mengizinkan komunikasi antar VLAN yang sama pada switch-switch yang berbeda.

VTP menyediakan metode untuk trunking antar perangkat/VLAN. VTP digunakan untuk menjaga konsistensi VLAN dalam melakukan penambahan, penghapusan dan perubahan VLAN didalam jaringan.

VLAN Trunking Protocol

Manfaat VTP:

- Konsistensi VLAN di dalam jaringan,
- Pelacakan dan pemantauan VLAN yang lebih akurat,
- Penambahan VLAN dilakukan secara Dinamis



VLAN Trunking Protocol #5

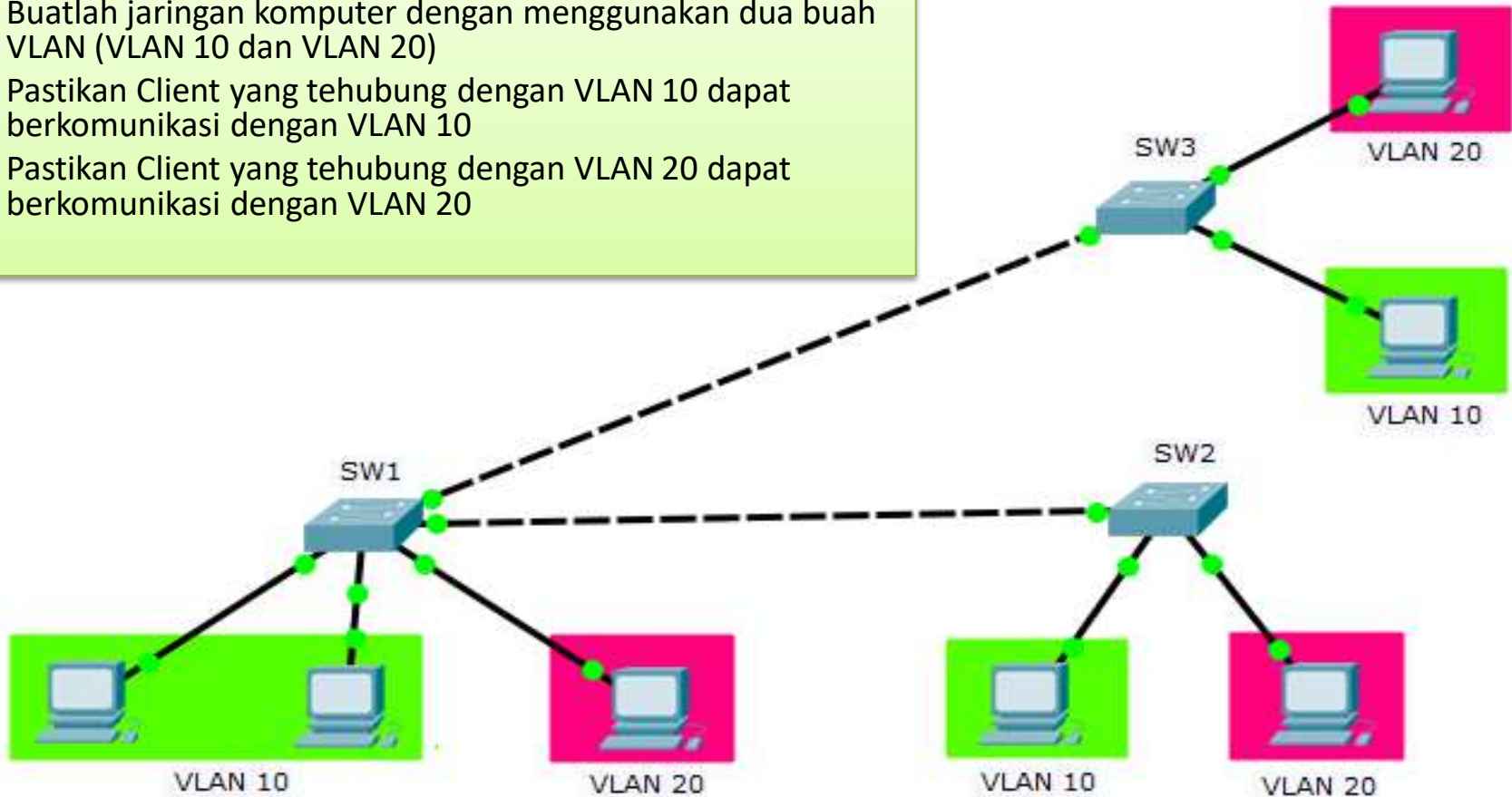
Fungsi utama VTP yaitu menyederhanakan pembuatan VLAN pada banyak switch.

- **VTP Server:** dapat melakukan create, add, dan delete VLAN. Kemudian mengirimkan informasi VLAN melalui jalur Trunk
- **VTP Client:** menerima dan menyimpan informasi VLAN pada NVRAM.
- **VTP Transparant:** tidak dapat menyimpan informasi VLAN pada NVRAM. Hanya dapat meneruskan info VLAN yang diterima dari VTP Server ke VTP Client.

Skema Jaringan

Tugas Mandiri

1. Buatlah jaringan komputer dengan menggunakan dua buah VLAN (VLAN 10 dan VLAN 20)
2. Pastikan Client yang terhubung dengan VLAN 10 dapat berkomunikasi dengan VLAN 10
3. Pastikan Client yang terhubung dengan VLAN 20 dapat berkomunikasi dengan VLAN 20



PERTEMUAN 10

Inter-VLAN Routing

Perbedaan VLAN dengan InterVLAN?

- VLAN merupakan sekelompok perangkat pada satu LAN atau lebih yang dikonfigurasi (menggunakan perangkat lunak pengelolaan) sehingga dapat berkomunikasi seperti halnya bila perangkat tersebut terhubung ke jalur yang sama,
- Sedangkan komunikasi antar host dalam sebuah VLAN dengan host dalam VLAN yang lain dinamakan Inter-VLAN. Jadi perbedaannya VLAN adalah sekelompok perangkat LAN yang saling terkonfigurasi, sedangkan interVLAN bisa dikatakan sebagai penghubung komunikasi host antar VLAN satu dengan lainnya.

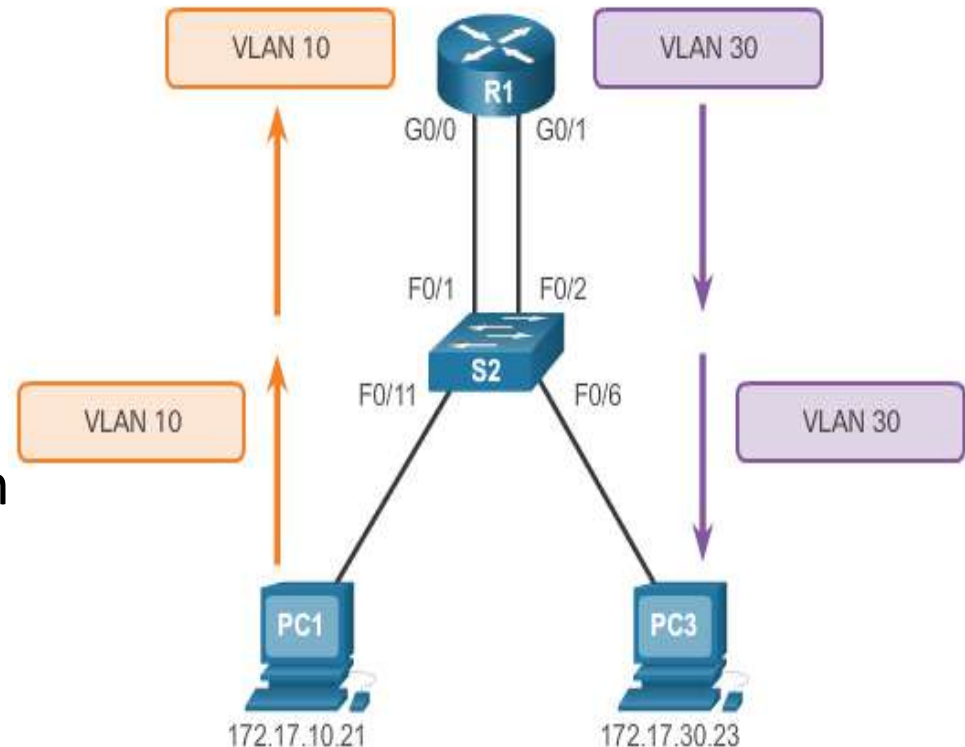
Definisi Inter-VLAN Routing

Inter-VLAN Routing pada dasarnya berfungsi untuk menghubungkan beberapa VLAN yang berbeda agar dapat saling berkomunikasi. Dikarenakan setiap paket data yang akan dikirimkan akan melalui proses routing terlebih dahulu, baru diteruskan ke tujuan. Hal ini dilakukan karena proses routing hanya meneruskan paket data saja, bukan menyebarkan paket data ataupun broadcast untuk menemukan alamat tujuan

Definisi Inter-VLAN Routing

Layer 2 switch tidak mampu untuk meneruskan lalu lintas antara VLAN tanpa bantuan router.

Untuk dapat menghubungkan antar VLAN kita menggunakan perangkat yang memiliki kapasitas pada Layer 3 Switch atau menggunakan Router.



Keuntungan Penggunaan InterVLAN

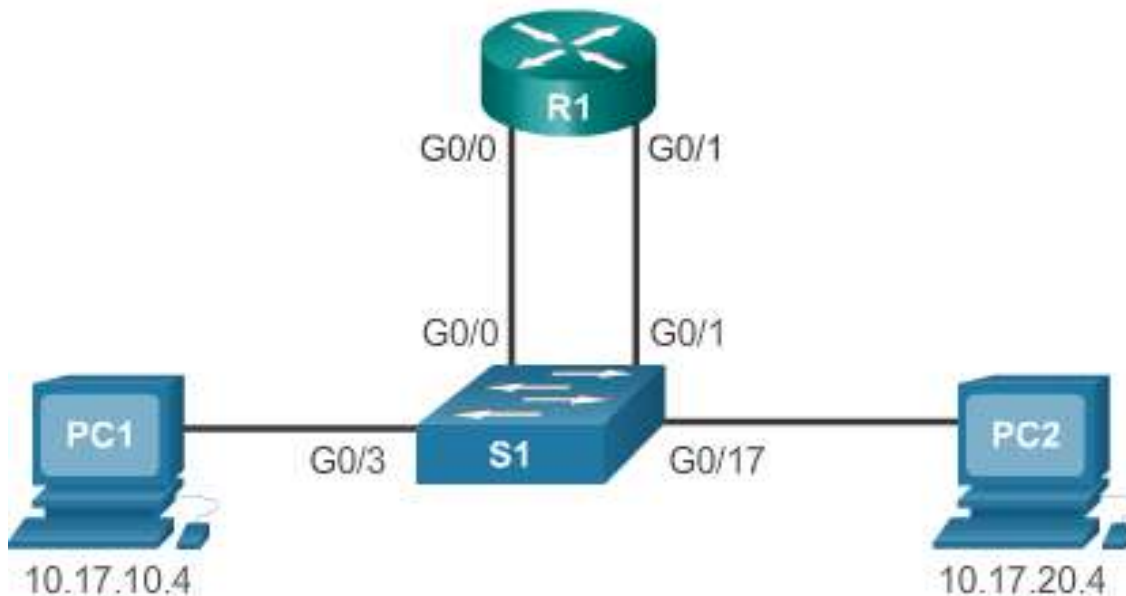
- Ketika menggunakan router untuk memfasilitasi inter-VLAN routing, interface pada router dapat dihubungkan dengan VLAN yang berbeda.
- Implementasi yang mudah
- Tidak membutuhkan layanan layer 3 pada switch
- Router menyediakan komunikasi antar VLAN
- InterVLAN routing memungkinkan komunikasi antar jaringan VLAN
- Switch terbaru mampu menggabungkan kemampuan routing dalam switch (Enterprise Switch)

Legacy Inter-VLAN Routing

- Legacy inter-VLAN routing mengharuskan router untuk memiliki interface fisik.
- Masing-masing dari interface fisik router terhubung dengan ID VLAN yang unik.
- Setiap interface juga dikonfigurasi dengan IP Address.
- Menggunakan router sebagai gateway untuk melakukan akses terhadap perangkat yang terhubung dengan VLAN lain.

Topologi

Legacy Inter-VLAN Routing

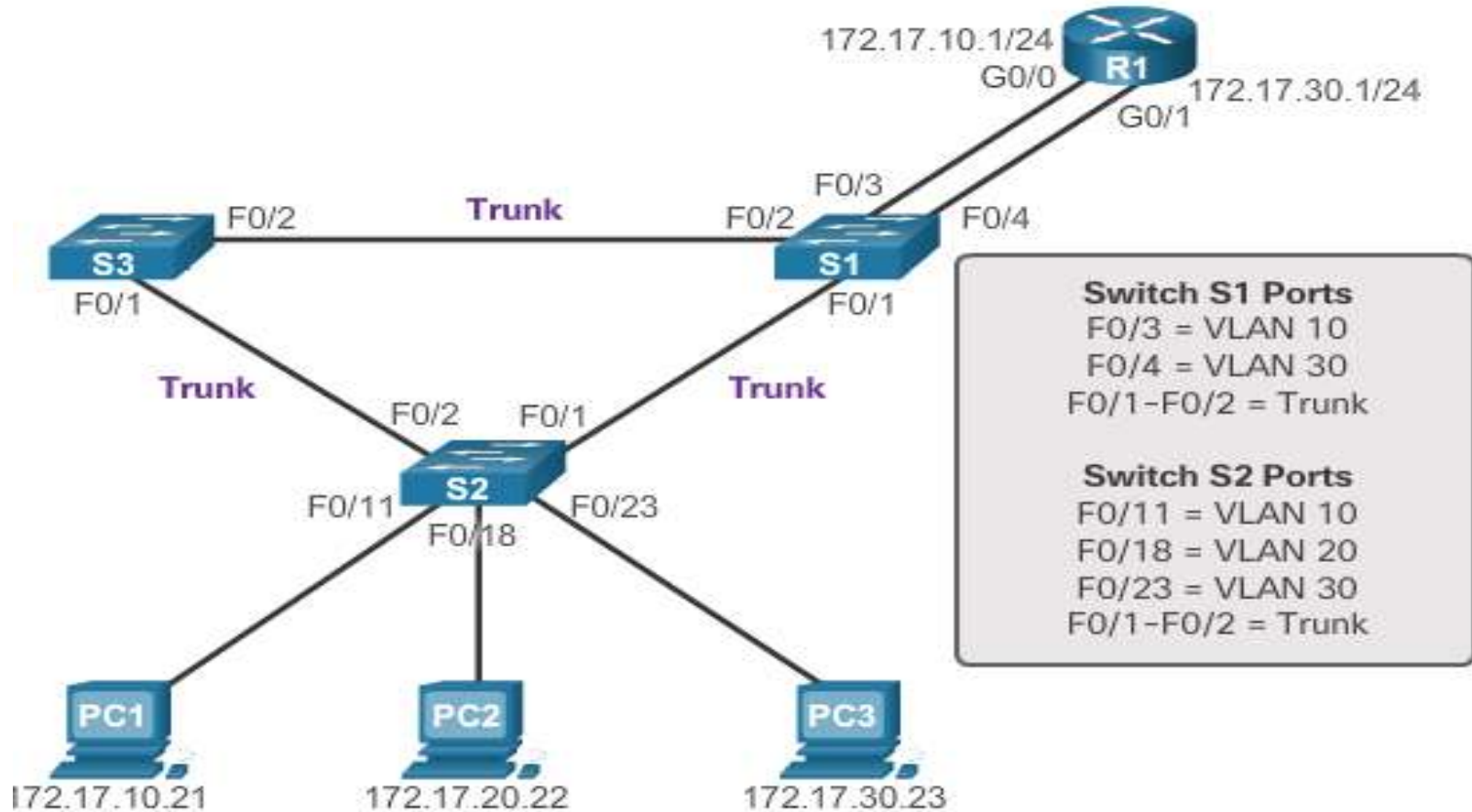


R1 Interface
G0/0 10.17.10.1/28
G0/1 10.17.20.1/28

S1 Ports
G0/3 = VLAN 10
G0/17 = VLAN 20

End Devices
PC1 - VLAN 10
10.17.10.4/28
PC2 - VLAN 20
10.17.20.4/28

Topologi Legacy Inter-VLAN Routing



Legacy Inter-VLAN Routing

Konfigurasi Router

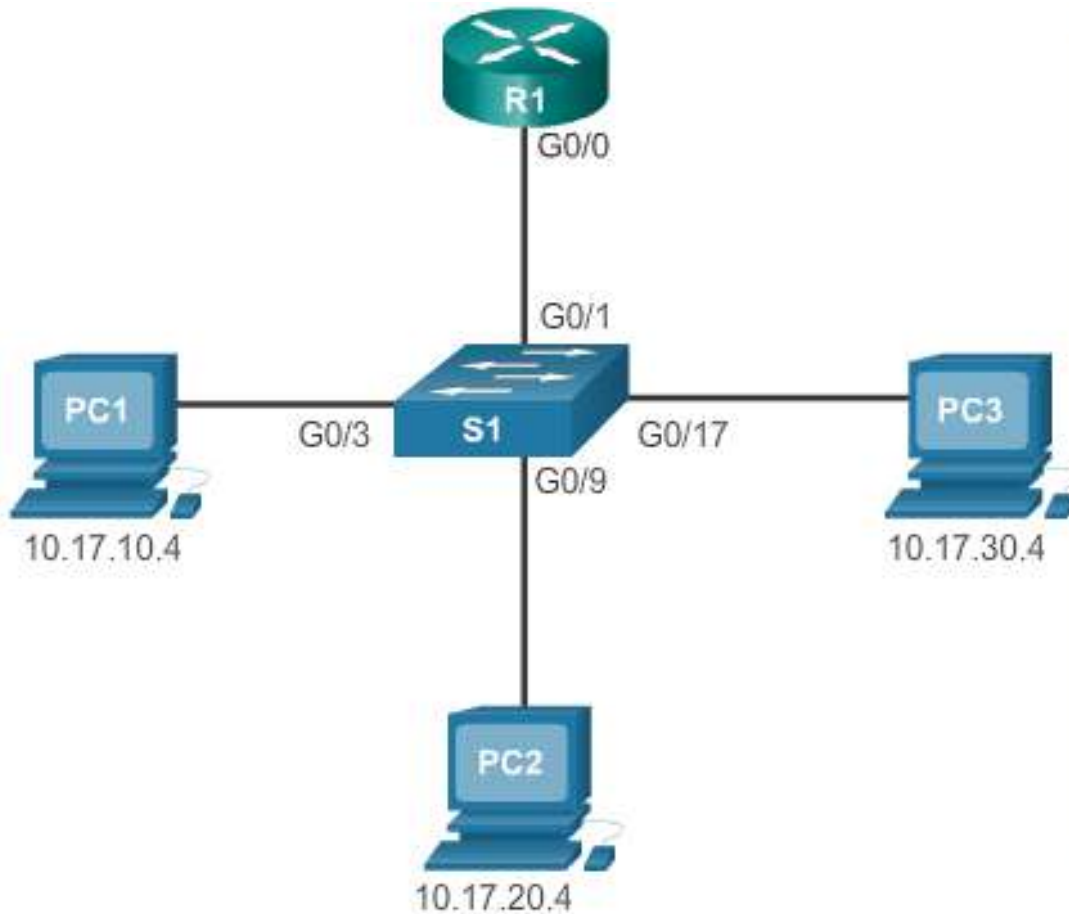
```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

Router on a Stick

- Router On a Stick Inter-VLAN Routing adalah sebuah konsep dari Inter-VLAN Routing yang hanya menggunakan satu buah interface saja pada router. Salah satu interface router dikonfigurasi menggunakan port trunk dengan protokol IEEE 802.1Q sehingga mampu memahami VLAN dibawahnya.
- Setiap sub interface pada Router On a Stick dikonfigurasi menggunakan IP Address dari masing-masing VLAN yang terhubung pada interface router. Alamat yang digunakan pada sub interface router nantinya akan digunakan sebagai gateway dari host pada anggota VLAN.

Topologi Inter-VLAN Routing

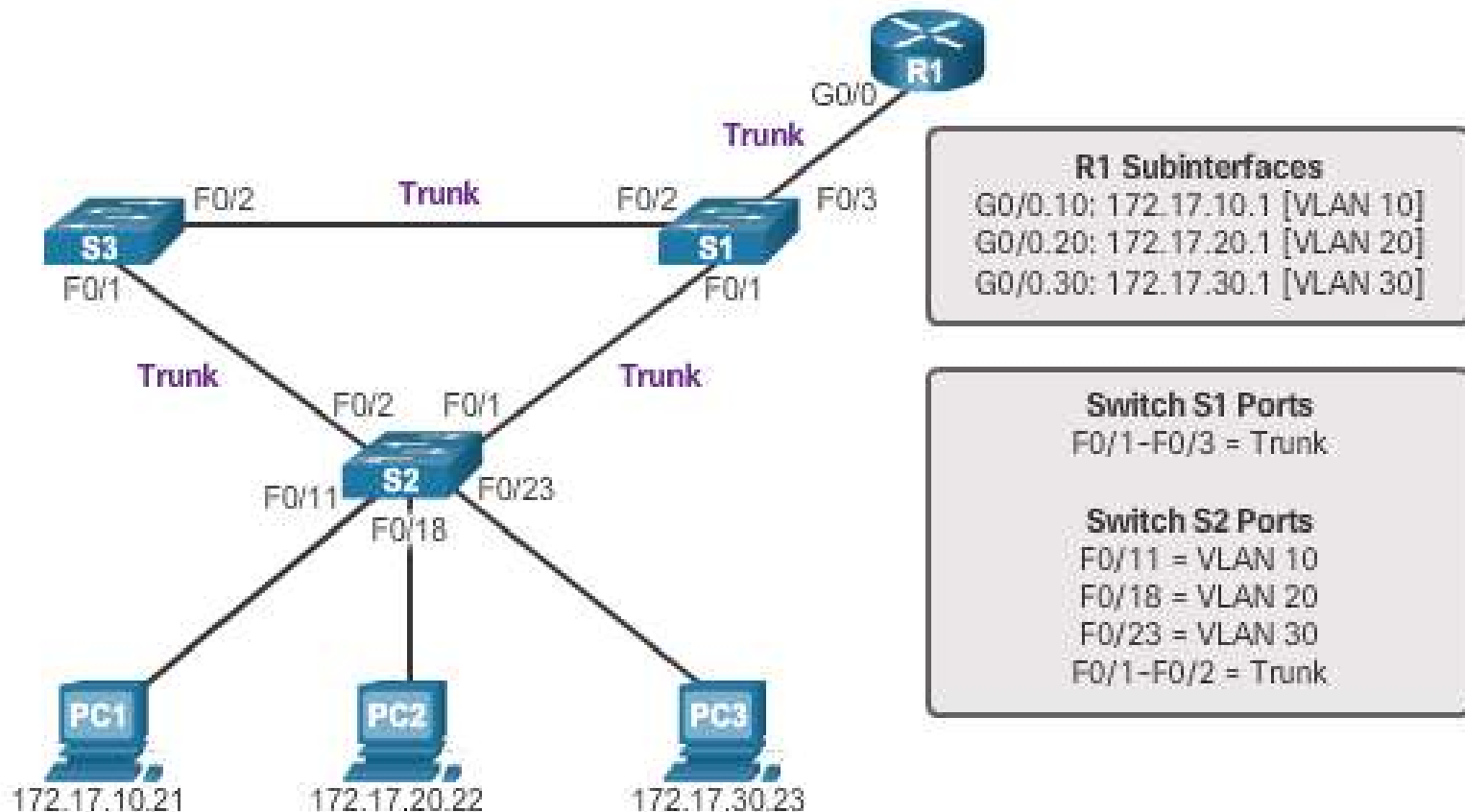
Router on a Stick



R1 Interface	
G0/0 Trunk Link	
R1 Subinterfaces	
G0/0.10	10.17.10.1/28
G0/0.20	10.17.20.1/28
G0/0.30	10.17.30.1/28
S1 Ports	
G0/1 Trunk Link	
G0/3 = VLAN 10	
G0/9 = VLAN 20	
G0/17 = VLAN 30	
End Devices	
PC1 - VLAN 10	10.17.10.4/28
PC2 - VLAN 20	10.17.20.4/28
PC3 - VLAN 30	10.17.30.4/28

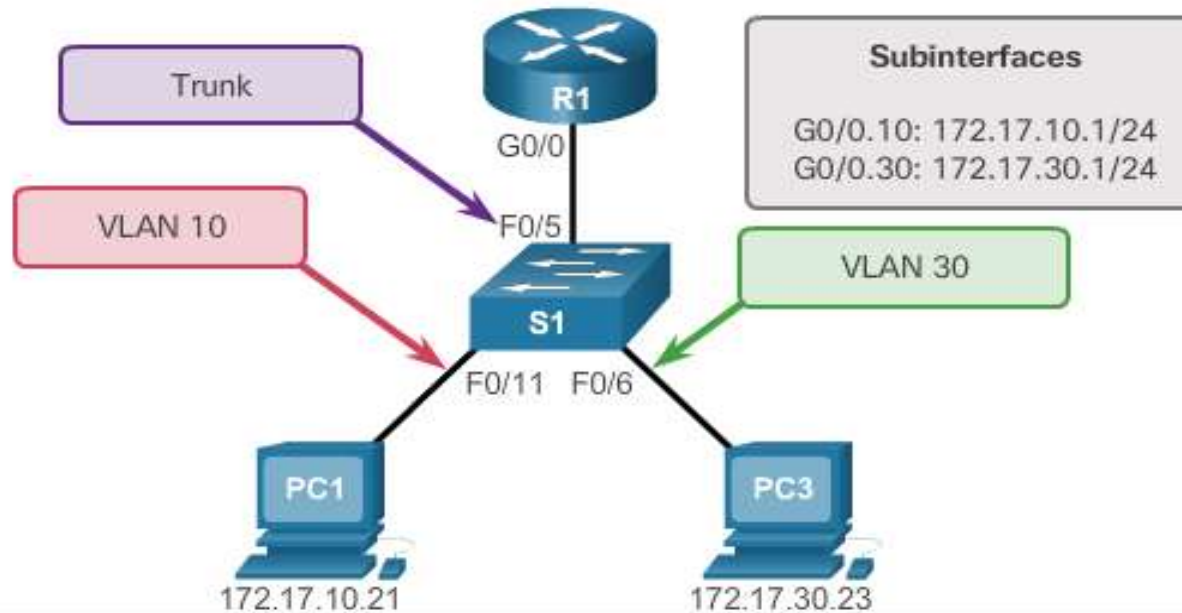
Topologi Inter-VLAN Routing

Router on a Stick



Router on a Stick

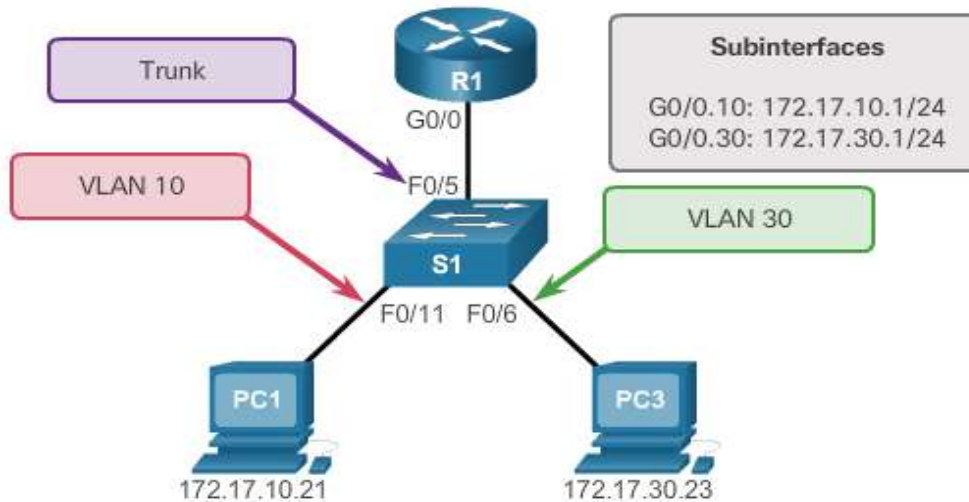
Konfigurasi Switch



```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Router on a Stick

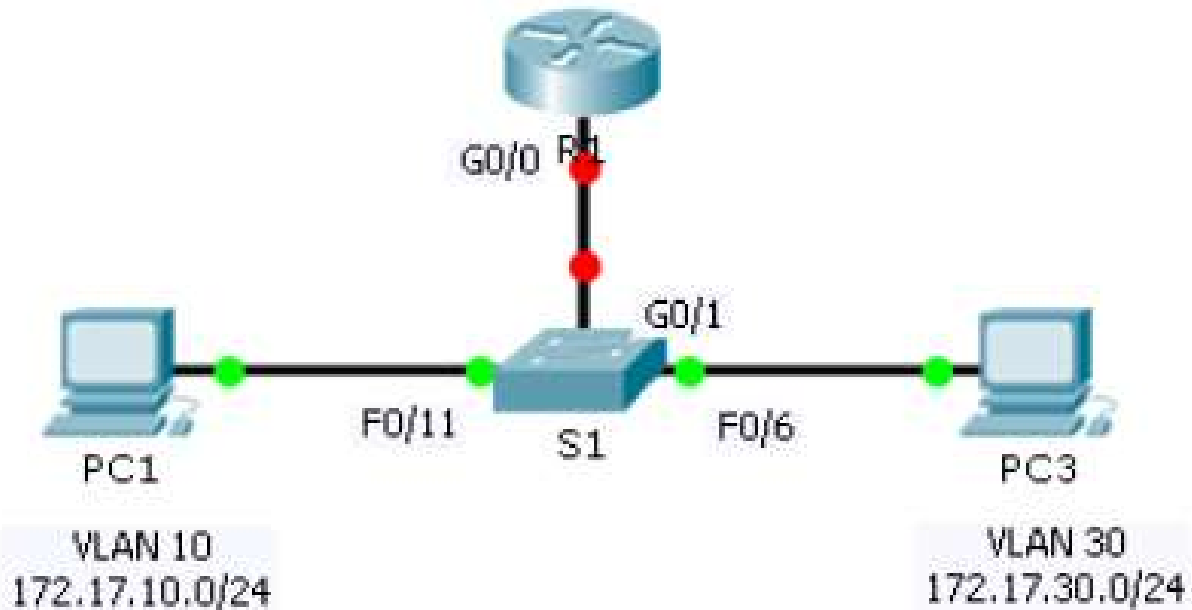
Konfigurasi Router



```
R1 (config) # interface g0/0.10
R1 (config-subif) # encapsulation dot1q 10
R1 (config-subif) # ip address 172.17.10.1 255.255.255.0
R1 (config-subif) # interface g0/0.30
R1 (config-subif) # encapsulation dot1q 30
R1 (config-subif) # ip address 172.17.30.1 255.255.255.0
R1 (config) # interface g0/0
R1 (config-if) # no shutdown
```

Diskusi - Skema Jaringan 1

Router on a Stick

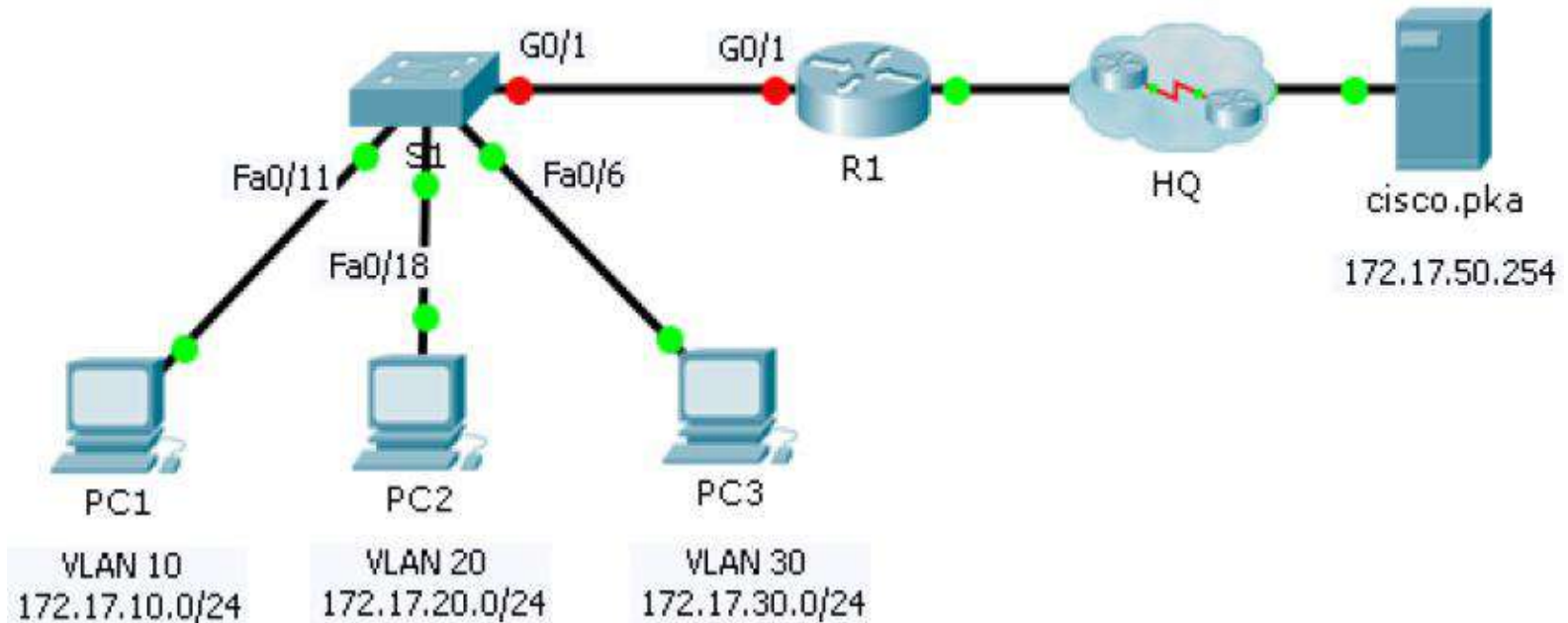


Buatlah jaringan komputer dengan menggunakan model Router on a Stick dengan menggunakan PKA yang telah disediakan:

[6.3.3.6 Packet Tracer - Configuring Router-on-a-Stick Inter-VLAN Routing](#)

Diskusi - Skema Jaringan 2

Inter-VLAN Routing



Buatlah jaringan komputer dengan menggunakan model Inter-VLAN Routing dengan menggunakan PKA yang telah disediakan:

[6.3.3.8 Packet Tracer - Inter-VLAN Routing Challenge](#)

PERTEMUAN 11

ACCESS CONTROL LIST

Access Control List

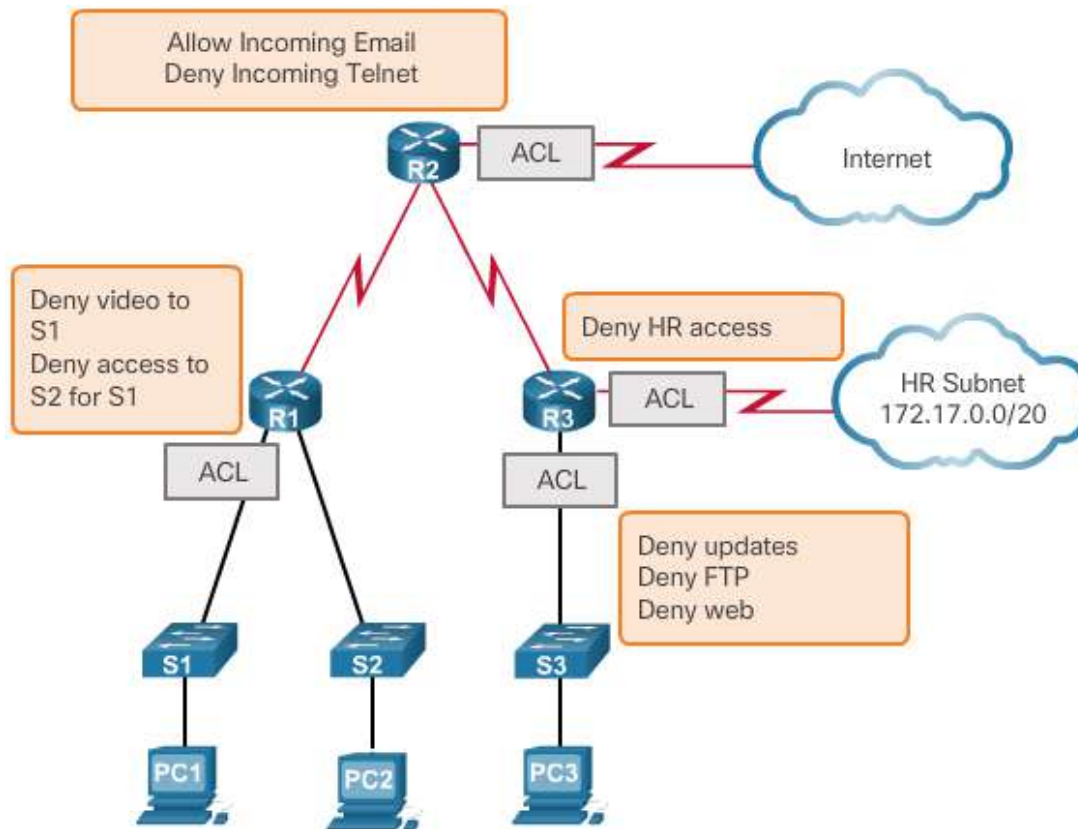
- Access Control List (ACL) pada dasarnya berfungsi untuk mengelola dan mengatasi sebuah permasalahan jaringan dibidang keamanan dan akses.
- ACL merupakan perintah konfigurasi router yang dapat mengontrol apakah router mengizinkan atau menolak paket data untuk melewatinya berdasarkan kriteria yang ditentukan dalam sebuah paket.
- Secara default router tidak memiliki ACL.

Access Control List

- Penggunaan ACL memungkinkan secara spesifik dengan beberapa parameter yang menjadi dasar kegiatan penyaringan paket, terlepas dari apakah penyaringan bergantung pada metode stateless atau stateful.
- Salah satu penggunaan daftar akses yang paling umum dan paling mudah dipahami adalah untuk melakukan filtering terhadap paket yang tidak diinginkan sesuai dengan kebijakan keamanan

Apa ACL itu?

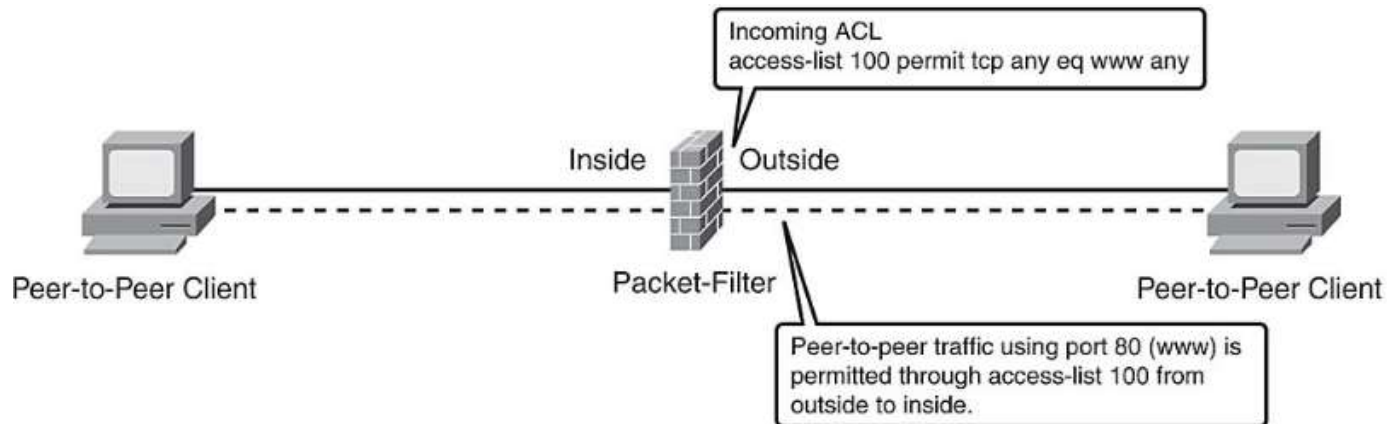
Secara default router tidak memiliki ACL, Oleh karena itu, secara default router tidak menyaring lalu lintas jaringan.



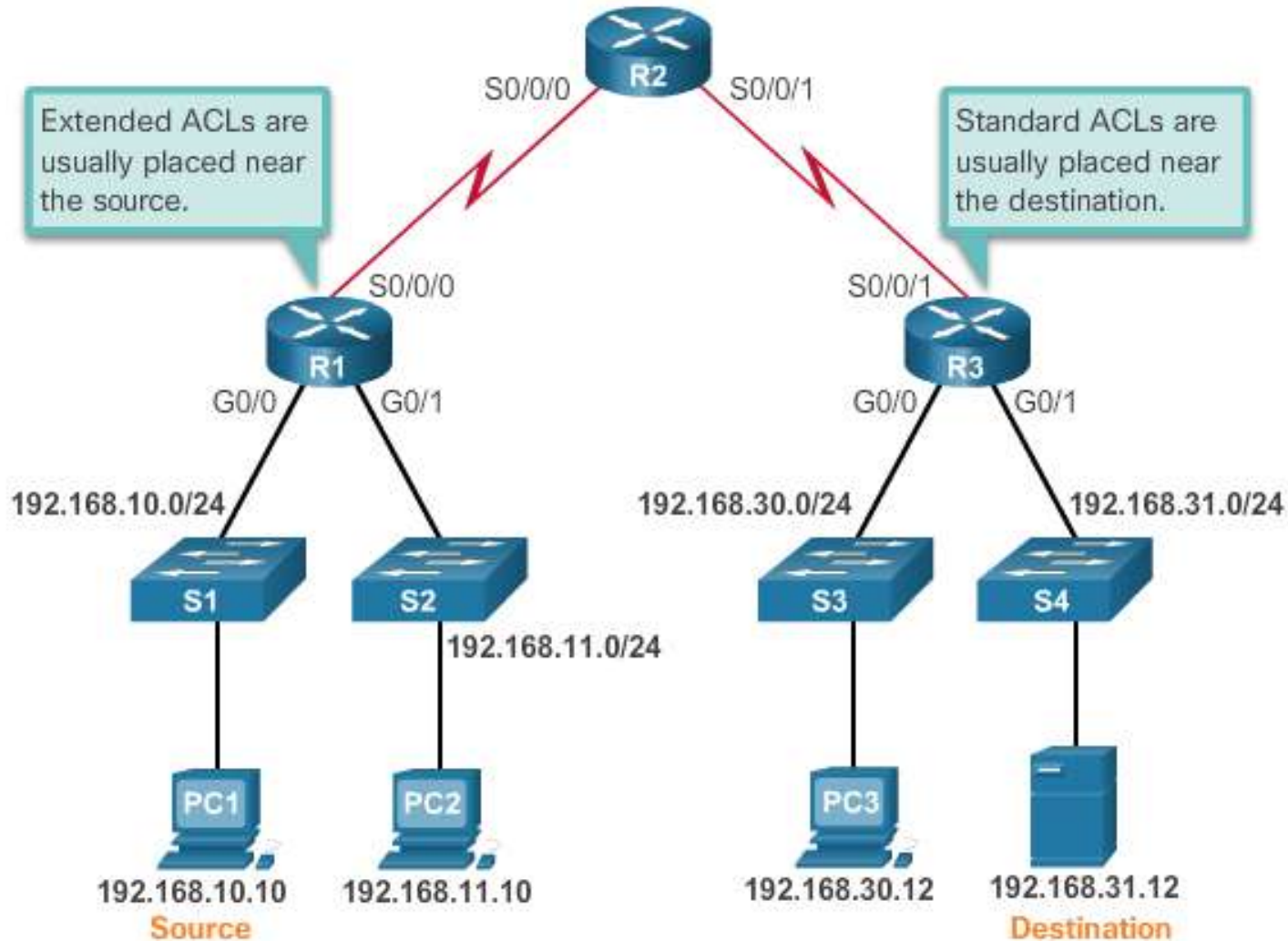
Access Control List

Packet Filtering

Packet filtering, kadang-kadang disebut juga dengan statis packet filtering, berfungsi untuk mengontrol akses ke jaringan dengan menganalisis paket masuk dan keluar dan melewati atau menolak mereka berdasarkan kriteria tertentu, seperti sumber IP address, tujuan IP Address, dan protokol yang digunakan.



Pedoman Penempatan Access Control List



Pedoman Penempatan Access Control List

Setiap ACL harus ditempatkan pada lokasi yang memiliki dampak terbesar pada efisiensi jaringan. Aturan dasar ACL adalah:

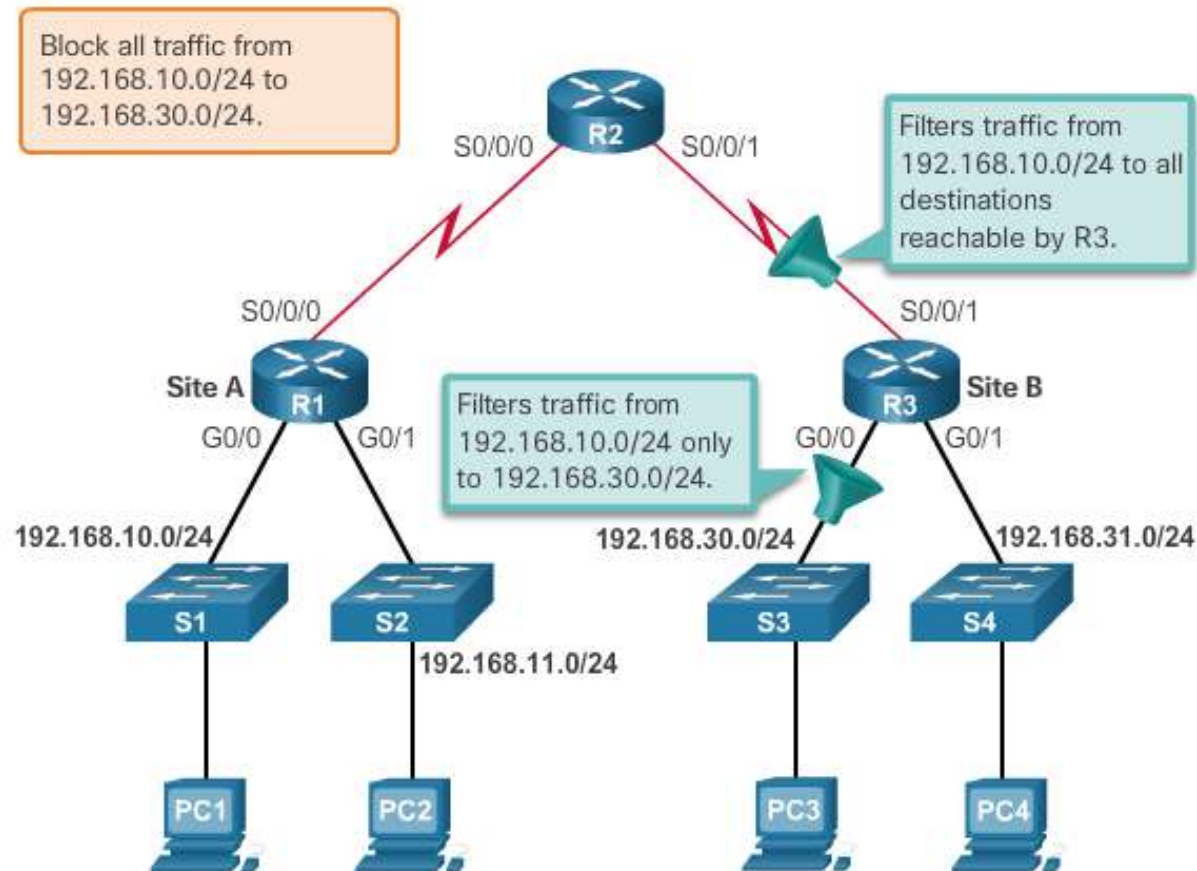
- Extended ACL diletakan sedekat mungkin untuk melakukan penyaringan dengan sumber lalu lintas yang akan disaring. Biasanya menggunakan nomor 100-199 serta dapat melakukan pemilihan protokol ataupun port yang akan dikonfigurasi.
- Standart ACL diletakan sedekat mungkin dengan alamat tujuan. Nomor yang digunakan biasanya diantara 1-99, tidak dapat memilih sebagian port atau traffic yang akan diatur.

Standart ACL

- Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest.
- Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol.
- ACL ini **tidak** dapat membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, dll.
- Standart ACL memiliki number yang dapat digunakan, yaitu 1-99 atau 1300-1999 (expanded range).

Contoh Standar ACL

Administrator ingin mencegah lalu lintas jaringan yang berasal dari 192.168.10.0/24 untuk mencapai alamat 192.168.30.0/24.



Standart ACL

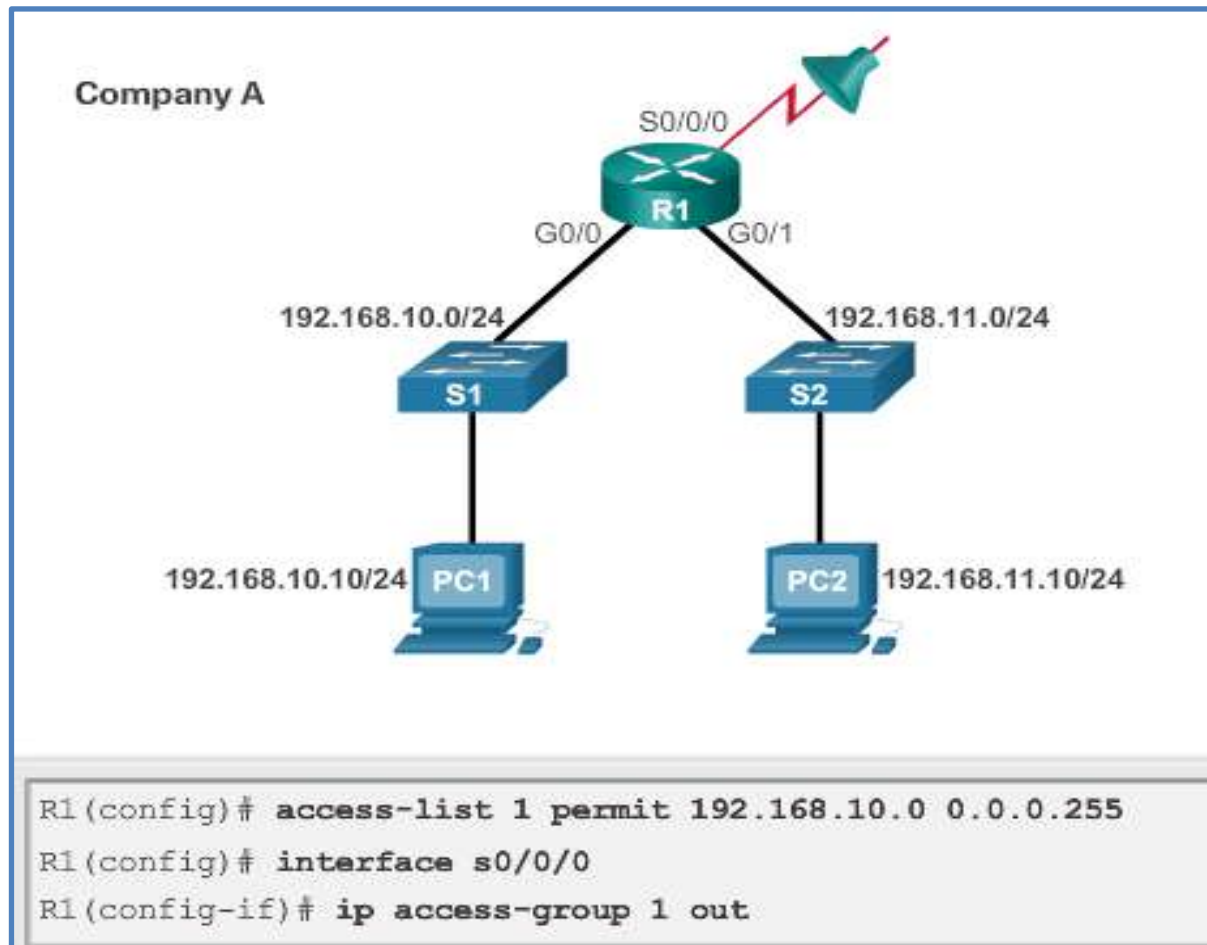
IPv4

router (config) # **access-list** *access-list-number* {deny | permit | remark } *source* [*source-wildcard*] [log]

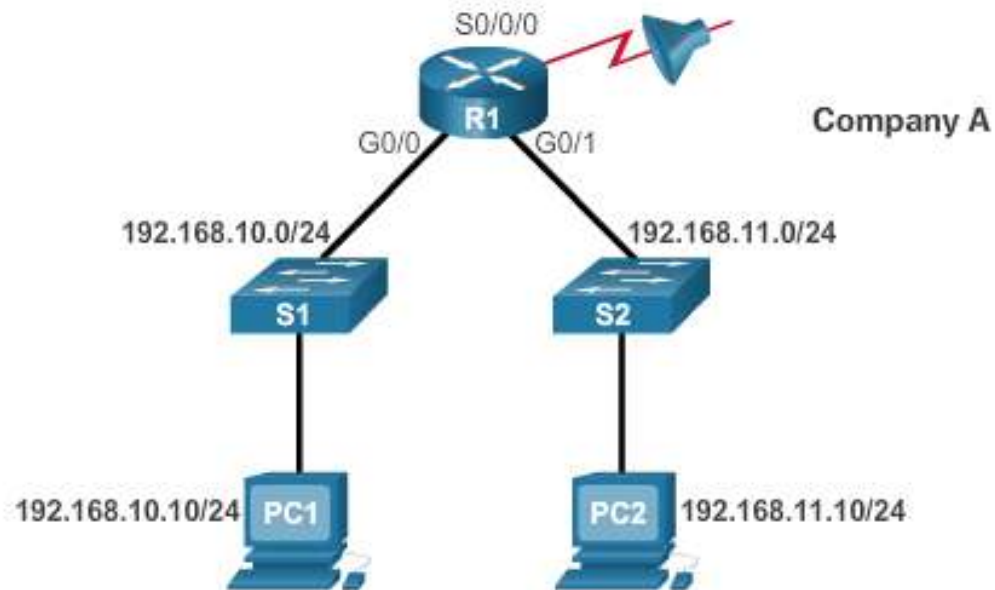
```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
 10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1# show access-lists
R1#
```

```
R1(config)# access-list 10 remark Permit hosts from the
192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
R1#
```

Implementasi Standart ACL

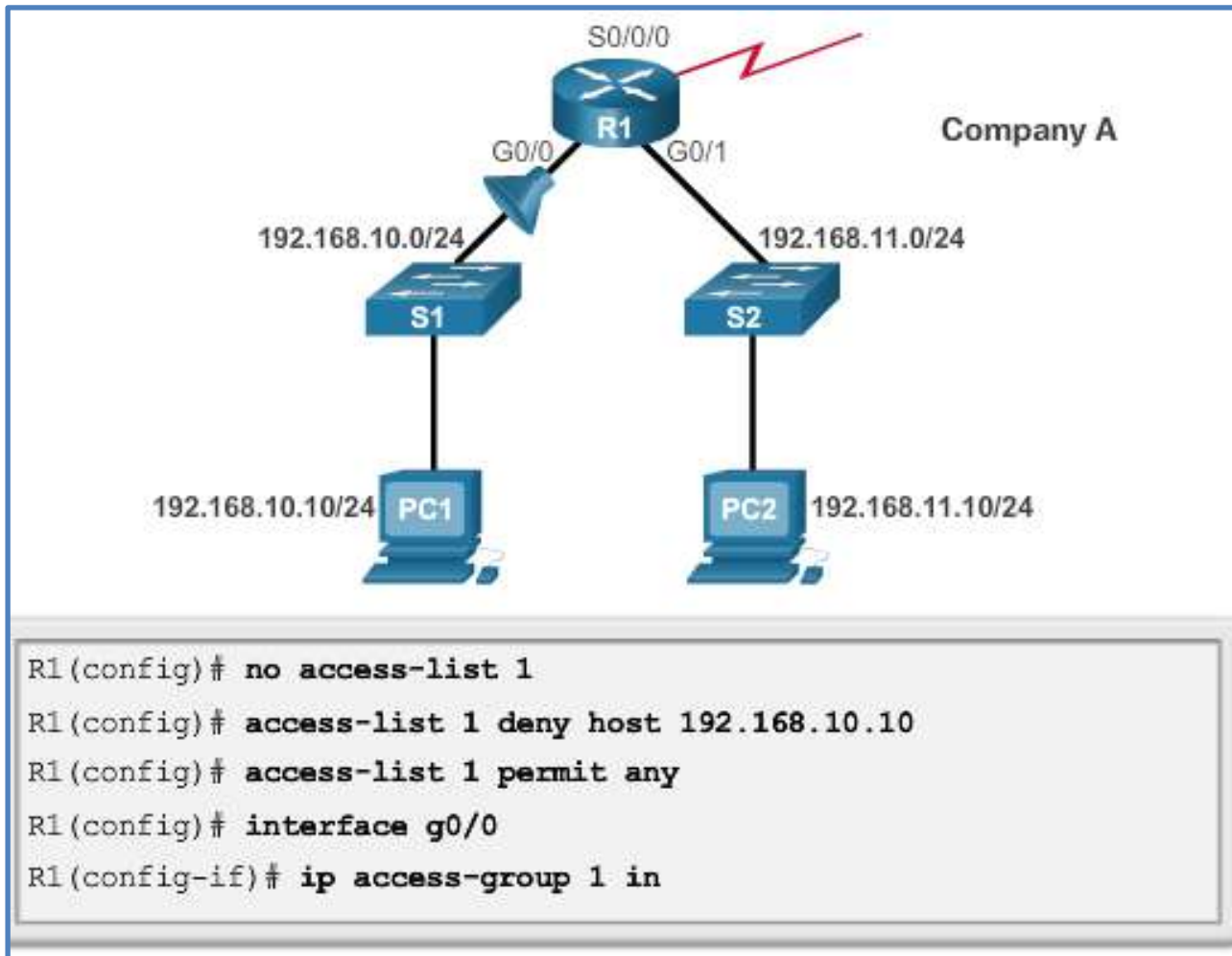


Implementasi Standart ACL



```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Implementasi Standart ACL



Verifikasi ACL

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound access list is not set
<output omitted>
```

```
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access li
  Inbound access li
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
  10 deny 192.168.10.10
  20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
  15 deny 192.168.11.11
  10 deny 192.168.11.10
  20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Extended ACL

Penggunaan Extended ACL dapat melakukan filterisasi lalu lintas berdasarkan alamat sumber dan tujuan, protokol, serta port sumber dan tujuan seperti TCP dan UDP. Anda dapat menggunakan dua buah metode untuk mengidentifikasi ACL standart dan extended:

- Numbered ACL menggunakan nomor untuk mengidentifikasi
- Named ACL menggunakan nama ataupun nomor untuk melakukan identifikasi

Konfigurasi Extended ACL

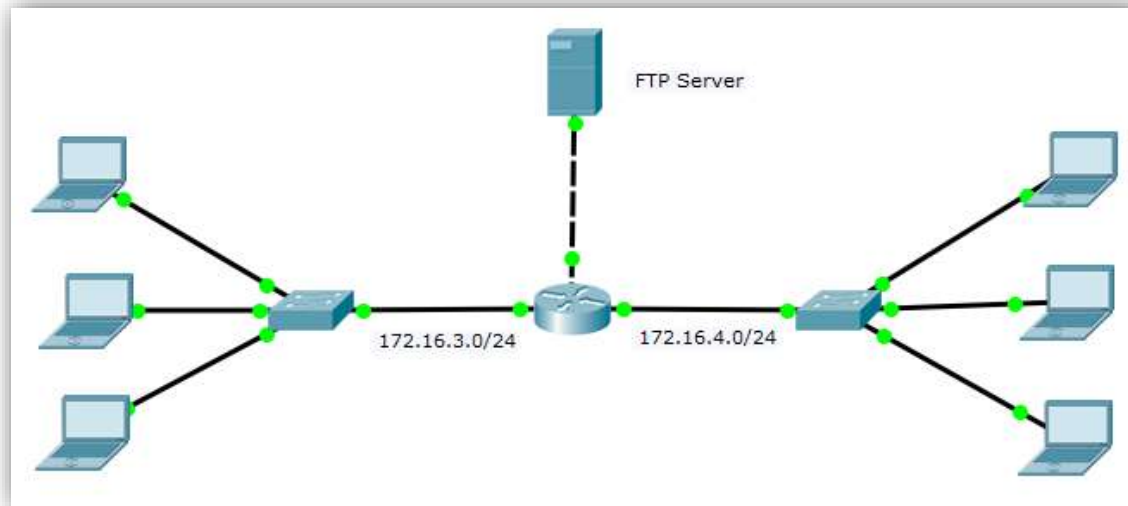
- Untuk melakukan konfigurasi Extended ACL dapat menggunakan perintah:

```
Router(config)#access-list numberacl permit | deny protocol  
sourcenetwrok wildcard sourcenetwrok destinationnetwork  
wildcarddestinationnetwork eq | lt | gt | neq servicename/serviceport
```

- Serta konfigurasi yang digunakan terhadap interface:

```
Router(config)#interface interface number  
Router(config-if)#ip access-group numberacl in/out
```

Konfigurasi Extended ACL



Contoh Konfigurasi Extended ACL Deny FTP...

```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 eq 21
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 eq 20
Router(config)#access-list 101 permit ip any any
Router(config)#interface Ethernet 0
Router(config-if)#ip access-group 101 out
```

Wildcard Mask

Pada dasarnya, penulisan wildcard mask merupakan kebalikan (inverse) dari subnet mask, dapat digunakan pada Access Control List (ACL) statement dan routing protocol OSPF. Wildcard mask default pada dasarnya dibagi berdasarkan class, yaitu:

- Class A: Wildcard Mask-nya 0.255.255.255
- Class B: Wildcard Mask-nya 0.0.255.255
- Class C: Wildcard Mask-nya 0.0.0.255

Menghitung Wildcard Mask

Cara mudah untuk menentukan wildcard mask sebuah network yaitu dengan jumlah host dikurangi satu. Sebagai contoh penulisan Wildcard Mask dengan Subnet Mask:

1. Network : 192.168.10.32/27
Subnetmask : 255.255.255.224
Wildcard Mask : 0.0.0.31
2. Network : 200.10.10.0/24
Subnetmask : 255.255.255.0
Wildcard Mask : 0.0.0.255

Wildcard Mask pada Access Control List

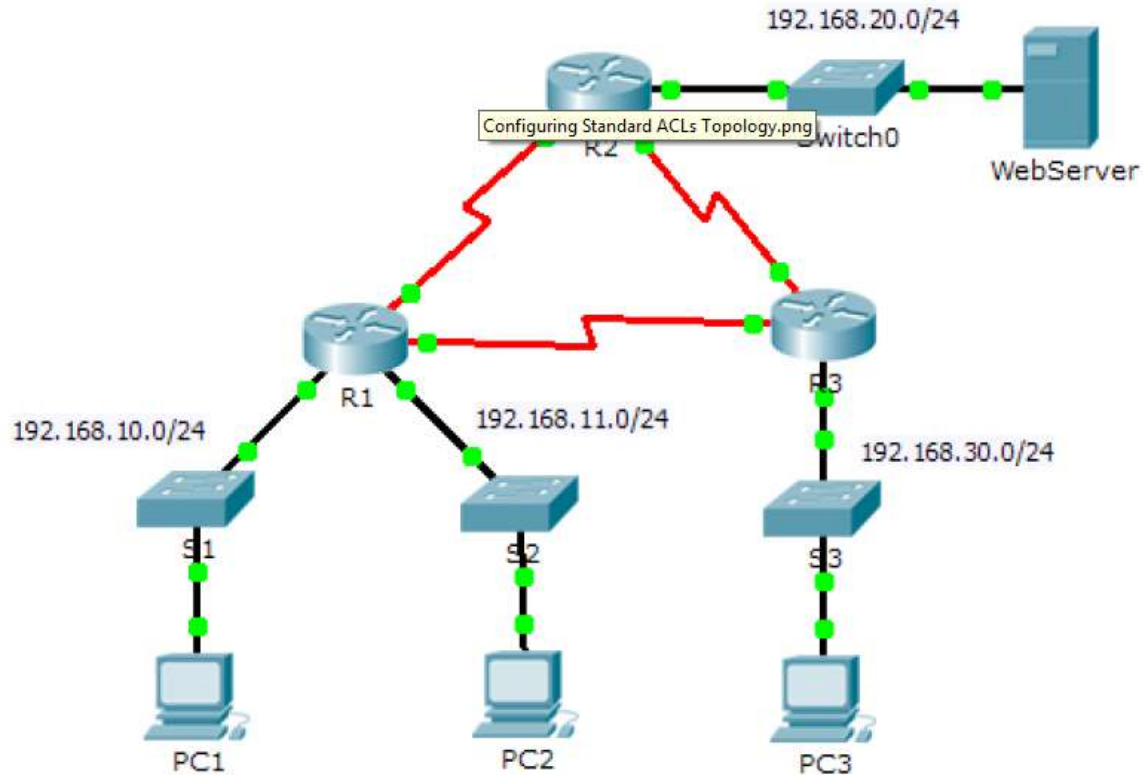
Example 1:

```
R1 (config)# access-list 1 permit 0.0.0.0 255.255.255.255  
!OR  
R1 (config)# access-list 1 permit any
```

Example 2:

```
R1 (config)# access-list 1 permit 192.168.10.10 0.0.0.0  
!OR  
R1 (config)# access-list 1 permit host 192.168.10.10
```

Skema Jaringan



Buatlah jaringan komputer dengan menggunakan PKA yang telah disediakan:

[7.2.1.6 Packet Tracer Configuring Numbered Standard IPv4 ACLs](#)

PERTEMUAN 12

Dynamic Host Configuration Protocol

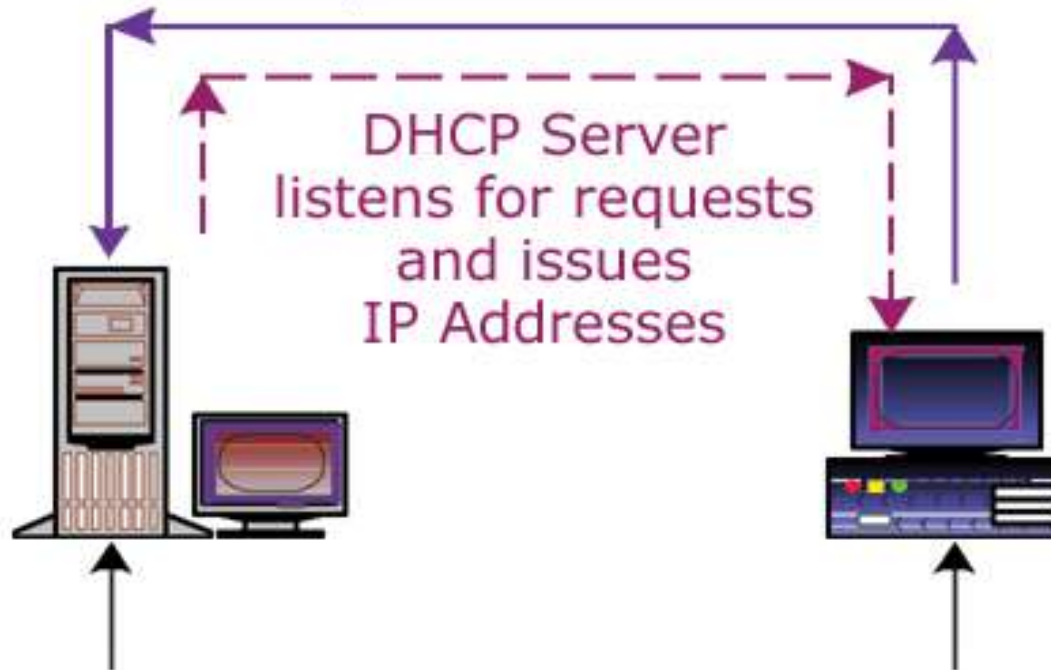
DHCP

(Dynamic Host Configuration Protocol)

DHCP Server merupakan sebuah layanan yang secara otomatis memberikan IP Address kepada komputer yang memintanya, sedangkan komputer yang melakukan request disebut dengan DHCP Client.

Cara Kerja DHCP

Windows DHCP Clients
Make Requests for IP Addresses

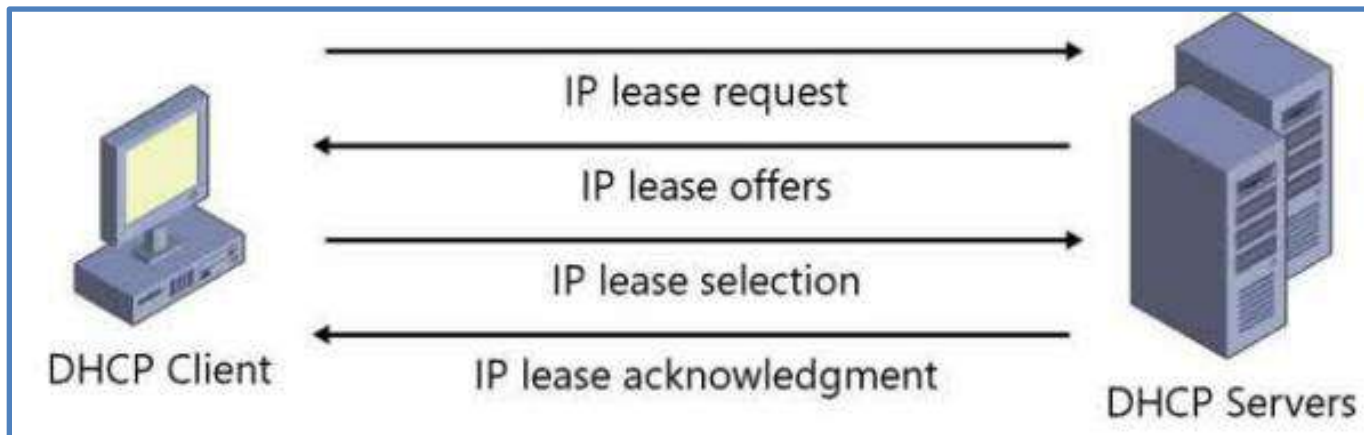


File Server running DHCP Services
(IP Address Server)

Network Workstation
(PC)

Cara Kerja DHCP

- IP Lease Request
- IP Lease Offer
- IP Lease Selection
- IP Lease Acknowledgment



Manfaat DHCP

- Memudahkan seorang administrator jaringan dalam memberikan ip address secara otomatis di komputer dalam jaringan tanpa harus mengisi secara manual.
- Didesain untuk melayani network yang besar dan konfigurasi TCP/IP yang kompleks.
- Memungkinkan suatu client menggunakan alamat IP yang reusable, artinya alamat IP tersebut bisa dipakai oleh client yang lain jika client tersebut tidak sedang menggunakannya.

Manfaat DHCP

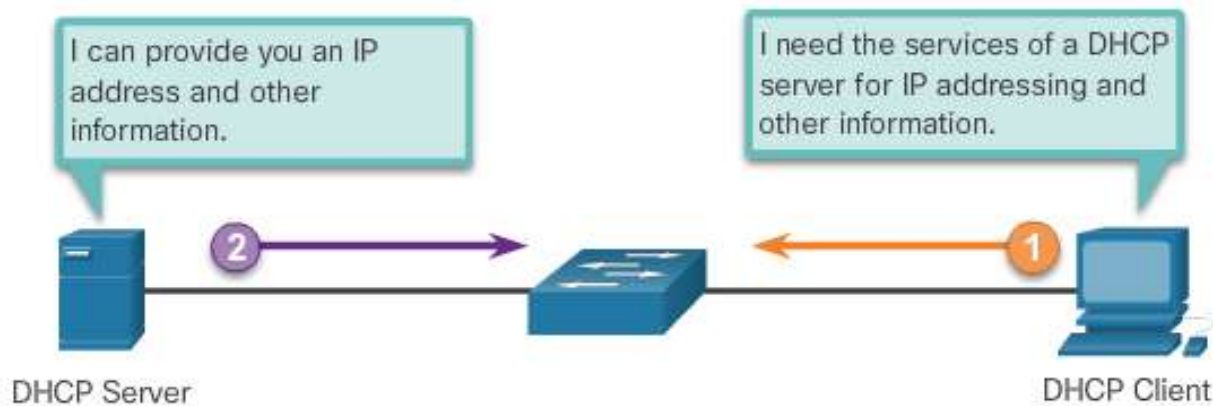
- Memungkinkan suatu client menggunakan satu IP Address untuk jangka waktu tertentu.
- Memberikan satu IP Address dan parameter-parameter konfigurasi lainnya kepada client, seperti pemberian DNS Server & Default Gateway.
- Mampu mencegah terjadinya IP Conflict didalam jaringan yang besar.

Kerugian DHCP

- Semua pemberian IP Address bergantung pada Server. Jadi, jika server mati/off maka semua komputer client akan terkena dampaknya juga seperti disconnect dan tidak saling terhubung.
- Tidak adanya autentifikasi (*pembuktian keaslian*) selama terjadinya komunikasi antara DHCP server dengan DHCP client. Sehingga DHCP server tidak dapat mengetahui jika terdapat DHCP client yang tidak sah didalam jaringan.

DHCPv4 Server

- DHCPv4:
 - Memberikan alokasi IPv4 dan informasi jaringan secara dinamis.
 - Berguna dan hemat waktu untuk seorang network administrator.
- Router Cisco dapat dikonfigurasi untuk menyediakan layanan DHCPv4.



DHCPv4 Server

Konfigurasi Dasar

Sebuah router Cisco dapat melakukan konfigurasi DHCPv4 server. Untuk mengatur DHCP harus memperhatikan beberapa hal berikut ini:

1. Exclude address.
2. Mengatur nama DHCP pool.
3. Menentukan range IP dan subnet mask.
4. Menggunakan perintah **default-router** untuk gateway default.
5. Parameter opsional yang dapat dimasukkan dalam *pool-dns server, domain-name*.
6. Untuk menonaktifkan DHCP, gunakan perintah **no service dhcp**.

DHCPv4 Server

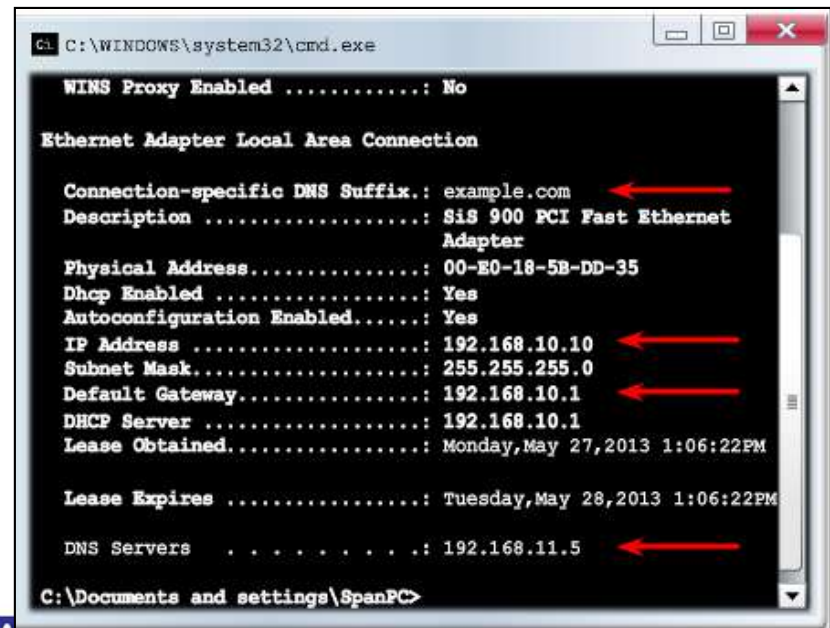
Konfigurasi Dasar

```
R1 (config) # ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1 (config) # ip dhcp excluded-address 192.168.10.254
R1 (config) # ip dhcp pool LAN-POOL-1
R1 (dhcp-config) # network 192.168.10.0 255.255.255.0
R1 (dhcp-config) # default-router 192.168.10.1
R1 (dhcp-config) # dns-server 192.168.11.5
R1 (dhcp-config) # domain-name example.com
R1 (dhcp-config) # end
R1 #
```

DHCPv4 Server

Verifikasi

- Perintah yang digunakan untuk melakukan verifikasi DHCP adalah:
 - show running-config | section dhcp
 - show ip dhcp binding
 - show ip dhcp server statistics
- Sedangkan pada PC, menggunakan perintah **ipconfig /all**.



```
C:\WINDOWS\system32\cmd.exe

WINS Proxy Enabled .....: No

Ethernet Adapter Local Area Connection

Connection-specific DNS Suffix.: example.com
Description .....: SiS 900 PCI Fast Ethernet Adapter
Physical Address.....: 00-E0-18-5B-DD-35
Dhcp Enabled .....: Yes
Autoconfiguration Enabled.....: Yes
IP Address .....: 192.168.10.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1
DHCP Server .....: 192.168.10.1
Lease Obtained.....: Monday, May 27, 2013 1:06:22PM

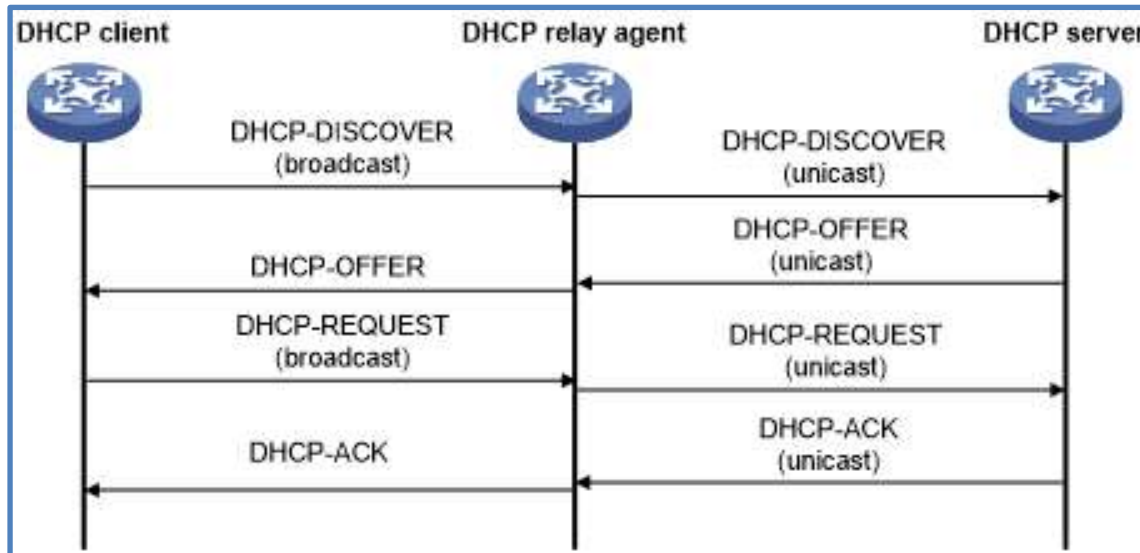
Lease Expires .....: Tuesday, May 28, 2013 1:06:22PM

DNS Servers . . . . .: 192.168.11.5

C:\Documents and settings\SpanPC>
```

DHCPv4 Relay

DHCP Relay adalah sebuah proxy yang mampu meneruskan paket **DHCP** antara client dengan server saat client dan server tidak berada pada satu subnet



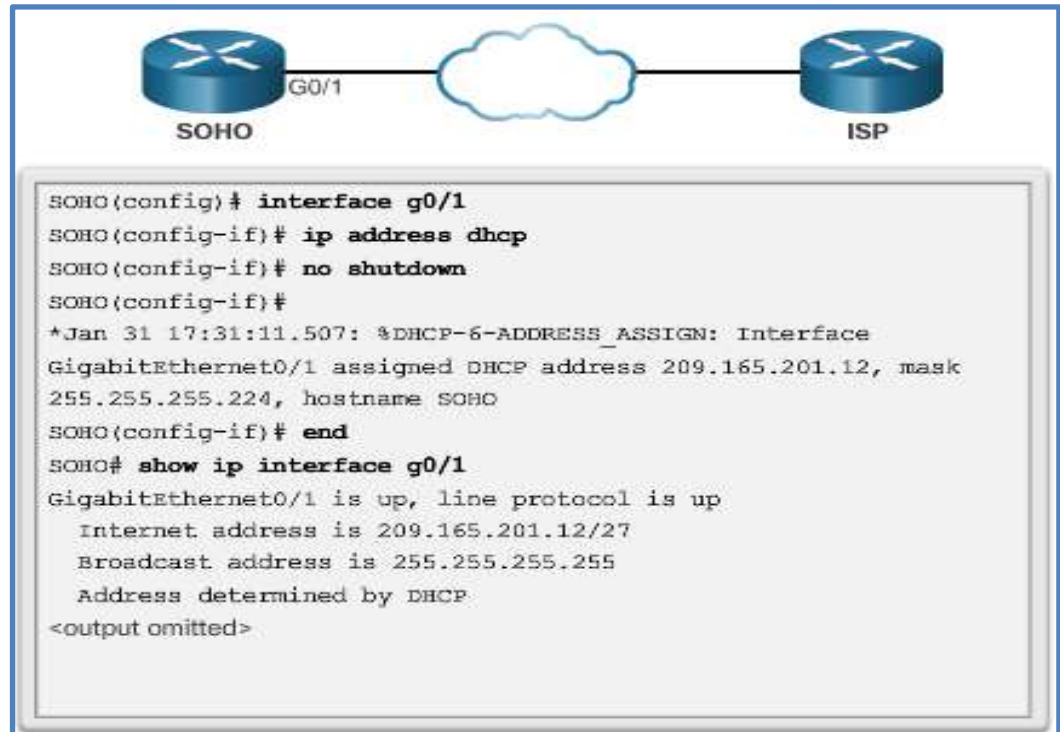
Menggunakan ip helper-address untuk memungkinkan router meneruskan broadcast DHCP Server

DHCPv4 Relay Konfigurasi Dasar

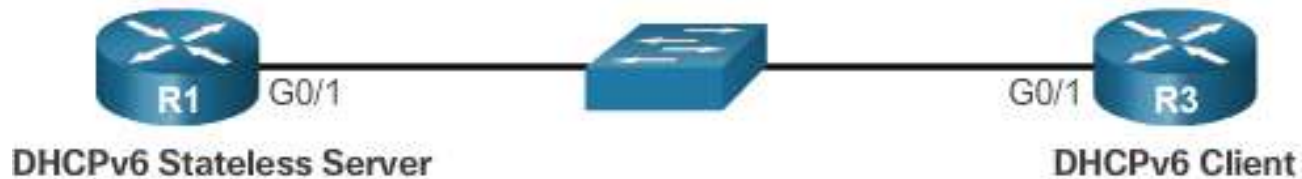
```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<Output omitted>
```

DHCPv4 Client Konfigurasi

Konfigurasi pada Router
sebagai DHCP Client



DHCPv6 Server



```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Untuk mengaktifkan fitur **IPv6** dapat menggunakan
“ipv6 unicast-routing”

DHCPv6 Client

Konfigurasi pada Router sebagai DHCP Client menggunakan IPv6



```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#
```

Studi Kasus DHCP Server

Buatlah jaringan komputer menggunakan fitur DHCP Server dengan ketentuan sebagai berikut:

1. Gunakan IP Address 172.168.10.1/24 sebagai gateway dari jaringan LAN,
2. Range IP Address yang dapat digunakan adalah 172.168.10.10 – 172.168.10.50.

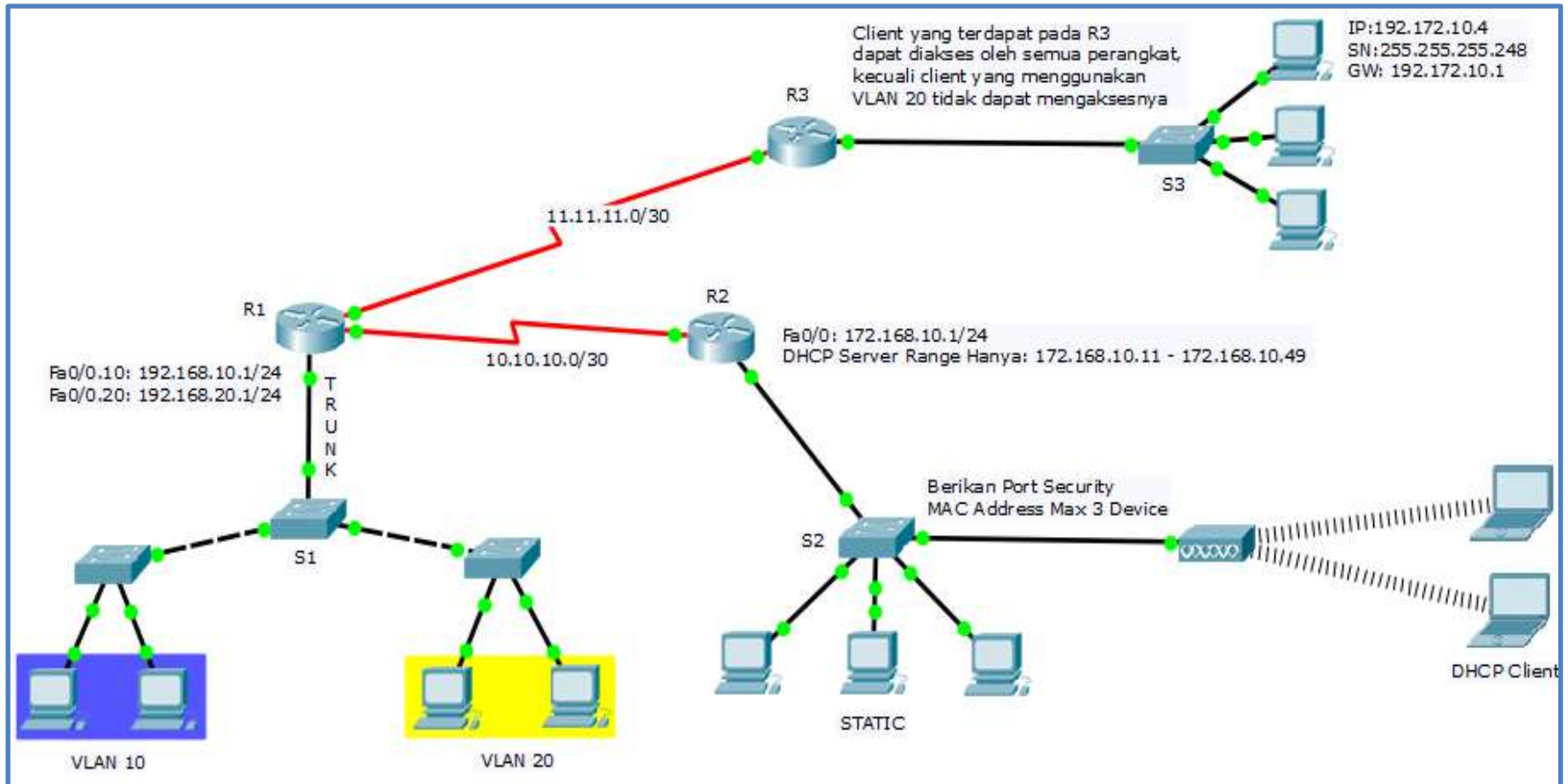
PERTEMUAN 13

SKEMA JARINGAN

SKEMA JARINGAN

Buatlah jaringan komputer sesuai dengan skema jaringan yang telah ditentukan...!

SKEMA JARINGAN

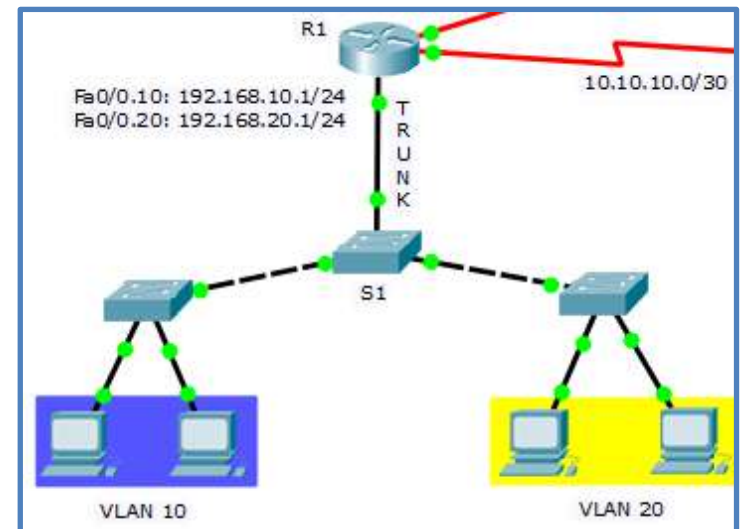


KETENTUAN

1. R1,

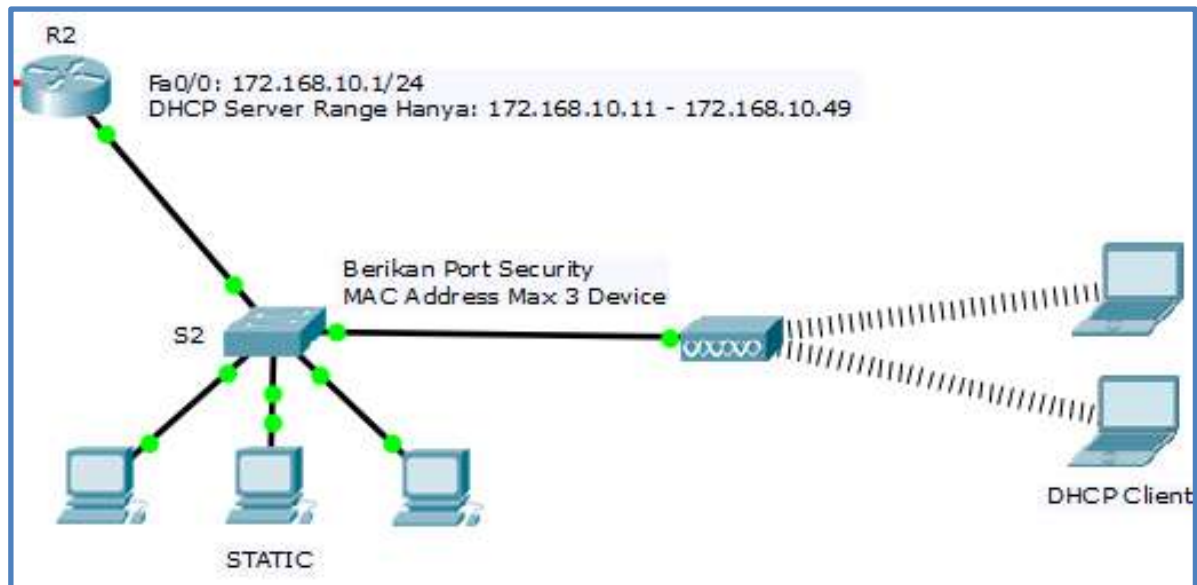
1. Interface Fast Ethernet 0/0 digunakan sebagai Inter-VLAN Routing yang digunakan untuk menghubungkan VLAN 10 dan VLAN 20 dibawahnya.
2. Sedangkan, dua (2) interface lainnya pada router (R1) digunakan untuk menghubungkan router to router

2. S1 menyediakan VLAN database (VLAN 10 & VLAN 20)



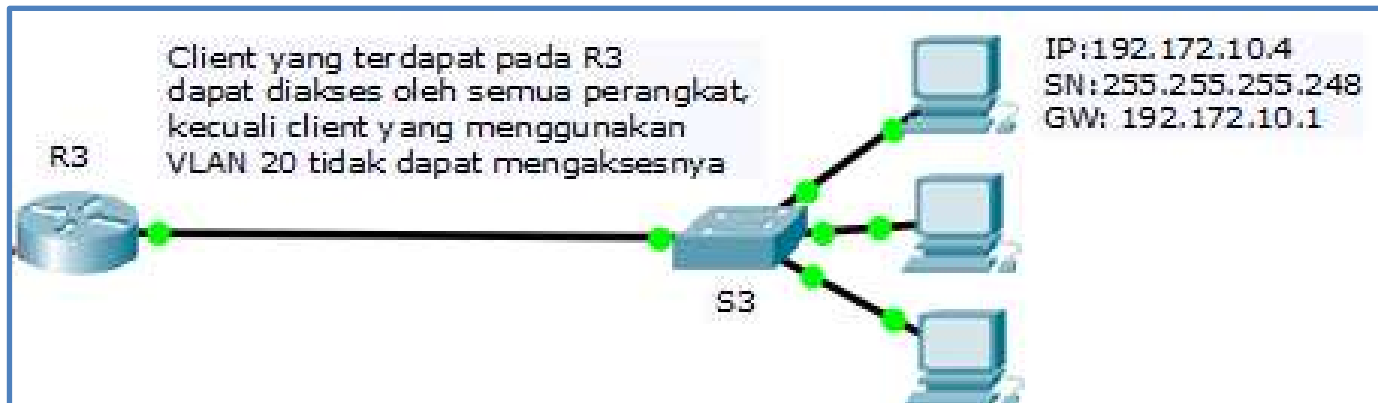
KETENTUAN

3. Pada **R2**, interface Fa0/0 mengaktifkan fitur DHCP Server, dengan range DHCP 172.168.10.11 – 172.168.10.49
4. Pada **S2**, menerapkan keamanan jaringan menggunakan Port Security MAC-Address (akses untuk Access Point)



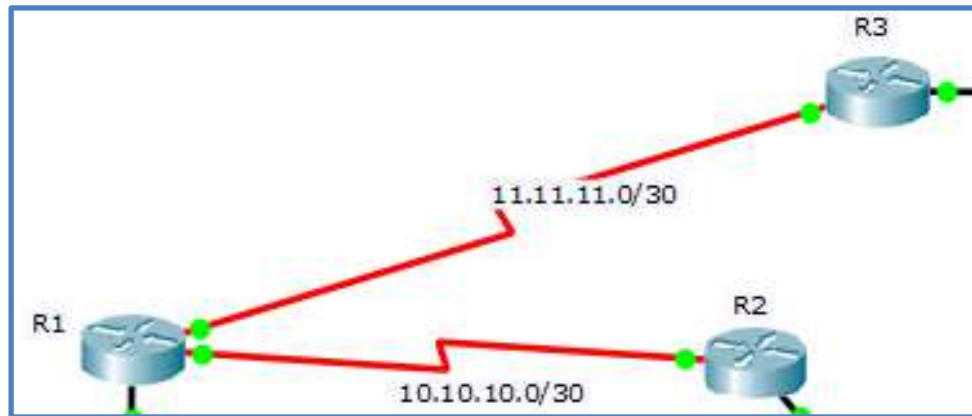
KETENTUAN

5. Pada **S3**, menggunakan keamanan Access Control List untuk **menolak** lalu lintas jaringan dari VLAN 20, selain VLAN 20 dapat melakukan komunikasi dengan Client yang tersedia pada R3.



KETENTUAN

6. Lengkapi IP Address pada R1, R2 dan R3
7. Lakukan konfigurasi Dynamic Routing untuk menghubungkan semua Network yang dibentuk



PERTEMUAN 14

Teknologi dan Standarisasi Wireless

Support Mobility

- Produktifitas tidak lagi terbatas dengan lokasi
- Dapat digunakan dimana saja, dan kapan saja
- Pengguna layanan saat ini sudah berharap menggunakan jaringan wireless
- Roaming memungkinkan perangkat nirkabel untuk mempertahankan akses terhadap internet tanpa kehilangan koneksi

Manfaat Wireless

- Lebih fleksibilitas
- Lebih produktif
- Mengurangi biaya instalasi
- Mudah dalam beradaptasi dari setiap perubahan yang terjadi

Infrastruktur Wireless

Wireless NIC

Penerapan jaringan wireless membutuhkan:

- End Device dengan menggunakan Wireless NIC
- Perangkat infrastruktur, seperti wireless router atau Wireless Access Point

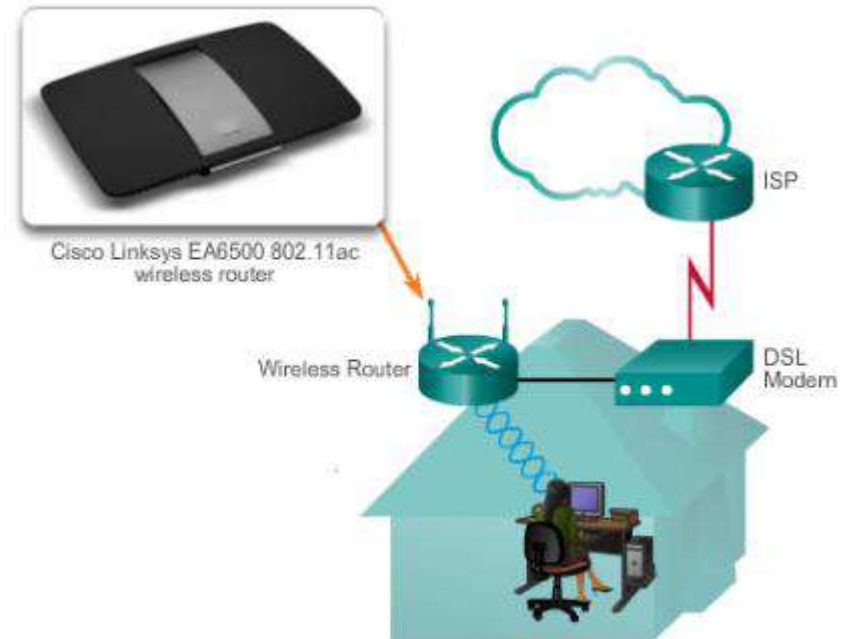


Infrastruktur Wireless

Wireless Home Router

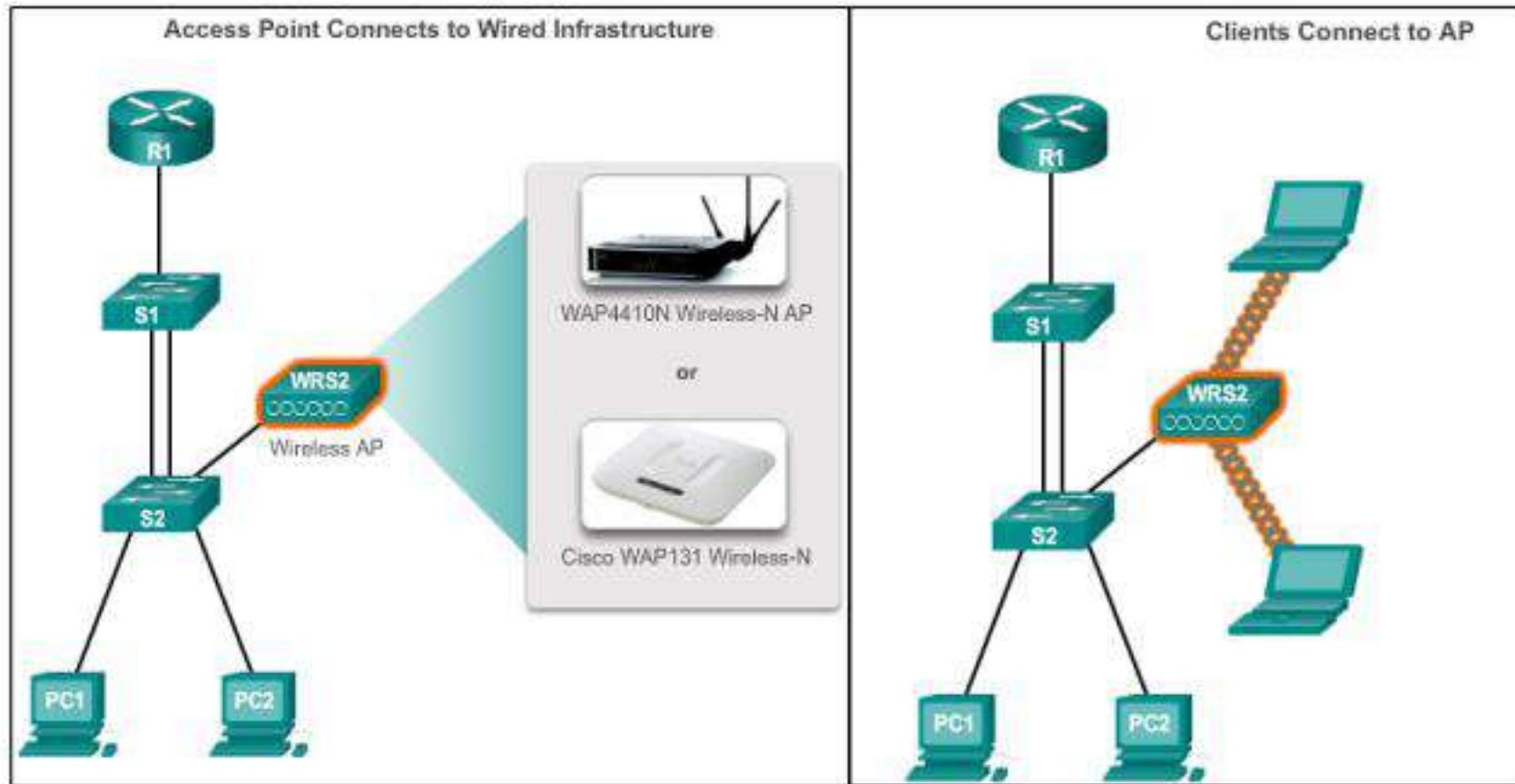
Penerapan jaringan wireless pada rumah dapat saja membutuhkan:

- Wireless Router
- Access Point
- Ethernet Switch
- Router



Infrastruktur Wireless

Wireless Business Router



Wireless Operation

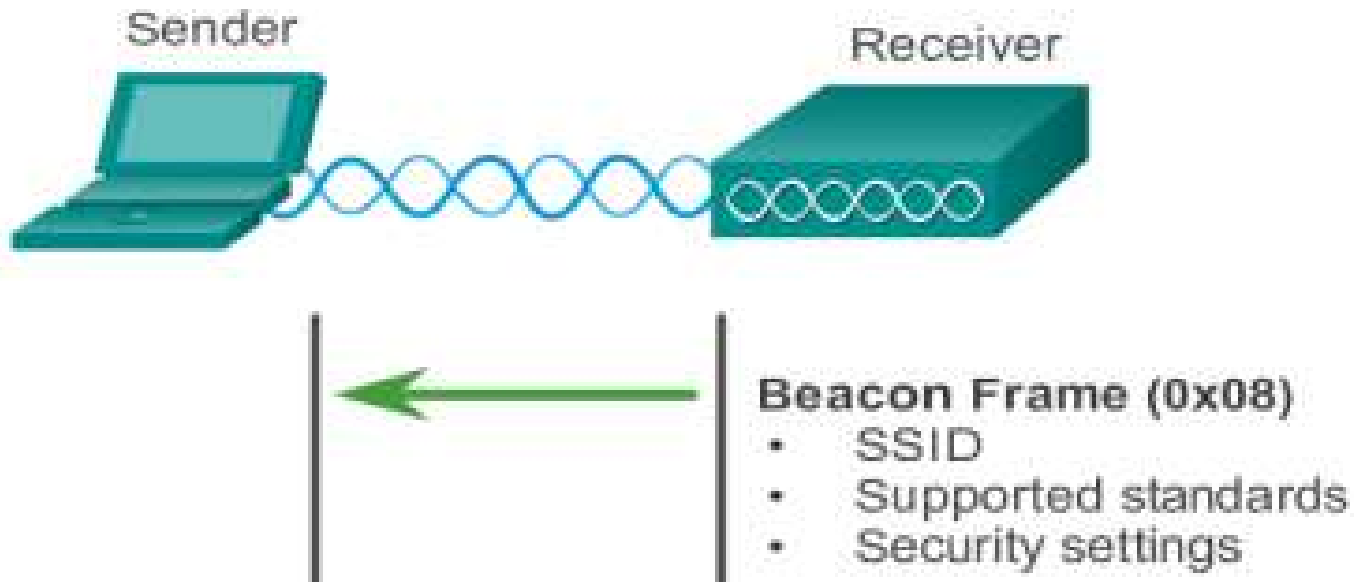
- Access Point mode Passive
 - Mode ini melakukan broadcast dengan melakukan pengiriman frame menggunakan SSID, standar layanan serta penerapan keamanan.
 - Tujuan dari mode ini adalah untuk memungkinkan penggunaan layanan wireless pada client dengan AP yang tersedia.
- Access Point mode Active

Wireless Operation

- Access Point mode Active
 - Client pengguna layanan harus mengetahui SSID.
 - Client harus melakukan permintaan layanan broadcast yang tersedia seperti hak akses keamanan yang digunakan.

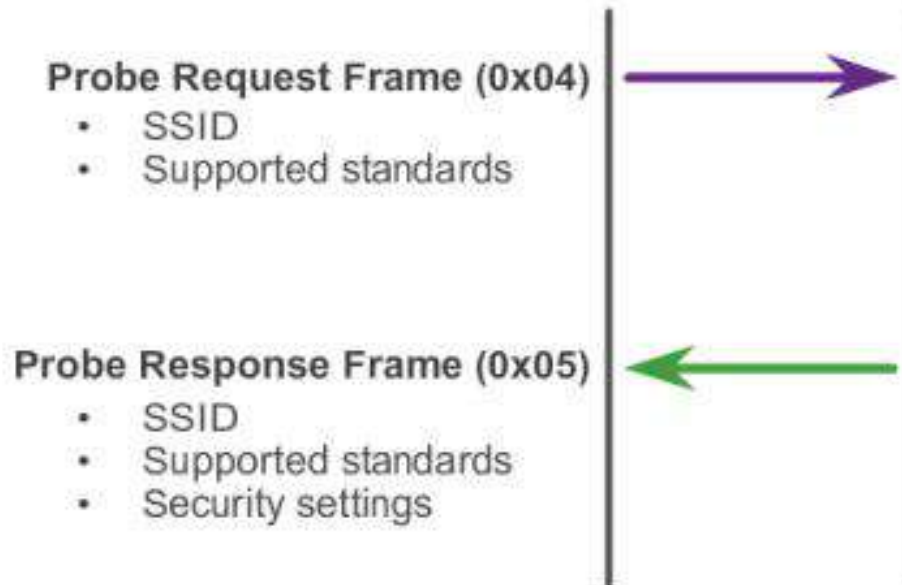
Wireless Operation

Client Devices Listen for an AP



Wireless Operation

AP Broadcast Frame



Perkenalan Teknologi Wireless

10 Tahun yang lalu,

Wi-Fi laptop

Saya bisa menggunakan Wi-Fi di ruang pertemuan, tapi saya akan kehilangan sinyal jika saya pindah



Wired Phone

Beberapa ponsel telah memiliki fitur Wi-Fi, akan tetapi masih kurangnya fasilitas jaringan wireless.

Perkenalan Teknologi Wireless

Di Tahun 2010,



Multi Wi-Fi

Seperti kebanyakan orang, saya memiliki 2 atau 3 perangkat Wi-Fi

Fasilitas Wi-Fi sudah tersedia di Rumah, Kantor dan Tempat Umum.

More Applications

Mengandalkan jaringan Wi-Fi untuk beberapa aplikasi dan untuk menjalankan video

Perkenalan Teknologi Wireless

Di Tahun 2015,

802.11ac
802.11n
Everything uses Wi-Fi...
Everything?

Far Reaching Wi-Fi

Saya dapat menggunakan
Wi-Fi dimana saja



More Applications

Saat ini hampir semua orang
menggunakan layanan Wi-Fi

Perkenalan Teknologi Wireless

Hari ini,



802.11ac -> 802.11ad

Perangkat Anda kini sudah dapat melakukan Streaming ke TV, Laptop, Telepon dan Tablet



802.11ah – Wireless for IoT

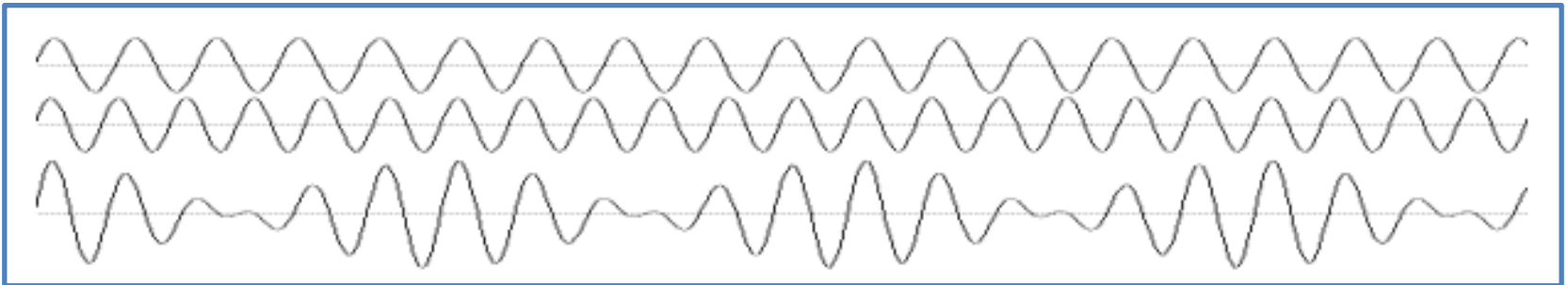
Wi-Fi sudah digunakan untuk melakukan monitoring terhadap dunia industri

Teknologi Wireless

- PAN/WPAN
 - Bluetooth, IEEE 802.15.4
- LAN
 - IEEE 802.11
- MAN
 - IEEE 802.11, IEEE 802.16, 802.20
- WAN
 - GSM, CDMA, Satelit

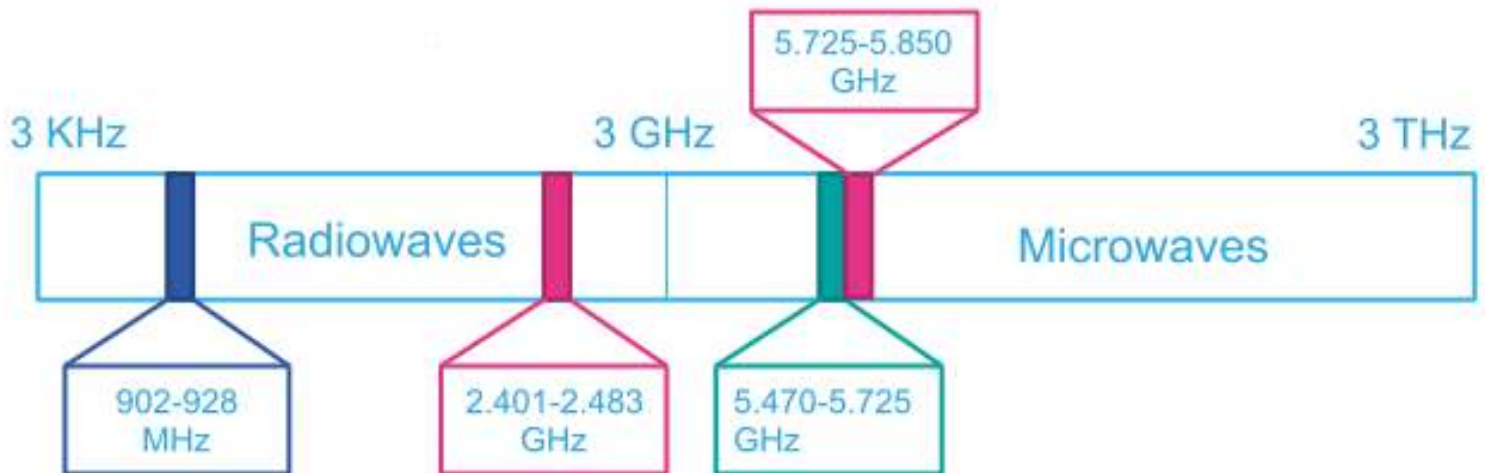
Teknologi Wireless

- Teknologi wireless menggunakan gelombang elektromagnetik



Frequency LAN

- ISM – Industrial Scientific Medical
- 2,4 dan 5 Ghz Bands



CSMA/CA

Terdapat beberapa permasalahan terhadap akses jaringan wireless medium, diantaranya:

- Wireless selalu bersifat half-duplex jika berkomunikasi menggunakan 10Base5 dan 10 Base2 dalam pengimplementasiannya.
- Jika 2 station melakukan transmit secara bersamaan maka akan terjadi collision.
- Metode kontrol terhadap akses sangat diperlukan pada jaringan wireless

Komunikasi Channel

- Media Transmisi wireless bersifat broadcast,
- Tidak mungkin untuk melakukan pengiriman paket data didalam frekuensi yang sama tanpa terjadinya collision,

IEEE 802.11

- Legacy – released pada 1997
- Spesifik untuk infrared dan wireless
- Speed 1-2 Mbps
- Frequency 2,4 Ghz dan 900 Mhz

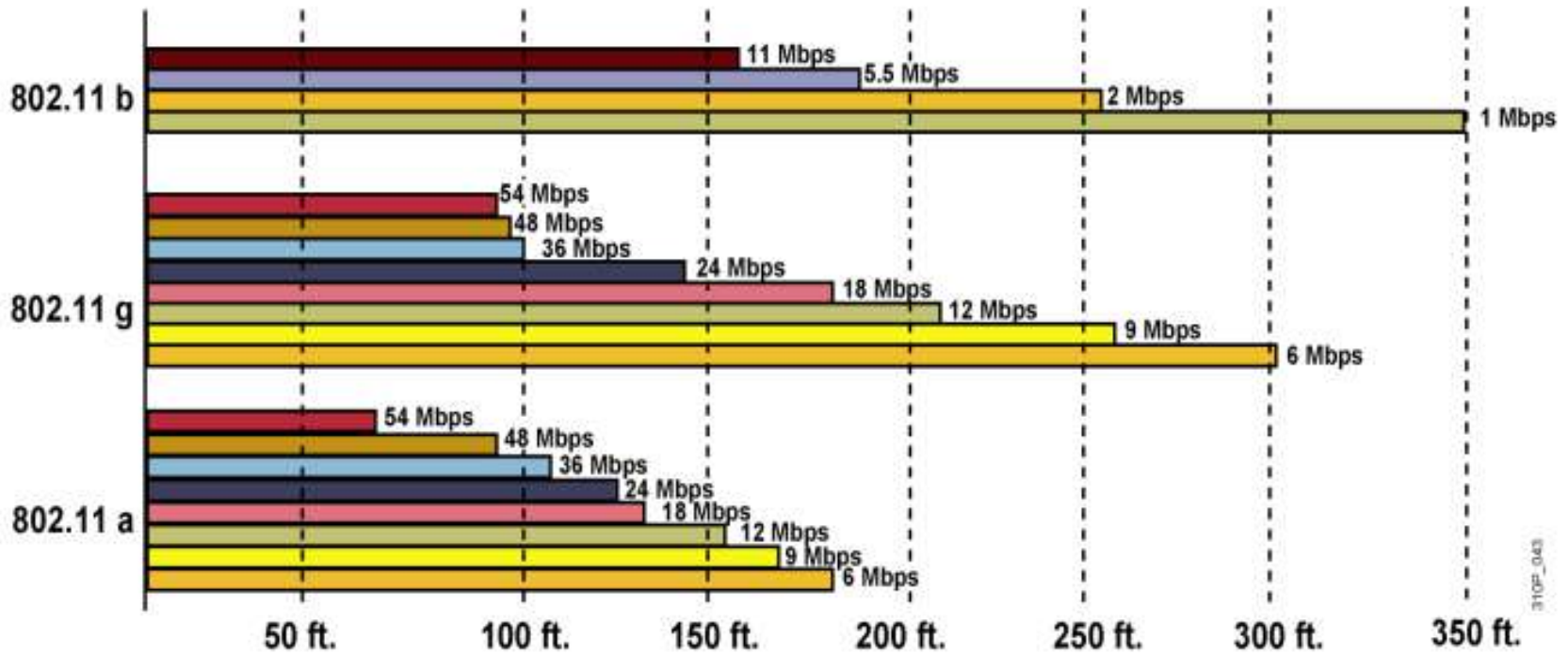
IEEE 802.11 a&b

- Digunakan mulai 1999
- 802.11a
 - Bandwidth up to: 54 Mbps
 - Frequency: 5 Ghz
 - Distance untuk transmit signal: 25m
- 802.11b
 - Bandwidth up to: 11 Mbps
 - Frequency: 2,4 Ghz
 - Sangat popular dengan jaringan Wi-Fi

IEEE 802.11g

- Digunakan mulai 2003
- Kompatibel 802.11a dan 802.11b
- Frequency: 2,4 Ghz
- Bandwidth: 54 Mbps

IEEE 802.11a/b/g Area Coverage



310P_043

IEEE 802.11n

- 802.11n digunakan 29 Oktober 2009
- Kecepatan jauh lebih besar Maximum 600 Mbps
- Cakupan dan Sinyal yang lebih baik
- Kompatibel dengan 802.11a/b/g
- Menggunakan banyak antena dengan teknologi MIMO

Standard

Standard	802.11a	802.11b	802.11g	802.11n
Published	1999	1999	2003	2009
Frequency	5GHz	2.4GHz	2.4GHz	2.4GHz / 5GHz
Bandwidth	54Mbps	11Mbps	54Mbps	160-600 Mbps
Modulation	OFDM	DSSS	OFDM, DSSS	OFDM
Coverage Interior Exterior	35m 120m	38m 140m	38m 140m	70m 250m
Advantages	Strong signal in a small office	Low price	Good speed and good coverage	Very big speed Very big coverage
Disadvantages	Incompatible with g and b	Interference	Interference	More expensive

Support Mobility

- Produktifitas tidak lagi terbatas dengan lokasi
- Dapat digunakan dimana saja, dan kapan saja
- Pengguna layanan saat ini sudah berharap menggunakan jaringan wireless
- Roaming memungkinkan perangkat nirkabel untuk mempertahankan akses terhadap internet tanpa kehilangan koneksi

Manfaat Wireless

- Lebih fleksibilitas
- Lebih produktif
- Mengurangi biaya instalasi
- Mudah dalam beradaptasi dari setiap perubahan yang terjadi

Infrastruktur Wireless

Wireless NIC

Penerapan jaringan wireless membutuhkan:

- End Device dengan menggunakan Wireless NIC
- Perangkat infrastruktur, seperti wireless router atau Wireless Access Point

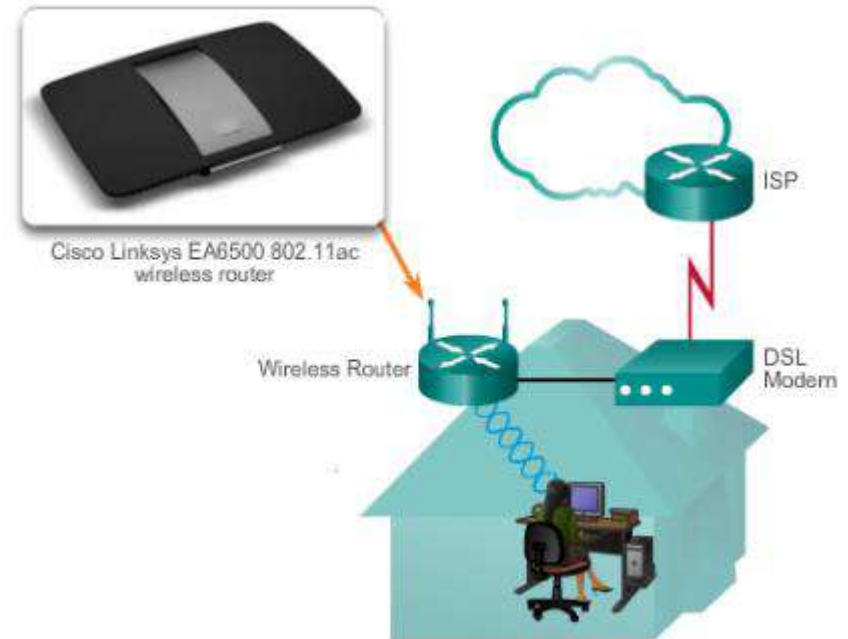


Infrastruktur Wireless

Wireless Home Router

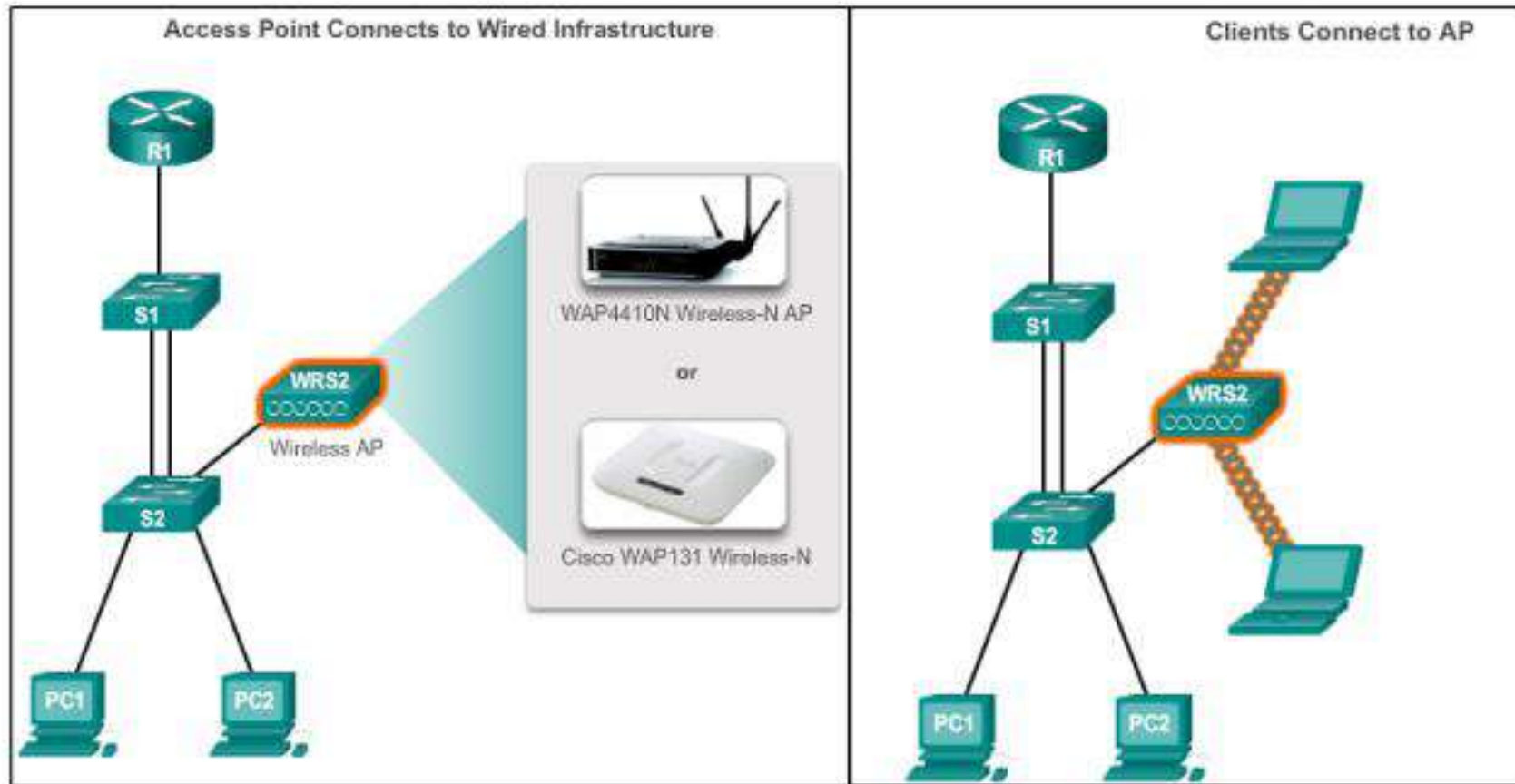
Penerapan jaringan wireless pada rumah dapat saja membutuhkan:

- Wireless Router
- Access Point
- Ethernet Switch
- Router



Infrastruktur Wireless

Wireless Business Router



Wireless Operation

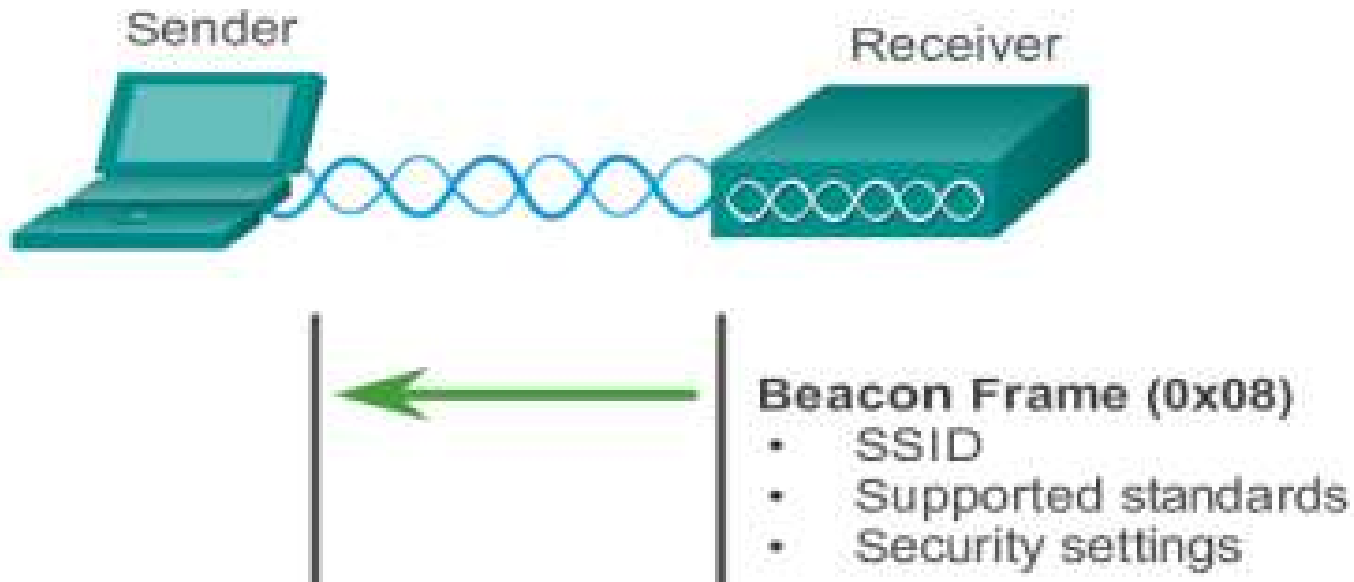
- Access Point mode Passive
 - Mode ini melakukan broadcast dengan melakukan pengiriman frame menggunakan SSID, standar layanan serta penerapan keamanan.
 - Tujuan dari mode ini adalah untuk memungkinkan penggunaan layanan wireless pada client dengan AP yang tersedia.
- Access Point mode Active

Wireless Operation

- Access Point mode Active
 - Client pengguna layanan harus mengetahui SSID.
 - Client harus melakukan permintaan layanan broadcast yang tersedia seperti hak akses keamanan yang digunakan.

Wireless Operation

Client Devices Listen for an AP



Wireless Operation

AP Broadcast Frame

