

## BAB 5 IMPLEMENTASI

Pada bab ini akan dibahas tentang mengimplementasikan autentikasi mode *multi-auth* pada jaringan *local area network* berbasis kabel menggunakan protokol IEEE 802.1X dan RADIUS Server. Implementasi merupakan proses realisasi dari perancangan sistem yang telah dirancang sebelumnya.

### 5.1 Sistem Keamanan Autentikasi Menggunakan Protokol IEEE 802.1X

Konfigurasi menggunakan Protected Extensible Authentication Protokol (PEAP) dengan Microsoft Challenge Handshake Authentication Protokol (MS-CHAP) version 2 di jaringan berbasis kabel dengan Microsoft Network Policy Server (NPS) sebagai Radius Server.

Kebutuhan komponen untuk mengimplementasikan *prototype* ini adalah:

- Windows 2008 Enterprise Server dengan layanan Active Directory (AD), Certificate Authority (CA), Dynamic Host Control Protokol (DHCP), Domain Name System (DNS) dan Network Policy Server (NPS).
- *Managed Switch* Cisco Catalyst yang support protokol IEEE 802.1X.
- Microsoft Windows 10 sebagai *Supplicant* atau *suplicant*.

### 5.2 Konfigurasi Microsoft Windows Server 2008 R2

- Konfigurasi Active Directory Domain Services (ADDS) sebagai Active Directory.
- Konfigurasi Domain Name Service (DNS) Server untuk menterjemahkan domain name ke alamat IP dan juga sebaliknya.
- Konfigurasi Dynamic Host Control Protokol (DHCP) server untuk memberikan alamat IP kepada *supplicant* atau pengguna jaringan local berbasis kabel.
- Konfigurasi Certificate Authority (CA). Metode PEAP dengan MS-CHAP v2 memvalidasi server RADIUS berdasarkan sertifikat yang ada di server.
- Konfigurasi Network Policy Server (NPS) yang digunakan sebagai server RADIUS untuk mengautentikasi *supplicant* berbasis kabel dengan autentikasi Metode PEAP – MSCHAPv2.

### 5.3 Konfigurasi Protokol IEEE 802.1X dengan Mode Multi-Auth

- Peangaktifan AAA (Authentication, Authorization, *Accounting*) dan 802.1X pada Switch dan dialihkan ke radius server.
- VLAN yang akan digunakan untuk pemberian hak akses autentikasi.
- Alamat IP *interface* VLAN 10 untuk *supplicant* yang autentikasi menggunakan kredensial grup “user”.
- Alamat IP *interface* VLAN 30 untuk grup “Guest” dan konfigurasi DHCP Relay pada VLAN 30.
- Pengaktifan 802.1X di Switch.

- Konfigurasi port berbasis autentikasi 802.1X pada salah satu port switch.

#### **5.4 Aktivasi Protokol IEEE 802.1X pada *Supplicant***

- *Wired AutoConfig* digunakan untuk mendeteksi dan melakukan koneksi ke jaringan berbasis kabel.
- Mode autentikasi berdasarkan “user or computer authentication”
- Metode autentikasi jaringan menggunakan metode PEAP-MSCHAPv2.

Konfigurasi radius server, switch dan *supplicant* sudah selesai maka proses implementasi autentikasi mode *multi-auth* pada jaringan *local area network* berbasis kabel menggunakan protokol IEEE 802.1X dan RADIUS Server siap digunakan. Untuk langkah – langkah pengimplementasian secara lengkap dalam bab ini dapat dilihat pada bagian LAMPIRAN.