Student Identity	
Student 1	**Student 2**
Name: Denise Felicia Tiowanni	Name: Erdianti Wiga Putri Andini
Student ID: 13522013	Student ID: 13522053

Network Analysis

a

1. Head Office at Sudirman

VLAN Information (*including subnet)

VLAN ID	VLAN Name	IP Address Range	CIDR	Subnet	Default Gateway
21	NET_SUDIRMAN_RING	172.16.1.11	172.16.1.0/24	255.255.255.0	172.16.1.254
41	NET_INTER	172.31.0.1	172.31.0.0/24	255.255.255.0	172.31.0.1
50	USER_ENGINEERING	10.0.1.1 - 10.0.1.62	10.0.1.0/26	255.255.255.254	10.0.1.62
51	USER_SALES	10.0.1.65 - 10.0.1.94	10.0.1.64/27	255.255.255.254	10.0.1.94
52	USER_MARKETING	10.0.1.97 - 10.0.1.126	10.0.1.96/27	255.255.255.254	10.0.1.126
53	USER_FINANCE	10.0.1.129 - 10.0.1.158	10.0.1.128/27	255.255.255.254	10.0.1.158
54	USER_HR	10.0.1.161 - 10.0.1.190	10.0.1.160/27	255.255.255.254	10.0.1.190

ACL

ACL Name	Traffic	Kesimpulan
ENGINEERING	**Permitted**: 10 permit ip 10.0.2.0 0.0.0.31 any 20 permit tcp 10.255.0.0 0.0.255.255 eq 443 any 30 permit tcp 10.255.0.0 0.0.255.255 eq www any 40 permit udp 10.255.0.0 0.0.255.255 eq domain any 70 permit ip any any	ACL ini mengizinkan subnet 10.0.2.0/27 dan lalu lintas HTTPS (port 443), HTTP (port 80), dan DNS (port 53) dari 10.255.0.0/16, tetapi membatasi akses ke subnet 172.16.0.0/12 dan ke jaringan 10.0.0.0/8 sendiri. Di baris terakhir, kita mengetahui bahwa lalu lintas lainnya diizinkan.
	Denied: 50 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255 60 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255	
HR, FINANCE, SALES, dan MARKETING	**Permitted**: 10 permit tcp 10.255.0.0 0.0.255.255 eq 443 any	ACL ini mengizinkan lalu lintas HTTPS (port 443), HTTP (port 80), dan DNS (port 53) dari subnet 10.255.0.0/16,

	20 permit tcp 10.255.0.0 0.0.255.255 eq www any 30 permit udp 10.255.0.0 0.0.255.255 eq domain any 60 permit ip any any	tetapi membatasi akses ke subnet 172.16.0.0/12 dan ke jaringan 10.0.0.0/8 sendiri. Di baris terakhir, kita mengetahui bahwa lalu lintas lainnya diizinkan.
	Denied: 40 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255 50 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255	
SUDIRMAN_OUTBOUND	**Permitted**: 20 permit ip any any	ACL ini menghalangi semua lalu lintas dari jaringan 10.0.0.0/8 menuju 172.16.0.0/12, tetapi mengizinkan semua jenis lalu lintas lainnya.
	Denied: 10 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255	

Connection between VLAN and Devices

VLAN ID	VLAN Name	Devices
21	NET_SUDIRMAN_RING	
41	NET_INTER	
50	USER_ENGINEERING	S-Engineering-L1-1
		S-Engineering-L1-2
51	USER_SALES	S-Sales-GF-1
		S-Sales-GF-2
52	USER_MARKETING	S-Marketing-GF-1
		S-Marketing-GF-2
53	USER_FINANCE	S-Finance-L1-1
		S-Finance-L1-2
54	USER_HR	S-HR-L1-1
		S-HR-L1-2

Detail Tiap Subnet

Subnet	Subnet Mask	Subnet Address	Broadcast Address	Host Address (Range)	Address yang Tercakup
10.0.1.00xxxxxx	255.255.255.192 (/26)	10.0.1.0/26	10.0.1.63/26	10.0.1.1/26 – 10.0.1.62/26	10.0.1.1/26 (S-Engineering-L1-1), 10.0.1.2/26 (S-Engineering-L1-2), 10.0.1.62/26 (VLAN 50)
10.0.1.010xxxxx	255.255.255.224 (/27)	10.0.1.64/27	10.0.1.95/27	10.0.1.65 – 10.0.1.94/27	10.0.1.65/27 (S-Sales-GF-1), 10.0.1.66/27 (S-Sales-GF-1), 10.0.1.94/27 (VLAN 51)

10.0.1.011xxxxx	255.255.255.224 (/27)	10.0.1.96/27	10.0.1.127/27	10.0.1.97/27 – 10.0.1.126/27	10.0.1.97/27 (S-Marketing-GF-1), 10.0.1.98/27 (S-Marketing-GF-2), 10.0.1.126/27 (VLAN52)
10.0.1.100xxxxx	255.255.255.224 (/27)	10.0.1.128/27	10.0.1.159/27	10.0.1.129/27 – 10.0.1.158/27	10.0.1.129/27 (S-Finance-L1-1), 10.0.1.130/27 (S-Finance-L1-2), 10.0.1.158/27 (VLAN53)
10.0.1.101xxxxx	255.255.255.224 (/27)	10.0.1.160/27	10.0.1.191/27	10.0.1.161/27 – 10.0.1.190/27	10.0.1.161/27 (S-HR-L1-1), 10.0.1.162/27 (S-HR-L1-2), 10.0.1.190/27 (VLAN54)
172.16.1.xxxxxxxx	255.255.255.0 (/24)	172.16.1.0/24	172.16.1.255/ 24	172.16.1.1/24 – 172.16.1.254/24	172.16.1.1/24 (Sudirman GF-1), 172.16.1.2/24 (Sudirman GF-2), 172.16.1.11/24 (Sudirman L1-1), 172.16.1.12/24 (Sudirman L1-2), 172.16.1.254/24 (Sudirman Border)

2. Company's Data Center

VLAN Information (*including subnet)

VLAN ID	VLAN Name	IP Address Range	CIDR	Subnet	Default Gateway
41	NET_INTER	172.31.0.1	172.31.0.0/24	255.255.255.0	172.31.0.1
200	NET_DC_TREE	172.16.255.1	172.16.255.0/24	255.255.255.0	172.16.255.254
500	CORP_SERVER	10.255.0.1 - 10.255.255.253	10.255.0.0/16	255.255.0.0	10.255.255.254
501	CORP_VMS	10.254.0.1 - 10.254.255.253	10.254.0.0/16	255.255.0.0	10.254.255.254
600	CORP_OFFICE	10.0.255.1 - 10.0.255.253	10.0.255.0/24	255.255.255.0	10.0.255.254

ACL

ACL Name	Traffic	Kesimpulan
OFFICE	**Permitted**: - 10 permit tcp 10.255.0.0 0.0.255.255 eq 443 any - 20 permit tcp 10.255.0.0 0.0.255.255 eq www any - 30 permit udp 10.255.0.0 0.0.255.255 eq domain any - 60 permit ip any any	ACL ini mengizinkan lalu lintas HTTPS (port 443), HTTP (port 80), dan DNS (port 53) dari subnet 10.255.0.0/16, serta semua jenis lalu lintas lainnya. ACL ini membatasi akses ke subnet 172.16.0.0/12 dan ke jaringan 10.0.0.0/8 sendiri.
	Denied:	

	- 40 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255 - 50 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255	
VMS	**Permitted**: - 10 permit tcp 10.255.0.0 0.0.255.255 eq 443 any - 20 permit tcp 10.255.0.0 0.0.255.255 eq www any - 30 permit udp 10.255.0.0 0.0.255.255 eq domain any - 40 permit ip 172.16.0.0 0.15.255.255 any	ACL ini mengizinkan lalu lintas HTTPS, HTTP, dan DNS dari subnet 10.255.0.0/16 dan semua lalu lintas dari subnet 172.16.0.0/12. ACL ini membatasi akses antar-subnet dalam jaringan 10.0.0.0/8 sendiri.
	Denied: - 50 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255	
DC_OUTBOUND	**Permitted**: - 10 permit ip 10.254.0.0 0.0.255.255 172.16.0.0 0.15.255.255 - 30 permit ip any any	ACL ini mengizinkan semua lalu lintas dari subnet 10.254.0.0/16 ke subnet 172.16.0.0/12, serta semua jenis lalu lintas lainnya. ACL ini membatasi semua lalu lintas dari jaringan 10.0.0.0/8 menuju 172.16.0.0/12.
	Denied: - 20 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255	

Connection between VLAN and Devices

VLAN ID	VLAN Name	Devices
41	NET_INTER	
200	NET_DC_TREE	
500	CORP_SERVER	DC-Web-Server
501	CORP_VMS	Monitoring-PC
600	CORP_OFFICE	Office-PC

Detail Tiap Subnet

Subnet	Subnet Mask	Subnet Address	Broadcast Address	Host Address (Range)	Address yang Digunakan
172.30.0.000000xx	255.255.255.252 (/30)	172.30.0.0/30	172.30.0.3/30	172.30.0.1/30 – 172.30.0.2/30	GigabitEthernet1/0/2 (DC-Border): 172.30.0.1/30 → to DC-Server-Firewall, GigabitEthernet1/1 (DC-Server-Firewall): 172.30.0.2/30 → to DC-Border
172.30.0.000001xx	255.255.255.252 (/30)	172.30.0.4/30	172.30.0.7/30	172.30.0.5/30 – 172.30.0.6/30	GigabitEthernet1/0/1 (DC-Border): 172.30.0.5/30 → to

					DC-External-Firewall, GigabitEthernet1/2 (DC-External-Firewall): 172.30.0.6/30 → to DC-Border
172.30.0.000010xx	255.255.255.252 (/30)	172.30.0.8/30	172.30.0.11/30	172.30.0.9/30 – 172.30.0.10/30	GigabitEthernet1/2 (DC-Server-Firewall): 172.30.0.9/30 → to DC-Server-Switch, GigabitEthernet1/0/1 (DC-Server-Switch): 172.30.0.10/30 → to DC-Server-Firewall
10.0.255.xxxxxxxx	255.255.255.0 (/24)	10.0.255.0/24	10.0.255.255/24	10.0.255.1/24 – 10.0.255.254/24	Office-PC: 10.0.255.1/24, VLAN600: 10.0.255.254/24
10.254.xxxxxxxx	255.255.0.0 (/16)	10.254.0.0/16	10.254.255.255/16	10.254.0.1/16 – 10.254.255.254/16	Monitoring-PC: 10.254.0.1/16, VLAN501: 10.254.255.254/16
172.16.255.xxxxxxxx	255.255.255.0 (/24)	172.16.255.0/24	172.16.255.255/24	172.16.255.1/24 – 172.16.255.254/24	VLAN200(DC Office): 172.16.255.1/24, VLAN200(DC VMS): 172.16.255.11/24, VLAN200(DC Border): 172.16.255.254/24
172.30.255.111111xx	255.255.255.252 (/30)	172.30.255.252/30	172.30.255.255/30	172.30.255.253/30 – 172.30.255.254/30	GigabitEthernet1/1 (DC-External-Firewall): 172.30.255.253/30 → to DC-Router-External, GigabitEthernet0/0 (DC-Router-External): 172.30.255.254/30 → to DC-External-Firewall

3. Regional Office at Bojongsoang

VLAN Information (*including subnet)

VLAN ID	VLAN Name	IP Address Range	CIDR	Subnet	Default Gateway
22	NET_BOJONGSOANG_BUS	172.16.2.1	172.16.2.0/24	255.255.255.0	172.16.2.254
41	NET_INTER	172.31.0.1	172.31.0.0/24	255.255.255.0	172.31.0.1
50	USER_ENGINEERING	10.0.2.1 - 10.0.2.30	10.0.2.0/27	255.255.255.224	10.0.2.30
51	USER_SALES	10.0.2.33 - 10.0.2.62	10.0.2.32/27	255.255.255.224	10.0.2.62
52	USER_MARKETING				
53	USER_FINANCE				
54	USER_HR				

ACL

ACL Name	Traffic	Kesimpulan
ENGINEERING	**Permitted**: - 10 permit ip 10.0.1.0 0.0.0.63 any - 20 permit udp 10.255.0.0 0.0.255.255 eq domain any - 30 permit tcp 10.255.0.0 0.0.255.255 eq www any - 40 permit tcp 10.255.0.0 0.0.255.255 eq 443 any - 70 permit ip any any **Denied**: - 50 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255 - 60 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255	ACL ini mengizinkan subnet 10.0.1.0/26 dan lalu lintas HTTPS, HTTP, dan DNS dari 10.255.0.0/16, serta semua jenis lalu lintas lainnya. ACL ini membatasi akses ke subnet 172.16.0.0/12 dan ke jaringan 10.0.0.0/8 sendiri.
SALES, MARKETING, FINANCE, HR	**Permitted**: - 10 permit udp 10.255.0.0 0.0.255.255 eq domain any - 20 permit tcp 10.255.0.0 0.0.255.255 eq www any - 30 permit tcp 10.255.0.0 0.0.255.255 eq 443 any - 60 permit ip any any **Denied**: - 40 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255 - 50 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255	ACL ini mengizinkan lalu lintas HTTPS, HTTP, dan DNS dari subnet 10.255.0.0/16, serta semua jenis lalu lintas lainnya. ACL ini membatasi akses ke subnet 172.16.0.0/12 dan ke jaringan 10.0.0.0/8 sendiri.
BOJONGSOANG_OUTBOUND	**Permitted**: - 20 permit ip any any **Denied**: - 10 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255	ACL ini membatasi semua lalu lintas dari jaringan 10.0.0.0/8 menuju 172.16.0.0/12. ACL ini mengizinkan semua jenis lalu lintas lainnya.

Connection between VLAN and Devices

VLAN ID	VLAN Name	Devices
22	NET_BOJONGSOANG_BUS	
41	NET_INTER	
50	USER_ENGINEERING	B-Engineering-GF-1
		B-Engineering-L1-1
51	USER_SALES	B-Sales-GF-1
52	USER_MARKETING	
53	USER_FINANCE	
54	USER_HR	

Detail Tiap Subnet

Subnet	Subnet Mask	Subnet Address	Broadcast Address	Host Address (Range)	Address yang Tercakup
172.16.2.xxxxxxxx	255.255.255.0 (/24)	172.16.2.0	172.16.2.255	172.16.2.1 – 172.16.2.254	172.16.2.1 (Bojongsoang-GF-1), 172.16.2.11 (Bojongsoang-L1-1), 172.16.2.254 (Bojongsoang Border)
10.0.2.000xxxxx	255.255.255.224 (/27)	10.0.2.0/27	10.0.2.31/27	10.0.2.1/27 – 10.0.2.30/27	10.0.2.1/27 (B-Engineering-GF-1), 10.0.2.2/27 (B-Engineering-L1-1), 10.0.2.3/27 (B-Sales-GF-1), 10.0.2.30/27 (VLAN50)
10.0.2.001xxxxx	255.255.255.224 (/27)	10.0.2.32/27	10.0.2.63/27	10.0.2.33/27 – 10.0.2.62/27	10.0.2.62/27 (VLAN51)

b Semua default gateway PC di area Office Sudirman adalah 0.0.0.0, sehingga default gateway setiap PC harus dikonfigurasi menjadi alamat IP VLAN Switch Sudirman Border. Routing untuk IP address subnet di Office Sudirman belum dikonfigurasi untuk melalui Sudirman Border.

Bukti:

Device Name: S-Engineering-L1-1
Device Model: PC-PT

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	10.0.1.1/26	<not set>	00D0.978C.51E2
Bluetooth	Down	<not set>	<not set>	0002.1740.2A65

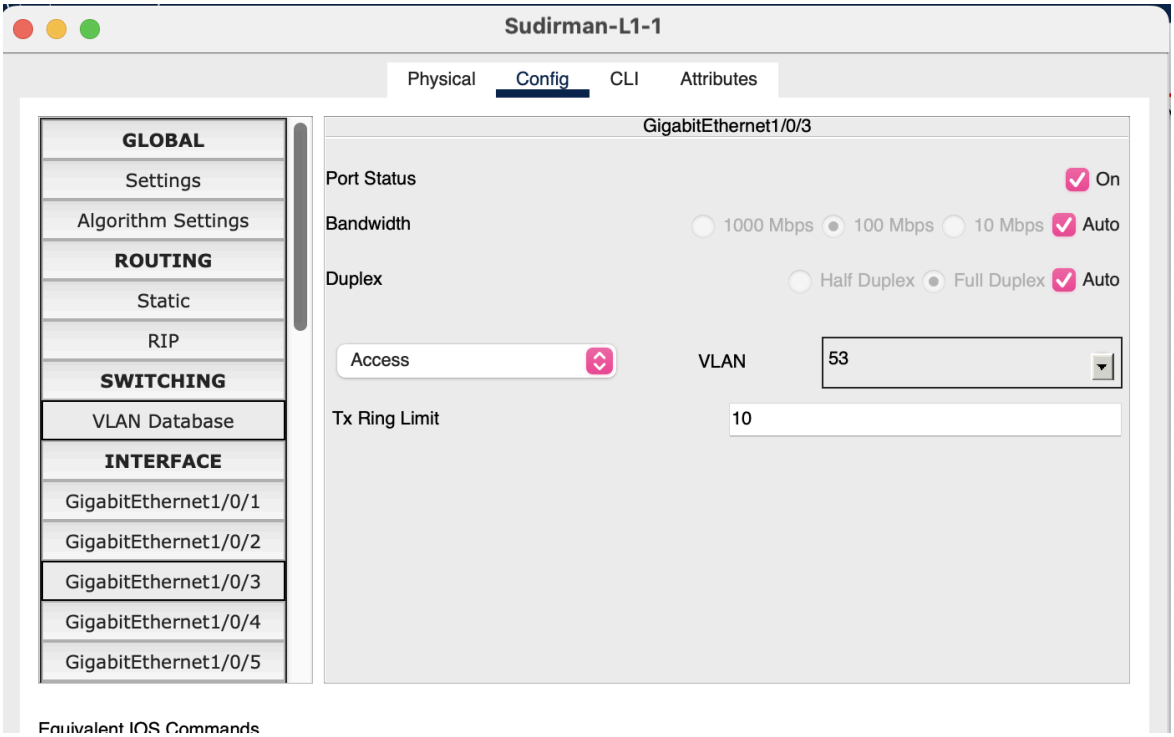
Gateway: <not set>
DNS Server: 10.255.0.1
Line Number: <not set>

Oleh karena itu, kita harus me-assign default getaway masing-masing PC pada area Office Sudirman sesuai dengan VLAN-nya.

Cek VLAN:

GigabitEthernet1/1/4	Down	1	<not set>	<not set>	0001.64DE.4904
Vlan1	Down	1	<not set>	<not set>	0001.428A.A3D7
Vlan21	Up	21	172.16.1.254/24	<not set>	0001.428A.A301
Vlan41	Up	41	172.31.0.1/16	<not set>	0001.428A.A302
Vlan50	Up	50	10.0.1.62/26	<not set>	0001.428A.A303
Vlan51	Up	51	10.0.1.94/27	<not set>	0001.428A.A304
Vlan52	Up	52	10.0.1.126/27	<not set>	0001.428A.A305
Vlan53	Up	53	10.0.1.158/27	<not set>	0001.428A.A306
Vlan54	Up	54	10.0.1.190/27	<not set>	0001.428A.A307

Cek di masing-masing PC dia berada di VLAN berapa:



Untuk PC ini, berada di VLAN 53, maka kita assign defauly getawaynya dengan default getaway VLAN 53. Begitu seterusnya.

c

```
DC-Border>en
DC-Border#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.30.0.6 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.255.0/24 is directly connected, Vlan600
C       10.254.0.0/16 is directly connected, Vlan501
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.255.0 is directly connected, Vlan200
     172.30.0.0/30 is subnetted, 4 subnets
C       172.30.0.0 is directly connected, GigabitEthernet1/0/2
C       172.30.0.4 is directly connected, GigabitEthernet1/0/1
O       172.30.0.8 [110/2] via 172.30.0.2, 02:56:48, GigabitEthernet1/0/2
O       172.30.255.252 [110/2] via 172.30.0.6, 02:56:58, GigabitEthernet1/0/1
C    172.31.0.0/16 is directly connected, Vlan41
S*   0.0.0.0/0 [1/0] via 172.30.0.6
```

Terdapat beberapa IP address yang belum dikonfigurasi DC Border (10.0.1.0/26, 10.0.1.64/27, 10.0.1.96/27, 10.0.1.128/27, 10.0.1.160/27). Hal ini menyebabkan paket yang ditujukan ke address tersebut akan diarahkan ke interface pertama yang ditemukan yaitu Gig1/0/1 (ke sebelah kanan, bukan kiri yaitu tempat Web Server). Untuk mengatasi masalah ini, harus dilakukan konfigurasi subnet pada switch DC-Border dengan static routing dengan tujuan agar hop berikutnya benar setelah dari Office Sudirman.

```
DC-Border#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DC-Border(config)#ip route 10.0.1.0 255.255.255.192 172.31.0.1
DC-Border(config)#ip route 10.0.1.64 255.255.255.224 172.31.0.1
DC-Border(config)#ip route 10.0.1.96 255.255.255.224 172.31.0.1
DC-Border(config)#ip route 10.0.1.128 255.255.255.224 172.31.0.1
DC-Border(config)#ip route 10.0.1.160 255.255.255.224 172.31.0.1
```

d

Tabel routing di Bojongsoang Border kemungkinan sudah benar, harusnya dia sudah tau tujuan paket mau kemana. Untuk jalur next-hop nya juga sudah benar.

```
Bojongsoang-Border#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.31.255.254 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 5 subnets, 4 masks
B       10.0.1.0/26 [20/0] via 172.31.255.254, 00:00:00
C       10.0.2.0/27 is directly connected, Vlan50
C       10.0.2.32/27 is directly connected, Vlan51
B       10.0.255.0/24 [20/0] via 172.31.255.254, 00:00:00
B       10.254.0.0/16 [20/0] via 172.31.255.254, 00:00:00
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Vlan22
B       172.16.255.0 [20/0] via 172.31.255.254, 00:00:00
C    172.31.0.0/16 is directly connected, Vlan41
S*   0.0.0.0/0 [1/0] via 172.31.255.254
```

Ternyata ada ACL yang diterapkan pada interface keluar, yang diberi label **ENGINEERING**. ACL ini diterapkan untuk mengontrol traffic yang diperbolehkan atau ditolak berdasarkan kriteria tertentu. ACL memiliki aturan (deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255) yang menolak semua traffic IP dari jaringan 10.0.0.0 (dengan wildcard mask yang mencakup semua alamat dalam range 10.x.x.x) ke jaringan yang sama (10.0.0.0/8). Aturan ini mencegah semua komunikasi antar IP dalam range 10.0.0.0/8. Karena IP departemen Engineering berada dalam range 10.0.0.0/8, aturan ini menolak komunikasi antar perangkat Engineering yang berada di lantai berbeda.

```
ip access-list extended ENGINEERING
 permit ip 10.0.1.0 0.0.0.63 any
 permit udp 10.255.0.0 0.0.255.255 eq domain any
 permit tcp 10.255.0.0 0.0.255.255 eq www any
 permit tcp 10.255.0.0 0.0.255.255 eq 443 any
 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255
 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip any any
```

Oleh karena itu, kita lakukan konfigurasi.

```
Bojongsoang-Border(config)#ip access-list extended ENGINEERING
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.1.0 0.0.0.63
Bojongsoang-Border(config-ext-nacl)#ip access-list extended HR
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.1.160 0.0.0.31
Bojongsoang-Border(config-ext-nacl)#ip access-list extended FINANCE
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.1.128 0.0.0.31
Bojongsoang-Border(config-ext-nacl)#ip access-list extended SALES
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.1.64 0.0.0.31
Bojongsoang-Border(config-ext-nacl)#ip access-list extended MARKETING
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.1.96 0.0.0.31
Bojongsoang-Border(config-ext-nacl)#
Bojongsoang-Border(config-ext-nacl)#ip access-list extended ENGINEERING
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.2.0 0.0.0.31
% Duplicate sequence number
Bojongsoang-Border(config-ext-nacl)#ip access-list extended SALES
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.2.32 0.0.0.31
% Duplicate sequence number
Bojongsoang-Border(config-ext-nacl)#
Bojongsoang-Border(config-ext-nacl)#ip access-list extended OFFICE
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.0.0.0 0.0.255.255
Bojongsoang-Border(config-ext-nacl)#ip access-list extended VMS
Bojongsoang-Border(config-ext-nacl)#5 permit ip 10.255.0.0 0.0.255.255 10.254.0.0 0.0.255.255
```

e Secara keseluruhan, jaringan ini sudah didesain dengan baik namun bisa ditingkatkan untuk meningkatkan beberapa hal seperti beralih dari routing statis ke routing dinamis yang akan membuat jaringan lebih fleksibel dan mengurangi cost administrasi. Mengoptimalkan ACL agar tidak terlalu luas juga akan memungkinkan komunikasi antar departemen yang lebih baik. Selain itu, menambahkan redundansi dan meningkatkan standarisasi IP dan VLAN di seluruh kantor akan memastikan ketersediaan jaringan yang lebih tinggi dan memudahkan pengelolaannya. Dengan menerapkan saran-saran ini, jaringan diharapkan dapat mendukung pertumbuhan di masa depan dengan lebih efisien dan tetap tangguh terhadap potensi masalah.

Network Design

a File topologi dapat diakses di:
[IF2230_Assignment1_2-I.pkt]

b IF2230_Assignment1_2-II

VLAN Information (*including subnet)

VLAN ID	VLAN Name	IP Address CIDR	CIDR	Subnet	Default Gateway
10	Control_SecondFloor	192.168.10.1 - 192.168.10.14	/28	255.255.255.240	192.168.10.1
20	Server_SecondFloor	192.168.20.1 - 192.168.20.14	/28	255.255.255.240	192.168.20.1
30	Office_SecondFloor	192.168.30.1 -	/25	255.255.255.128	192.168.30.1

		192.168.30.126			
40	Building_SecondFloor	192.168.40.1 - 192.168.40.62	/26	255.255.255.192	192.168.40.1
50	Office_FirstFloor	192.168.50.1 - 192.168.50.30	/27	255.255.255.224	192.168.50.1
60	Guest_FirstFloor	192.168.60.1 - 192.168.60.126	/25	255.255.255.128	192.168.60.1
70	Building_FirstFloor	192.168.70.1 - 192.168.70.62	/26	255.255.255.192	192.168.70.1

ACL

ACL Name	Traffic	Kesimpulan
100	**Permitted**: access-list 100 permit ip 192.168.10.0 0.0.0.15 192.168.20.0 0.0.0.15 access-list 100 permit ip 192.168.10.0 0.0.0.15 192.168.30.0 0.0.0.127 access-list 100 permit ip 192.168.10.0 0.0.0.15 192.168.40.0 0.0.0.63 access-list 100 permit ip 192.168.10.0 0.0.0.15 192.168.50.0 0.0.0.31 access-list 100 permit ip 192.168.10.0 0.0.0.15 192.168.70.0 0.0.0.63 access-list 100 deny ip 192.168.10.0 0.0.0.15 192.168.60.0 0.0.0.127 access-list 100 permit ip 192.168.10.0 0.0.0.15 any access-list 100 permit udp any any eq bootps access-list 100 permit udp any any eq bootpc access-list 100 permit ip any any	ACL 100 mengatur akses dari VLAN Control (192.168.10.0/28). Mengizinkan akses dari 192.168.10.0/28 ke VLAN Server (192.168.20.0/28), VLAN Office (192.168.30.0/25), VLAN Building di lantai 2 (192.168.40.0/26), VLAN Office di lantai 1 (192.168.50.0/27), dan VLAN Building di lantai 1 (192.168.70.0/26). Menolak akses dari VLAN Control (192.168.10.0/28) ke VLAN Guest (192.168.60.0/25). Selain itu, juga mengizinkan akses DHCP.
	Denied: access-list 100 deny ip 192.168.10.0 0.0.0.15 192.168.60.0 0.0.0.127	
110	**Permitted**: access-list 110 permit ip 192.168.60.0 0.0.0.127 192.168.60.0 0.0.0.127 access-list 110 permit udp any any eq bootps access-list 110 permit udp any any eq bootpc access-list 110 permit ip any any	Menolak akses dari VLAN Guest ke semua jaringan lain, kecuali VLAN Guest itu sendiri. Selain itu, juga mengizinkan akses DHCP.
	Denied: access-list 110 deny ip 192.168.60.0 0.0.0.127 any	
120	**Permitted**: access-list 110 deny ip 192.168.60.0 0.0.0.127 any access-list 120 permit ip 192.168.30.0 0.0.0.127 any	ACL 120 mengontrol akses dari VLAN Office di lantai 2 (192.168.30.0/25). Mengizinkan akses ke VLAN Office di lantai 1

	access-list 120 permit udp any any eq bootps access-list 120 permit udp any any eq bootpc access-list 120 permit ip any any **Denied**: access-list 120 deny ip 192.168.30.0 0.0.0.127 192.168.20.0 0.0.0.15 access-list 120 deny ip 192.168.30.0 0.0.0.127 192.168.40.0 0.0.0.63 access-list 120 deny ip 192.168.30.0 0.0.0.127 192.168.60.0 0.0.0.127	(192.168.50.0/27). Menolak akses ke VLAN Server (192.168.20.0/28), VLAN Building di lantai 2 (192.168.40.0/26), dan VLAN Guest (192.168.60.0/25). Selain itu, juga mengizinkan akses DHCP.
104	**Permitted**: access-list 104 permit ip 192.168.40.0 0.0.0.63 192.168.70.0 0.0.0.63 access-list 104 permit ip 192.168.40.0 0.0.0.63 any **Denied**: access-list 104 deny ip 192.168.40.0 0.0.0.63 192.168.10.0 0.0.0.15 access-list 104 deny ip 192.168.40.0 0.0.0.63 192.168.20.0 0.0.0.15 access-list 104 deny ip 192.168.40.0 0.0.0.63 192.168.30.0 0.0.0.127 access-list 104 deny ip 192.168.40.0 0.0.0.63 192.168.60.0 0.0.0.127	ACL 104 mengatur akses untuk VLAN Building di lantai 2 (192.168.40.0/26). Mengizinkan akses ke VLAN Building di lantai 1 (192.168.70.0/26). Menolak akses ke VLAN Control (192.168.10.0/28), VLAN Server (192.168.20.0/28), VLAN Office di lantai 2 (192.168.30.0/25), dan VLAN Guest (192.168.60.0/25).
125	**Permitted**: access-list 125 permit ip 192.168.20.0 0.0.0.15 any access-list 125 permit udp any any eq bootps access-list 125 permit udp any any eq bootpc access-list 125 permit ip any any **Denied**: access-list 125 deny ip 192.168.20.0 0.0.0.15 192.168.10.0 0.0.0.15 access-list 125 deny ip 192.168.20.0 0.0.0.15 192.168.30.0 0.0.0.127 access-list 125 deny ip 192.168.20.0 0.0.0.15 192.168.40.0 0.0.0.63 access-list 125 deny ip 192.168.20.0 0.0.0.15 192.168.50.0 0.0.0.31 access-list 125 deny ip 192.168.20.0 0.0.0.15 192.168.70.0 0.0.0.63 access-list 125 deny ip 192.168.20.0 0.0.0.15 192.168.60.0 0.0.0.127	ACL 125 mengontrol akses untuk VLAN Server (192.168.20.0/28). Menolak akses ke VLAN Control (192.168.10.0/28), VLAN Office di lantai 2 (192.168.30.0/25), VLAN Building di lantai 2 (192.168.40.0/26), VLAN Office di lantai 1 (192.168.50.0/27), VLAN Guest (192.168.60.0/25), dan VLAN Building di lantai 1 (192.168.70.0/26). Selain itu, juga mengizinkan akses DHCP.
130	**Permitted**: access-list 130 permit ip 192.168.40.0 0.0.0.15 192.168.40.0 0.0.0.63 access-list 130 permit ip 192.168.40.0 0.0.0.15 192.168.70.0 0.0.0.63	ACL 130 mengatur akses dari subnet 192.168.40.0/28 yang merupakan bagian dari VLAN Building di lantai 2. Menolak akses ke VLAN Control (192.168.10.0/28) dan VLAN Office di lantai 2

	access-list 130 permit ip 192.168.40.0 0.0.0.15 192.168.20.0 0.0.0.15 access-list 130 permit ip 192.168.40.0 0.0.0.15 any access-list 130 permit udp any any eq bootps access-list 130 permit udp any any eq bootpc access-list 130 permit ip any any **Denied**: access-list 130 deny ip 192.168.40.0 0.0.0.15 192.168.10.0 0.0.0.15 access-list 130 deny ip 192.168.40.0 0.0.0.15 192.168.30.0 0.0.0.127 access-list 130 deny ip 192.168.40.0 0.0.0.15 192.168.50.0 0.0.0.31 access-list 130 deny ip 192.168.40.0 0.0.0.15 192.168.60.0 0.0.0.127	(192.168.30.0/25). Mengizinkan akses ke VLAN Building di lantai 2 (192.168.40.0/26) dan VLAN Building di lantai 1 (192.168.70.0/26). Menolak akses ke VLAN Office di lantai 1 (192.168.50.0/27) dan VLAN Guest (192.168.60.0/25), tetapi mengizinkan akses ke VLAN Server (192.168.20.0/28). Selain itu, juga mengizinkan akses DHCP.
150	**Permitted**: access-list 150 permit ip 192.168.50.0 0.0.0.127 192.168.50.0 0.0.0.31 access-list 150 permit ip 192.168.50.0 0.0.0.127 any access-list 150 permit udp any any eq bootps access-list 150 permit udp any any eq bootpc access-list 150 permit ip any any **Denied**: access-list 150 deny ip 192.168.50.0 0.0.0.127 192.168.20.0 0.0.0.15 access-list 150 deny ip 192.168.50.0 0.0.0.127 192.168.40.0 0.0.0.63 access-list 150 deny ip 192.168.50.0 0.0.0.127 192.168.60.0 0.0.0.127	ACL 150 mengontrol akses untuk VLAN Office di lantai 1 (192.168.50.0/27). Mengizinkan akses hanya ke jaringan internalnya sendiri. Menolak akses ke VLAN Server (192.168.20.0/28), VLAN Building di lantai 2 (192.168.40.0/26), dan VLAN Guest (192.168.60.0/25). Selain itu, juga mengizinkan akses DHCP.
180	**Permitted**: access-list 180 permit ip 192.168.70.0 0.0.0.15 192.168.40.0 0.0.0.63 access-list 180 permit ip 192.168.70.0 0.0.0.15 192.168.70.0 0.0.0.63 access-list 180 permit ip 192.168.70.0 0.0.0.15 192.168.20.0 0.0.0.15 access-list 180 permit ip 192.168.70.0 0.0.0.15 any access-list 180 permit udp any any eq bootps access-list 180 permit udp any any eq bootpc access-list 180 permit ip any any **Denied**: access-list 180 deny ip 192.168.70.0 0.0.0.15 192.168.10.0 0.0.0.15 access-list 180 deny ip 192.168.70.0 0.0.0.15 192.168.30.0 0.0.0.127	ACL 180 mengatur akses untuk subnet 192.168.70.0/28, bagian dari VLAN Building di lantai 1. Menolak akses ke VLAN Control (192.168.10.0/28), VLAN Office di lantai 2 (192.168.30.0/25), dan VLAN Office di lantai 1 (192.168.50.0/27). Mengizinkan akses ke VLAN Building di lantai 2 (192.168.40.0/26), VLAN Building di lantai 1 (192.168.70.0/26), dan VLAN Server (192.168.20.0/28). Selain itu, juga mengizinkan akses DHCP.

	access-list 180 deny ip 192.168.70.0 0.0.0.15 192.168.50.0 0.0.0.31 access-list 180 deny ip 192.168.70.0 0.0.0.15 192.168.60.0 0.0.0.127	
1	**Permitted**: access-list 1 permit 192.168.30.0 0.0.0.127 access-list 1 permit 192.168.50.0 0.0.0.31 access-list 1 permit 192.168.60.0 0.0.0.127 access-list 1 permit 192.168.20.0 0.0.0.15 access-list 1 permit any **Denied**: access-list 1 deny 92.168.40.0 0.0.0.63 access-list 1 deny 192.168.70.0 0.0.0.63 access-list 1 deny 192.168.10.0 0.0.0.15	Mengizinkan akses dari VLAN Office di lantai 2 (192.168.30.0/25), VLAN Office di lantai 1 (192.168.50.0/27), VLAN Guest (192.168.60.0/25), dan VLAN Server (192.168.20.0/28). Menolak akses dari VLAN Building di lantai 2 (192.168.40.0/26), VLAN Building di lantai 1 (192.168.70.0/26), dan VLAN Control (192.168.10.0/28).

Routing

Konfigurasi routing pada router:

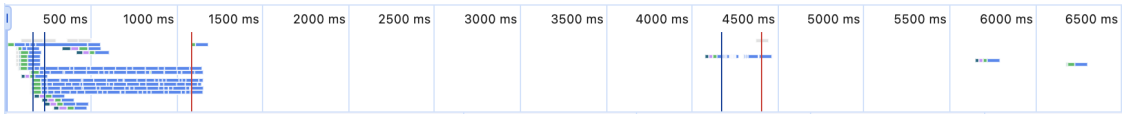
1. **Default Route (Static Route)**
   - **0.0.0.0/0** (default route) diarahkan ke **8.8.8.8.**
2. **Interface GigabitEthernet0/1**
   - **8.0.0.0/8:** Terhubung langsung melalui **GigabitEthernet0/1.**
   - **8.8.4.4/32:** IP ini juga langsung terhubung melalui **GigabitEthernet0/1.**
3. **Interface GigabitEthernet0/0**
   - **192.168.1.0/24:** Jaringan ini langsung terhubung melalui **GigabitEthernet0/0.**
   - **192.168.1.1/32:** IP ini adalah alamat IP lokal pada **GigabitEthernet0/0.**
4. **Subinterface untuk VLAN**
   - **192.168.10.0/28 (VLAN 10):** Terhubung langsung melalui **GigabitEthernet0/0.10.** Ini adalah jaringan untuk **Control (Second Floor).**
   - **192.168.20.0/28 (VLAN 20):** Terhubung langsung melalui **GigabitEthernet0/0.20.** Ini adalah jaringan untuk **Server (Second Floor).**
   - **192.168.30.0/25 (VLAN 30):** Terhubung langsung melalui **GigabitEthernet0/0.30.** Ini adalah jaringan untuk **Office (Second Floor).**
   - **192.168.40.0/26 (VLAN 40):** Terhubung langsung melalui **GigabitEthernet0/0.40.** Ini adalah jaringan untuk **Building (Second Floor).**

- **192.168.50.0/27 (VLAN 50):** Terhubung langsung melalui **GigabitEthernet0/0.50.** Ini adalah jaringan untuk **Office (First Floor).**
- **192.168.60.0/25 (VLAN 60):** Terhubung langsung melalui **GigabitEthernet0/0.60.** Ini adalah jaringan untuk **Guest (First Floor).**
- **192.168.70.0/26 (VLAN 70):** Terhubung langsung melalui **GigabitEthernet0/0.70.** Ini adalah jaringan untuk **Building (First Floor).**

DHCP Pool

Terdapat beberapa konfigurasi DHCP pool pada router untuk secara otomatis meng-*assign* IP address pada perangkat-perangkat dalam jaringan.

```
ip dhcp pool Control
 network 192.168.10.0 255.255.255.240
 default-router 192.168.10.1
ip dhcp pool Server
 network 192.168.20.0 255.255.255.240
 default-router 192.168.20.1
ip dhcp pool Office_SecondFloor
 network 192.168.30.0 255.255.255.128
 default-router 192.168.30.1
ip dhcp pool Building_SecondFloor
 network 192.168.40.0 255.255.255.192
 default-router 192.168.40.1
ip dhcp pool Office_FirstFloor
 network 192.168.50.0 255.255.255.224
 default-router 192.168.50.1
ip dhcp pool Guest
 network 192.168.60.0 255.255.255.128
 default-router 192.168.60.1
ip dhcp pool Building_FirstFloor
 network 192.168.70.0 255.255.255.192
 default-router 192.168.70.1
```

HTTP/2 Demo Website		
1	a	 Dari waterfall chart yang diperoleh, dapat dilihat bahwa gambar pada HTTP/1.1 berhasil termuat dengan waktu sekitar 1000 ms, sementara gambar pada HTTP/2 (aktivitas setelahnya) berhasil termuat dengan waktu sekitar 500 ms saja. Dari sana,

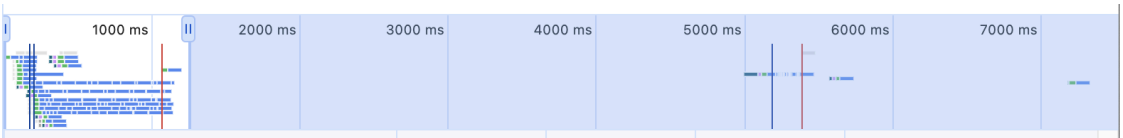
disimpulkan bahwa **HTTP/2 lebih cepat** dibandingkan dengan HTTP/1.1.

b

HTTP/1.1 (bagian pertama/kiri dari waterfall chart) memuat gambar dengan mengirim banyak request secara berurutan, tetapi setiap request harus menunggu koneksi yang tersedia karena HTTP/1.1 memiliki batasan jumlah koneksi simultan yang dapat dibuka per waktunya. Jadi, meskipun request dikirim secara paralel melalui koneksi yang tersedia, setiap koneksi hanya dapat menangani satu request pada satu waktu (sebelum mengirim request berikutnya, harus tunggu response sebelumnya dulu).

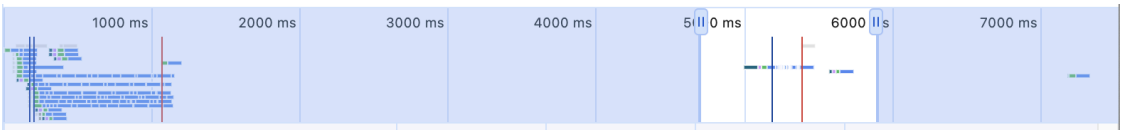
Sementara itu, HTTP/2 (bagian kedua/kanan dari waterfall chart) menggunakan satu koneksi TCP untuk semua request dan mengirim beberapa request gambar secara bersamaan melalui satu koneksi yang tersedia. Dapat dilihat dari grafik bahwa bahwa hampir semua request dimulai pada waktu yang bersamaan dan mereka tidak perlu saling menunggu response karena mereka sudah berjalan secara paralel.

c



Name	Status	Protocol	Size	Connection ID
tile_100.png	200	http/1.1	3.1 kB	368275
tile_64.png	200	http/1.1	4.7 kB	368223
tile_134.png	200	http/1.1	3.5 kB	368258
tile_130.png	200	http/1.1	4.8 kB	368293
tile_142.png	200	http/1.1	2.3 kB	368264
tile_128.png	200	http/1.1	5.1 kB	368152
tile_77.png	200	http/1.1	4.1 kB	368275
tile_68.png	200	http/1.1	4.3 kB	368293
tile_16.png	200	http/1.1	4.1 kB	368223
tile_110.png	200	http/1.1	4.6 kB	368258
tile_29.png	200	http/1.1	4.0 kB	368264
tile_42.png	200	http/1.1	4.2 kB	368152
tile_103.png	200	http/1.1	3.1 kB	368275
tile_122.png	200	http/1.1	2.6 kB	368293
tile_136.png	200	http/1.1	3.2 kB	368223
tile_157.png	200	http/1.1	3.0 kB	368258
tile_102.png	200	http/1.1	3.2 kB	368264

HTTP/1.1 menggunakan **beberapa koneksi TCP**, di mana setiap koneksi menangani satu request gambar dalam satu waktu. Hal ini dapat dilihat dari connection ID yang berbeda-beda untuk setiap requestnya.



Name	Status	Protocol	Size	Connection ID
tile_142.png	200	h2	2.2 kB	369191
tile_143.png	200	h2	2.2 kB	369191
tile_144.png	200	h2	2.6 kB	369191
tile_145.png	200	h2	4.4 kB	369191
tile_146.png	200	h2	4.9 kB	369191
tile_147.png	200	h2	4.3 kB	369191
tile_148.png	200	h2	4.2 kB	369191
tile_149.png	200	h2	4.8 kB	369191
tile_150.png	200	h2	4.1 kB	369191
tile_151.png	200	h2	3.2 kB	369191
tile_152.png	200	h2	3.2 kB	369191
tile_153.png	200	h2	3.0 kB	369191
tile_154.png	200	h2	3.3 kB	369191
tile_155.png	200	h2	3.3 kB	369191
tile_156.png	200	h2	3.1 kB	369191
tile_157.png	200	h2	2.8 kB	369191

HTTP/2 hanya menggunakan **satu koneksi TCP** untuk menangani beberapa request gambar secara bersamaan. Hal ini dapat dilihat dari connection ID yang sama untuk semua request gambar.

d Gambar dimuat lebih cepat dengan protokol HTTP/2 dibandingkan dengan HTTP/1.1 karena pertama, HTTP/2 mendukung multiplexing, yang memungkinkan beberapa request dan response dikirim secara bersamaan dalam satu koneksi. Hal ini menghilangkan masalah head-of-line blocking yang sering terjadi pada HTTP/1.1, di mana satu request yang tertunda karena menunggu response dapat menahan request lain pada koneksi yang sama. Kedua, HTTP/2 hanya membutuhkan satu koneksi TCP yang sama untuk semua permintaan ke satu domain, sehingga mengurangi overhead dari membuka dan menutup banyak koneksi, serta mengurangi latensi dari proses handshake TCP dan TLS yang diperlukan pada setiap koneksi baru di HTTP/1.1.

2

http1.html	200	http/1.1	document	2.2 kB	368152
http2.html	200	h2	document	2.1 kB	369191

Request yang memuat halaman web memiliki response yang berukuran **2.2 kB untuk HTTP/1.1** dan **2.1 kB untuk HTTP/2**.

a Saat browser mengirimkan request, browser menambahkan header Accept-Encoding dalam permintaan HTTP. Header ini menunjukkan metode kompresi yang didukung oleh browser, seperti gzip, br, atau deflate. Server membaca header Accept-Encoding dan memilih metode kompresi yang didukung oleh browser dan server itu sendiri. Misalnya, jika browser mendukung gzip dan br, server akan memilih salah satu metode ini (biasanya yang paling

		efisien, seperti br untuk konten web).
	b	Setelah server mengompres response, ia menambahkan header Content-Encoding dalam response HTTP. Header ini menunjukkan metode kompresi yang digunakan, misalnya Content-Encoding: gzip atau Content-Encoding: br. Browser membaca Content-Encoding ini dan menggunakan metode kompresi yang ditentukan untuk mendekompresi konten sebelum menampilkannya. Dari sinilah browser bisa mengetahui bahwa konten yang diterimanya sudah terkompresi dan metode kompresinya. ▼Response Headers ☐ Raw Access-Control-Allow-Origin: * Cache-Control: no-cache Connection: keep-alive Content-Encoding: gzip (dalam kasus ini, Content-Encoding: gzip)
	c	http1.html 200 http/1.1 document 18.3 kB 405451 http2.html 200 h2 document 18.2 kB 406856 Setelah menonaktifkan Accepted Content-Encodings section, kita dapat melihat bahwa ukuran request yang memuat halaman web memiliki response yang berukuran **18.3 kB untuk HTTP/1.1** dan **18.2 kB untuk HTTP/2**. Hal ini hampir 9 kali lipatnya ukuran yang sudah dikompresi.

		Analyzing HTTP Request With Wireshark
1	a	GET /download.html HTTP/1.1 Wireshark · Packet 4 · http.cap Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00) Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223 Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479 Hypertext Transfer Protocol GET /download.html HTTP/1.1\r\n HTTP version yang digunakan untuk request adalah HTTP/1.1.

b

```
> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
v Hypertext Transfer Protocol
  > GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=…
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
    [Response in frame: 38]
    [Full request URI: http://www.ethereal.com/download.html]
```

Pesan **HTTP request** memiliki beberapa bagian utama:
- Request Line: Berisi metode HTTP (seperti GET atau POST), URL yang diminta, dan versi HTTP yang digunakan.
- Headers: Sekumpulan informasi tambahan tentang permintaan, seperti Host, User-Agent, Accept, dll.
- Body (opsional): Biasanya hanya ada pada metode POST atau PUT, berisi data yang dikirim ke server (dalam kasus ini, tidak ada karena dia metode requestnya GET).

```
> Frame 27: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
> Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)
> Internet Protocol Version 4, Src: 216.239.59.99, Dst: 145.254.160.237
> Transmission Control Protocol, Src Port: 80, Dst Port: 3371, Seq: 1431, Ack: 722, Len: 160
> [2 Reassembled TCP Segments (1590 bytes): #26(1430), #27(160)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    P3P: policyref="http://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD IVA PVD OTP OUR OTR IND OTC"\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    Content-Encoding: gzip\r\n
    Server: CAFE/1.0\r\n
    Cache-control: private, x-gzip-ok=""\r\n
  > Content-length: 1272\r\n
    Date: Thu, 13 May 2004 10:17:14 GMT\r\n
    \r\n
    [Request in frame: 18]
    [Time since request: 0.971397000 seconds]
    [Request URI […]: /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fwww
    [Full request URI […]: http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=4
    Content-encoded entity body (gzip): 1272 bytes -> 3608 bytes
    File Data: 3608 bytes
v Line-based text data: text/html (3 lines)
    <html><head><style><!--\n
     […].ch{cursor:pointer;cursor:hand}a.ad:link { color: #000000 }a.ad:visited { color: #000000 }a.ad:hover { color: #000000 }a.ad:active { color: #0
     […]function ss(w,id) {window.status = w;return true;}function cs(){window.status='';}function ca(a){ top.location.href=document.getElementById(a)
```

Pesan **HTTP response** memiliki struktur yang mirip:
- Status Line: Menyertakan versi HTTP, kode status (misalnya 200 untuk sukses, 404 untuk not found), dan pesan status.
- Headers: Informasi tambahan seperti Content-Type, Content-Length, dan Set-Cookie.
- Body: Berisi data konten dari response, seperti HTML, JSON, atau gambar (dalam kasus ini, bodynya berisi HTML).

2 a

Pada file http2-h2c.pcap, paket pertama menggunakan protokol HTTP dan paket berikutnya menggunakan HTTP/2. Cara klien dan server berkomunikasi untuk menentukan jenis HTTP yang akan digunakan pada koneksi adalah dengan memulai komunikasi dengan **Upgrade pada HTTP/1.1**. Klien mengirim permintaan HTTP/1.1 dengan header Upgrade: h2c untuk menunjukkan bahwa klien mendukung HTTP/2.

```
> Frame 1: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
> Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 1, Ack: 1, Len: 178
v Hypertext Transfer Protocol
  > GET /robots.txt HTTP/1.1\r\n
    Host: nghttp2.org\r\n
    User-Agent: curl/7.61.0\r\n
    Accept: */*\r\n
    Connection: Upgrade, HTTP2-Settings\r\n
    Upgrade: h2c\r\n
  > HTTP2-Settings: AAMAAABkAARAAAAAAAAIAAAAA\r\n
    \r\n
    [Response in frame: 2]
    [Full request URI: http://nghttp2.org/robots.txt]
```

Server kemudian pun merespons dengan menerima upgrade dan mengubah koneksi ke HTTP/2.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.9.0.2	139.162.123.134	HTTP	244	GET /robots.txt HTTP/1.1
2	0.600079	139.162.123.134	10.9.0.2	HTTP2	164	HTTP/1.1 101 Switching Protocols , SETTINGS[0]

b

Pada HTTP/2, struktur pesan request dan response dipecah menjadi frame. Beberapa jenis frame utama adalah:
- HEADERS: Berisi header permintaan atau respons.
- DATA: Berisi konten atau body dari pesan.
- SETTINGS: Digunakan di awal koneksi untuk mengkonfigurasi komunikasi.

Contoh untuk request (stream HEADERS):

```
> Frame 8: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
> Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
> Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 252, Ack: 375, Len: 49
v HyperText Transfer Protocol 2
  v Stream: HEADERS, Stream ID: 3, Length 40, GET /humans.txt
      Length: 40
      Type: HEADERS (1)
    > Flags: 0x05, End Headers, End Stream
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
      [Pad Length: 0]
      Header Block Fragment: 3fe11f820488627b691d485d3e53864188aa69d29ac4b9ec9b7a8825b650c3abb815c153032a2f2a
      [Header Length: 136]
      [Header Count: 7]
    > Header table size update
    > Header: :method: GET
    > Header: :path: /humans.txt
    > Header: :scheme: http
    > Header: :authority: nghttp2.org
    > Header: user-agent: curl/7.61.0
    > Header: accept: */*
      [Full request URI: http://nghttp2.org/humans.txt]
      [Response in frame: 10]
```

Contoh untuk response (stream DATA):

```
        0... .... .... .... .... .... .... .... = Reserved: 0x0
        .000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
        [Pad Length: 0]
        Header Block Fragment: 8d6196dd6d5f4a044a436cca08017940bb71905c684a62d1bf5f92497ca58ae819aafb50938ec415305a99567b0f0d01397f068602e0005f75dfc
        [Header Length: 311]
        [Header Count: 10]
      > Header: :status: 404 Not Found
      > Header: date: Sun, 12 Aug 2018 17:30:42 GMT
      > Header: content-type: text/plain; charset=utf-8
      > Header: content-length: 9
      > Header: x-backend-header-rtt: 0.001977
      > Header: server: nghttpx
      > Header: via: 2 nghttpx
      > Header: x-frame-options: SAMEORIGIN
      > Header: x-xss-protection: 1; mode=block
      > Header: x-content-type-options: nosniff
        [Time since request: 0.315106000 seconds]
        [Request in frame: 8]
  HyperText Transfer Protocol 2
    Stream: DATA, Stream ID: 3, Length 9
        Length: 9
        Type: DATA (0)
      > Flags: 0x01, End Stream
        0... .... .... .... .... .... .... .... = Reserved: 0x0
        .000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
        [Pad Length: 0]
        Data: 6e6f7420666f756e64
        [Connection window size (before): 1073741762]
        [Connection window size (after): 1073741753]
        [Stream window size (before): 1073741824]
        [Stream window size (after): 1073741815]
    Line-based text data: text/plain (1 lines)
        not found
```

c HTTP/1.1 menggunakan teks plain, di mana header dan body dikirim sebagai teks yang dapat dibaca oleh kita manusia, dengan garis baru (newline) sebagai pemisah antar header.

Sementara itu, HTTP/2 menggunakan binary framing, di mana data dikirim sebagai frame biner yang tidak bisa langsung dibaca manusia. Ini memungkinkan multiplexing (mengirim beberapa pesan bersamaan) pada satu koneksi, yang tidak dimungkinkan pada HTTP/1.1.

d Header yang diawali dan diakhiri dengan : pada HTTP/2 disebut pseudo-header dan digunakan untuk menyampaikan informasi dasar tentang permintaan, seperti metode (:method), jalur (:path), dan otoritas (:authority). Pseudo-header ini digunakan untuk menggantikan komponen utama dari HTTP request line dan status line pada HTTP/1.1, sehingga pesan HTTP/2 menjadi lebih terstruktur dan terhindar dari ambiguitas.

e HTTP/2 menggunakan kompresi header dengan HPACK, yang mencakup penggunaan tabel statis. Tabel statis adalah kumpulan header umum yang sudah diindeks. Setiap kali header yang sering digunakan seperti :method GET muncul, klien hanya akan mengirimkan indeksnya alih-alih mengirim seluruh teks (klien hanya akan mengirimkan angka yang mengacu pada entri di tabel statis HPACK untuk header tersebut).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.9.0.2	139.162.123.134	HTTP	244	GET /robots.txt HTTP/1.1
2	0.600079	139.162.123.134	10.9.0.2	HTTP2	164	HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3	0.600465	10.9.0.2	139.162.123.134	HTTP2	90	Magic
4	0.600541	10.9.0.2	139.162.123.134	HTTP2	93	SETTINGS[0]
5	0.600575	10.9.0.2	139.162.123.134	HTTP2	75	SETTINGS[0]
6	0.600596	139.162.123.134	10.9.0.2	HTTP2	342	HEADERS[1]: 200 OK, DATA[1] (text/plain)
7	0.600603	10.9.0.2	139.162.123.134	HTTP2	79	WINDOW_UPDATE[0]
8	0.601307	10.9.0.2	139.162.123.134	HTTP2	115	HEADERS[3]: GET /humans.txt
9	0.912304	139.162.123.134	10.9.0.2	HTTP2	75	SETTINGS[0]
10	0.916413	139.162.123.134	10.9.0.2	HTTP2	156	HEADERS[3]: 404 Not Found, DATA[3] (text/plain)

Dapat dilihat pada tabel, alih-alih menuliskan metode GET

langsung, HTTP/2 menggunakan HEADERS[1] dan HEADERS[3] yang ketika ditekan, baru terlihat bahwa itu adalah metode GET.

```
HyperText Transfer Protocol 2
  Stream: HEADERS, Stream ID: 3, Length 40, GET /humans.txt
      Length: 40
      Type: HEADERS (1)

  Header: :method: GET
      Name Length: 7
      Name: :method
      Value Length: 3
      Value: GET
      :method: GET
      [Unescaped: GET]
      Representation: Indexed Header Field
      Index: 2
```

Bonus Point

FTP

ftp

No.	Time	Source	Destination	Protocol	Length	Info
665	5.115191	44.241.66.173	10.5.102.138	FTP	135	Response: \027\003\003\000@\001\025\017b9.;@#g=\001(9…
9207	34.106837	44.241.66.173	10.5.102.138	FTP	106	Response: 220 Welcome to the DLP Test FTP Server
9209	34.109431	10.5.102.138	44.241.66.173	FTP	76	Request: AUTH TLS
9343	34.335121	44.241.66.173	10.5.102.138	FTP	97	Response: 234 Proceed with negotiation.
117…	45.671770	44.241.66.173	10.5.102.138	FTP	106	Response: 220 Welcome to the DLP Test FTP Server
117…	45.672434	10.5.102.138	44.241.66.173	FTP	76	Request: AUTH TLS
117…	45.895782	44.241.66.173	10.5.102.138	FTP	97	Response: 234 Proceed with negotiation.

a FTP diatur oleh RFC 959 (Request for Comments), yang ditetapkan oleh Internet Engineering Task Force (IETF). Dokumen ini memberikan standar untuk implementasi FTP di seluruh jaringan.

b FTP biasanya digunakan untuk mentransfer file antara perangkat klien dan server atau antar perangkat komputer melalui jaringan TCP/IP. Contoh penggunaannya ini dapat berupa mengunggah dan mengunduh file dari server, backup data dari satu perangkat ke perangkat lainnya, ataupun akses ke repositori file di perangkat yang jauh.

c FTP menggunakan dua saluran komunikasi, control channel dan data channel. Control channel digunakan untuk bertukar request dan response antara klien dan server, sementara data channel digunakan untuk mentransfer data file.

Struktur pesan FTP meliputi request yang dikirim dari klien ke

	server serta response dari server ke klien. Contoh command ada beberapa, seperti AUTH, USER, PASS, LIST, CWD, DELE, PUT, GET, RETR, STOR, dll. Sementara itu, contoh response adalah kode status, seperti 220, 234, 200, 331, 230, 550, dll.
d	Ada beberapa alternatif daripada FTP: ● SFTP (SSH File Transfer Protocol): Menggunakan enkripsi SSH untuk mengamankan transfer file, sehingga lebih aman dibandingkan FTP yang tidak terenkripsi. ● FTPS (FTP Secure): Menggunakan SSL/TLS untuk enkripsi, sehingga juga lebih aman dibanding FTP. ● HTTP/HTTPS (Hypertext Transfer Protocol): Dapat digunakan untuk transfer file pada aplikasi berbasis web dan juga mendukung enkripsi melalui HTTPS.