Jurnal CKI On SPOT p-ISSN 1979-7044
Vol. 18, No. 1, Desember 2025, Hal. 18-28 e-ISSN 2598-2990

Implementasi High Availability dan Kemanan Jaringan Fabric Menggunakan BGP EVPN VXLAN Pada Infrastruktur Multi-Lokasi Menggunakan DCLOUD CISCO SIMULATOR

Yuma Akbar[1], **Mesra Betty Yel**[2], **Mohammad Royger Febriansyah Putra**[3]
[1] Teknik Informatika, St Ilmu Komputer Cipta Karya Informatika
[2] Sistem Informasi, St Ilmu Komputer Cipta Karya Informatika
[3]Teknik Informatika, St Ilmu Komputer Cipta Karya Informatika
*Email: yumakhan@stikomcki.ac.id, mesrabettyyel@stikomcki.ac.id, royger.febriansyah@stikomcki.ac.id.

Abstrak

Perkembangan teknologi jaringan menuntut solusi yang memberikan kesederhanaan desain dan operasi sekaligus fleksibilitas dalam pengelolaan infrastruktur. Arsitektur jaringan berbasis fabric memungkinkan pembuatan segmen jaringan logis yang independen dari topologi fisik dan pengalamatan, sehingga memudahkan skalabilitas dan pengelolaan. BGP EVPN VXLAN merupakan teknologi standar yang menggabungkan Border Gateway Protocol (BGP) dan Ethernet Virtual Private Network (EVPN) dengan Virtual Extensible LAN (VXLAN) untuk mendukung komunikasi efisien dan skalabel antar perangkat dalam jaringan. Teknologi ini memungkinkan pembuatan jaringan Layer 2 datar yang luas, mendukung mobilitas host, segmentasi jaringan, dan pengelolaan terpusat .Studi ini mengkaji penerapan BGP EVPN VXLAN dalam arsitektur spine-leaf dua lapis yang mengoptimalkan routing, forwarding, serta integrasi kebijakan keamanan dengan memperhatikan high availability. Melalui lab praktikum, aspek pembuatan overlay jaringan, segmentasi Layer 2 dan Layer 3, serta konektivitas fabric dengan jaringan eksternal dipelajari sebagai dasar pengembangan Campus Catalyst BGP EVPN Fabrics. Hasil penelitian ini memberikan wawasan tentang efisiensi, fleksibilitas, dan skalabilitas arsitektur fabric berbasis BGP EVPN VXLAN dalam mendukung kebutuhan jaringan yang memiliki keamanan dan high availability. Selain itu, pemanfaatan platform virtualisasi Hyper Virtual dCloud Cisco digunakan sebagai lingkungan laboratorium untuk menguji skenario multi-lokasi secara realistis.

Kata kunci: BGP EVPN VXLAN, High Availability, Keamanan, Jaringan Multi-Lokasi.

Abstract

The development of networking technology demands solutions that provide simplicity of design and operation while also offering flexibility in infrastructure management. Fabric-based network architecture enables the creation of logical network segments that are independent of physical topology and addressing, thus facilitating scalability and management. BGP EVPN VXLAN is a standard technology that combines Border Gateway Protocol (BGP) and Ethernet Virtual Private Network (EVPN) with Virtual Extensible LAN (VXLAN) to support efficient and scalable communication between devices in the network. This technology enables the creation of large, flat Layer 2 networks, supporting host mobility, network segmentation, and centralized management. This study examines the implementation of BGP EVPN VXLAN in a two-tier spine–leaf architecture that optimizes routing, forwarding, and the integration of security policies while taking high availability into account. Through laboratory practice, aspects such as building network overlays, Layer 2 and Layer 3 segmentation, and fabric connectivity with external networks are studied as a basis for developing Campus Catalyst BGP EVPN Fabrics. The results of this research provide insight into the efficiency, flexibility, and scalability of BGP EVPN VXLAN–based fabric architecture in supporting network requirements that demand security and high availability. In addition, the use of Cisco's Hyper Virtual dCloud virtualization platform is employed as a laboratory environment to realistically test multi-location scenarios.

Keywords: *BGP EVPN VXLAN, High Availability, Security, Multi-Location Network*

PENDAHULUAN

Kebutuhan akan solusi yang tangguh, skalabel, efisien dan memperhatikan keamanan sangat penting dalam domain infrastruktur jaringan yang terus berkembang. *Virtual Extensible LAN* (VXLAN) telah muncul sebagai teknologi penting dalam mengatasi kompleksitas lingkungan jaringan modern, terutama di *data center* dan *cloud computing*. Kemampuan VXLAN untuk memungkinkan lebih banyak segmentasi jaringan skala luas dan mengatasi keterbatasan VLAN pada jaringan tradisional yang menjadikannya komponen penting dalam arsitektur jaringan kontemporer. Arsitektur berbasis *fabric* ini sangat ideal dengan menawarkan keseimbangan optimal antara kinerja *routing* dan *forwarding*, sekaligus memungkinkan integrasi keamanan dan kebijakan sebagai aspek fundamental dalam desain. BGP EVPN VXLAN adalah teknologi jaringan standar yang populer, yang menggabungkan *Border Gateway Protocol* (BGP) dan *Ethernet Virtual Private Network* (EVPN) dengan *Virtual Extensible Local Area Network* (VXLAN) untuk menyediakan komunikasi yang skalabel dan efisien antar perangkat dalam jaringan. Seperti yang kita ketahui keamanan jaringan telah menjadi tantangan utama bagi organisasi di era digital, maka dari itu VXLAN menyediakan segmentasi jaringan yang dapat mengisolasi berbagai *department* atau kelompok pengguna sekaligus berbagi infrastruktur fisik yang sama. Hal ini meningkatkan keamanan dan mengurangi potensi masalah jaringan serta memberikan *benefit mobility support* dengan adanya EVPN. Mekanisme ini untuk mendukung mobilitas user, memungkinkan perangkat berpindah ke Lokasi manapun tanpa perlu mengubah *IP Address*. Dan untuk menerapkan BGP EVPN VXLAN ini kita perlu menggunakan topologi *spine-leaf* yang mana topologi ini sudah memperhatikan *high availability* untuk endpoint ketika terjadi *failure* di salah satu kabel fisik pada perangkat jaringan. Dengan demikian, VXLAN menawarkan solusi yang tepat untuk masalah konektivitas antar jaringan di lokasi yang berbeda (Do Abdullah et al., n.d.). Hal ini memudahkan pengelolaan dan penskalaan infrastruktur jaringan sekaligus mengatasi permasalahan jaringan berbasis Spanning Tree lama dengan lebih baik. Pendekatan ini dirancang untuk menyediakan solusi jaringan *overlay* terpadu serta mengatasi tantangan dan kekurangan teknologi yang ada. Pada penelitian ini menggunakan metode virtualisasi dengan bantuan Dcloud Cisco Simulator. Tujuan Penelitian ini adalah untuk menciptakan *environment* jaringan *fabric* yang memperhatikan *High-Availability* serta memiliki keamanan.

TINJAUAN PUSTAKA

Analisis dan Perancangan *Virtual Extensible Local Area Network* (VXLAN) untuk Interkoneksi Lokasi yang berbeda di Universitas Khairun bertujuan untuk menciptakan lingkungan jaringan dalam satu koneksi meskipun berada di lokasi yang berbeda. Selain itu, evaluasi kinerja VXLAN saat mengatasi hambatan geografis akan menjadi fokus penelitian, memberikan wawasan yang berguna bagi para pengambil keputusan dalam hal efisiensi dan keamanan. Penelitian tentang Analisis dan Perancangan Virtual Extensible Local Area Network (VXLAN) untuk Interkoneksi Lokasi yang Berbeda di Universitas Khairun bertujuan untuk menciptakan lingkungan jaringan dalam satu koneksi meskipun dalam lokasi yang berbeda (Do Abdullah et al., n.d.).

Virtual Extensible Local Area Network (VXLAN) adalah sebuah virtualisasi lapisan OSI kedua yang membentuk suatu *Ethernet frame* menjadi paket *User Datagram Protocol* (UDP) yang terdaftar pada implementasi RFC 7348 (Fitra Diraja et al., 2025).

VXLAN menggunakan header berukuran 8 byte yang memiliki pengenal 24-bit (VNID) beserta beberapa bit cadangan. Header VXLAN ini disisipkan ke dalam payload UDP bersama dengan *frame* Ethernet asli. VNID 24-bit berperan penting dalam mengidentifikasi segmen Layer 2 dan menjaga isolasi antar segmen tersebut. Dengan alokasi 24-bit untuk VNID, VXLAN dapat mendukung hingga 16 juta segmen logis (Arfan Efendi et al., 2023).

Keamanan jaringan telah menjadi tantangan utama bagi organisasi di era digital. Peningkatan jumlah perangkat yang terhubung ke jaringan, termasuk perangkat *Internet of Things* (IoT), serta ancaman siber yang semakin canggih, telah mendorong para peneliti dan praktisi untuk mencari pendekatan keamanan

baru yang lebih efektif. Model keamanan tradisional, yang mengandalkan perimeter-based defens, telah terbukti tidak mampu melindungi jaringan dari serangan yang datang dari dalam, seperti serangan yang dilakukan oleh pihak dalam (*insider threats*), maupun serangan eksternal yang berhasil menembus perimeter (Kusnanto et al., 2024).

Terminologi utama yang digunakan untuk menggambarkan komponen kunci teknologi VXLAN adalah sebagai berikut: *Virtual Tunnel Endpoint* (VTEP): Elemen perangkat keras atau perangkat lunak (Hypervisor) yang bertugas membentuk tunneling VXLAN serta melakukan proses *enkapsulasi* dan *de-enkapsulasi*. Juga dikenal sebagai *LEAF*. VNI (*Virtual Network Instance*): Instance jaringan logis yang menyediakan layanan L2 atau L3 dan mendefinisikan domain siar (*broadcast domain*) layer 2. VNID (*Virtual Network Identifier*): Pengidentifikasi 24-bit yang memungkinkan hingga 16 juta jaringan logis. *Bridge-Domain*: Sekumpulan port fisik atau logis yang berbagi domain siar yang sama. *SPINE*: Perangkat yang menghubungkan antar VTEP (Naranjo & Salazar Ch. Gustavo D, 2017).

Teknologi VXLAN, sangat berguna dengan berbagai keunggulan dibandingkan VLAN. Hal ini tidak hanya terbatas pada kemampuan untuk menempatkan segmen multi-tenant di seluruh *data center* secara fleksibel, tetapi juga lebih mudah diskalakan karena cakupan segmen VXLAN yang luas dan, yang paling penting, pemanfaatan sumber daya jaringan yang tersedia pada infrastruktur underlay secara efisien (Fadokun, 2025).
Meskipun VXLAN menentukan mekanisme enkapsulasi dan penerusan untuk *packet overlay*, teknologi ini tidak menyediakan cara yang sistematis bagi perangkat untuk mempelajari lokasi alamat MAC atau IP. Fungsi tersebut ditangani oleh BGP EVPN, yang berperan sebagai control plane bagi segmen VXLAN. Alih-alih meneruskan paket begitu saja hingga menemukan tujuan, EVPN membagikan pasangan alamat melalui pengumuman rute terstruktur dan bersifat inkremental—sebuah proses yang meningkatkan konsistensi data dan ketepatan routing di seluruh sistem terdistribusi, mirip dengan mekanisme konsistensi yang digunakan pada basis data terdistribusi seperti MongoDB (12, 13). Tiga tipe rute yang paling penting. Tipe Rute 2 membawa pemetaan alamat MAC dan, secara opsional, alamat IP overlay, sehingga VTEP jarak jauh dapat memuat tabel penerusannya dengan ketergantungan minimum pada flooding. Tipe Rute 5 mengiklankan prefiks IP, sehingga memungkinkan routing antar-subnet di dalam domain siar yang diperluas yang dibentuk oleh *overlay*. Terakhir, Tipe Rute 6 meneruskan informasi grup *multicast*, memungkinkan fabric mengarahkan aliran data pasar dan harga secara cerdas hanya ke pihak-pihak yang berkepentingan (20). Secara keseluruhan, mekanisme ini mengurangi chatter yang tidak perlu pada *control plane*, mengurangi *flooding* pada *data plane*, dan mempercepat konvergensi—atribut yang penting pada jaringan apa pun, tetapi menjadi sangat krusial ketika latensi dalam hitungan milidetik dan pengiriman paket yang deterministik menjadi penentu kualitas layanan (Chandra Jha, 2025).

METODOLOGI PENELITIAN

3.1 Data Penilitian

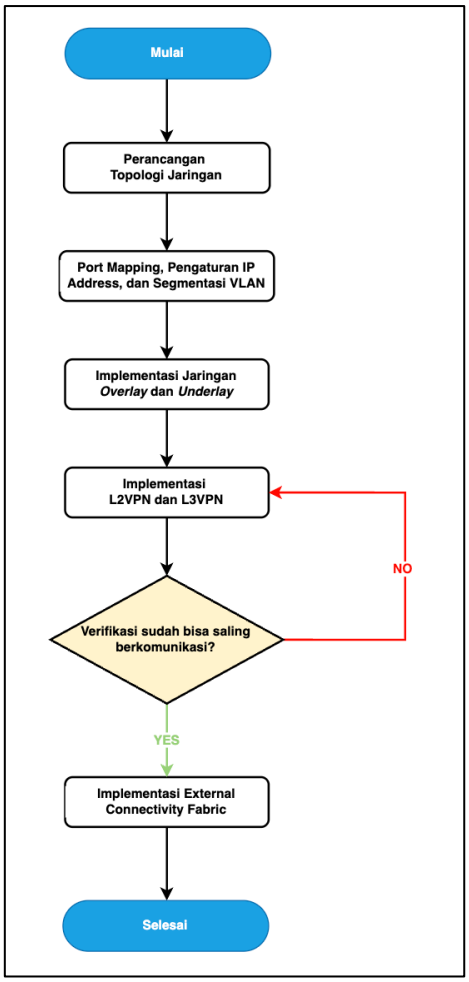
Penelitian ini dibuat oleh penulis menggunakan pendekatan ujicoba yang dilakukan secara sistematis atau bisa disebut eksperimen terapan berbasis simulasi virtual, dengan membuat topologi jaringan menggunakan Dcloud Cisco sebagai platform simulasi. Pada Dcloud Cisco, penulis menggunakan *node BETA CAT9000V S1* untuk melakukan pengujian serta konfigurasi Implementasi *High Availability* dan Keamanan Jaringan *Fabric* Menggunakan *BGP EVPN VXLAN* pada Infrastruktur Multi-Lokasi menggunakan *Dcloud Cisco* Simulator.

Dengan Penilitian ini penulis berharap dapat memberikan gambaran yang menyeluruh kepada pembaca mengenai Implementasi *High Availability* dan Keamanan menggunakan BGP EVPN VXLAN pada infrastruktur *Multi-Lokasi*.

3.2 Penerapan Metodologi

Pada penelitian ini penilitian metodologi yang digunakan oleh penulis adalah eksperimen terapan. Eksperimen ini dilakukan melalui tahapan konfigurasi dan simulasi yang menggambarkan implementasi nyata high availability dan keamanan menggunakan BGP EVPN VXLAN. Untuk detail tahapan pengerjaannya adalah sebagai berikut:

p-ISSN 1979-7044
e-ISSN 2598-2990



Gambar 1 Penerapan Metodologi

3.2.1 Perancangan Topologi Jaringan

Pada tahap awal, perancangan topologi spine-leaf dilakukan secara virtual menggunakan platform dcloud Cisco. Topologi ini terdiri dari switch BETA CAT9000V S1 yang berperan sebagai spine, leaf, dan leaf border. Selain itu, terdapat beberapa node Ubuntu yang berfungsi sebagai endpoint untuk pengujian yang akan mewakili kelompok IT Team Endpoint, Employee Endpoint, Public App Server, dan IT App Server yang nantinya seluruh endpoint tersebut akan diisolasi dalam jaringan fabric. Perancangan ini memungkinkan simulasi yang realistis terhadap kondisi jaringan real tanpa memerlukan perangkat fisik.

3.2.2 Port Mapping, Pengaturan IP Address dan Segmentasi VLAN

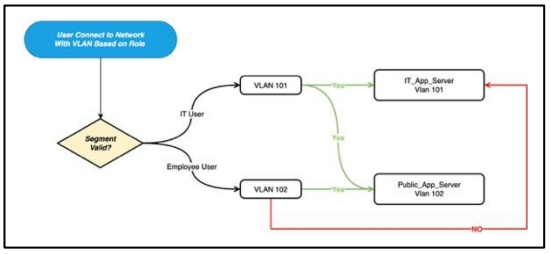
Pada tahap selanjutnya, dilakukan port mapping antar node topologi *spine-leaf*. Selain *port mapping* dan *IP address* pada topologi *spine-leaf* kita juga perlu konfigurasi segmentasi VLAN menuju ke endpoint pada topologi *spine-leaf* untuk mengelompokkan IT User, Employee User, Public App Server dan IT App Server.

3.2.3 Implementasi Jaringan Underlay dan Overlay

Setelah proses sebelumnya sudah dikonfigurasi kita lanjukan untuk konfigurasi jaringan *underlay* dan jaringan *overlay*. Tujuannya pada step ini adalah untuk menghubungkan setiap *IP Loopback* pada setiap perangkat yang mana nantinya kita akan membangun jaringan *overlay* menggunakan IP Loopback. Jaringan *underlay* dibangun dari oleh *routing* yang *routing* OSPF dan pada jaringan *overlay* kita menggunakan *Internal* BGP. Pada step ini setiap endpoint yang memiliki VLAN yang sama pada jaringan *multi-lokasi* masih saling terisolasi.

3.2.4 Implementasi L2VPN dan L3VPN

Implementasi Jaringan L2VPN ini kita akan konfigurasi EVPN Layer 2 antar jaringan multi-lokasi. Tujuan konfigurasi L2VPN adalah untuk menghubungkan endpoint yang memiliki VLAN yang sama pada jaringan yang berbeda Lokasi dapat saling berkomunikasi. Impementasi Jaringan L3VPN ini kita akan konfigurasi EVPN Layer 3 antar jaringan multi-lokasi. Tujuan konfigurasi L3VPN adalah untuk menghubungkan endpoint yang memiliki VLAN yang berbeda pada jaringan yang berbeda Lokasi dapat saling berkomunikasi. Pada tahap ini kita memiliki tujuan agar VLAN sama yang berbeda lokasi bisa saling berkomunikasi, dan IT-Endpoint bisa berkomunikasi ke public-server-app.



Gambar 2 Flowchart Use-Case L2VPN dan L3VPN

3.2.5 Implementasi External Connectivity Fabric

Menambahkan *external connectivity* ke fabric memungkinkan pertukaran rute dengan jaringan yang terhubung ke external jaringan. Konektivitas external memperluas jangkauan ke jaringan *overlay* Layer 2 atau Layer 3 di luar jaringan VXLAN. Proses memperluas jaringan Layer 2 atau Layer 3 di luar jaringan EVPN VXLAN juga dikenal sebagai handoff. Dalam fabric BGP EVPN VXLAN, konektivitas eksternal biasanya dicapai dengan menggunakan VTEP (VXLAN Tunnel Endpoints) di *edge* jaringan untuk meneruskan rute ke jaringan eksternal Layer 2 atau Layer 3. Hal ini memungkinkan komunikasi antara perangkat di dalam fabric VXLAN dan perangkat atau jaringan di luarnya.

3.3 Rancangan Pengujian

Perlu dilakukan pengujian agar *Research Problem* dan *Research Objective* yang disusun oleh penulis bisa terbukti. Tujuan Pengujian adalah untuk membuktikan bahwa Implementasi *High Availability* dan Keamanan pada jaringan *fabric* menggunakan BGP EVPN VXLAN pada infrastruktrur *multi-lokasi* bisa diterapkan, serta melakukan evaluasi beberapa kekurangan yang ada pada penelitian. Berikut adalah beberapa pengujian yang dilakukan oleh penulis:

3.3.1 Pengujian endpoint dengan VLAN Sama Terisolasi

Pengujian ini untuk memberikan bukti bahwa *by default* jaringan *fabric* ketika menjalankan konfigurasi BGP EVPN VXLAN, endpoint jika berjalan dengan VLAN yang sama namun berbeda lokasi tidak bisa saling berkomunikasi dan tidak bisa saling akses terkecuali dari team administrator jaringan memberikan *authorization*.

3.3.2 Pengujian Authorization Antar Endpoint

Pengujian ini digunakan untuk memberikan *authorization* akses antar endpoint pada jaringan infrastruktur *multi-lokasi* sehingga endpoint dapat saling berkomunikasi satu sama lain baik yang memiliki VLAN yang sama maupun VLAN yang berbeda. Selain itu pada tahap ini kita juga akan memberikan *authorization* pada endpoint agar bisa akses ke luar jaringan *fabric* seperti ke internet.

3.3.3 Pengujian High Availability

Pengujian ini bertujuan untuk membuktikan topologi *spine-leaf* sudah memperhatikan aspek *high availability* yang mana aspek ini sangat diperlukan pada jaringan modern. Untuk pengujiannya kita akan mencoba cabut salah satu *link leaf* ke *spine* untuk membuktikan traffic antar endpoint yang berbeda lokasi masih bisa saling berkomunikasi.

HASIL DAN PEMBAHASAN

4.1 Alat Penilitian

Pada Proses Penelitian, penulis menggunakan *hardware* dan *software* ketika melakukan konfigurasi dan testing. Berikut adalah *hardware* dan *software* yang digunakan oleh penulis,

Tabel 1. Spesifikasi Hardware

No	Jenis	Spesifikasi
1	Laptop	Macbook Air, M4 Chip, RAM 16 GB, Storage 256 GB

Tabel 2. Spesifikasi Software

No	Jenis	Spesifikasi
1	Google Chrome	Version 143.0.7499.41 (Official Build) (arm64)
2	Cisco Secure Client	Version 5.1.8.122

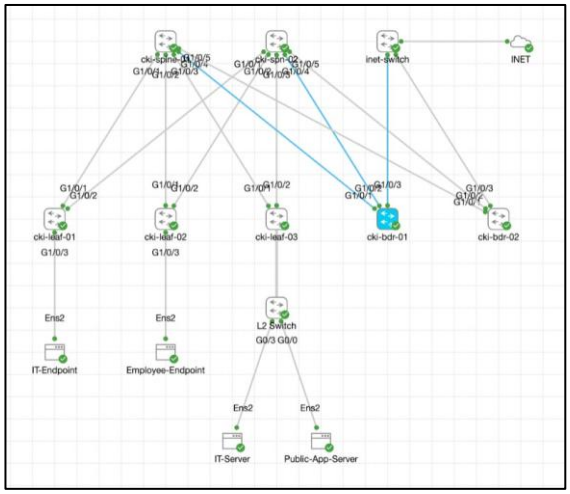
4.2 Implementasi dan Pengujian

Pada tahap implementasi dan pengujian disusun berdasarkan metodologi yang sudah di susun penulis yang meliputi perancangan topologi jaringan, *port mapping*, pengaturan *IP Address*, segmentasi VLAN, implementasi jaringan *underlay* dan *overlay*, implementasi L2VPN dan L3VPN, dan implementasi *external connectivity* BGP EVPN VXLAN Fabric.

4.2.1 Perancangan Topologi Jaringan

Pada tahap pertama, membuat perancangan topologi jaringan virtual menggunakan DCloud Cisco Simulator. Topologi yang digunakan adalah topologi *spine-leaf* yang dirancang untuk menerapkan *high*

availability dan keamanan jaringan fabric pada infrastruktur *multi-lokasi* yang memanfaatkan BGP EVPN VXLAN.



Gambar 3 Rancangan Topologi

4.2.2 Port Mapping, Pengaturan IP Address dan Segmentasi VLAN

Untuk memudahkan pembaca, Rincian *port mapping*, pengaturan *IP Address* dan Segmentasi VLAN sudah penulis susun. Untuk port mapping dan pengaturan *IP Address* terlampir Gambar 4 sebagai berikut,

No	Source Device	Source Port	Source IP	Destination Device	Destination Port	Destination IP
1	cki-leaf-01	Gi1/0/1	198.18.1.2/30	cki-spine-01	Gi1/0/1	198.18.1.1/30
2	cki-leaf-01	Gi1/0/2	198.18.1.6/30	cki-spine-02	Gi1/0/1	198.18.1.5/30
3	cki-leaf-01	Gi1/0/3	-	IT_Endpoint	Ens2	198.18.101.2/24
4	cki-leaf-01	lo0	10.10.10.1/32	-	-	-
5	cki-leaf-01	lo1	10.10.10.101/32	-	-	-
6	cki-leaf-02	Gi1/0/1	198.18.2.2/30	cki-spine-01	Gi1/0/2	198.18.2.1/30
7	cki-leaf-02	Gi1/0/2	198.18.2.6/30	cki-spine-02	Gi1/0/2	198.18.2.5/30
8	cki-leaf-02	Gi1/0/3	-	Employee-endpoint	Ens2	198.18.101.3/24
9	cki-leaf-02	lo0	10.10.10.2/32	-	-	-
10	cki-leaf-02	lo1	10.10.10.102/32	-	-	-
11	cki-leaf-03	Gi1/0/1	198.18.3.2/30	cki-spine-01	Gi1/0/3	198.18.3.1/30
12	cki-leaf-03	Gi1/0/2	198.18.3.6/30	cki-spine-02	Gi1/0/3	198.18.3.5/30
13	cki-leaf-03	Gi1/0/3	-	L2 Switch	G0/1	-
14	cki-leaf-03	Gi1/0/4	-	L2 Switch	G0/2	-
15	cki-leaf-03	lo0	10.10.10.3/32	-	-	-
16	cki-leaf-03	lo1	10.10.10.103/32	-	-	-
17	cki-bdr-01	Gi1/0/1	198.18.4.2/30	cki-spine-01	Gi1/0/4	198.18.4.1/30
18	cki-bdr-01	Gi1/0/2	198.18.4.6/30	cki-spine-02	Gi1/0/4	198.18.4.5/30
19	cki-bdr-01	Gi1/0/3		inet-switch	Port0	
20	cki-bdr-01	lo0	10.10.10.4/32	-	-	-
21	cki-bdr-01	lo1	10.10.10.104/32	-	-	-
22	cki-bdr-02	Gi1/0/1	198.18.5.2/30	cki-spine-01	Gi1/0/5	198.18.5.1/30
23	cki-bdr-02	Gi1/0/2	198.18.5.6/30	cki-spine-02	Gi1/0/5	198.18.5.5/30
24	cki-bdr-02	Gi1/0/3		inet-switch	Port1	
25	cki-bdr-02	lo0	10.10.10.5/32	-	-	-
26	cki-bdr-02	lo1	10.10.10.105/32	-	-	-
27	L2 Switch	G0/0	-	Pub-App-Server	Ens2	198.18.102.3/24
28	L2 Switch	G0/3	-	IT Server	Ens2	198.18.101.3/24
29	inet-switch	Port2	-	INET	Port	Bridge

Gambar 4 Port Mapping IP Address

No	Vlan	Network	Gateway IP	Endpoint	IP Address
1	101	198.18.101.0/24	198.18.101.1	IT-Endpoint	198.18.101.2/24
				IT App Server	198.18.101.3/24
2	102	198.18.102.0/24	198.18.102.1	Employee-Endpoint	198.18.102.2/24
				Public App Server	198.18.102.3/24

Gambar 5 Segmentasi VLAN

4.2.3 Implementasi Jaringan Underlay dan Overlay

Implementasi Jaringan *Underlay* dilakukan untuk *IP loopback* dapat saling terhubung antar *node fabric* dengan menerapkan *routing ospf* dan mendaftarkan *IP Loopback* kedalam *routing ospf* selaku *routing* untuk *jaringan underlay*. Pada tabel 3 adalah konfigurasi *routing ospf* dan *advertise IP loopback* dan *IP physical interface* ke *routing ospf*,

Tabel 3 Konfigurasi Jaringan Underlay

cki-leaf-01

```
!
router ospf 1
 router-id 10.10.10.1
!
interface  GigabitEthernet1/0/1
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface  GigabitEthernet1/0/2
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface Loopback0
  ip ospf 1 area 0
!
interface Loopback1
  ip ospf 1 area 0
```

Ulangi konfigurasi *underlay* diatas pada node lain sesuai dengan *interface* dan *IP Address* yang terlampir pada gambar 4.

Tabel 4 Konfigurasi Jaringan Overlay

cki-spine-01

```
router bgp 65000
 template peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  route-reflector-client
  soft-reconfiguration inbound
  send-community both
 exit-peer-policy
 bgp router-id 10.10.10.6
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.10.10.1 remote-as 65000
 neighbor 10.10.10.1 description *to cki-leaf-01*
 neighbor 10.10.10.1 update-source Loopback0
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 description *to cki-leaf-02*
 neighbor 10.10.10.2 update-source Loopback0
 neighbor 10.10.10.3 remote-as 65000
 neighbor 10.10.10.3 description *to cki-leaf-03*
 neighbor 10.10.10.3 update-source Loopback0
 neighbor 10.10.10.4 remote-as 65000
 neighbor 10.10.10.4 description *to cki-bdr-01*
 neighbor 10.10.10.4 update-source Loopback0
 neighbor 10.10.10.5 remote-as 65000
 neighbor 10.10.10.5 description *to cki-bdr-02*
 neighbor 10.10.10.5 update-source Loopback0
 neighbor 10.10.10.7 remote-as 65000
 neighbor 10.10.10.7 description *to cki-spine-02*
 neighbor 10.10.10.7 update-source Loopback0

 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  bgp nexthop trigger delay 0
  neighbor 10.10.10.1 activate
  neighbor 10.10.10.1 send-community both
  neighbor 10.10.10.1 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.2 activate
  neighbor 10.10.10.2 send-community both
  neighbor 10.10.10.2 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.3 activate
  neighbor 10.10.10.3 send-community both
  neighbor 10.10.10.3 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.4 activate
  neighbor 10.10.10.4 send-community both
  neighbor 10.10.10.4 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.5 activate
  neighbor 10.10.10.5 send-community both
  neighbor 10.10.10.5 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.7 activate
  neighbor 10.10.10.7 send-community both
 exit-address-family
!
```

cki-bdr-01

```
router bgp 65000
 template peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  soft-reconfiguration inbound
  send-community both
 exit-peer-policy
 !
 bgp router-id 10.10.10.4
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.10.10.6 remote-as 65000
 neighbor 10.10.10.6 update-source Loopback0
```

```
 neighbor 10.10.10.7 remote-as 65000
 neighbor 10.10.10.7 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  bgp nexthop trigger delay 0
  neighbor 10.10.10.6 activate
  neighbor 10.10.10.6 send-community both
  neighbor 10.10.10.6 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.7 activate
  neighbor 10.10.10.7 send-community both
  neighbor 10.10.10.7 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
 exit-address-family
```

cki-leaf-01

```
router bgp 65000
 template peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  soft-reconfiguration inbound
  send-community both
 exit-peer-policy
 !
 bgp router-id 10.10.10.1
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.10.10.6 remote-as 65000
 neighbor 10.10.10.6 update-source Loopback0
 neighbor 10.10.10.7 remote-as 65000
 neighbor 10.10.10.7 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  bgp nexthop trigger delay 0
  neighbor 10.10.10.6 activate
  neighbor 10.10.10.6 send-community both
  neighbor 10.10.10.6 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
  neighbor 10.10.10.7 activate
  neighbor 10.10.10.7 send-community both
  neighbor 10.10.10.7 inherit peer-policy OVERLAY-SPINE-EVPN-PEER-POLICY
 exit-address-family
```

Ulangi konfigurasi overlay diatas pada node lain sesuai dengan interface dan IP Address yang terlampir pada gambar 4.

4.2.4 Implementasi Jaringan L2VPN dan L3VPN

Pada jaringan fabric yang menerapkan BGP EVPN VXLAN ini by default endpoint VLAN yang sama tidak bisa saling berkomunikasi begitu juga endpoint VLAN yang berbeda tidak bisa saling berkomunikasi dan inilah yang membedakan jaringan fabric modern dengan jaringan traditional. Konfigurasi L2VPN ini kita perlu konfigurasi antar leaf yang memiliki connection ke endpoint untuk endpoint VLAN yang sama bisa saling berkomunikasi dan terlampir konfigurasi L2VPN pada tabel 5 sebagai berikut,

Tabel 5 Konfigurasi L2VPN

cki-leaf-01

```
l2vpn evpn
 replication-type static
 router-id Loopback0
 default-gateway advertise
!
l2vpn evpn instance 101 vlan-based
 encapsulation vxlan
!
vlan configuration 101
 member evpn-instance 101 vni 500101
!
interface nve1
```

```
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 500101 mcast-group 238.1.1.1
```

Ulangi konfigurasi L2VPN diatas pada cki-leaf-02 dan cki-leaf-03 sesuai dengan *interface* dan *IP Address* yang terlampir pada gambar 4.

Tabel 6 Konfigurasi L3VPN

cki-leaf-01
vlan configuration 1000 member vni 501000 ! interface Vlan1000 description core sv for l3vni vrf forwarding prod ip unnumbered Loopback1 no autostate interface nve1 member vni 501000 vrf prod ! router bgp 65000 address-family ipv4 vrf prod advertise l2vpn evpn redistribute static redistribute connected maximum-paths ibgp 4 exit-address-family

Ulangi konfigurasi L3VPN diatas pada *node* cki-leaf-03 sesuai dengan *use case* pada *flow chart* pada gambar 2.

4.2.5 Implementasi External Connectivity Fabric

Dalam sebuah jaringan tidak mungkin endpoint hanya berkomunikasi ke *Intranet* saja dalam artian endpoint juga punya kebutuhan agar bisa berkomunikasi ke luar dari jaringan *fabric* dan *Internet* maka dari kita memerlukan konfigurasi *external connectivity* pada border leaf. Dan berikut terlampir konfigurasi *external connectivity* pada border switch pada Tabel 7,

Tabel 7 Konfigurasi External Connectivity

cki-bdr-01
ip prefix-list bgp_to_ospf seq 10 permit 198.18.101.0/24 ip prefix-list bgp_to_ospf seq 20 permit 198.18.102.0/24 ! ip prefix-list default_route seq 5 permit 0.0.0.0/0 ! route-map allow_default permit 10 match ip address prefix-list default_route route-map bgp_to_ospf permit 10 match ip address prefix-list bgp_to_ospf ! router ospf 1000 vrf prod router-id 10.10.10.111 redistribute bgp 65000 route-map bgp_to_ospf ! interface GigabitEthernet1/0/3 no switchport mtu 1500 vrf forwarding prod ip address 198.18.174.1 255.255.192.0 ip ospf 1000 area 0 ! router bgp 65000 address-family ipv4 vrf prod default-information originate redistribute ospf 1000 route-map allow_default

Ulangi konfigurasi *external connectivity* diatas pada *node* cki-bdr-02 sesuai dengan interface dan IP Address yang terlampir pada gambar 4.

p-ISSN 1979-7044
e-ISSN 2598-2990

4.3 Hasil Pengujian

4.3.1 Endpoint Dengan VLAN Sama Terisolated

Semua endpoint yang memiliki VLAN sama namun berbeda lokasi yang sebelumnya pada jaringan *traditional by default* bisa saling berkomunikasi pada topologi *spine-leaf* dengan menerapkan BGP EVPN VXLAN antar endpoint sekarang *by default* tidak bisa saling berkomunikasi.

A. Hasil Ping 198.18.101.3 (IT-App-Server) dari 198.18.101.2 (IT-Endpoint) dan sebaliknya,

```
cisco@ITEndpoint:~$ ping 198.18.101.3
PING 198.18.101.3 (198.18.101.3) 56(84) bytes of data.
From 198.18.101.1 icmp_seq=1 Destination Host Unreachable
From 198.18.101.1 icmp_seq=2 Destination Host Unreachable
From 198.18.101.1 icmp_seq=3 Destination Host Unreachable
From 198.18.101.1 icmp_seq=4 Destination Host Unreachable
From 198.18.101.1 icmp_seq=5 Destination Host Unreachable
From 198.18.101.1 icmp_seq=6 Destination Host Unreachable
```

Gambar 6 Verifikasi Isolasi VLAN 101

B. Hasil ping 198.18.102.3 (Public-App-Server) dari 198.18.102.2 (Employee-Endpoint) dan sebaliknya,

```
cisco@Public-App-Server:~$ ping 198.18.102.2
PING 198.18.102.2 (198.18.102.2) 56(84) bytes of data.
From 198.18.102.3 icmp_seq=1 Destination Host Unreachable
From 198.18.102.3 icmp_seq=2 Destination Host Unreachable
From 198.18.102.3 icmp_seq=3 Destination Host Unreachable
From 198.18.102.3 icmp_seq=4 Destination Host Unreachable
From 198.18.102.3 icmp_seq=5 Destination Host Unreachable
From 198.18.102.3 icmp_seq=6 Destination Host Unreachable
^C
```

Gambar 7 Verifikasi Isolasi VLAN 102

4.3.2 Endpoint Akses Menuju Endpoint VLAN Sama, Endpoint VLAN Berbeda dan Jaringan Diluar Fabric

Endpoint setelah dikonfigurasi L2VPN dan L3VPN akan memiliki *authorize* untuk akses ke endpoint baik VLAN yang sama dan VLAN yang berbeda, pada penelitian ini kita menyesuaikan *flowchart* pada gambar 2. Selain menyesuaikan hal tersebut kita juga memberikan *authorize* untuk user agar bisa akses ke jaringan diluar *fabric* seperti ke Internet.

```
cisco@ITEndpoint:~$ ping 198.18.102.3
PING 198.18.102.3 (198.18.102.3) 56(84) bytes of data.
64 bytes from 198.18.102.3: icmp_seq=1 ttl=60 time=91.7 ms
64 bytes from 198.18.102.3: icmp_seq=2 ttl=60 time=81.7 ms
64 bytes from 198.18.102.3: icmp_seq=3 ttl=60 time=80.5 ms
^C
--- 198.18.102.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 80.522/84.658/91.742/5.032 ms
```

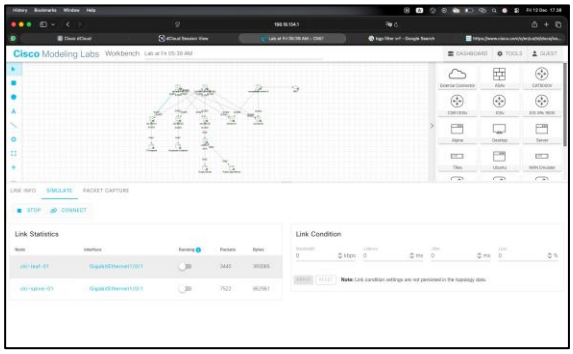
Gambar 8 Ping IT Endpoint ke Public-App-Server

```
cisco@ITEndpoint:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=82.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=86.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=91.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=83.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=91.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=109 time=79.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=109 time=77.6 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 77.642/84.494/91.429/5.062 ms
```

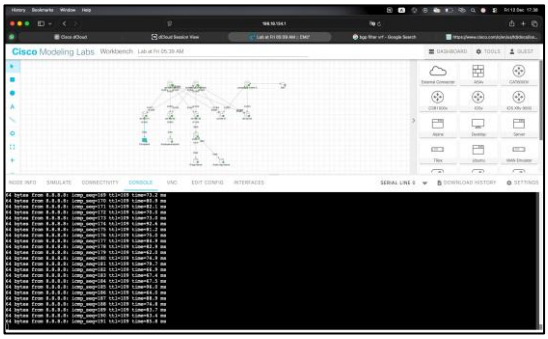
Gambar 9 Ping dari IT Endpoint ke Internet

4.3.3 High Availability Pada Topology Spine-Leaf

Setiap user ingin memiliki jaringan yang memiliki ketersediaan 24/7, kita memilih Topology *Spine-leaf* untuk mencegah adanya *issue failure* pada salah satu *physical cable* jika terjadi.



Gambar 10 Port cki-leaf-01 to cki-spine-01 down



Gambar 11 Verifikasi Ping Internet

Seperti yang kita lihat pada gambar 11 Ping menuju Internet dari IT-Endpoint masih berjalan normal ketika salah satu *uplink* cki-leaf-01 mati dan ini menunjukan bahwa topology *spine-leaf* memiliki ketersediaan yang sangat bagus.

KESIMPULAN

Berdasarkan pembahasan, hasil dan pengujian yang telah dilakukan dalam penerapan implementasi *high availability* dan keamanan

jaringan *fabric* menggunakan BGP EVPN VXLAN pada infrastruktur *multi-lokasi* menggunakan dcloud cisco simulator maka dapat diambil kesimpulan bahwa Mengimplementasikan Jaringan Fabric menggunakan topology spine-leaf dengan BGP EVPN VXLAN dapat memberikan benefit sebagai berikut,

a. Keamanan pada jaringan fabric yang mana endpoint saling terisolasi antar departmentyang sama dan departmentyang berbeda.

b. Jaringan Fabric memiliki komunikasi yang skalabel, efisien dan ketersediaan 24/7.

UCAPAN TERIMAKASIH

Alhamdulillah, kami panjatkan rasa syukur kepada Allah Subhanahu Wa Ta'ala yang telah melimpahkan nikmat kesehatan dan waktu luang sehingga kami dapat menyelesaikan penelitian ini. Ucapan terima kasih kami sampaikan kepada keluarga tercinta, Bapak Yuma Akbar sebagai dosen pembimbing, serta seluruh rekan rekan yang telah memberikan dukungan dalam pelaksanaan kegiatan penelitian ini.

DAFTAR PUSTAKA

Arfan Efendi, Diyanatul Husna, & I Gde Dharma Nugraha. (2023). Advancing Network Infrastructure: Integrating VXLAN Technology with Automated Circuit Operations and NOS Configurations. *International Journal of Electrical, Computer, and Biomedical Engineering*, *1*(2), 32–53. https://doi.org/10.62146/ijecbe.v1i2.30

Chandra Jha, A. (2025). VXLAN/BGP EVPN for Trading: Multicast Scaling Challenges for Trading Colocations. *International Journal of Computational and Experimental Science and Engineering*, *11*(3). https://doi.org/10.22399/ijcesen.3478

Do Abdullah, S., Lutfi, S., Fuad, A., Wahyudin Nur, A., & Ibrahim, A. (n.d.). *Analisis dan Desain VXLAN untuk Interkoneksi Lokasi yang Berbeda di Universitas Khairun VXLAN Analysis and Design for Interconnecting Different Locations at Khairun University*.

Fadokun, O. (2025). *Implementation of a Virtual Extensible Local Area Network (VXLAN)*.

Fitra Diraja, A., Basuki, A., & Amron, K. (2025). *Implementasi dan Evaluasi Kinerja VXLAN over WireGuard untuk Ekstensi LAN Antar-Lokasi* (Vol. 9, Issue 6). http://j-ptiik.ub.ac.id

Kusnanto, Y., Nugroho, M. A., & Kartadie, R. (2024). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi IMPLEMENTASI ZERO TRUST ARCHITECTURE UNTUK MENINGKATKAN KEAMANAN JARINGAN: PENDEKATAN BERBASIS SIMULASI*. *9*(4), 2357–2364. https://doi.org/10.29100/jipi.v4i1.6943

Naranjo, E. F., & Salazar Ch. Gustavo D. (2017). *Underlay and Overlay Networks: The approach to solve addressing and segmentation problems in the new networking era*. IEEE.