Week 14

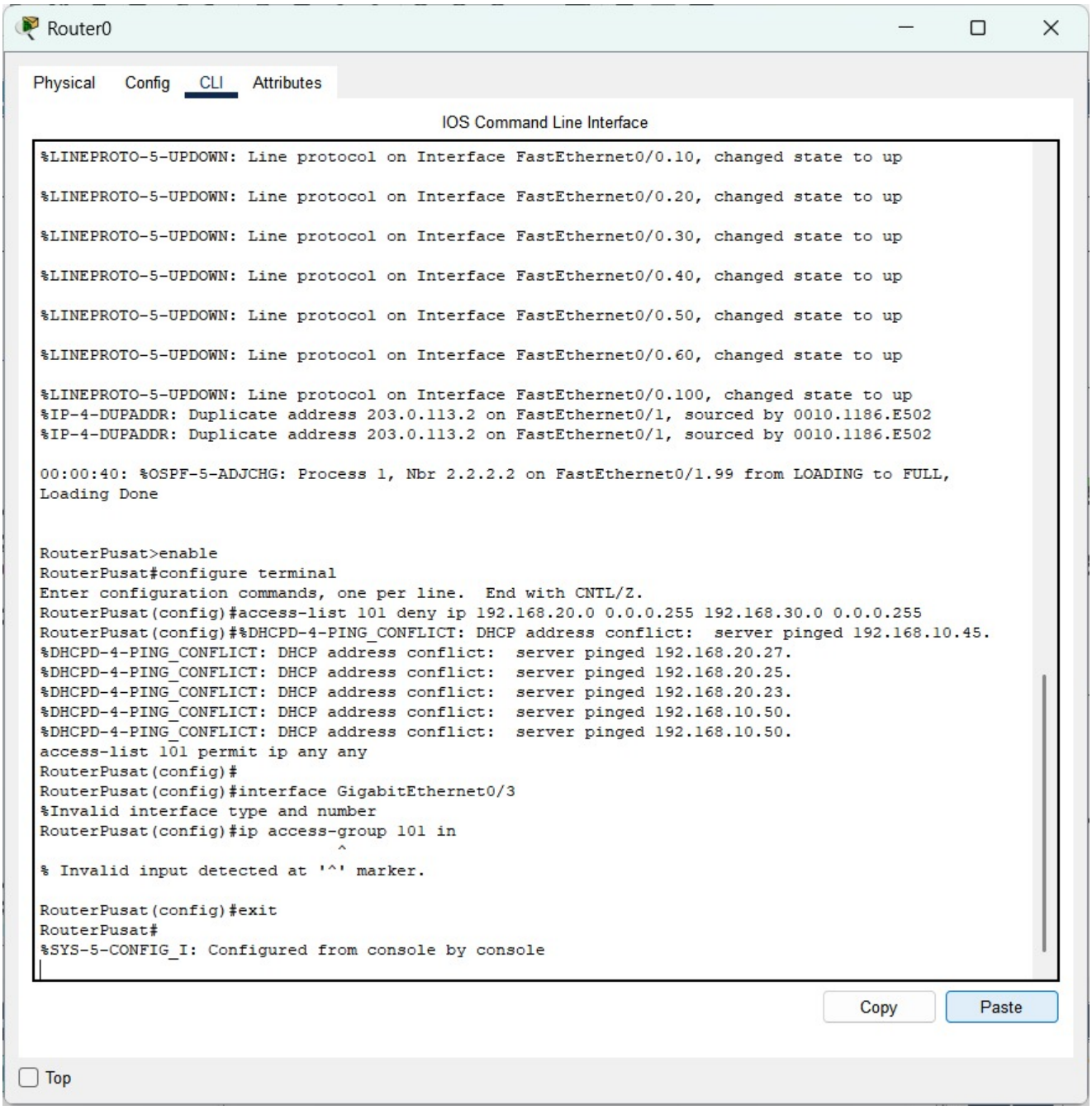
- Ade Ayu Kholifah Putri (10231004) - Network Architech
- Arya Wijaya Saroyo (10231020) - Network Engineer
- Krishandy Dhanysa Pratama (10231050) - Network Services Specialist
- Muhammad Dani (10231062) - Security & Documentation Specialist

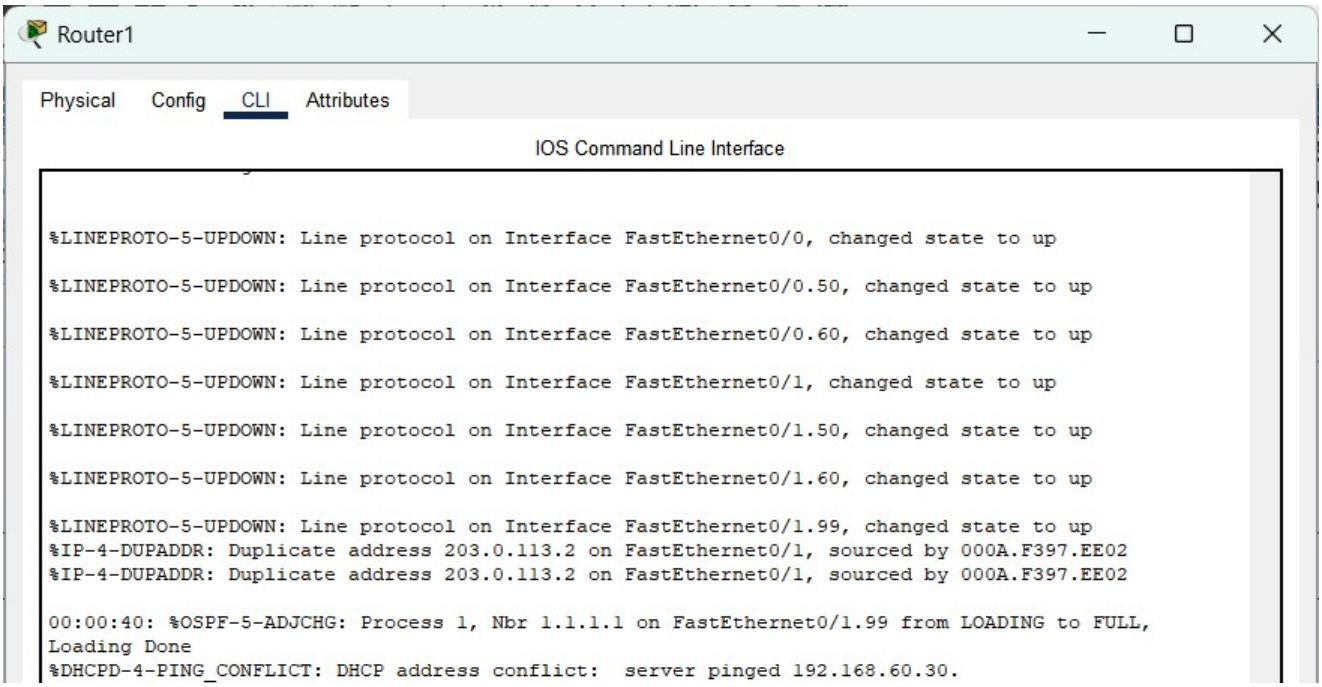
Daftar Isi

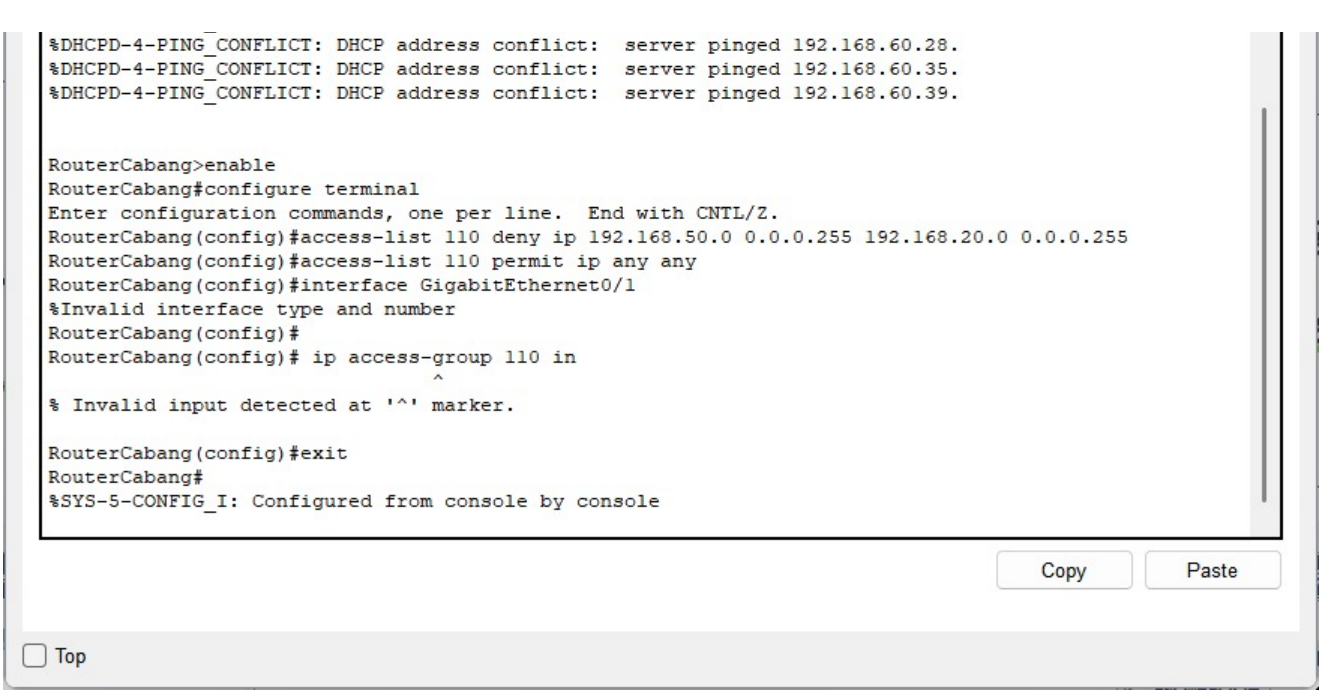
1. Implementasi Access Control List (ACL) sesuai kebijakan keamanan.

Access COntrol List (ACL) digunakan untuk mengontrol lalu lintas data masuk atau keluar dari jaringan berdasarkan aturan yang ditentukan (misalnya, alamat IP sumber dan tujuan, protokol, dan port).

1.1 Dokumentasi konfigurasi CLI lengkap untuk implementasi ACL

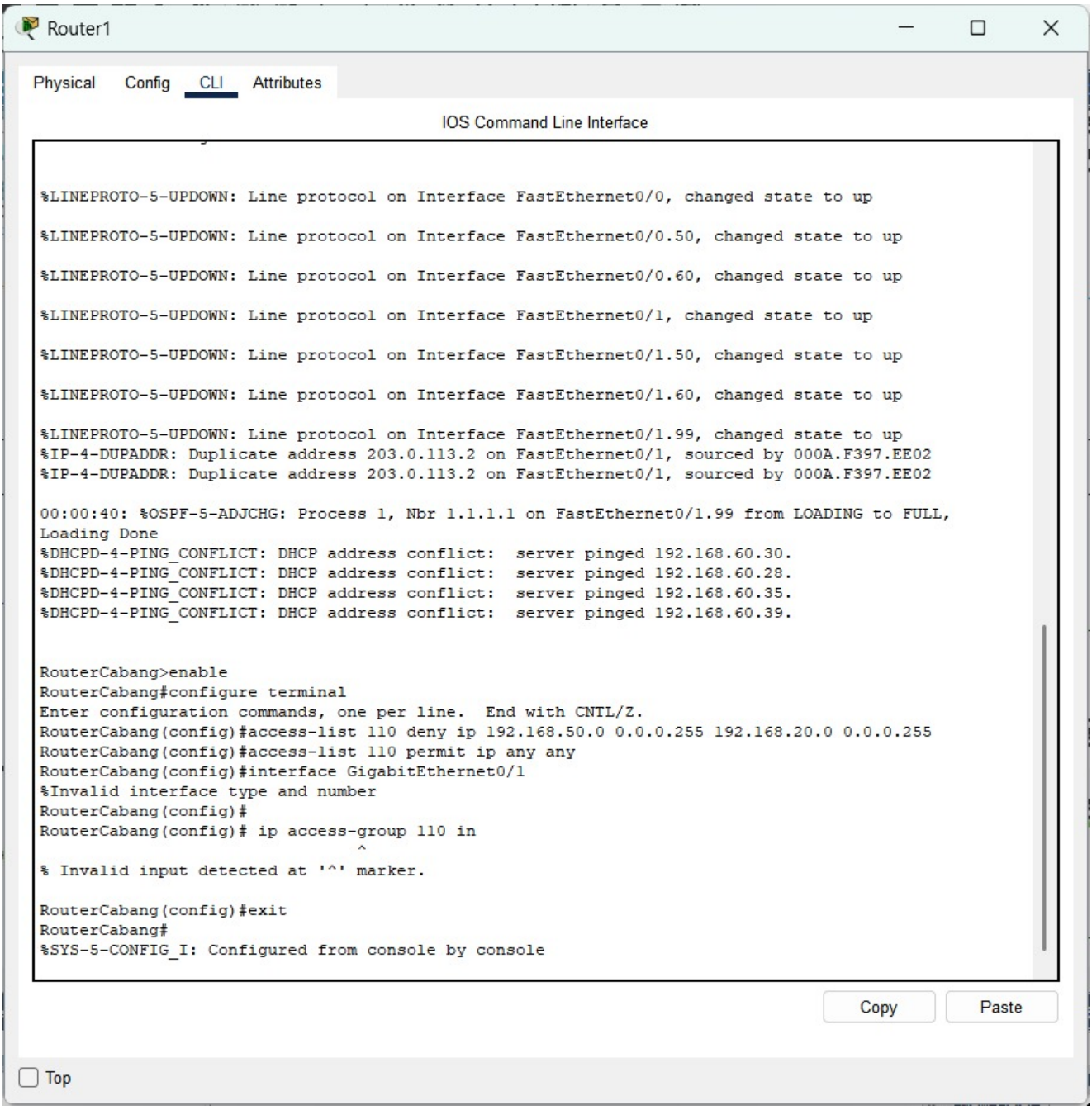

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.50, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.60, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.100, changed state to up
%IP-4-DUPADDR: Duplicate address 203.0.113.2 on FastEthernet0/1, sourced by 0010.1186.E502
%IP-4-DUPADDR: Duplicate address 203.0.113.2 on FastEthernet0/1, sourced by 0010.1186.E502
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/1.99 from LOADING to FULL,
Loading Done
RouterPusat>enable
RouterPusat#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterPusat(config)#access-list 101 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
RouterPusat(config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.10.45.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.20.27.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.20.25.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.20.23.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.10.50.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.10.50.
access-list 101 permit ip any any
RouterPusat(config)#
RouterPusat(config)#interface GigabitEthernet0/3
%Invalid interface type and number
RouterPusat(config)#ip access-group 101 in
^
% Invalid input detected at '^' marker.
RouterPusat(config)#exit
RouterPusat#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Paste
Top


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.50, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.60, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.50, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.60, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.99, changed state to up
%IP-4-DUPADDR: Duplicate address 203.0.113.2 on FastEthernet0/1, sourced by 000A.F397.EE02
%IP-4-DUPADDR: Duplicate address 203.0.113.2 on FastEthernet0/1, sourced by 000A.F397.EE02
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/1.99 from LOADING to FULL,
Loading Done
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.60.30.



Pada tahap implementasi Access Control List (ACL), dilakukan konfigurasi pada router Gedung B (RouterCabang) untuk membatasi akses jaringan Marketing (192.168.50.0/24) agar tidak dapat mengakses jaringan Keuangan (192.168.20.0/24). Konfigurasi ACL berhasil dibuat dengan perintah access-list 110 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255 dan permit ip any any untuk mengizinkan lalu lintas lain tetap berjalan. Namun, terdapat kesalahan saat menerapkan ACL ke interface karena salah penulisan nama interface dan perintah ip access-group dimasukkan di mode konfigurasi global, bukan di mode interface. Solusi yang dilakukan adalah mengecek nama interface yang aktif menggunakan perintah show ip interface brief, lalu masuk ke mode interface yang sesuai sebelum menerapkan ACL. Selain itu, ditemukan konflik IP dari DHCP Server yang disebabkan adanya perangkat dengan IP statis yang sama, sehingga perlu dilakukan pengecekan manual untuk menghindari duplikasi IP.

Konfigurasi Router Gedung A



Konfigurasi Router Gedung B

```
RouterCabang#enable
RouterCabang# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterCabang(config)#access-list 130 deny ip 192.168.60.0 0.0.0.255 192.168.20.0 0.0.0.255
RouterCabang(config)#access-list 130 permit ip any any
RouterCabang(config)#
RouterCabang(config)#interface FastEthernet0/1
RouterCabang(config-if)#ip access-group 130 in
RouterCabang(config-if)#exit
RouterCabang(config)#
```

Cisco Packet Tracer

Link PKT

2 Pengujian menyeluruh semua fitur jaringan

Hasil pengujian pada seluruh semua fitur jaringan gagal dilakukan, Hal ini sesuai dengan kebijakan keamanan yang telah diterapkan menggunakan ACcess Control List (ACL)

2.1 Matrix pengujian yang menunjukkan semua fitur.

Sumber	Tujuan	Hasil Ping
PC IT	❌ Gagal	Sesuai kebijakan ACL: akses ditolak
PC Marketing	❌ Gagal	Sesuai kebijakan ACL: akses ditolak
PC Keuangan	❌ Gagal	Sesuai kebijakan ACL: akses ditolak
PC SDM	❌ Gagal	Sesuai kebijakan ACL: akses ditolak
PC Server	❌ Gagal	Sesuai kebijakan ACL: akses ditolak
PC Operasional	❌ Gagal	Sesuai kebijakan ACL: akses ditolak

3 Troubleshooting dan Perbaikan Masalah

3.1 Hasil

Permasalahan yang Ditemukan:

- Interface VLAN tidak aktif.
- Kesalahan konfigurasi IP atau subnet.
- ACL diterapkan ke interface yang salah.
- Routing statis/OSPF belum sepenuhnya menyambung.

Langkah Troubleshooting:

- Menjalankan show ip interface brief untuk melihat status interface.
- Memverifikasi subnet dan default gateway di setiap perangkat.
- Mengecek ACL dengan show access-lists dan show run.
- Memastikan semua interface no shutdown.

Link Github Pekan 14