Infrastruktur Jaringan Industrial CpwE dengan Platform GNS3
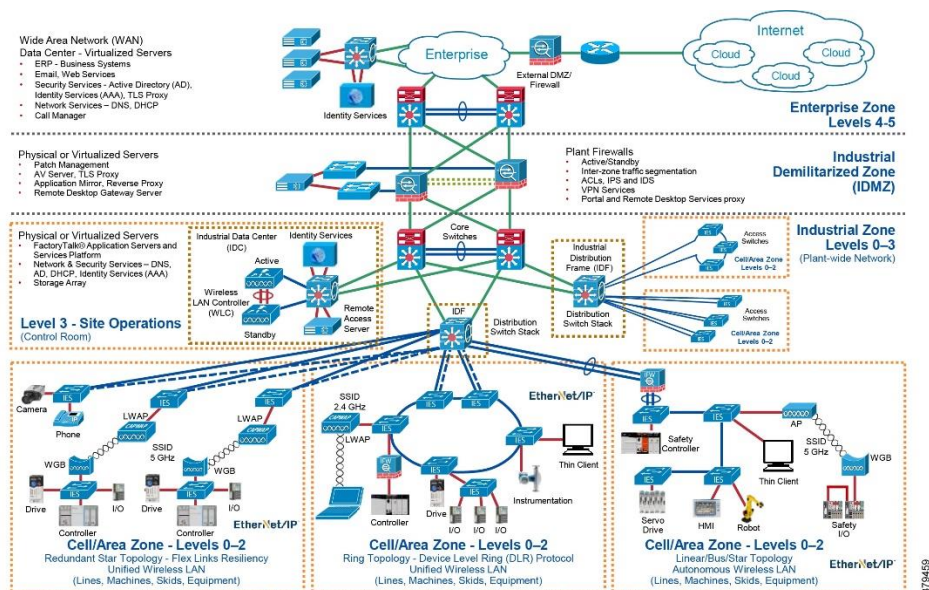
AHMAD SYAFI NURROYYAN

1. LATAR BELAKANG

Revolusi Industri 4.0 telah mengubah cara kerja pabrik-pabrik modern. Konsep Smart Factory yang menghubungkan semua sistem produksi secara otomatis kini makin banyak diterapkan. Kunci utamanya ada pada teknologi Industrial Internet of Things (IIoT) yang memungkinkan semua mesin dan peralatan di pabrik saling terhubung dan berbagi data secara langsung. Namun, keberhasilan teknologi ini justru memunculkan masalah baru: bagaimana menggabungkan sistem IT (teknologi informasi) dengan OT (teknologi operasional) di pabrik?

Selama ini, jaringan komputer di kantor (IT) dan jaringan di area produksi (OT) bekerja terpisah. Kantor lebih mementingkan keamanan dan kerahasiaan data, sementara lantai pabrik butuh sistem yang terus berjalan tanpa henti dengan respon yang cepat. Banyak proyek IIoT gagal karena infrastruktur jaringannya tidak bisa menyatukan dua sistem yang berbeda ini. Laporan McKinsey (2023) menyebutkan hanya 26% pabrik yang berhasil menerapkan IIoT dengan baik karena masalah infrastruktur jaringan. IDC (2022) juga mencatat 42% kegagalan transformasi digital di sektor manufaktur disebabkan desain jaringan yang kurang tepat.

Masalahnya makin rumit karena kebanyakan orang IT tidak paham sistem pabrik, begitu juga sebaliknya. Akibatnya, banyak pabrik masih mengandalkan cara manual untuk menghubungkan data dari kantor ke produksi.
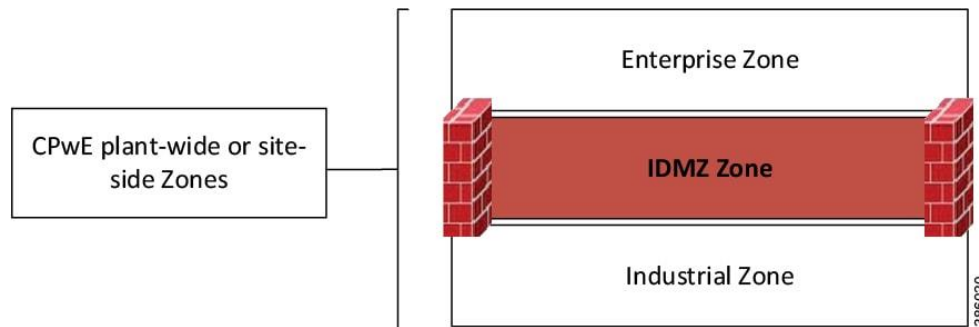
Untuk mengatasi masalah ini, perusahaan besar seperti Cisco dan Rockwell Automation membuat standar bernama Converged Plantwide Ethernet (CPwE). Ini bukan produk jadi, tapi lebih ke panduan desain yang sudah diuji dan terbukti berhasil untuk membangun jaringan pabrik yang handal, aman, dan bisa dikembangkan sesuai kebutuhan.

Arsitektur CPwE yang lengkap punya 5 tingkat (Level 0-4/5), mulai dari sensor di lantai pabrik sampai server di cloud perusahaan.

Meski model 5 tingkat ini sangat detail, inti dari CPwE sebenarnya ada pada pembagian zona (segmentasi). Idenya sederhana: memisahkan jaringan menjadi tiga zona utama yaitu Enterprise Zone

1

(area kantor), Industrial Zone (area pabrik), dan zona penyangga di tengahnya yang disebut Industrial Demilitarized Zone atau IDMZ.
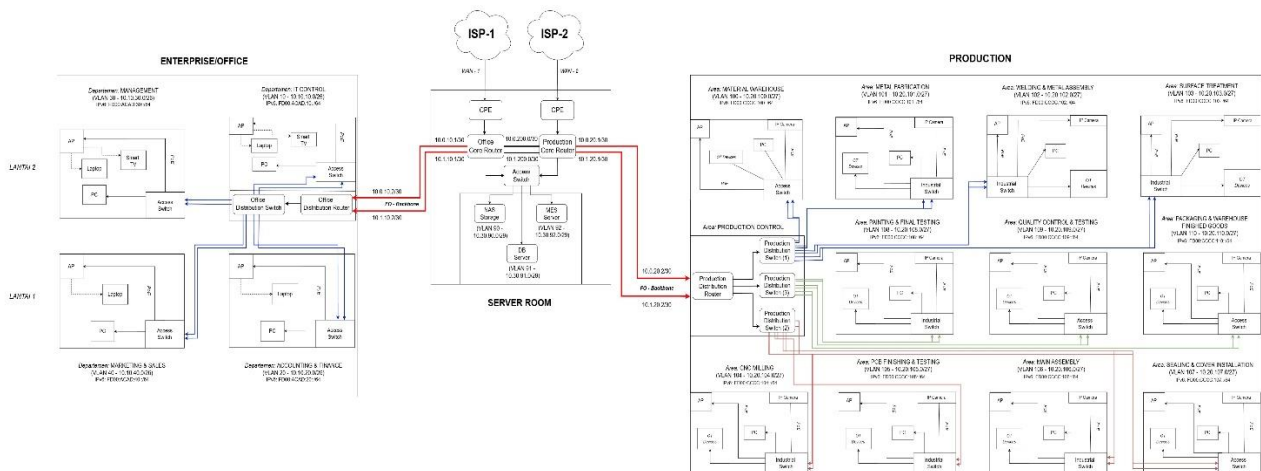

Pembagian zona ini memang terbukti efektif. Studi dari Siemens (2021) menunjukkan pabrik yang menerapkan segmentasi VLAN dan edge computing produktivitasnya naik sampai 28% dan waktu mesin berhenti berkurang 35%.

Proyek ini bertujuan merancang infrastruktur jaringan untuk pabrik skala menengah dengan menggunakan konsep 3 zona dari CPwE. Desainnya memetakan Enterprise Zone untuk bagian IT dan Accounting, IDMZ sebagai ruang server, dan Industrial Zone untuk area kontrol produksi.

Sesuai fokus proyek, perancangan ini hanya berfokus pada infrastruktur network saja tanpa mencakup konfigurasi atau pemrograman dari perangkat *Operation Technology* (OT) spesifik seperti PLC, HMI, atau SCADA. Selain itu, perancangan topologinya juga lebih ke arsitektur jaringan logis, sehingga untuk aspek fisik seperti ketahanan perangkat terhadap lingkungan (M.I.C.E.), grounding, dan UPS memang penting di dunia nyata, namun tidak dibahas dalam lingkup simulasi kali ini.

2. PERANCANGAN TOPOLOGI

2.1 Desain Rancangan Topologi

Dalam topologi yang dirancang, bagian Office terdiri dari 4 departemen dan Production terdiri dari 11 area. Pada setiap departemen Office dan area Production, terdapat satu managed switch atau industrial switch yang berfungsi menyediakan akses VLAN kepada perangkat client seperti PC, Access Point, dan perangkat lainnya. Switch ini juga melakukan trunk ke interface yang terhubung dengan distribution switch. Untuk mencegah masalah *Single Point of Failure (SPOF)*, setiap managed switch dihubungkan ke distribution switch menggunakan 2 link sebagai redundansi.

Distribution switch selanjutnya terhubung ke office router untuk menerima keseluruhan traffic trunk dari router. Masing-masing router pada office dan production dihubungkan ke jalur backbone fiber optik dengan 2 link yang memiliki IP berbeda sebagai redundansi fisik. Penggunaan fiber optik untuk link backbone dipilih karena ketahanannya di lingkungan outdoor dan kemampuannya menjangkau jarak jauh tanpa degradasi sinyal. Selain itu, karena tidak menghantarkan listrik, fiber optik jauh lebih aman dari gangguan yang biasanya muncul di area dengan tegangan tinggi. Misalnya interferensi listrik, ground loop, atau sambaran petir yang bisa merusak perangkat jaringan.

Pada server room terdapat 2 core router yang bertugas menerima dan mendistribusikan traffic ke office maupun production. Kedua core router ini juga saling terhubung menggunakan 2 link fisik sebagai redundansi. Kedua core router tersebut terhubung ke switch yang mengakomodasi server-server internal perusahaan seperti NAS Storage, DB Server, dan MES Server. Koneksi ke kedua core router dilakukan karena server-server tersebut bersifat shared resource yang digunakan oleh office dan production. Untuk koneksi internet, digunakan 2 ISP sebagai mekanisme load balancing sekaligus failover.

2.2 Batasan Sistem (Limitations)

Beberapa batasan lain yang diterapkan pada implementasi simulasi ini dikarenakan keterbatasan fitur perangkat lunak (*software image*) dan sumber daya perangkat keras:

1. **Redundansi Layer 2 via STP (Bukan LACP):** Koneksi redundan antar-*switch* menggunakan protokol *Spanning Tree* (mode *Active/Standby*). Hal ini dikarenakan keterbatasan *image switch* yang digunakan pada GNS3 tidak mendukung fitur LACP/*EtherChannel* secara penuh.

2. **Limitasi EtherChannel pada Router:** Desain awal merencanakan penerapan LACP pada tautan dari *Office/Production Router* ke *Distributed Switch* untuk redundansi. Namun, hal ini tidak dapat diimplementasikan karena *image* yang digunakan adalah *router* murni (*pure router*) yang tidak mendukung fitur *Layer 2 EtherChannel* layaknya *Layer 3 Switch*. Oleh karena itu, koneksi tetap menggunakan link ganda namun tanpa agregasi LACP.

3. **Akses Internet pada Zona Produksi:** Mengacu pada standar CPwE, perangkat pada zona produksi (OT) seharusnya terisolasi dan tidak diperbolehkan mengakses internet demi keamanan data. Namun, dalam simulasi ini, akses internet pada zona produksi dibuka secara terbatas untuk keperluan pengujian (*testing*). Hal ini dilakukan karena perangkat *wireless* disimulasikan menggunakan *switch* bawaan GNS3 yang memiliki keterbatasan fitur (tidak dapat melakukan *ping*), sehingga konektivitas perlu uji coba langsung melalui akses internet dari *end-device*.

4. **Absensi Perangkat Firewall Dedikasi:** Desain keamanan ideal menyertakan *Firewall* khusus di antara ISP dan *Core Router*. Namun, komponen ini ditiadakan karena ketiadaan lisensi untuk *image firewall enterprise* dan keterbatasan sumber daya komputasi (RAM/CPU) laptop untuk menjalankan *image open source* (seperti VyOS). Sebagai gantinya, fungsi keamanan dan filter trafik diterapkan menggunakan ACL (*Access Control List*) pada router.

5. **Simulasi Server:** Perangkat server (NAS, DB, MES) diimplementasikan menggunakan *virtual node* ringan (VPCS/Router) yang berfungsi hanya untuk memverifikasi konektivitas IP dan validasi aturan ACL, tanpa menjalankan layanan aplikasi *real* (seperti *service* SQL atau Web Server).

2.3 Pembagian IP Address

Lokasi	Nama Jaringan (Departemen/Area)	VLAN ID	IPv4 Subnet	Ipv6 Subnet
Office	IT Control	10	10.10.10.0/26	FD00:ACAD:10::/64
Office	Accounting & Finance	20	10.10.20.0/26	FD00:ACAD:20::/64
Office	Management	30	10.10.30.0/26	FD00:ACAD:30::/64
Office	Marketing & Sales	40	10.10.40.0/26	FD00:ACAD:40::/64
Server	NAS Storage	90	10.30.90.0/29	-
Server	DB Server	91	10.30.91.0/29	-
Server	MES Server	92	10.30.92.0/29	-
Production	Material Warehouse	100	10.20.100.0/27	FD00:CCCC:100::/64
Production	Metal Fabrication	101	10.20.101.0/27	FD00:CCCC:101::/64

Production	Welding & Metal Assembly	102	10.20.102.0/27	FD00:CCCC:102::/64
Production	Surface Treatment	103	10.20.103.0/27	FD00:CCCC:103::/64
Production	CNC Milling	104	10.20.104.0/27	FD00:CCCC:104::/64
Production	PCB Finishing & Testing	105	10.20.105.0/27	FD00:CCCC:105::/64
Production	Main Assembly	106	10.20.106.0/27	FD00:CCCC:106::/64
Production	Sealing & Cover Installation	107	10.20.107.0/27	FD00:CCCC:107::/64
Production	Painting & Final Testing	108	10.20.108.0/27	FD00:CCCC:108::/64
Production	Quality Control & Testing	109	10.20.109.0/27	FD00:CCCC:109::/64
Production	Packaging & Warehouse Finished Goods	110	10.20.110.0/27	FD00:CCCC:110::/64

Koneksi Dari	Koneksi Ke	Link #	IPv4 Subnet	IP Address Sisi 1	IP Address Sisi 2
Office Core Router	Office Router	Link 1	10.0.10.0/30	10.0.10.1	10.0.10.2
Office Core Router	Office Router	Link 2	10.1.10.0/30	10.1.10.1	10.1.10.2
Production Core Router	Production Router	Link 1	10.0.20.0/30	10.0.20.1	10.0.20.2
Production Core Router	Production Router	Link 2	10.1.20.0/30	10.1.20.1	10.1.20.2
Office Core Router	Production Core Router	Link 1	10.0.200.0/30	10.0.200.1	10.0.200.2
Office Core Router	Production Core Router	Link 2	10.1.200.0/30	10.1.200.1	10.1.200.2

3. IMPLEMENTASI DAN KONFIGURASI

1. Konfigurasi Office Core Router

Langkah 1: Menetapkan hostname menjadi OFFICE-CORE-ROUTER serta menonaktifkan fitur IP domain lookup untuk mencegah terjadinya jeda (hang) ketika terjadi kesalahan pengetikan perintah selama proses konfigurasi.

Langkah 2: Mengonfigurasi IP address pada interface yang terhubung ke OFFICE-ROUTER.

Langkah 3: Mengonfigurasi IP Address pada interface yang terhubung ke PRODUCTION-CORE-ROUTER.

Langkah 4: Mengonfigurasi IP Address sebagai gateway VLAN pada Servers.

Langkah 5: Mengonfigurasi OSPF agar dapat terhubung dengan jaringan Office dan Production.

Langkah 6: Membuat Access Control List (ACL) untuk mengamankan NAS Storage. Pada tahap ini seluruh trafik OSPF dan tunnel GRE diizinkan melewati perangkat. Selain itu, host pada jaringan IT Control, DB Server, dan MES Server juga diberikan akses penuh. Semua trafik lain di luar ketentuan tersebut diblokir.

Aturan ini diterapkan karena di lingkungan industri, NAS Storage dianggap sangat sensitif. Akses menuju NAS biasanya tidak dilakukan langsung, tetapi melalui DB atau MES sebagai perantara antara server, perangkat produksi, dan departemen akuntansi. Jaringan IT Control tetap diperbolehkan mengakses secara langsung karena mereka yang bertanggung jawab melakukan monitoring dan manajemen seluruh jaringan.

Langkah 7: Mengonfigurasi HSRP sebagai mekanisme redundansi gateway karena terdapat dua link sebagai gateway VLAN Servers, masing-masing berasal dari Office Core Router dan Production Core Router. Dengan HSRP, Office Core Router bertindak sebagai Active Router, sedangkan Production Core Router berperan sebagai Standby Router. Jika Active Router mengalami gangguan, Standby Router otomatis mengambil alih alamat IP virtual sehingga trafik tetap dapat berjalan tanpa mengganggu layanan. Selanjutnya, Access Control List (ACL) diterapkan pada interface VLAN 90 untuk melindungi NAS Storage.

```
Enter configuration commands, one per line.  End with CNTL/Z.
OFFICE-CORE-ROUTER(config)#int g0/4.90
OFFICE-CORE-ROUTER(config-subif)#standby 90 ip 10.30.90.6
OFFICE-CORE-ROUTER(config-subif)#standby 90 priority 110
OFFICE-CORE-ROUTER(config-subif)#standby 90 preempt
OFFICE-CORE-ROUTER(config-subif)#ip access-group PROTECT_NAS out
OFFICE-CORE-ROUTER(config-subif)#
```

Langkah 8: Membuat Access Control List (ACL) untuk melindungi DB Server dengan ketentuan: mengizinkan seluruh trafik OSPF dan tunnel (GRE) untuk dapat melewati perangkat, serta memberikan izin akses penuh kepada seluruh host pada jaringan IT Control, Accounting, seluruh area pada Production, dan MES Server. Seluruh jenis trafik lain di luar ketentuan tersebut diblokir.

```
ip access-list extended PROTECT_DB_SERVER
 permit ospf any any
 permit gre any any
 permit ip 10.10.10.0 0.0.0.63 any
 permit ip 10.10.20.0 0.0.0.63 any
 permit ip 10.20.0.0 0.0.255.255 any
 permit ip 10.30.92.0 0.0.0.7 any
 deny   ip any any log
```

Langkah 9: Mengonfigurasi HSRP sebagai mekanisme redundansi gateway karena terdapat dua link sebagai gateway VLAN Servers, masing-masing berasal dari Office Core Router dan Production Core Router. Selanjutnya, Access Control List (ACL) diterapkan pada interface VLAN 91 untuk melindungi DB Server.

```
OFFICE-CORE-ROUTER(config)#int g0/4.91
OFFICE-CORE-ROUTER(config-subif)#standby 91 ip 10.30.91.6
OFFICE-CORE-ROUTER(config-subif)#standby 91 priority 110
OFFICE-CORE-ROUTER(config-subif)#standby 91 preempt
OFFICE-CORE-ROUTER(config-subif)#ip access-group PROTEC
*Nov  7 09:08:28.094: %HSRP-5-STATECHANGE: GigabitEthernet0/4.91 Grp 91 sta
OFFICE-CORE-ROUTER(config-subif)#ip access-group PROTECT_DB_SERVER out
```

Langkah 10: Membuat Access Control List (ACL) untuk melindungi MES Server dengan ketentuan: mengizinkan seluruh trafik OSPF dan tunnel (GRE) untuk dapat melewati perangkat, serta memberikan izin akses penuh kepada seluruh host pada jaringan IT Control, dan seluruh area pada Production. Seluruh jenis trafik lain di luar ketentuan tersebut diblokir.

```
ip access-list extended PROTECT_MES_SERVER
 permit ospf any any
 permit gre any any
 permit ip 10.10.10.0 0.0.0.63 any
 permit ip 10.20.0.0 0.0.255.255 any
 deny   ip any any log
```

Langkah 11: Mengonfigurasi HSRP sebagai mekanisme redundansi gateway karena terdapat dua link sebagai gateway VLAN Servers, masing-masing berasal dari Office Core Router dan Production Core Router. Selanjutnya, Access Control List (ACL) diterapkan pada interface VLAN 92 untuk melindungi MES Server.

```
OFFICE-CORE-ROUTER(config)#int g0/4.92
OFFICE-CORE-ROUTER(config-subif)#standby 92 ip 10.30.92.6
OFFICE-CORE-ROUTER(config-subif)#standby 92 priority 110
OFFICE-CORE-ROUTER(config-subif)#standby 92 preempt
OFFICE-CORE-ROUTER(config-subif)#ip access-group PROTECT_MES_SER
*Nov  7 09:09:33.240: %HSRP-5-STATECHANGE: GigabitEthernet0/4.92 Grp 92 state St
OFFICE-CORE-ROUTER(config-subif)#ip access-group PROTECT_MES_SERVER
% Incomplete command.

OFFICE-CORE-ROUTER(config-subif)#ip access-group PROTECT_MES_SERVER out
OFFICE-CORE-ROUTER(config-subif)#
```

Langkah 12: Menerapkan DHCP client pada interface g0/0 untuk mendapatkan alamat IP secara otomatis dari ISP, kemudian mengonfigurasi interface tersebut sebagai NAT outside karena berfungsi sebagai sumber koneksi internet.

```
OFFICE-CORE-ROUTER(config)#int g0/0
OFFICE-CORE-ROUTER(config-if)#ip address dhcp
OFFICE-CORE-ROUTER(config-if)#ip dhcp client default-router distance 10
OFFICE-CORE-ROUTER(config-if)#ip nat outside
-Traceback= 13148Bz 16079Ez 1604DBz 1602B8z 15A275z 15AE3Fz 3EAA141z 3EA9575z
E8297Cz 1E16248z 1175473z - Process "Exec", CPU hog, PC 0x00155F4C

OFFICE-CORE-ROUTER(config-if)#
OFFICE-CORE-ROUTER(config-if)#
*Nov  7 10:07:02.463: %SYS-3-CPUHOG: Task is running for (1999)msecs, more th
*Nov  7 10:07:02.856: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, c
OFFICE-CORE-ROUTER(config-if)#no sh
OFFICE-CORE-ROUTER(config-if)#
*Nov  7 10:07:14.653: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed s
*Nov  7 10:07:15.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gigabit
OFFICE-CORE-ROUTER(config-if)#
```

Langkah 13: Menerapkan NAT inside pada interface yang terhubung ke Office Router dan Production Core Router, sedangkan interface yang menuju VLAN Servers tidak dikonfigurasi NAT karena server internal perusahaan tidak diperbolehkan mengakses internet. Hal ini dilakukan untuk menjaga keamanan dan integritas data sensitif di lingkungan internal, mencegah kebocoran informasi atau serangan dari luar, serta memastikan server hanya dapat diakses melalui jalur yang sah, misalnya melalui firewall, DB Server, atau MES Server.

9

Langkah 14: Menerapkan access-list untuk mengizinkan semua alamat IP pada topologi yang diperbolehkan mengakses internet agar dapat terhubung ke jaringan publik.

Langkah 15: Mengumumkan default route ke seluruh router OSPF lainnya, sehingga jika sumber internet dari ISP 2 pada Production Core mengalami gangguan, router ini dapat berfungsi sebagai failover.

2. **Konfigurasi Production Core Router**

Langkah 1: Menetapkan hostname menjadi PRODUCTION-CORE-ROUTER serta menonaktifkan fitur IP domain lookup untuk mencegah terjadinya jeda (hang) ketika terjadi kesalahan pengetikan perintah selama proses konfigurasi.

Langkah 2: Mengonfigurasi IP address pada interface yang terhubung ke PRODUCTION-ROUTER.

Langkah 3: Mengonfigurasi IP Address pada interface yang terhubung ke OFFICE-CORE-ROUTER.

Langkah 4: Mengonfigurasi IP Address sebagai gateway VLAN pada Servers.

Langkah 5: Mengonfigurasi OSPF agar dapat terhubung dengan jaringan Office dan Production.

11

```
Enter configuration commands, one per line.  End with CNTL/Z.
PRODUCTION-CORE-ROUT(config)#router ospf 1
PRODUCTION-CORE-ROUT(config-router)#network 10.0.20.1 0.0.0.3 area 0
PRODUCTION-CORE-ROUT(config-router)#network 10.1.20.1 0.0.0.3 area 0
PRODUCTION-CORE-ROUT(config-router)#network 10.30.90.1 0.0.0.7 area 0
PRODUCTION-CORE-ROUT(config-router)#network 10.30.91.1 0.0.0.7 area 0
PRODUCTION-CORE-ROUT(config-router)#network 10.30.92.1 0.0.0.7 area 0
PRODUCTION-CORE-ROUT(config-router)#network 10.0.200.1 0.0.0.3 area 0
PRODUCTION-CORE-ROUT(config-router)#network 10.0.200.1 0.0.0.3 area 0
*Nov  6 16:18:59.727: %OSPF-5-ADJCHG: Process 1, Nbr 10.30.92.2 on GigabitEth
PRODUCTION-CORE-ROUT(config-router)#network 10.1.200.1 0.0.0.3 area 0
PRODUCTION-CORE-ROUT(config-router)#e
*Nov  6 16:19:09.794: %OSPF-5-ADJCHG: Process 1, Nbr 10.30.92.2 on GigabitEth
PRODUCTION-CORE-ROUT(config-router)#
```

Langkah 6: Membuat Access Control List (ACL) untuk mengamankan NAS Storage. Pada tahap ini seluruh trafik OSPF dan tunnel GRE diizinkan melewati perangkat. Selain itu, host pada jaringan IT Control, DB Server, dan MES Server juga diberikan akses penuh. Semua trafik lain di luar ketentuan tersebut diblokir.

Aturan ini diterapkan karena di lingkungan industri, NAS Storage dianggap sangat sensitif. Akses menuju NAS biasanya tidak dilakukan langsung, tetapi melalui DB atau MES sebagai perantara antara server, perangkat produksi, dan departemen akuntansi. Jaringan IT Control tetap diperbolehkan mengakses secara langsung karena mereka yang bertanggung jawab melakukan monitoring dan manajemen seluruh jaringan.

```
ip access-list extended PROTECT_NAS
 permit ospf any any
 permit gre any any
 permit ip 10.10.10.0 0.0.0.63 any
 permit ip 10.30.91.0 0.0.0.7 any
 permit ip 10.30.92.0 0.0.0.7 any
 deny   ip any any log
```

Langkah 7: Mengonfigurasi HSRP sebagai mekanisme redundansi gateway karena terdapat dua link sebagai gateway VLAN Servers, masing-masing berasal dari Office Core Router dan Production Core Router. Dengan HSRP, Production Core Router bertindak sebagai Standby Router, sehingga jika salah satu router mengalami gangguan, trafik tetap dapat berjalan melalui Production Core Router tanpa mengganggu layanan. Selanjutnya, Access Control List (ACL) diterapkan pada interface VLAN 90 untuk melindungi NAS Storage.

```
PRODUCTION-CORE-ROUT(config)#int g0/4.90
PRODUCTION-CORE-ROUT(config-subif)#standby 90 ip 10.30.90.6
PRODUCTION-CORE-ROUT(config-subif)#standby 90 priority 100
PRODUCTION-CORE-ROUT(config-subif)#ip access-group PROTECT_NAS
*Nov  7 09:25:19.610: %HSRP-5-STATECHANGE: GigabitEthernet0/4.90 Grp 9
PRODUCTION-CORE-ROUT(config-subif)#ip access-group PROTECT_NAS out
PRODUCTION-CORE-ROUT(config-subif)#
```

Langkah 8: Membuat Access Control List (ACL) untuk melindungi DB Server dengan ketentuan: mengizinkan seluruh trafik OSPF dan tunnel (GRE) untuk dapat melewati perangkat, serta memberikan izin akses penuh kepada seluruh host pada jaringan IT Control,

Accounting, seluruh area pada Production, dan MES Server. Seluruh jenis trafik lain di luar ketentuan tersebut diblokir.

```
ip access-list extended PROTECT_DB_SERVER
 permit ospf any any
 permit gre any any
 permit ip 10.10.10.0 0.0.0.63 any
 permit ip 10.10.20.0 0.0.0.63 any
 permit ip 10.20.0.0 0.0.255.255 any
 permit ip 10.30.92.0 0.0.0.7 any
 deny   ip any any log
```

Langkah 9: Mengonfigurasi HSRP sebagai mekanisme redundansi gateway karena terdapat dua link sebagai gateway VLAN Servers, masing-masing berasal dari Office Core Router dan Production Core Router. Selanjutnya, Access Control List (ACL) diterapkan pada interface VLAN 91 untuk melindungi DB Server.

```
PRODUCTION-CORE-ROUT(config-subif)#exit
PRODUCTION-CORE-ROUT(config)#int g0/4.91
PRODUCTION-CORE-ROUT(config-subif)#standby 91 ip 10.30.91.6
PRODUCTION-CORE-ROUT(config-subif)#standby 91 priority 100
PRODUCTION-CORE-ROUT(config-subif)#ip access-group PROTECT_DB_SERVER
% Incomplete command.

PRODUCTION-CORE-ROUT(config-subif)#ip access-group PROTECT_DB_SERVER out
PRODUCTION-CORE-ROUT(config-subif)#
```

Langkah 10: Membuat Access Control List (ACL) untuk melindungi MES Server dengan ketentuan: mengizinkan seluruh trafik OSPF dan tunnel (GRE) untuk dapat melewati perangkat, serta memberikan izin akses penuh kepada seluruh host pada jaringan IT Control, dan seluruh area pada Production. Seluruh jenis trafik lain di luar ketentuan tersebut diblokir.

```
ip access-list extended PROTECT_MES_SERVER
 permit ospf any any
 permit gre any any
 permit ip 10.10.10.0 0.0.0.63 any
 permit ip 10.20.0.0 0.0.255.255 any
 deny   ip any any log
```

Langkah 11: Mengonfigurasi HSRP sebagai mekanisme redundansi gateway karena terdapat dua link sebagai gateway VLAN Servers, masing-masing berasal dari Office Core Router dan Production Core Router. Selanjutnya, Access Control List (ACL) diterapkan pada interface VLAN 92 untuk melindungi MES Server.

```
PRODUCTION-CORE-ROUT(config-subif)#exit
PRODUCTION-CORE-ROUT(config)#int g0/4.92
PRODUCTION-CORE-ROUT(config-subif)#standby 92 ip 10.30.92.6
PRODUCTION-CORE-ROUT(config-subif)#standby 92 priority 100
PRODUCTION-CORE-ROUT(config-subif)#ip access-group PROTECT_MES_SERVER out
PRODUCTION-CORE-ROUT(config-subif)#
```

Langkah 12: Menerapkan DHCP client pada interface g0/0 untuk mendapatkan alamat IP secara otomatis dari ISP, kemudian mengonfigurasi interface tersebut sebagai NAT outside karena berfungsi sebagai sumber koneksi internet.

Langkah 13: Menerapkan NAT inside pada interface yang terhubung ke Office Router dan Production Core Router, sedangkan interface yang menuju VLAN Servers tidak dikonfigurasi NAT karena server internal perusahaan tidak diperbolehkan mengakses internet. Hal ini dilakukan untuk menjaga keamanan dan integritas data sensitif di lingkungan internal, mencegah kebocoran informasi atau serangan dari luar.

Langkah 14: Menerapkan access-list untuk mengizinkan semua alamat IP pada topologi yang diperbolehkan mengakses internet agar dapat terhubung ke jaringan publik.

Langkah 15: Mengumumkan default route ke seluruh router OSPF lainnya, sehingga jika sumber internet dari ISP 1 pada Office Core mengalami gangguan, router ini dapat berfungsi sebagai failover.

3. **Konfigurasi Office Router**

Langkah 1: Menetapkan hostname menjadi OFFICE-ROUTER serta menonaktifkan fitur IP domain lookup untuk mencegah terjadinya jeda (hang) ketika terjadi kesalahan pengetikan perintah selama proses konfigurasi.

Langkah 2: Mengonfigurasi IP Address pada interface yang terhubung dengan OFFICE-CORE-ROUTER.

Langkah 3: Mengonfigurasi IP Address sebagai gateway VLAN 10 (IT Control) dan VLAN 20 (Departemen Accounting).

Langkah 4: Mengonfigurasi IPv6 sebagai gateway VLAN 10 dan VLAN 20.

Langkah 5: Mengonfigurasi DHCP Server untuk masing-masing VLAN

Langkah 6: Mengonfigurasi OSPF agar dapat terhubung dengan jaringan Servers dan Production.

Langkah 7: Membuat Access Control List (ACL) untuk VLAN 10 (IT Controll). Pada tahap ini seluruh trafik OSPF, tunnel GRE, protokol udp untuk dhcp server, dan icmp diizinkan melewati perangkat. Selain itu, semua host VLAN 10 dapat mengakses jaringan manapun.

16

Langkah 8: Membuat Access Control List (ACL) untuk VLAN 20. Pada tahap ini, seluruh trafik OSPF, tunnel GRE, serta protokol UDP untuk DHCP Server diizinkan melewati perangkat. Selanjutnya dilakukan pemfilteran: VLAN 20 (Accounting) tidak diperbolehkan mengakses NAS maupun MES Server, dan juga tidak boleh terhubung dengan area Production. Sementara itu, akses ICMP, DB Server, dan internet tetap diizinkan. Semua trafik lain di luar ketentuan tersebut diblokir.

```
ip access-list extended ACL_FROM_FINANCE
 permit ospf any any
 permit gre any any
 permit udp any eq bootpc any eq bootps
 deny   ip 10.10.20.0 0.0.0.63 10.30.90.0 0.0.0.7
 deny   ip 10.10.20.0 0.0.0.63 10.30.92.0 0.0.0.7
 deny   ip 10.10.20.0 0.0.0.63 10.20.0.0 0.0.255.255
 permit icmp any any
 permit ip 10.10.20.0 0.0.0.63 10.30.91.0 0.0.0.7
 permit ip 10.10.20.0 0.0.0.63 any
 deny   ip any any log
```

Langkah 9: Menerapkan ACL pada interface VLAN 10 dan VLAN 20.

```
OFFICE-ROUTER(config)#int g0/2.10
OFFICE-ROUTER(config-subif)#ip access-group ACL_FROM_IT in
OFFICE-ROUTER(config-subif)#exit
OFFICE-ROUTER(config)#int g0/2.20
OFFICE-ROUTER(config-subif)#ip access-group ACL_FROM_FINANCE in
OFFICE-ROUTER(config-subif)#exit
OFFICE-ROUTER(config)#
```

Langkah 10: Mengaktifkan unicast routing pada router agar host di jaringan dapat melakukan SLAAC (Stateless Address Autoconfiguration) untuk mendapatkan alamat IPv6 secara otomatis.

```
OFFICE-ROUTER(config)#ipv6 unicast-routing
OFFICE-ROUTER(config)#
```

Langkah 11: Mengonfigurasi tunnel GRE untuk melewatkan trafik IPv6 pada jaringan.

```
Enter configuration commands, one per line.  End with CNTL/Z.
OFFICE-ROUTER(config)#int tu0
OFFICE-ROUTER(config-if)#
*Nov 14 12:56:46.740: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
OFFICE-ROUTER(config-if)#tunnel source Loopback0
OFFICE-ROUTER(config-if)#tunnel destination 1.1.1.2
OFFICE-ROUTER(config-if)#
*Nov 14 12:57:20.229: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
OFFICE-ROUTER(config-if)#tunnel mode gre ip
OFFICE-ROUTER(config-if)#ipv6 enable
OFFICE-ROUTER(config-if)#ipv6 address FD00:1111:1::1/64
OFFICE-ROUTER(config-if)#
```

Langkah 12: Membuat static route untuk menghubungkan jaringan IPv6 dari Office ke Production.

```
ipv6 route FD00:CCCC:100::/64 Tunnel0
ipv6 route FD00:CCCC:101::/64 Tunnel0
ipv6 route FD00:CCCC:102::/64 Tunnel0
ipv6 route ::/0 FD00:1111:1::2
ipv6 ioam timestamp
!
```

4. **Konfigurasi Production Router**

Langkah 1: Menetapkan hostname menjadi PRODUCTION-ROUTER serta menonaktifkan fitur IP domain lookup untuk mencegah terjadinya jeda (hang) ketika terjadi kesalahan pengetikan perintah selama proses konfigurasi.

```
Router(config)#hostname PRODUCTION-ROUTER
% Hostname "PRODUCTION-ROUTE " is not a legal LAT n
PRODUCTION-ROUTER(config)#no ip domain-lookup
PRODUCTION-ROUTER(config)#
```

Langkah 2: Mengonfigurasi IP Address pada interface yang terhubung dengan PRODUCTION-CORE-ROUTER.

```
PRODUCTION-ROUTER(config)#int g0/0
PRODUCTION-ROUTER(config-if)#ip add 10.0.20.2 255.255.255.252
PRODUCTION-ROUTER(config-if)#no sh
PRODUCTION-ROUTER(config-if)#exi
PRODUCTION-ROUTER(config)#int g
*Nov  6 17:19:16.650: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
PRODUCTION-ROUTER(config)#int g0/5
*Nov  6 17:19:17.649: %LINEPROTO-5-UPDOWN: Line protocol on Interface
PRODUCTION-ROUTER(config)#int g0/7
PRODUCTION-ROUTER(config-if)#ip add 10.1.20.2 255.255.255.252
PRODUCTION-ROUTER(config-if)#no sh
PRODUCTION-ROUTER(config-if)#exit
PRODUCTION-ROUTER(config)#
```

Langkah 3: Mengonfigurasi IP Address sebagai gateway area Production.

Langkah 4: Mengonfigurasi IPv6 sebagai gateway area Production.

Langkah 5: Mengonfigurasi DHCP Server untuk masing-masing VLAN.

Langkah 6: Mengonfigurasi OSPF agar dapat terhubung dengan jaringan Servers dan Office.

```
PRODUCTION-ROUTER(config)#
PRODUCTION-ROUTER(config)#router ospf 1
PRODUCTION-ROUTER(config-router)#network 10.0.20.0 0.0.0.3 area 0
PRODUCTION-ROUTER(config-router)#network 10.20.100.0 0.0.0.31 area 0
PRODUCTION-ROUTER(config-router)#network 10.20.101.0 0.0.0.31 area 0
PRODUCTION-ROUTER(config-router)#network 10.20.102.0 0.0.0.31 area 0
PRODUCTION-ROUTER(config-router)#network 10.1.20.0 0.0.0.3 area 0
PRODUCTION-ROUTER(config-router)#
```

Langkah 7: Membuat Access Control List (ACL) untuk seluruh area Production. Pada tahap ini, seluruh trafik OSPF, tunnel GRE, serta protokol UDP untuk DHCP Server diizinkan melewati perangkat. Selanjutnya dilakukan pemfilteran: tidak diperbolehkan mengakses NAS server, dan juga tidak boleh terhubung dengan area Office. Sementara itu, akses ICMP, DB Server, MES Server dan internet tetap diizinkan. Semua trafik lain di luar ketentuan tersebut diblokir.

```
ip access-list extended ACL_FROM_AREA_1
 permit ospf any any
 permit gre any any
 permit udp any eq bootpc any eq bootps
 deny    ip 10.20.100.0 0.0.0.31 10.30.90.0 0.0.0.7
 deny    ip 10.20.100.0 0.0.0.31 10.10.0.0 0.0.255.255
 permit icmp any any
 permit ip 10.20.100.0 0.0.0.31 10.30.91.0 0.0.0.7
 permit ip 10.20.100.0 0.0.0.31 10.30.92.0 0.0.0.7
 permit ip 10.20.100.0 0.0.0.31 any
 deny    ip any any log
```

```
ip access-list extended ACL_FROM_AREA_2
 permit ospf any any
 permit gre any any
 permit udp any eq bootpc any eq bootps
 deny    ip 10.20.101.0 0.0.0.31 10.30.90.0 0.0.0.7
 deny    ip 10.20.101.0 0.0.0.31 10.10.0.0 0.0.255.255
 permit icmp any any
 permit ip 10.20.101.0 0.0.0.31 10.30.91.0 0.0.0.7
 permit ip 10.20.101.0 0.0.0.31 10.30.92.0 0.0.0.7
 permit ip 10.20.101.0 0.0.0.31 any
 deny    ip any any log
```

```
ip access-list extended ACL_FROM_AREA_3
 permit ospf any any
 permit gre any any
 permit udp any eq bootpc any eq bootps
 deny    ip 10.20.102.0 0.0.0.31 10.30.90.0 0.0.0.7
 deny    ip 10.20.102.0 0.0.0.31 10.10.0.0 0.0.255.255
 permit icmp any any
 permit ip 10.20.102.0 0.0.0.31 10.30.91.0 0.0.0.7
 permit ip 10.20.102.0 0.0.0.31 10.30.92.0 0.0.0.7
 permit ip 10.20.102.0 0.0.0.31 any
 deny    ip any any log
PRODUCTION-ROUTER#
```

Langkah 8: Menerapkan ACL pada seluruh area Production.

```
Enter configuration commands, one per line.  End with CNTL/Z.
PRODUCTION-ROUTER(config)#int g0/1.100
PRODUCTION-ROUTER(config-subif)#ip access-group ACL_FROM_AREA_1
% Incomplete command.

PRODUCTION-ROUTER(config-subif)#ip access-group ACL_FROM_AREA_1 in
PRODUCTION-ROUTER(config-subif)#exit
PRODUCTION-ROUTER(config)#int g0/4.101
PRODUCTION-ROUTER(config-subif)#ip access-group ACL_FROM_AREA_2 in
PRODUCTION-ROUTER(config-subif)#exit
PRODUCTION-ROUTER(config)#int g0/6.102
PRODUCTION-ROUTER(config-subif)#ip access-group ACL_FROM_AREA_3 in
PRODUCTION-ROUTER(config-subif)#exit
PRODUCTION-ROUTER(config)#
```

Langkah 9: Mengaktifkan unicast routing pada router agar host di jaringan dapat melakukan SLAAC (Stateless Address Autoconfiguration) untuk mendapatkan alamat IPv6 secara otomatis.

```
Enter configuration commands, one per line.  End with C
PRODUCTION-ROUTER(config)#ipv6 unicast-routing
PRODUCTION-ROUTER(config)#
```

Langkah 10: Mengonfigurasi tunnel GRE untuk melewatkan trafik IPv6 pada jaringan.

```
Enter configuration commands, one per line.  End with CNTL/Z.
PRODUCTION-ROUTER(config)#int tu0
PRODUCTION-ROUTER(config-if)#
Nov 14 12:58:13.782: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
PRODUCTION-ROUTER(config-if)#tunnel source Loopback0
PRODUCTION-ROUTER(config-if)#tunnel destination 2.2.2.2
PRODUCTION-ROUTER(config-if)#
Nov 14 12:58:47.324: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
PRODUCTION-ROUTER(config-if)#tunnel mode gre ip
PRODUCTION-ROUTER(config-if)#ipv6 enable
PRODUCTION-ROUTER(config-if)#ipv6 address FD00:1111:1::2/64
PRODUCTION-ROUTER(config-if)#
```

Langkah 11: Membuat static route untuk menghubungkan jaringan IPv6 dari Production ke Office.

```
!
ipv6 route FD00:ACAD:10::/64 Tunnel0
ipv6 route FD00:ACAD:20::/64 Tunnel0
ipv6 route ::/0 FD00:1111:1::1
ipv6 ioam timestamp
!
```

5. **Konfigurasi Distribusi Switch (Office)**

   Langkah 1: Membuat Vlan database (vlan 10 dan vlan 20)

Langkah 2: Mengonfigurasi Mode Trunk untuk menerima semua vlan dari Office Router.

Langkah 3: Mengonfigurasi Mode Trunk dan hanya mengijinkan vlan 10 ke departemen IT Control. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Primary, yang berarti switch ini akan menjadi root bridge dalam topologi spanning-tree. Spanning-tree digunakan untuk mencegah looping di jaringan layer 2 dengan menonaktifkan jalur cadangan secara otomatis jika jalur utama aktif. Karena LACP tidak dapat digunakan akibat keterbatasan image switch, redundansi dilakukan melalui mekanisme spanning-tree, sehingga jaringan tetap aman dari loop sekaligus menjaga ketersediaan jalur cadangan.

Langkah 4: Mengonfigurasi Mode Trunk dan hanya mengijinkan vlan 20 ke departemen Accounting. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Primary, yang berarti switch ini akan menjadi root bridge dalam topologi spanning-tree.

6. **Konfigurasi Distribusi Switch 1 (Production)**

Langkah 1: Membuat Vlan database (vlan 100).

Langkah 2: Mengonfigurasi Mode Trunk untuk menerima semua vlan dari Production Router.

Langkah 3: Mengonfigurasi Mode Trunk dan hanya mengijinkan vlan 100 ke Area 1. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Primary, yang berarti switch ini akan menjadi root bridge dalam topologi spanning-tree.

7. **Konfigurasi Distribusi Switch 2 (Production)**
    Langkah 1: Membuat Vlan database (vlan 101).

Langkah 2: Mengonfigurasi Mode Trunk untuk menerima semua vlan dari Production Router.

Langkah 3: Mengonfigurasi Mode Trunk dan hanya mengijinkan vlan 101 ke Area 2. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Primary, yang berarti switch ini akan menjadi root bridge dalam topologi spanning-tree.

8. **Konfigurasi Distribusi Switch 3 (Production)**

   Langkah 1: Membuat Vlan database (vlan 102).

   Langkah 2: Mengonfigurasi Mode Trunk untuk menerima semua vlan dari Production Router.

   Langkah 3: Mengonfigurasi Mode Trunk dan hanya mengijinkan vlan 102 ke Area 3. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Primary, yang berarti switch ini akan menjadi root bridge dalam topologi spanning-tree.

9. **Konfigurasi Managed-Switch (Office - IT Controll)**

   Langkah 1: Membuat Vlan database (vlan 10).

   Langkah 2: Melakukan konfigurasi Mode Trunk pada interface yang terhubung ke Distributed Switch. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Secondary, yang berarti switch tersebut akan menjadi cadangan utama jika Root Primary (Distributed Switch)

tidak aktif. Ketika Root Primary gagal, managed switch otomatis naik mengambil posisi sebagai Root Bridge.

Langkah 3: Mengonfigurasi Switch Mode Access ke interface client.

10. Konfigurasi Managed-Switch (Office - Accounting)

Langkah 1: Membuat Vlan database (vlan 20).

Langkah 2: Melakukan konfigurasi Mode Trunk pada interface yang terhubung ke Distributed Switch. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Secondary, yang berarti switch tersebut akan menjadi cadangan utama jika Root Primary (Distributed Switch) tidak aktif. Ketika Root Primary gagal, managed switch otomatis naik mengambil posisi sebagai Root Bridge.

```
MANAGED-SWITCH1(config)#int range f1/0 - 1
MANAGED-SWITCH1(config-if-range)#switchport trunk encapsulation dot1q
MANAGED-SWITCH1(config-if-range)#switchport mode trunk
MANAGED-SWITCH1(config-if-range)#switchport
*Mar  1 00:03:11.819: %DTP-5-TRUNKPORTON: Port Fa1/0-1 has become dot1q trunk
MANAGED-SWITCH1(config-if-range)#$trunk allowed vlan 20,1-2,1002-1005
MANAGED-SWITCH1(config-if-range)#spanning-tree vlan 20 root secondary
 VLAN 20 bridge priority set to 16384
 VLAN 20 bridge max aging time unchanged at 20
 VLAN 20 bridge hello time unchanged at 2
 VLAN 20 bridge forward delay unchanged at 15
MANAGED-SWITCH1(config)#
```

solarwinds | Solar-PuTTY *free tool*

Langkah 3: Mengonfigurasi Switch Mode Access ke interface client.

```
MANAGED-SWITCH1(config)#int range f1/2 - 3
MANAGED-SWITCH1(config-if-range)#switchport mode access
MANAGED-SWITCH1(config-if-range)#switchport access vlan 20
MANAGED-SWITCH1(config-if-range)#
```

11. Konfigurasi Managed-Switch (Production – Area 1)

Langkah 1: Membuat Vlan database (vlan 100).

```
INDUSTRIAL-SWITCH#vlan database
INDUSTRIAL-SWITCH(vlan)#vlan 100
VLAN 100 added:
    Name: VLAN0100
INDUSTRIAL-SWITCH(vlan)#
```

Langkah 2: Melakukan konfigurasi Mode Trunk pada interface yang terhubung ke Distributed Switch. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Secondary, yang berarti switch tersebut akan menjadi cadangan utama jika Root Primary (Distributed Switch) tidak aktif. Ketika Root Primary gagal, managed switch otomatis naik mengambil posisi sebagai Root Bridge.

27

Langkah 3: Mengonfigurasi Switch Mode Access ke interface client.

12. Konfigurasi Managed-Switch (Production – Area 2)

Langkah 1: Membuat Vlan database (vlan 101).

Langkah 2: Melakukan konfigurasi Mode Trunk pada interface yang terhubung ke Distributed Switch. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Secondary, yang berarti switch tersebut akan menjadi cadangan utama jika Root Primary (Distributed Switch) tidak aktif. Ketika Root Primary gagal, managed switch otomatis naik mengambil posisi sebagai Root Bridge.

```
INDUSTRIAL-SWITCH1(config)#int f1/0
INDUSTRIAL-SWITCH1(config-if)#switchport trunk encapsulation dot1q
INDUSTRIAL-SWITCH1(config-if)#switchport mode trunk
INDUSTRIAL-SWITCH1(config-if)#switchport t
*Mar  1 00:02:05.355: %DTP-5-TRUNKPORTON: Port Fa1/0 has become dot1q trunk
INDUSTRIAL-SWITCH1(config-if)#switchport trunk allowed vlan 101,1-2,1002-1005
INDUSTRIAL-SWITCH1(config-if)#spanning-tree vlan 101 root secondary
 VLAN 101 bridge priority set to 16384
 VLAN 101 bridge max aging time unchanged at 20
 VLAN 101 bridge hello time unchanged at 2
 VLAN 101 bridge forward delay unchanged at 15
INDUSTRIAL-SWITCH1(config)#int f1/5
INDUSTRIAL-SWITCH1(config-if)#switchport trunk encapsulation dot1q
INDUSTRIAL-SWITCH1(config-if)#switchport mode trunk
INDUSTRIAL-SWITCH1(config-if)#s
*Mar  1 00:02:51.795: %DTP-5-TRUNKPORTON: Port Fa1/5 has become dot1q trunk
INDUSTRIAL-SWITCH1(config-if)#switchport trunk allowed vlan 101,1-2,1002-1005
INDUSTRIAL-SWITCH1(config-if)#spanning-tree vlan 101 root secondary
 VLAN 101 bridge priority unchanged at 16384
 VLAN 101 bridge max aging time unchanged at 20
 VLAN 101 bridge hello time unchanged at 2
 VLAN 101 bridge forward delay unchanged at 15
INDUSTRIAL-SWITCH1(config)#
```

Langkah 3: Mengonfigurasi Switch Mode Access ke interface client.


```
INDUSTRIAL-SWITCH1(config)#int range f1/1 - 4
INDUSTRIAL-SWITCH1(config-if-range)#switchport mode access
INDUSTRIAL-SWITCH1(config-if-range)#switchport access vlan 101
INDUSTRIAL-SWITCH1(config-if-range)#
```

13. Konfigurasi Managed-Switch (Production – Area 3)

Langkah 1: Membuat Vlan database (vlan 102).


```
INDUSTRIAL-SWITCH2#vlan database
INDUSTRIAL-SWITCH2(vlan)#vlan 102
VLAN 102 added:
    Name: VLAN0102
INDUSTRIAL-SWITCH2(vlan)#exit
APPLY completed.
Exiting....
```

Langkah 2: Melakukan konfigurasi Mode Trunk pada interface yang terhubung ke Distributed Switch. Selanjutnya, dilakukan konfigurasi Spanning-Tree Root Secondary, yang berarti switch tersebut akan menjadi cadangan utama jika Root Primary (Distributed Switch) tidak aktif. Ketika Root Primary gagal, managed switch otomatis naik mengambil posisi sebagai Root Bridge.

Langkah 3: Mengonfigurasi Switch Mode Access ke interface client.

14. Konfigurasi Managed-Switch (Servers)

Langkah 1: Membuat Vlan database (vlan 90, vlan 91, dan vlan 92).

Langkah 2: Melakukan konfigurasi Mode Trunk pada interface yang terhubung ke Distributed Switch.

Langkah 3: Mengonfigurasi mode access pada interface yang terhubung ke masing-masing server.

4. PENGUJIAN

4.1 Pengujian DHCP dan Alokasi IP

Pengujian dilakukan pada sisi client untuk memastikan bahwa DHCP Server berfungsi dengan benar dan mampu memberikan alamat IP sesuai konfigurasi yang telah ditetapkan.

1. Pengujian pertama dilakukan pada seluruh client di area Production. Hasilnya menunjukkan bahwa alokasi IP sudah sesuai dengan konfigurasi DHCP Pool serta pembagian alamat VLAN pada masing-masing area.

Area 2


```
PC5> ip dhcp -r
DDORA IP 10.20.101.2/27 GW 10.20.101.1

PC5>
```

Area 3


```
PC12> ip dhcp -r
DDORA IP 10.20.102.2/27 GW 10.20.102.1

PC12>
```

Area 1


```
PC6> ip dhcp -r
DDORA IP 10.20.100.2/27 GW 10.20.100.1

PC6>
```

2. Pengujian kedua dilakukan pada seluruh client di area Office. Hasilnya menunjukkan bahwa alokasi IP sudah sesuai dengan konfigurasi DHCP Pool serta pembagian alamat VLAN pada masing-masing area.

IT Controll


```
PC1> ip dhcp -r
DORA IP 10.10.10.2/26 GW 10.10.10.1

PC1>
```

Accounting & Finance

3. Alokasi IP Address static pada masing-masing server.

DB-Server

NAS-Storage

MES-Server

4.2 Pengujian Rute OSPF pada Setiap Router

Pengujian dilakukan pada seluruh router yang telah dikonfigurasi menggunakan OSPF untuk memastikan bahwa masing-masing perangkat berhasil mempelajari seluruh rute yang diperlukan untuk berkomunikasi ke seluruh jaringan dalam topologi.

1. Pengujian pertama dilakukan pada Office Router. Hasilnya menunjukkan bahwa router tersebut telah mempelajari seluruh rute menuju router-router lain yang tergabung dalam proses OSPF.

2. Pengujian kedua dilakukan pada Office Core Router. Hasilnya menunjukkan bahwa router tersebut telah mempelajari seluruh rute menuju router-router lain yang tergabung dalam proses OSPF.

3. Pengujian ketiga dilakukan pada Production Router. Hasilnya menunjukkan bahwa router tersebut telah mempelajari seluruh rute menuju router-router lain yang tergabung dalam proses OSPF.

4. Pengujian keempat dilakukan pada Production Core Router. Hasilnya menunjukkan bahwa router tersebut telah mempelajari seluruh rute menuju router-router lain yang tergabung dalam proses OSPF.

4.3 Pengujian Inter-VLAN Routing

Pengujian dilakukan pada masing-masing departemen atau area di setiap divisi, baik Office maupun Production, untuk memastikan bahwa proses inter-VLAN routing berjalan sesuai konfigurasi dan tiap VLAN dapat saling berkomunikasi sesuai ketentuan.

1. Pengujian pertama dilakukan pada Office. Hasilnya menunjukkan bahwa vlan 10 dan vlan 20 dapat saling terhubung.

vlan 10 test ping ke vlan 20

vlan 20 test ping ke vlan 10

2. Pengujian kedua dilakukan pada Production. Hasilnya menunjukkan bahwa vlan 100, vlan 101 dan vlan 102 dapat saling terhubung.

vlan 100 test ping ke vlan 101, vlan 102

vlan 101 test ping ke vlan 100, vlan 102

vlan 102 test ping ke vlan 100, vlan 101

4.4 Pengujian Ping Antar Divisi dan Penerapan Access-List

Pengujian dilakukan pada setiap departemen atau area di kedua divisi, baik Office maupun Production, untuk memastikan bahwa seluruh koneksi antar VLAN telah berjalan sesuai dengan aturan access-list yang telah diterapkan. Pengujian ini bertujuan memverifikasi apakah tiap area hanya dapat mengakses resource yang memang diizinkan oleh kebijakan jaringan.

1. Pengujian pertama dilakukan pada departemen IT Control di divisi Office. Hasilnya menunjukkan bahwa VLAN 10 (IT Control) dapat terhubung ke server serta ke seluruh area di Production sesuai dengan ketentuan access-list yang berlaku.

Test ping ke servers

Test ping ke production

2. Pengujian kedua dilakukan pada departemen Accounting dan Finance di divisi Office. Hasilnya menunjukkan bahwa VLAN 20 (Accounting) hanya dapat terhubung ke DB server.

Test ping ke servers

Test ping ke production

3. Pengujian ketiga dilakukan pada seluruh area pada divisi Production karena aturan access-listnya sama. Hasilnya menunjukkan bahwa seluruh area hanya dapat terhubung ke DB server dan MES Server.

Test ping Area 1 ke servers

```
PC6> ping 10.30.90.3

*10.20.100.1 icmp_seq=1 ttl=255 time=35.843 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.100.1 icmp_seq=2 ttl=255 time=4.807 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC6> ping 10.30.91.3

84 bytes from 10.30.91.3 icmp_seq=1 ttl=61 time=480.171 ms
84 bytes from 10.30.91.3 icmp_seq=2 ttl=61 time=282.309 ms
^C
PC6> ping 10.30.92.3

84 bytes from 10.30.92.3 icmp_seq=1 ttl=61 time=611.350 ms
84 bytes from 10.30.92.3 icmp_seq=2 ttl=61 time=47.619 ms
^C
PC6>
```

Test ping Area 1 ke office

```
^C
PC6> ping 10.10.10.2

*10.20.100.1 icmp_seq=1 ttl=255 time=52.579 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.100.1 icmp_seq=2 ttl=255 time=16.161 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC6> ping 10.10.20.2

*10.20.100.1 icmp_seq=1 ttl=255 time=14.307 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.100.1 icmp_seq=2 ttl=255 time=18.552 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC6>
```

Test ping Area 2 ke servers

```
PC5> ping 10.30.90.3

*10.20.101.1 icmp_seq=1 ttl=255 time=55.244 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.101.1 icmp_seq=2 ttl=255 time=54.495 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC5> ping 10.30.91.3

84 bytes from 10.30.91.3 icmp_seq=1 ttl=61 time=26.530 ms
84 bytes from 10.30.91.3 icmp_seq=2 ttl=61 time=91.066 ms
^C
PC5> ping 10.30.92.3

84 bytes from 10.30.92.3 icmp_seq=1 ttl=61 time=36.262 ms
84 bytes from 10.30.92.3 icmp_seq=2 ttl=61 time=93.055 ms
^C
PC5>
```

Test ping Area 2 ke office

```
^C
PC5> ping 10.10.10.2

*10.20.101.1 icmp_seq=1 ttl=255 time=48.897 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.101.1 icmp_seq=2 ttl=255 time=15.924 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC5> ping 10.10.20.2

*10.20.101.1 icmp_seq=1 ttl=255 time=16.078 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.101.1 icmp_seq=2 ttl=255 time=32.999 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC5>
```

Test ping Area 3 ke servers

Test ping Area 3 ke office

4.5 Pengujian Akses Internet

Pengujian dilakukan pada setiap departemen atau area di kedua divisi, baik Office maupun Production, termasuk seluruh server. Tujuannya untuk memastikan bahwa perangkat yang diizinkan mengakses internet dapat terhubung dengan baik, sementara perangkat yang tidak memiliki izin benar-benar tidak dapat mengakses internet sesuai kebijakan access-list dan konfigurasi NAT yang telah diterapkan.

1. Pengujian pertama dilakukan pada divisi Office. Hasilnya menunjukkan bahwa VLAN 10 (IT Control) dan VLAN 20 (Accounting) dapat terhubung ke internet.

Ping IT Control ke Internet

Ping Accounting ke Internet

2. Pengujian kedua dilakukan pada divisi Production. Hasilnya menunjukkan bahwa VLAN 100 (Area 1), VLAN 101 (Area 2) dan VLAN 102 (Area 3) dapat terhubung ke internet.

Ping Area 1 ke Internet

Ping Area 2 ke Internet

Ping Area 3 ke Internet

3. Pengujian ketiga dilakukan pada Servers. Hasilnya menunjukkan bahwa seluruh server tidak dapat terhubung ke internet sesuai dengan aturan access-list yang telah diimplementasikan.

Ping NAS Storage ke Internet

Ping DB Server ke Internet

Ping MES Server ke Internet

4.6 Pengujian SLACC IPv6

Pengujian dilakukan pada setiap departemen atau area di kedua divisi, baik Office maupun Production.

1. Pengujian pertama dilakukan pada divisi Office. Hasilnya menunjukkan bahwa VLAN 10 (IT Control) dan VLAN 20 (Accounting) mendapatkan IPv6 secara otomatis.

Vlan 10

```
PC1> ip auto
GLOBAL SCOPE       : fd00:acad:10:0:2050:79ff:fe66:680d/64
ROUTER LINK-LAYER : 0c:77:c7:a3:00:02
```

Vlan 20

```
PC3> ip auto
GLOBAL SCOPE       : fd00:acad:20:0:2050:79ff:fe66:6802/64
ROUTER LINK-LAYER : 0c:77:c7:a3:00:02
```

2. Pengujian kedua dilakukan pada divisi Production. Hasilnya menunjukkan bahwa VLAN 100 (Area 1), VLAN 101 (Area 2) dan VLAN 102 (Area 3) mendapatkan IPv6 secara otomatis.

Vlan 100

```
PC6> ip auto
GLOBAL SCOPE       : fd00:cccc:100:0:2050:79ff:fe66:6805/64
ROUTER LINK-LAYER : 0c:92:4e:3c:00:01

PC6>
```

Vlan 101

```
PC5> ip auto
GLOBAL SCOPE       : fd00:cccc:101:0:2050:79ff:fe66:6806/64
ROUTER LINK-LAYER : 0c:92:4e:3c:00:04

PC5>
```

Vlan 102

```
PC12> ip auto
GLOBAL SCOPE       : fd00:cccc:102:0:2050:79ff:fe66:6808/64
ROUTER LINK-LAYER : 0c:92:4e:3c:00:06

PC12>
```

4.7 Pengujian Tunnel GRE

Pengujian ini dilakukan pada Host di sisi Office maupun Production. Tujuannya untuk memverifikasi apakah Tunnel GRE yang sudah dikonfigurasi benar-benar berfungsi mengalirkan trafik IPv6 antar kedua lokasi tersebut.

1. Pengujian pertama dilakukan dari sisi Office. Hasilnya sukses, di mana VLAN 10 (IT Control) dan VLAN 20 (Accounting) terbukti dapat terhubung ke seluruh area di Production menggunakan jaringan IPv6.

VLAN 10

VLAN 20

2. Pengujian kedua dilakukan dari sisi Production. Hasilnya sukses, di mana VLAN 100 (Area 1), VLAN 101 (Area 2) dan VLAN 102 (Area 3) terbukti dapat terhubung ke seluruh area di Office menggunakan jaringan IPv6.

VLAN 100

```
PC6> trace fd00:acad:10:0:2050:79ff:fe66:680d

trace to fd00:acad:10:0:2050:79ff:fe66:680d, 64 hops max
 1 fd00:cccc:100::1   167.226 ms  29.082 ms  39.618 ms
 2 fd00:1111:1::1    250.223 ms  194.593 ms  457.265 ms
 3 fd00:acad:10:0:2050:79ff:fe66:680d   543.730 ms  264.052 ms  147.900 ms

PC6> trace fd00:acad:20:0:2050:79ff:fe66:6802

trace to fd00:acad:20:0:2050:79ff:fe66:6802, 64 hops max
 1 fd00:cccc:100::1    402.942 ms  26.453 ms  52.234 ms
 2 fd00:1111:1::1    554.340 ms  718.709 ms  562.421 ms
 3 fd00:acad:20:0:2050:79ff:fe66:6802   77.709 ms  144.201 ms  70.246 ms

PC6> []
```

VLAN 101

```
PC5> trace fd00:acad:10:0:2050:79ff:fe66:680d

trace to fd00:acad:10:0:2050:79ff:fe66:680d, 64 hops max
 1 fd00:cccc:101::1    530.948 ms  42.702 ms  82.532 ms
 2 fd00:1111:1::1    306.371 ms  536.333 ms  685.844 ms
 3 fd00:acad:10:0:2050:79ff:fe66:680d   108.834 ms  114.713 ms  219.247 ms

PC5> trace fd00:acad:20:0:2050:79ff:fe66:6802

trace to fd00:acad:20:0:2050:79ff:fe66:6802, 64 hops max
 1 fd00:cccc:101::1    332.673 ms  25.574 ms  18.348 ms
 2 fd00:1111:1::1    356.462 ms  527.131 ms  531.704 ms
 3 fd00:acad:20:0:2050:79ff:fe66:6802   571.530 ms  116.873 ms  208.757 ms

PC5> []
```

VLAN 102

```
PC12>  trace fd00:acad:10:0:2050:79ff:fe66:680d

trace to fd00:acad:10:0:2050:79ff:fe66:680d, 64 hops max
 1 fd00:cccc:102::1   259.788 ms  30.824 ms  37.007 ms
 2 fd00:1111:1::1   146.767 ms  683.114 ms  112.416 ms
 3 fd00:acad:10:0:2050:79ff:fe66:680d   154.326 ms  152.562 ms  95.699 ms

PC12> trace fd00:acad:20:0:2050:79ff:fe66:6802

trace to fd00:acad:20:0:2050:79ff:fe66:6802, 64 hops max
 1 fd00:cccc:102::1   205.146 ms  20.768 ms  31.851 ms
 2 fd00:1111:1::1    561.998 ms  826.045 ms  660.345 ms
 3 fd00:acad:20:0:2050:79ff:fe66:6802   258.433 ms  69.273 ms  178.888 ms

PC12> []
```

5. DAFTAR PUSTAKA

Cisco, Panduit, & Rockwell Automation. (2023). *Physical Infrastructure for the Converged Plantwide Ethernet Architecture* (Publikasi No. ENET-TD020B-EN-P).

Pickard, J., Linn, J. B., Awojana, T. B., & Lunsford II, P. J. (2018). *Designing a Converged Plant-wide Ethernet/IP Lab for Hands-on Distance Learning: An Interdisciplinary Graduate Project*. 2018 ASEE Annual Conference & Exposition, Salt Lake City, UT, United States.

Santoso, I., Nursiaga, R., Firmansyah, H., Rantina, M., Asbari, M., & Santoso, G. (2025). Desain Sistem Jaringan Untuk Smart Factory Berbasis Industrial Internet of Things (iiot). *JAREKOM: Jurnal Jaringan dan Rekayasa Komputer*, *01*(1), 74–80.