

## Mod11

### ◆ 1. Tujuan Utama Teknologi Ini

Digunakan untuk:

- **Meningkatkan bandwidth**
- **Meningkatkan reliability (high availability)**
- **Menghilangkan single point of failure**
- **Menghindari link terblokir STP**

Solusi utama:

- **Eth-Trunk (Link Aggregation)**
- **iStack**
- **CSS**

11 Eth-Trunk iStack and CSS

---

### ◆ 2. Konsep Dasar Network Reliability

Reliability bisa diterapkan di:

1. **Card level** → MPU, SFU, LPU redundancy
2. **Device level** → dual-homing, master/backup
3. **Link level** → multiple physical links + aggregation

Masalah jaringan tradisional:

- STP bikin **link nganggur**
- Bandwidth tidak optimal
- Troubleshooting ribet

11 Eth-Trunk iStack and CSS

---

### ◆ 3. Eth-Trunk (Link Aggregation)

**Eth-Trunk = beberapa physical link → 1 logical link**

Keuntungan:

- Semua link **aktif**

- Bandwidth **akumulatif**
- Tetap **loop-free** tanpa STP

#### Istilah penting (WAJIB HAFAL):

- **LAG:** Link Aggregation Group
- **Member interface/link**
- **Active interface/link**
- **Inactive interface/link**
- **Upper & lower threshold**

11 Eth-Trunk iStack and CSS

---

#### ◆ 4. Mode Eth-Trunk

##### ◆ a. Manual Mode

Ciri:

- ✗ Tidak pakai LACP
- Semua link aktif
- Cocok untuk device lama (tidak support LACP)

##### ⚠ Kekurangan:

- Tidak bisa deteksi error layer atas
- Salah konfigurasi → **loop berbahaya**
- Hanya cek **physical up/down**

11 Eth-Trunk iStack and CSS

---

##### ◆ b. LACP Mode (PALING SERING DIUJI)

Ciri:

- ✅ Pakai **LACPDU**
- Negotiation antar device
- Lebih aman & pintar

Isi **LACPDU**:

- System priority
- MAC address
- Interface priority
- Interface number

11 Eth-Trunk iStack and CSS

---

#### ◆ 5. Actor Election (PENTING BANGET)

Actor ditentukan oleh:

1. **System priority** (kecil = menang)
2. Jika sama → **MAC address** (kecil = menang)

Default:

- System priority = **32768**
- Interface priority = **32768**

Actor yang menentukan:

- Interface mana yang **active**
- Interface mana yang **backup**

11 Eth-Trunk iStack and CSS

---

#### ◆ 6. Maximum Active Interfaces

- Bisa set **max active-link**
- Sisanya otomatis jadi **inactive (backup)**
- Jika active link mati → backup **langsung naik**

Catatan ujian:

- Jumlah max active **HARUS SAMA** di kedua device

11 Eth-Trunk iStack and CSS

---

#### ◆ 7. Load Balancing (JANGAN KETUKER)

##### ✗ Per-packet

- Bisa **packet disorder**

-  Tidak direkomendasikan

 **Per-flow (REKOMENDASI)**

- 1 flow → 1 link
- Urutan packet aman

Mode load balancing:

- Src MAC
- Dst MAC
- Src IP
- Dst IP
- Src + Dst IP (PALING UMUM)
- Src + Dst MAC

11 Eth-Trunk iStack and CSS

---

◆ **8. Use Case Eth-Trunk**

- Switch ↔ Switch
- Switch ↔ Server (NIC bonding)
- Switch ↔ Stack
- Firewall heartbeat link

11 Eth-Trunk iStack and CSS

---

◆ **9. Command Penting (Huawei Style)**

Wajib familiar:

- interface eth-trunk X
- mode lacp | manual
- trunkport gigabitethernet
- lacp priority
- max active-linknumber
- least active-linknumber

11 Eth-Trunk iStack and CSS

---

## ◆ 10. iStack & CSS

### iStack

- Banyak switch → **1 logical switch**
- Biasanya **fixed switch**
- Expand port & bandwidth

### CSS

- **HANYA 2 switch**
- Biasanya **modular switch**
- Control plane & forwarding plane unified

Keuntungan:

- **✗** Tidak perlu STP
- **✗** Tidak perlu VRRP
- **✓** Semua link aktif
- **✓** Fast convergence
- **✓** Simple management

## 11 Eth-Trunk iStack and CSS

---

## ◆ 11. Perbandingan Singkat

Teknologi	Jumlah Device	Target
Eth-Trunk	2+ device	Link
iStack	Banyak	Access / Aggregation
CSS	2	Core / Aggregation

Mod12

## ACL (Access Control List) – Principles & Configuration

### 1 Apa itu ACL (WAJIB PAHAM)

- **ACL = kumpulan rule (permit / deny) untuk memfilter traffic**

- ACL **mencocokkan paket** berdasarkan header (IP, protocol, port)
- Dipakai untuk:
  - Security
  - Traffic filtering
  - NAT
  - Routing policy
  - Firewall
  - QoS

12 ACL Principles and Configura...

---

## 2 Struktur ACL (SERING KELUAR)

Satu ACL terdiri dari:

- **ACL number / name**
- **Rule ID**
- **Action** → permit / deny
- **Matching criteria** (source IP, destination IP, port, protocol)
- **Implicit deny di akhir** (hidden rule)

### 📌 Penting

➡ Kalau tidak kena rule apa pun → **DENY**

---

## 3 Rule ID & Step

- Rule diproses **dari ID terkecil ke terbesar**
- Default **step = 5**
- Step memudahkan **insert rule di tengah**

12 ACL Principles and Configura...

Contoh:

rule 5 deny

rule 10 permit

---

## 4 Wildcard Mask (INI FAVORIT UJIAN)

Wildcard ≠ Subnet mask

### Nilai Arti

0 HARUS sama (strict match)

1 Bebas / diabaikan

📌 Contoh:

- 192.168.1.0 0.0.0.255  
→ match **1 network /24**
- 192.168.1.1 0.0.0.0  
→ match **1 IP saja**
- any = 0.0.0.0 255.255.255.255

12 ACL Principles and Configura...

---

## 5 Klasifikasi ACL (WAJIB HAFAL)

Jenis ACL	Nomor	Ciri
<b>Basic ACL</b>	2000–2999	Source IP saja
<b>Advanced ACL</b>	3000–3999	Src IP, Dst IP, Protocol, Port
<b>Layer 2 ACL</b>	4000–4999	MAC address
<b>User-defined ACL</b>	5000–5999	Custom
<b>User ACL</b>	6000–9999	Lebih fleksibel

12 ACL Principles and Configura...

---

## 6 Basic vs Advanced ACL (UJIAN SUKA BANGET)

### Basic ACL

- Filter berdasarkan **SOURCE IP**
- Lebih sederhana

rule deny source 192.168.1.0 0.0.0.255

### Advanced ACL

- Bisa filter:

- Source IP
- Destination IP
- Protocol (TCP/UDP/ICMP)
- Port

```
rule deny tcp source 10.1.1.0 0.0.0.255 destination-port eq 21
```

---

## 7 Mekanisme Matching ACL (INI KUNCI)

- Rule dicek **SATU PER SATU**
- **Begitu cocok → STOP**
- Tidak lanjut ke rule bawah
- Tidak cocok semua → **implicit deny**

12 ACL Principles and Configura...

---

## 8 Inbound vs Outbound (SERING KECOH)

- **Inbound** → sebelum routing decision
- **Outbound** → setelah routing decision

📌 Salah pasang arah = ACL **tidak bekerja**

---

## 9 Perintah Dasar (HAFAL POLANYA)

### Basic ACL

```
acl 2000
```

```
rule deny source 192.168.1.0 0.0.0.255
```

```
rule permit source any
```

### Apply ke interface

```
interface g0/0/1
```

```
traffic-filter inbound acl 2000
```

## Mod13

### AAA – Principles and Configuration

---

#### 1 Konsep Inti AAA (WAJIB HAFAL URUTANNYA)

**AAA = Authentication, Authorization, Accounting**

Urutan proses **TIDAK BOLEH TERBALIK**:

1. **Authentication** → siapa kamu?
2. **Authorization** → boleh ngapain?
3. **Accounting** → ngapain aja?

📌 Ini soal teori favorit dosen

---

#### 2 Authentication (AUTHEN)

Fungsi:

- Memverifikasi **identitas user**
- Berdasarkan:
  - Username & password
  - Certificate
  - Token

Metode authentication:

- **Local**
- **Remote (Server AAA)**

📌 Authentication gagal → proses **BERHENTI**

---

#### 3 Authorization (AUTHOR)

Fungsi:

- Menentukan **hak akses**
- Setelah user **berhasil login**

Contoh:

- User A boleh akses:

- VLAN tertentu
- Command tertentu
- Service tertentu

📌 Tidak menentukan identitas, tapi **hak**

---

#### 4 Accounting (ACCOUNTING)

Fungsi:

- Mencatat aktivitas user:
  - Login / logout
  - Command yang dijalankan
  - Lama koneksi
  - Resource yang dipakai

Dipakai untuk:

- Audit
- Billing
- Security log

📌 Accounting **tidak memblokir**, hanya mencatat

---

#### 5 AAA Architecture (Client–Server)

Komponen:

- **AAA Client** → router / switch
- **AAA Server** → RADIUS / TACACS+
- **User**

Alur:

User → Device → AAA Server

---

#### 6 Protokol AAA (SERING KELUAR)

- ◆ **RADIUS**

- Authentication + Authorization **digabung**
- Accounting terpisah
- Berbasis **UDP**
- Port:
  - Auth: **1812**
  - Accounting: **1813**
- Enkripsi: **password saja**

❖ Paling umum (WiFi, ISP)

---

#### ◆ TACACS+

- Authentication, Authorization, Accounting **dipisah**
- Berbasis **TCP**
- Port: **49**
- Enkripsi: **seluruh payload**

❖ Lebih aman, sering di enterprise

---

### 7 Local AAA vs Server AAA

Aspek	Local	Server
Skalabilitas	Rendah	Tinggi
Keamanan	Rendah	Tinggi
Management	Sulit	Terpusat

❖ Jaringan besar → **Server AAA**

---

### 8 AAA Policy & Domain

- AAA bisa dibedakan per:
  - User
  - Interface
  - Service

- Bisa pakai **domain** untuk kontrol akses berbeda
- 📌 Biasanya keluar sebagai konsep
- 

## 9 Konsep Fallback (UJIAN SUKA)

Jika AAA server **down**:

- Bisa fallback ke:
    - Local authentication
    - Secondary server
- 📌 Kalau tidak diset → user **LOCKED OUT**

Mod14

## Network Address Translation (NAT)

---

### 1 Konsep Inti NAT (WAJIB PAHAM)

**NAT = mekanisme menerjemahkan IP address**

- Private IP ↔ Public IP
- Tujuan utama:
  - **Hemat IPv4**
  - **Akses internet**
  - **Security dasar (hide internal IP)**

---

### 2 Istilah Penting NAT (SERING KELUAR)

- **Inside Local** → IP private di dalam jaringan
- **Inside Global** → IP public hasil NAT
- **Outside Local** → IP tujuan dilihat dari dalam
- **Outside Global** → IP public asli tujuan

📌 Soal teori sering nanya definisi ini

---

### 3 Jenis-Jenis NAT (WAJIB HAFAL)

#### ◆ Static NAT

- 1 private IP ↔ 1 public IP
- Mapping **tetap**
- Cocok: server (web, mail)

❖ Boros IP public

---

#### ◆ Dynamic NAT

- Private IP ↔ **pool IP public**
  - Mapping **sementara**
  - Jika pool habis → client gagal akses
- 

#### ◆ PAT / NAT Overload ★ (PALING SERING)

- Banyak private IP → **1 public IP**
  - Dibedakan pakai **port number**
  - Paling umum dipakai ISP & router rumahan
- 

### 4 Alur Kerja NAT (LOGIKA UJIAN)

1. Client kirim paket (private IP)
2. Router NAT:
  - Ganti source IP
  - (PAT: ganti port juga)
3. Paket keluar ke internet
4. Balasan masuk → NAT table → client

❖ NAT pakai **NAT table** sebagai mapping

---

### 5 NAT Table (PENTING)

Isi:

- Inside local IP
- Inside global IP
- Port (PAT)

📌 Kalau entry habis / timeout → koneksi putus

---

## 6 NAT vs ACL (SERING DIKOMBINASI)

- ACL digunakan untuk:
    - Menentukan IP mana yang di-NAT
  - NAT tidak bekerja tanpa ACL (di banyak vendor)
- 

## 7 Kelebihan & Kekurangan NAT

### Kelebihan

- Hemat IPv4
- Sembunyikan internal network

### Kekurangan

- End-to-end principle rusak
- Beberapa aplikasi sulit (VoIP, P2P)
- Tambah latency

Mod15

## Network Services and Applications

---

## 1 Konsep Inti Network Service

**Network Service** = layanan yang disediakan jaringan agar user & aplikasi bisa berjalan dengan baik.

Tujuan utama:

- Mempermudah komunikasi
- Otomatisasi konfigurasi
- Manajemen & monitoring jaringan

❖ Biasanya berbasis **client-server**

---

## 2 Service yang WAJIB DIHAFAL (SERING KELUAR)

### ◆ DHCP (Dynamic Host Configuration Protocol)

Fungsi:

- Memberikan IP **otomatis**

Informasi yang diberikan:

- IP address
- Subnet mask
- Default gateway
- DNS server

Port:

- UDP **67 (server)**
- UDP **68 (client)**

❖ Tanpa DHCP → IP harus manual

---

### ◆ DNS (Domain Name System)

Fungsi:

- Mengubah **nama domain** → **IP address**

Contoh:

google.com → 142.xxx.xxx.xxx

Port:

- UDP **53 (query)**
- TCP **53 (zone transfer)**

❖ Tanpa DNS → akses pakai IP, bukan nama

---

### ◆ FTP (File Transfer Protocol)

Fungsi:

- Transfer file client ↔ server

Port:

- TCP **21** (control)
- TCP **20** (data, mode active)

Mode:

- **Active**
- **Passive** (lebih umum, NAT-friendly)

📌 **FTP = tidak terenkripsi**

---

#### ◆ **Telnet**

Fungsi:

- Remote login ke device

Port:

- TCP **23**

⚠️ Tidak aman (plaintext)

➡️ Biasanya dibandingkan dengan SSH

---

#### ◆ **SSH (WAJIB TAHU)**

Fungsi:

- Remote login **aman**

Port:

- TCP **22**

📌 Pengganti Telnet

---

#### ◆ **HTTP & HTTPS**

Service	Port	Keterangan
HTTP	TCP 80	Tidak terenkripsi
HTTPS	TCP 443	Terenkripsi (SSL/TLS)

---

## ◆ SNMP

Fungsi:

- Monitoring & manajemen jaringan

Port:

- UDP **161** (request)
- UDP **162** (trap)

Komponen:

- Manager
  - Agent
  - MIB
- 

## 3 Network Application

**Network application** = aplikasi yang menggunakan **network service**

Contoh:

- Browser → DNS, HTTP/HTTPS
- Email client → SMTP, POP3, IMAP
- File sharing → FTP, SMB

❖ Application ≠ Service, tapi **saling terkait**

---

## 4 Client–Server vs Peer-to-Peer (SERING KELUAR)

Aspek	Client–Server	P2P
Server	Ada	Tidak ada
Kontrol	Terpusat	Terdistribusi
Skalabilitas	Tinggi	Rendah

Mod16

### 1. Pengertian WLAN

- **WLAN (Wireless Local Area Network)** adalah jaringan lokal yang menggunakan **gelombang radio** sebagai media transmisi data.

- Menggantikan atau melengkapi jaringan kabel (LAN).
- 

## 2. Komponen Utama WLAN

- **Wireless Client**  
Laptop, smartphone, tablet, atau perangkat dengan wireless adapter.
  - **Access Point (AP)**  
Penghubung antara perangkat wireless dengan jaringan kabel/internet.
  - **Wireless Network Interface Card (NIC)**  
Perangkat keras agar client bisa terhubung ke WLAN.
  - **Distribution System (DS)**  
Infrastruktur jaringan (biasanya LAN kabel) yang menghubungkan AP.
- 

## 3. Standar WLAN (IEEE 802.11)

Yang paling penting diingat:

- **802.11a** → 5 GHz, cepat, jangkauan lebih pendek
- **802.11b** → 2.4 GHz, lambat, jangkauan luas
- **802.11g** → 2.4 GHz, lebih cepat dari b
- **802.11n** → 2.4 / 5 GHz, MIMO, lebih stabil
- **802.11ac** → 5 GHz, sangat cepat
- **802.11ax (Wi-Fi 6)** → efisien, cepat, banyak client

☞ Intinya: **semakin baru standar → semakin cepat & efisien**

---

## 4. Frekuensi WLAN

- **2.4 GHz**
  - Jangkauan lebih luas
  - Mudah interferensi (Bluetooth, microwave)
- **5 GHz**
  - Kecepatan tinggi
  - Jangkauan lebih pendek
  - Lebih sedikit gangguan

---

## 5. Mode Operasi WLAN

- **Infrastructure Mode**
    - Client ↔ Access Point
    - Paling umum digunakan
  - **Ad-Hoc Mode**
    - Client ↔ Client langsung
    - Tanpa AP
- 

## 6. Topologi WLAN

- **BSS (Basic Service Set)**  
Satu AP dan beberapa client
  - **ESS (Extended Service Set)**  
Beberapa AP, satu jaringan (SSID sama)
  - **IBSS**  
Ad-Hoc tanpa AP
- 

## 7. SSID (Service Set Identifier)

- Nama jaringan Wi-Fi
  - Bisa disiarkan (broadcast) atau disembunyikan
- 

## 8. Keamanan WLAN

Poin penting yang harus diingat:

- **WEP** → lemah (tidak aman)
- **WPA** → lebih baik dari WEP
- **WPA2** → standar umum, aman
- **WPA3** → paling aman saat ini

📌 **Gunakan minimal WPA2**

---

## 9. Masalah Umum WLAN

- Interferensi sinyal
  - Jarak terlalu jauh dari AP
  - Terlalu banyak pengguna
  - Channel tumpang tindih
- 

## 10. Kelebihan WLAN

- Mobilitas tinggi
  - Mudah instalasi
  - Fleksibel
  - Hemat kabel
- 

## 11. Kekurangan WLAN

- Keamanan lebih rentan dibanding LAN
  - Kecepatan dipengaruhi jarak & gangguan
  - Stabilitas lebih rendah dari kabel
- 

## Kesimpulan Inti Modul

WLAN memungkinkan koneksi jaringan tanpa kabel menggunakan standar IEEE 802.11, dengan komponen utama AP dan client, bekerja pada frekuensi 2.4 GHz dan 5 GHz, serta membutuhkan sistem keamanan yang baik agar data tetap aman.

### Mod17

## 1. Pengertian WAN

- **WAN (Wide Area Network)** adalah jaringan yang mencakup **area geografis luas** (antar kota, negara, benua).
  - Menghubungkan beberapa **LAN atau MAN**.
  - Biasanya menggunakan **infrastruktur milik ISP/penyedia layanan**.
- 

## 2. Perbedaan LAN vs WAN

- **LAN** → area kecil, kecepatan tinggi, milik sendiri

- **WAN** → area luas, kecepatan relatif lebih rendah, biaya lebih mahal, dikelola ISP
- 

### 3. Perangkat Utama WAN

- **Router** → menghubungkan jaringan lokal ke WAN
  - **Modem / CSU/DSU** → penghubung ke jaringan ISP
  - **WAN Interface** → port khusus WAN pada router
  - **Transmission Media** → kabel fiber, tembaga, radio, satelit
- 

### 4. Teknologi WAN Tradisional

Yang perlu kamu kenal:

- **Leased Line**
    - Koneksi dedicated (selalu aktif)
    - Mahal tapi stabil
  - **PSTN / Dial-up**
    - Menggunakan jaringan telepon
    - Lambat, sudah jarang digunakan
  - **ISDN**
    - Lebih cepat dari dial-up
    - Sekarang hampir tidak dipakai
- 

### 5. Teknologi WAN Modern

- **Frame Relay**
  - Packet-switched
  - Sudah mulai ditinggalkan
- **ATM (Asynchronous Transfer Mode)**
  - Sel data ukuran tetap
  - Kompleks, jarang digunakan
- **MPLS**
  - Cepat, efisien, banyak dipakai ISP

- Cocok untuk perusahaan besar
  - **Metro Ethernet**
    - Ethernet skala kota
    - Murah dan cepat
- 

## 6. WAN Berbasis Internet

- **DSL**
    - Menggunakan kabel telepon
  - **Cable Modem**
    - Menggunakan TV kabel
  - **Fiber Optic**
    - Sangat cepat dan stabil
  - **Wireless WAN**
    - Radio, microwave, seluler (4G/5G)
  - **Satellite WAN**
    - Jangkauan luas
    - Latensi tinggi
- 

## 7. Topologi WAN

- **Point-to-Point**
    - Dua lokasi langsung terhubung
  - **Hub-and-Spoke**
    - Satu pusat, banyak cabang
  - **Full Mesh**
    - Semua saling terhubung (mahal)
  - **Partial Mesh**
    - Kombinasi, lebih efisien
- 

## 8. Protokol WAN Penting

- **HDLC**
    - Default Cisco, efisien
  - **PPP**
    - Mendukung autentikasi (PAP, CHAP)
  - **PPPoE**
    - PPP di atas Ethernet (umum di ISP)
  - **GRE**
    - Tunneling
- 

## 9. Keamanan WAN

- **VPN (Virtual Private Network)**
    - Enkripsi data lewat internet
  - **IPSec**
    - Standar keamanan WAN
  - **SSL VPN**
    - Akses jarak jauh
- 

## 10. Kelebihan WAN

- Menghubungkan lokasi jauh
  - Mendukung operasional perusahaan besar
  - Akses data terpusat
- 

## 11. Kekurangan WAN

- Biaya tinggi
- Konfigurasi kompleks
- Ketergantungan pada ISP
- Latensi lebih besar dibanding LAN

## Mod18

### 1. Pengertian Network Management

- **Network Management** adalah proses mengelola, memantau, dan mengontrol jaringan agar berjalan optimal, stabil, dan aman.
  - Tujuan utama: **kinerja optimal, minim gangguan, dan layanan tetap tersedia.**
- 

### 2. Tujuan Network Management

- Menjaga ketersediaan jaringan (**availability**)
  - Meningkatkan **kinerja (performance)**
  - Menjamin **keamanan (security)**
  - Mengurangi downtime
  - Memudahkan troubleshooting
- 

### 3. FCAPS Model (Konsep Inti)

Ini bagian **PALING PENTING** dari modul ini:

- **F – Fault Management**
  - Deteksi & perbaikan gangguan
  - Alarm, log error
- **C – Configuration Management**
  - Konfigurasi perangkat
  - Backup & restore konfigurasi
- **A – Accounting Management**
  - Penggunaan resource
  - Billing & audit
- **P – Performance Management**
  - Monitoring bandwidth, latency, throughput
- **S – Security Management**
  - Kontrol akses
  - Proteksi dari serangan

❖ **FCAPS = fondasi manajemen jaringan**

---

## **4. Operation & Maintenance (O&M)**

- **Operation**
    - Aktivitas harian jaringan
    - Monitoring, provisioning, support user
  - **Maintenance**
    - Perawatan jaringan
    - Update, upgrade, perbaikan perangkat
- 

## **5. Jenis Maintenance**

- **Preventive Maintenance**
    - Pencegahan sebelum terjadi masalah
  - **Corrective Maintenance**
    - Perbaikan setelah terjadi gangguan
  - **Predictive Maintenance**
    - Berdasarkan analisis data/tren
- 

## **6. Network Monitoring**

- Mengawasi kondisi jaringan secara real-time
  - Parameter penting:
    - Bandwidth
    - Delay/latency
    - Packet loss
    - Jitter
    - CPU & memory perangkat
- 

## **7. Protokol & Tools Network Management**

- **SNMP (Simple Network Management Protocol)**

- Monitoring perangkat jaringan
  - **Syslog**
    - Pencatatan log sistem
  - **NetFlow**
    - Analisis trafik
  - **NMS (Network Management System)**
    - Contoh: Nagios, Zabbix, PRTG
- 

## 8. Troubleshooting Jaringan

Langkah umum:

1. Identifikasi masalah
  2. Tentukan sumber gangguan
  3. Isolasi masalah
  4. Perbaikan
  5. Dokumentasi
- 

## 9. Dokumentasi Jaringan

- Topologi jaringan
- IP addressing
- Konfigurasi perangkat
- SOP penanganan gangguan

📌 Dokumentasi = mempermudah O&M jangka panjang

---

## 10. Tantangan Network Management

- Jaringan semakin kompleks
  - Banyak perangkat & teknologi
  - Ancaman keamanan
  - Keterbatasan SDM
-

## Kesimpulan Inti Modul

Network Management dan O&M memastikan jaringan berjalan stabil melalui monitoring, pengelolaan konfigurasi, penanganan gangguan, dan keamanan, dengan FCAPS sebagai kerangka utama.

Mod19

### 1. Kenapa IPv6 Dibutuhkan

- **IPv4 habis** (alamat publik sudah exhausted sejak 2011).
  - IPv4 punya banyak keterbatasan: header kompleks, routing tidak efisien, ketergantungan ARP & NAT.
  - IPv6 dibuat untuk **menggantikan IPv4**, bukan sekadar upgrade.
- 

### 2. Keunggulan IPv6 dibanding IPv4

- **Alamat 128-bit** → hampir tak terbatas (cocok IoT, 5G).
  - **Hierarchical addressing** → routing lebih efisien.
  - **Plug-and-play (SLAAC)** → otomatis tanpa DHCP.
  - **Header sederhana (fixed 40 byte)** → forwarding lebih cepat.
  - **Keamanan bawaan (IPsec)**.
  - **Mendukung mobility & QoS (Flow Label)**.
  - **Tidak ada broadcast** (diganti multicast).
- 

### 3. Struktur Header IPv6

- Header dasar **tetap 40 byte**.
- Field penting:
  - Version
  - Traffic Class
  - Flow Label
  - Payload Length
  - Next Header
  - Hop Limit

- Source & Destination Address
  - Fitur tambahan pakai **Extension Header**, bukan opsi di header utama.
- 📌 Intinya: **lebih simpel & efisien dari IPv4**
- 

#### 4. Format Alamat IPv6

- Panjang **128 bit**, ditulis heksadesimal.
  - Dibagi **8 blok**, masing-masing 16 bit.
  - Contoh:  
2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64
- 

#### 5. Aturan Singkat Penulisan IPv6

- Nol di depan boleh dihapus.
  - Deretan nol bisa diganti :: (hanya sekali).
  - Huruf **tidak case-sensitive**.
  - Contoh:
    - 0000:0000:0000:0000:0000:0000:0001 → ::1
- 

#### 6. Jenis Alamat IPv6

##### a. Unicast (satu ke satu)

- **GUA (Global Unicast Address)**
  - Setara IP publik
  - Prefix: 2000::/3
- **ULA (Unique Local Address)**
  - Setara IP private
  - Prefix: FD00::/8
- **LLA (Link-Local Address)**
  - Wajib ada di tiap interface
  - Prefix: FE80::/10

##### b. Multicast

- Satu ke banyak
- Prefix: FF00::/8
- Digunakan untuk Neighbor Discovery, routing, dll

### c. Anycast

- Satu alamat, banyak perangkat
- Paket dikirim ke **node terdekat**

➔ **IPv6 tidak punya broadcast**

---

## 7. Struktur Alamat Unicast

- **Network Prefix** (biasanya 64 bit)
- **Interface ID** (64 bit)
- Interface ID bisa dibuat dengan:
  - Manual
  - Otomatis
  - **EUI-64 (paling umum)**

---

## 8. Neighbor Discovery Protocol (NDP)

- Pengganti ARP di IPv4.
- Menggunakan **ICMPv6**.
- Fungsi utama:
  - Address resolution
  - DAD (Duplicate Address Detection)
  - Prefix advertisement
  - SLAAC

ICMPv6 penting:

- RS (133)
- RA (134)
- NS (135)
- NA (136)

---

## 9. Duplicate Address Detection (DAD)

- Mengecek apakah alamat IPv6 **sudah dipakai atau belum**.
  - Wajib dilakukan sebelum alamat digunakan.
  - Menggunakan ICMPv6 NS & NA.
- 

## 10. Konfigurasi Alamat IPv6

- **Manual**
- **SLAAC (Stateless)**
  - Alamat otomatis dari RA
- **DHCPv6 (Stateful)**
  - Alamat dari server DHCPv6

📌 Satu interface bisa punya **lebih dari satu alamat IPv6**

---

## 11. Address Resolution IPv6

- Menggunakan **ICMPv6**, bukan ARP.
  - Mapping IPv6 ↔ MAC address.
  - Menggunakan **Solicited-node multicast address**.
- 

## 12. Konfigurasi Dasar IPv6 (Intinya)

- Aktifkan IPv6 global & interface
  - Konfigurasi LLA & GUA
  - Aktifkan RA untuk SLAAC
  - Konfigurasi static route IPv6 bila perlu
- 

## 13. Ringkasan Perbandingan IPv4 vs IPv6

- IPv6: 128 bit | IPv4: 32 bit
- IPv6: unicast, multicast, anycast | IPv4: broadcast masih ada
- IPv6: SLAAC + DHCPv6 | IPv4: DHCP

- IPv6: ICMPv6 | IPv4: ARP

## Mod20

### 1. Latar Belakang SDN & NFV

- Jaringan tradisional:
    - Konfigurasi manual
    - Perangkat proprietary (mahal)
    - Sulit diskalakan
  - SDN & NFV hadir untuk:
    - **Otomatisasi**
    - **Fleksibilitas**
    - **Efisiensi biaya**
- 

### 2. SDN (Software Defined Networking)

#### Pengertian

- SDN adalah arsitektur jaringan yang **memisahkan control plane dan data plane**.
  - Pengelolaan jaringan dilakukan secara **terpusat melalui software (controller)**.
- 

### 3. Arsitektur SDN

Terdiri dari 3 layer utama:

1. **Application Layer**
    - Aplikasi jaringan (monitoring, security, QoS)
  2. **Control Layer**
    - **SDN Controller** (otak jaringan)
    - Contoh: OpenDaylight, ONOS
  3. **Infrastructure Layer**
    - Switch/router fisik atau virtual
- 

### 4. Control Plane vs Data Plane

- **Control Plane**
  - Pengambilan keputusan routing/forwarding
- **Data Plane**
  - Forwarding paket aktual

📌 Di SDN: control plane **dipusatkan**

---

## 5. Protokol SDN

- **OpenFlow**
  - Protokol utama SDN
  - Controller ↔ switch
- Southbound API:
  - OpenFlow, NETCONF
- Northbound API:
  - REST API

---

## 6. Kelebihan SDN

- Konfigurasi cepat & otomatis
- Mudah dikelola
- Programmable network
- Vendor-neutral
- Skalabilitas tinggi

---

## 7. Kekurangan SDN

- Ketergantungan pada controller
- Isu keamanan controller
- Kompleksitas awal implementasi

---

## 8. NFV (Network Function Virtualization)

### Pengertian

- NFV adalah konsep **virtualisasi fungsi jaringan** yang sebelumnya berjalan di hardware khusus.
  - Fungsi dijalankan sebagai **software (VNF)** di server standar.
- 

## 9. Contoh Fungsi NFV

- Firewall
  - Load balancer
  - NAT
  - IDS/IPS
  - VPN
- 

## 10. Arsitektur NFV

Komponen utama:

- **VNF (Virtual Network Function)**
  - **NFVI (NFV Infrastructure)**
    - Server, storage, network
  - **MANO (Management and Orchestration)**
    - Orkestrasi & manajemen VNF
- 

## 11. Kelebihan NFV

- Hemat biaya hardware
  - Deployment cepat
  - Fleksibel & scalable
  - Mendukung cloud & data center modern
- 

## 12. Perbedaan SDN vs NFV

- **SDN**
  - Fokus pada **pengendalian trafik**
- **NFV**

- Fokus pada **virtualisasi fungsi jaringan**
  - Keduanya **saling melengkapi**, sering digunakan bersama.
- 

### 13. Use Case SDN & NFV

- Data center
  - Cloud computing
  - 5G networks
  - Enterprise networks
  - ISP & telco
- 

### Kesimpulan Inti Modul

SDN memisahkan control dan data plane untuk jaringan yang programmable dan terpusat, sedangkan NFV memvirtualisasi fungsi jaringan agar lebih fleksibel, efisien, dan scalable.

Mod21

#### 1. Masalah & Solusi

- **Masalah O&M Manual:** Lambat, tidak efisien pada ribuan perangkat, dan sulit diaudit.
- **Solusi Otomasi:** Menggunakan skrip (Python) atau alat seperti Ansible/Chef untuk mengurangi kerja manual.

#### 2. Tentang Python

- **Status:** Bahasa tingkat tinggi, *open-source*, dan mudah dipelajari (*elegant syntax*).
- **Cara Kerja:** Jenis *interpreted language* (dijalankan baris demi baris via PVM).
- **Kelemahan:** Eksekusi lebih lambat dibanding bahasa *compiled* seperti C/C++.

#### 3. Aturan Penulisan (Python Style)

- **Indentasi:** Wajib benar (disarankan 4 spasi) karena menentukan struktur blok kode.
- **Penamaan (Identifier):** Tidak boleh diawali angka dan bersifat *case sensitive*.
- **Komentar:** Gunakan # untuk satu baris atau "" untuk banyak baris.

#### 4. Modul telnetlib (Alat Utama)

- **Fungsi:** Modul standar Python untuk mengontrol perangkat jaringan via Telnet.

- **Perintah Penting:**
    - `read_until()`: Menunggu teks tertentu muncul (misal: "Password:").
    - `write()`: Mengirim perintah ke perangkat.
    - `close()`: Memutuskan koneksi.

## 5. Alur Praktik

- **Langkah:** Konfigurasi IP & Telnet di perangkat -> Buat skrip Python -> Jalankan skrip untuk kirim perintah otomatis.

Mod22

## **1. Apa itu Jaringan Kampus?**

- **Definisi:** Jaringan area lokal (LAN) yang menghubungkan orang dan benda dalam area tertentu (kantor, sekolah, mall) dengan satu entitas manajemen<sup>111</sup>.
  - **Arsitektur Umum:** Dirancang secara hierarkis (berlapis) dan modular<sup>2</sup>.

## **2. Klasifikasi Jaringan Kampus**

Jenis	Jumlah Terminal	Arsitektur
<b>Kecil</b>	< 200	Sederhana, biasanya satu lokasi <sup>5555</sup> .
<b>Menengah</b>	200 - 2000	Tiga lapis: <i>Core, Aggregation, Access</i> <sup>6666</sup> .
<b>Besar</b>	> 2000	Kompleks, mencakup banyak gedung/cabang <sup>777777777</sup> .

3.

### Siklus Hidup Proyek (Lifecycle)<sup>8</sup>

1. **Planning & Design:** Pemilihan model perangkat, topologi fisik/logis, dan protokol<sup>9</sup>.
  2. **Deployment:** Instalasi perangkat, komisioning (uji coba), dan migrasi<sup>10101010</sup>.
  3. **Network O&M:** Pemeliharaan rutin, backup konfigurasi, dan monitoring terpusat<sup>11</sup>.
  4. **Optimization:** Peningkatan keamanan dan pengalaman pengguna<sup>12</sup>.

#### **4. Desain Penting dalam Jaringan**

- **DHCP:** Untuk pengguna akhir (*end users*)<sup>16161616</sup>.
- **Routing:** Jaringan kecil cukup menggunakan **Static Route** tanpa protokol routing kompleks<sup>17171717</sup>.
- **Reliability:** Gunakan **Eth-Trunk** untuk meningkatkan bandwidth dan keandalan link antar switch<sup>18</sup>.

## 5. Keamanan & Manajemen

- **Egress NAT:** Menggunakan **Easy IP** jika IP publik dari ISP diberikan secara dinamis<sup>19191919</sup>.
- **DHCP Snooping:** Mencegah adanya router liar (*unauthorized routers*) yang menyebabkan konflik IP<sup>20</sup>.
- **Manajemen Perangkat:** Bisa melalui Web, SSH/Telnet, atau sistem terpusat seperti **Huawei iMaster NCE**<sup>21212121</sup>.