AB-NEXUS Enterprise Network Topology Documentation
CASE STUDY: Access Bank Plc, Victoria Island, Lagos
Version:1.1 | Architect: Chuks Gabriel | Date: November, 2025

1. Executive Summary

AB-NEXUS is a hierarchical three-layer (Core, Distribution, Access) enterprise network designed for Access Bank's Headquarters (HQ) and regional branches (Ikeja and Lekki). The design incorporates:

• Cisco Multilayer Switches for Layer 3 routing at the core and distribution layers.

• OSPF Multi-Area Routing for internal connectivity with Equal-Cost Multi-Path (ECMP) load balancing to ensure optimal path selection and redundancy. OSPF areas are segmented to reduce convergence time and limit routing updates: Area 0 as the backbone, with stub or totally stubby areas for branches and departments to minimize LSAs.

• BGP for Branch Connectivity: As per updated design, BGP is used for external peering between HQ and branches (Ikeja and Lekki) over ISP links. This replaces OSPF advertisement over public links in the provided configurations, providing better control over route policies, scalability for multi-homed connections, and AS path filtering. HQ uses AS 65000, branches use private AS (e.g., 65001 for Ikeja, 65002 for Lekki). Default routes are originated via BGP, with local preference and MED for path optimization.

• EtherChannel (Port-Channels) using LACP (mode "on" in configs, but recommend active/passive for production) for link aggregation, providing up to 2Gbps bandwidth and fault tolerance (if one link fails, traffic fails over seamlessly).

• VLAN Segmentation with SVIs (Switched Virtual Interfaces) for departmental isolation, inter-VLAN routing via Layer 3 switches, and DHCP relay (ip helper-address) to central servers.

• Spanning Tree Protocol (PVST+) to prevent loops in Layer 2 domains, with root bridge priority configurable on core switches.

• Security Features: ACLs for VTY access, extended ACLs for ICMP control (e.g., denying unsolicited pings while allowing replies), and logging to centralized syslog (203.1.100.1).

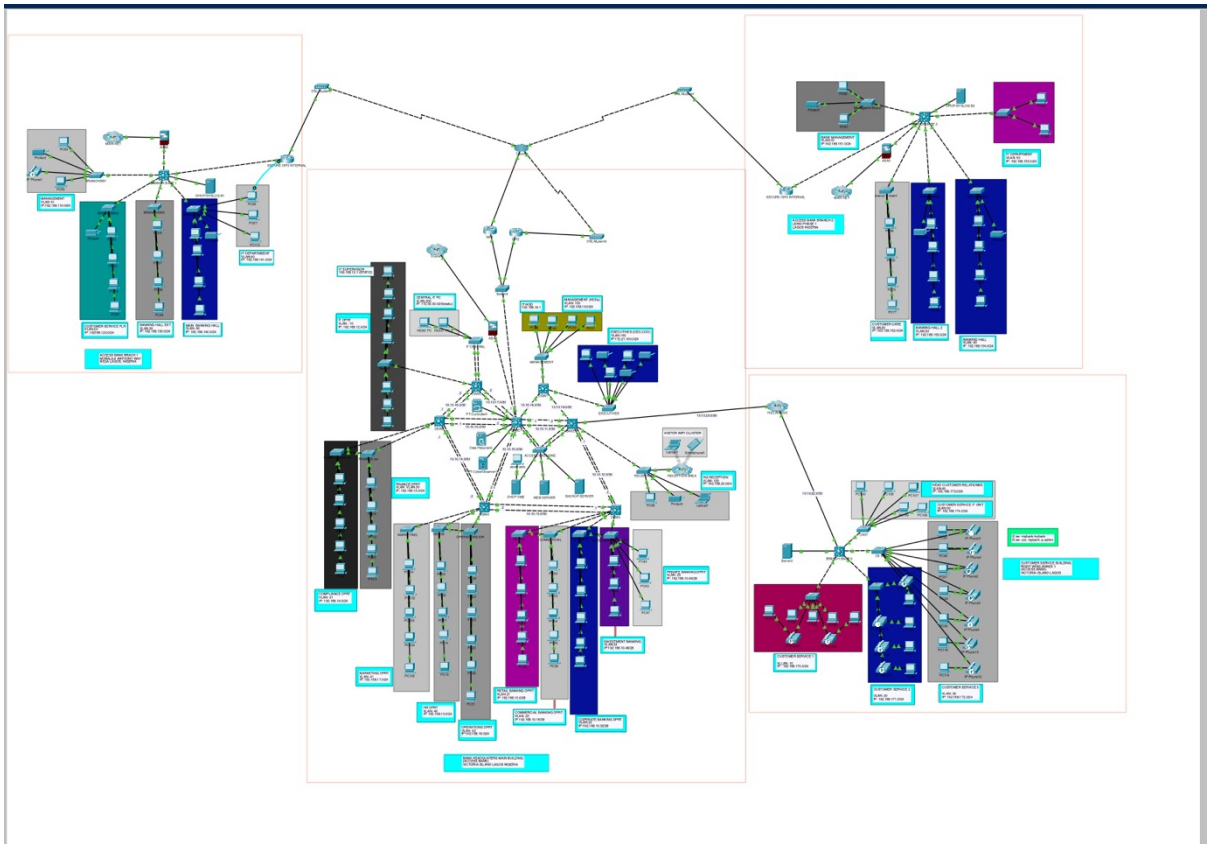
• Monitoring: SPAN (Switched Port Analyzer) sessions for traffic mirroring, NetFlow v9 for export, and SNMP traps enabled. Additionally, Cyber Observer is deployed for comprehensive threat monitoring, including real-time detection of anomalies, compliance auditing, and vulnerability scanning across the network topology. It integrates with SIEM systems to analyse logs from devices and alert on potential

cyber threats like malware or unauthorized access attempts. Network Controller is utilized for centralized link monitoring and orchestration, providing SDN-like capabilities for dynamic traffic steering, bandwidth allocation, and fault detection on core and distribution links. It uses APIs to interface with switches for proactive health checks, latency measurements, and automated rerouting during outages.
• High Availability: Dual core switches (BASE1, BASE2) with redundant links; future-ready for HSRP/VRRP on SVIs.
• Scalability: Supports cloud integration via BGP peering for AWS/Azure, with room for SD-WAN overlays.

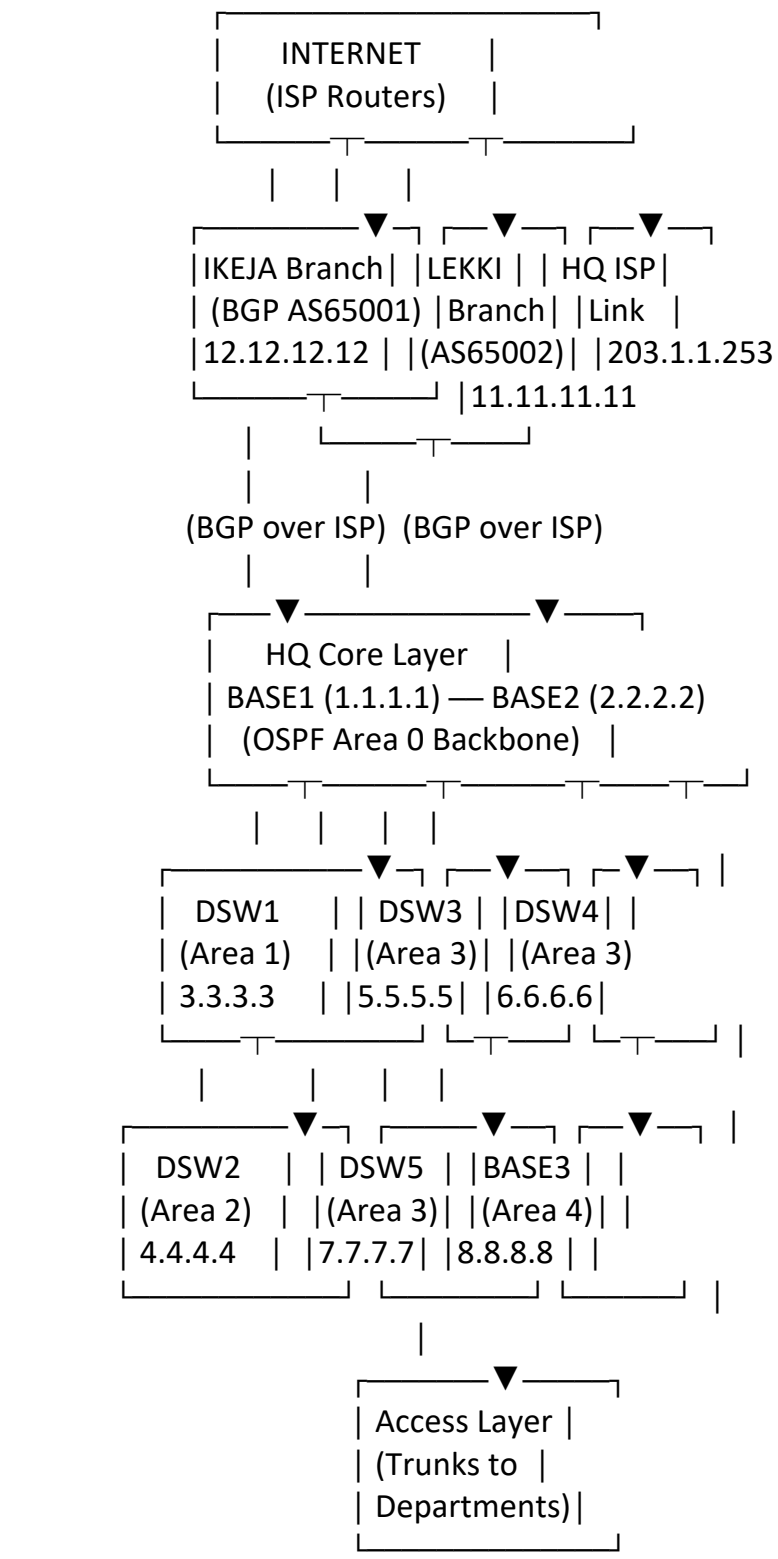
The provided running configurations use OSPF for all links, including branch connectivity over public IPs (203.x.x.x/24). However, as per design update, BGP is implemented for HQ-to-branch links to handle external routing securely, avoiding OSPF neighbor formation over untrusted ISP paths. This prevents potential adjacency issues and enhances policy control.

2. Network Topology Overview

The topology follows a collapsed core design at HQ, with BASE1 and BASE2 as core/aggregation, DSW1–5 as distribution, and implied access switches (not shown in configs) connected via trunks. Branches connect via ISP using BGP for route exchange. A dedicated web server is hosted at HQ (in VLAN 500, IP 203.1.100.2) solely for the bank's website, ensuring isolated and secure public-facing access without additional services. A central DHCP server (at 203.1.100.1) handles dynamic IP assignment across VLANs via relays and also serves as the syslog server for centralized logging of network events.



ASCII Topology Diagram



• Core Layer (BASE1, BASE2): Handles high-speed routing, OSPF Area 0, and BGP to branches. Redundant EtherChannels ensure no single point of failure. Cyber Observer and Network Controller are integrated here for topology-wide monitoring.
• Distribution Layer (DSW1–5): Aggregates access switches, performs inter-VLAN routing, and enforces ACLs. Areas 1–3 segment departments.
• Access Layer: Not fully configured; trunks (e.g., Po27 on BASE1) connect to end-user switches/hosts.
• Branches: Autonomous sites with local VLANs; BGP advertises local subnets to HQ, with default route to ISP.
• ISP Links: Public /24 subnets; BGP sessions established over these for secure route exchange (eBGP peering).

3. Device Inventory

Expanded with OSPF process ID, enable secret (hashed), SSH config, and management IP.

Hostname	Role	Loopback IP	OSPF Process/Area(s)	Management SVI (Vlan1)	Key Features
BASE1	HQ Core	1.1.1.1/32	Process 1 / Area 0	192.168.1.254/24	EtherChannels, NetFlow, SPAN, Logging to 203.1.100.1
BASE2	HQ Core/Aggregation	2.2.2.2/32	Process 2 / Area 0	192.168.2.254/24	DHCP Relay, SSH v2, Domain ccnabank.com
DSW1	Distribution (Area 1)	3.3.3.3/32	Process 3 / Areas 0,1	192.168.3.254/24	Passive Loopback, ACL 'icmpexe'
DSW2	Distribution (Area 2)	4.4.4.4/32	Process 4 / Areas 0,2	192.168.4.254/24	Passive Loopback, ACLs 'icmp', 'icmpvlan10'
DSW3	Distribution (Area 3)	5.5.5.5/32	Process 5 / Areas 0,2,3	192.168.5.254/24	Passive Loopback, ACL 'icmpcomp'
DSW4	Distribution (Area 3)	6.6.6.6/32	Process 6 / Areas 0,3	192.168.6.254/24	ACL 'icmphr'

| DSW5 | Distribution (Area 3) | 7.7.7.7/32 | Process 7 / Areas 0,3 | 192.168.7.254/24 | Subnetted VLANs (/28) |

| BASE3 | HQ Customer Service Wing | 8.8.8.8/32 | Process 10 / Areas 0,4 | 192.168.8.254/24 | Domain mybank.com, ACL 'icmpit' |

| BASE (Ikeja) | Branch Switch | 12.12.12.12/32 | Process 1 / Areas 0,6 | 192.168.1.254/24 | BGP to HQ, Default Route to ISP, Default-Info Originate |

| BASE (Lekki) | Branch Switch | 11.11.11.11/32 | Process 1 / Areas 0,5 | 192.168.1.254/24 | BGP to HQ, Passive Loopback, ACL 'icmpit' |

• Enable Secret: All devices use hashed secret 1mERr$vTbHul1N28cEp8lkLqr0f/ (MD5; recommend SHA-512 in production).
• Username: 'admin' or 'ccna' or 'mybank' with same secret.
• SSH: Version 2, domain ccnabank.com or mybank.com, transport input ssh only.
• No IP CEF/IPv6 CEF: Disabled; recommend enabling for performance in real deployments.

4. OSPF Area Design

OSPF is multi-area for scalability. Area 0 connects all; non-zero areas are stub-like (passive interfaces on Loopbacks). Log-adjacency-changes enabled for debugging.

```
Gateway of last resort is 203.1.1.253 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.10.11.2, 00:09:27, Port-channel23
     3.0.0.0/32 is subnetted, 1 subnets
O IA    3.3.3.3 [110/2] via 10.10.18.2, 00:09:27, GigabitEthernet1/0/3
     4.0.0.0/32 is subnetted, 1 subnets
O IA    4.4.4.4 [110/2] via 10.10.17.2, 00:09:27, Port-channel20
     5.0.0.0/32 is subnetted, 1 subnets
O IA    5.5.5.5 [110/2] via 10.10.10.1, 00:09:27, Port-channel21
     6.0.0.0/32 is subnetted, 1 subnets
O IA    6.6.6.6 [110/2] via 10.10.15.2, 00:09:27, Port-channel22
     7.0.0.0/32 is subnetted, 1 subnets
O IA    7.7.7.7 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                [110/3] via 10.10.11.2, 00:09:27, Port-channel23
     8.0.0.0/32 is subnetted, 1 subnets
O IA    8.8.8.8 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
     10.0.0.0/8 is variably subnetted, 18 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Port-channel21
L       10.10.10.2/32 is directly connected, Port-channel21
C       10.10.11.0/30 is directly connected, Port-channel23
L       10.10.11.1/32 is directly connected, Port-channel23
O       10.10.12.0/30 [110/2] via 10.10.11.2, 00:09:27, Port-channel23
O IA    10.10.13.0/30 [110/2] via 10.10.15.2, 00:09:27, Port-channel22
O IA    10.10.14.0/30 [110/2] via 10.10.10.1, 00:09:27, Port-channel21
                      [110/2] via 10.10.15.2, 00:09:27, Port-channel22
C       10.10.15.0/30 is directly connected, Port-channel22
L       10.10.15.1/32 is directly connected, Port-channel22
O IA    10.10.16.0/30 [110/2] via 10.10.17.2, 00:09:27, Port-channel20
                      [110/2] via 10.10.10.1, 00:09:27, Port-channel21
C       10.10.17.0/30 is directly connected, Port-channel20
L       10.10.17.1/32 is directly connected, Port-channel20
C       10.10.18.0/30 is directly connected, GigabitEthernet1/0/3
L       10.10.18.1/32 is directly connected, GigabitEthernet1/0/3
O       10.10.19.0/30 [110/2] via 10.10.11.2, 00:09:27, Port-channel23
                      [110/2] via 10.10.18.2, 00:09:27, GigabitEthernet1/0/3
O       10.10.20.0/30 [110/2] via 10.10.11.2, 00:09:27, Port-channel23
O       10.10.21.0/30 [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O       10.10.22.0/30 [110/4] via 10.10.11.2, 00:09:27, Port-channel23
     12.0.0.0/32 is subnetted, 1 subnets
O IA    12.12.12.12 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
     20.0.0.0/32 is subnetted, 1 subnets
O       20.20.20.20 [110/2] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
     21.0.0.0/32 is subnetted, 1 subnets
O       21.21.21.21 [110/2] via 203.1.1.252, 00:09:27, GigabitEthernet1/0/7
     23.0.0.0/32 is subnetted, 1 subnets
O       23.23.23.23 [110/3] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
     172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.16.10.0/24 is directly connected, GigabitEthernet1/0/5
L       172.16.10.254/32 is directly connected, GigabitEthernet1/0/5
C       172.16.11.0/24 is directly connected, GigabitEthernet1/0/6
L       172.16.11.254/32 is directly connected, GigabitEthernet1/0/6
C       172.16.13.0/24 is directly connected, GigabitEthernet1/0/14
L       172.16.13.254/32 is directly connected, GigabitEthernet1/0/14
     172.21.0.0/24 is subnetted, 1 subnets
O IA    172.21.100.0 [110/2] via 10.10.18.2, 00:09:27, GigabitEthernet1/0/3
     172.30.0.0/29 is subnetted, 1 subnets
O IA    172.30.30.0 [110/2] via 10.10.17.2, 00:09:27, Port-channel20
```

```
     172.21.0.0/24 is subnetted, 1 subnets
O IA    172.21.100.0 [110/2] via 10.10.18.2, 00:09:27, GigabitEthernet1/0/3
     172.30.0.0/29 is subnetted, 1 subnets
O IA    172.30.30.0 [110/2] via 10.10.17.2, 00:09:27, Port-channel20
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Vlan1
L       192.168.1.254/32 is directly connected, Vlan1
O    192.168.2.0/24 [110/2] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.3.0/24 [110/2] via 10.10.18.2, 00:09:27, GigabitEthernet1/0/3
O IA 192.168.5.0/24 [110/2] via 10.10.10.1, 00:09:27, Port-channel21
O IA 192.168.6.0/24 [110/2] via 10.10.15.2, 00:09:27, Port-channel22
O IA 192.168.7.0/24 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                    [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.8.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
     192.168.10.0/28 is subnetted, 5 subnets
O IA    192.168.10.0 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                     [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O IA    192.168.10.16 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                      [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O IA    192.168.10.32 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                      [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O IA    192.168.10.48 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                      [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O IA    192.168.10.64 [110/3] via 10.10.15.2, 00:09:27, Port-channel22
                      [110/3] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.12.0/24 [110/2] via 10.10.17.2, 00:09:27, Port-channel20
O IA 192.168.13.0/24 [110/2] via 10.10.10.1, 00:09:27, Port-channel21
O IA 192.168.14.0/24 [110/2] via 10.10.10.1, 00:09:27, Port-channel21
O IA 192.168.15.0/24 [110/2] via 10.10.15.2, 00:09:27, Port-channel22
O IA 192.168.16.0/24 [110/2] via 10.10.15.2, 00:09:27, Port-channel22
O IA 192.168.17.0/24 [110/2] via 10.10.15.2, 00:09:27, Port-channel22
O IA 192.168.19.0/24 [110/2] via 10.10.18.2, 00:09:27, GigabitEthernet1/0/3
O    192.168.20.0/24 [110/2] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.100.0/24 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O IA 192.168.110.0/24 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O IA 192.168.120.0/24 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O IA 192.168.130.0/24 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O IA 192.168.140.0/24 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O IA 192.168.141.0/24 [110/4] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O IA 192.168.170.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.171.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.172.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.173.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.174.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.175.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O IA 192.168.190.0/24 [110/5] via 10.10.11.2, 00:09:27, Port-channel23
O    200.100.100.0/24 [110/2] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
     203.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       203.1.1.0/24 is directly connected, GigabitEthernet1/0/7
L       203.1.1.1/32 is directly connected, GigabitEthernet1/0/7
     203.1.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       203.1.100.0/24 is directly connected, Vlan500
L       203.1.100.254/32 is directly connected, Vlan500
     203.1.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       203.1.200.0/24 is directly connected, Vlan501
L       203.1.200.254/32 is directly connected, Vlan501
O    203.3.3.0/24 [110/3] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
O*E2 0.0.0.0/0 [110/1] via 203.1.1.253, 00:09:27, GigabitEthernet1/0/7
```

OSPF Areas and Processes

Area	Type	Devices	Advertised Networks	OSPF Process	Explanation
0	Transit	BASE1, BASE2, DSW2 (partial), DSW3 (partial), DSW4 (partial), DSW5 (partial), BASE3 (partial)	10.10.x.0/30 (core links), 203.1.x.0/24 (HQ public), 172.16.x.0/24 (services), 192.168.1–8.0/24 (mgmt)	Varies (1–10)	Core backbone; ECMP load-balancing
1	Standard	DSW1	3.3.3.3/32, 172.21.100.0/24, 192.168.3.0/24, 192.168.19.0/24	3	Guest/Exec; passive Loopback
2	Standard	DSW2	4.4.4.4/32, 10.10.16.0/30, 172.30.30.0/29, 192.168.4.0/24, 192.168.12.0/24	4	Security/IT
3	Standard	DSW3, DSW4, DSW5	5.5.5.5/32–7.7.7.7/32, 10.10.12–15.0/30, 192.168.5–7.0/24, 192.168.10.0/24 (subnetted), 192.168.13–17.0/24	5–7	Departmental
4	Standard	BASE3	8.8.8.8/32, 10.10.22.0/30, 192.168.8.0/24, 192.168.170–175.0/24, 192.168.190.0/24	10	Customer Service
5	Stub	Lekki Branch (BRANCH2)	11.11.11.11/32, 192.168.1.0/24, 192.168.151–155.0/24, 192.168.160.0/24, 203.2.2.0/24	1	Branch local; BGP to HQ
6	Stub	Ikeja Branch (BRANCH1)	12.12.12.12/32, 192.168.1.0/24, 192.168.110–141.0/24, 192.168.100.0/24, 203.3.3.0/24	1	Branch local; BGP to HQ

Note on Branch OSPF: Configs advertise branch public nets in Area 0, but updated design uses BGP. OSPF default-information originate injects 0.0.0.0 into branches.

5. Inter-Switch Connectivity

All Layer 3 links are /30 for efficiency. EtherChannels use mode 'on' (static; recommend 'active' for negotiation). Trunks carry all VLANs (no allowed list).

EtherChannel Links

Device1	Port-Channel	Members	IP (Device1)	Device2	IP (Device2)	Mode	Explanation
BASE1	Po20	Gi1/0/1–2	10.10.17.1/30	DSW2	10.10.17.2/30	On	Core-to-Dist
BASE1	Po21	Gi1/0/10–11	10.10.10.2/30	DSW3	10.10.10.1/30	On	ECMP to Area 3
BASE1	Po22	Gi1/0/12–13	10.10.15.1/30	DSW4	10.10.15.2/30	On	Load-balancing
BASE1	Po23	Gi1/0/20–21	10.10.11.1/30	BASE2	10.10.11.2/30	On	Core interconnect
BASE1	Po27	Gi1/0/8–9	Trunk	Access	Trunk	On	L2 to access layer
BASE2	Po20	Gi1/0/10–11	10.10.12.1/30	DSW5	10.10.12.2/30	On	To Area 3
BASE2	Po21	Gi1/0/20–21	10.10.11.2/30	BASE1	10.10.11.1/30	On	Core interconnect
BASE2	Po25	Gi1/0/8–9	Trunk	Access	Trunk	On	L2 aggregation
DSW2	Po15	Gi1/0/1–2	10.10.17.2/30	BASE1	10.10.17.1/30	On	Uplink

| DSW2 | Po17 | Gi1/0/20–21 | 10.10.16.2/30 | DSW3 | 10.10.16.1/30 | On | Inter-distribution |

| DSW2 | Po18 | Gi1/0/4–5 | Trunk | Access | Trunk | On | Departmental |

| DSW3 | Po20 | Gi1/0/1–2 | 10.10.14.1/30 | DSW4 | 10.10.14.2/30 | On | Area 3 internal |

| DSW3 | Po21 | Gi1/0/10–11 | 10.10.10.1/30 | BASE1 | 10.10.10.2/30 | On | Uplink |

| DSW3 | Po22 | Gi1/0/20–21 | 10.10.16.1/30 | DSW2 | 10.10.16.2/30 | On | Cross-area |

| DSW4 | Po20 | Gi1/0/1–2 | 10.10.14.2/30 | DSW3 | 10.10.14.1/30 | On | Area 3 internal |

| DSW4 | Po21 | Gi1/0/10–11 | 10.10.15.2/30 | BASE1 | 10.10.15.1/30 | On | Uplink |

| DSW4 | Po23 | Gi1/0/20–21 | 10.10.13.2/30 | DSW5 | 10.10.13.1/30 | On | Area 3 internal |

| DSW5 | Po20 | Gi1/0/20–21 | 10.10.13.1/30 | DSW4 | 10.10.13.2/30 | On | Area 3 internal |

| DSW5 | Po21 | Gi1/0/12–13 | 10.10.12.2/30 | BASE2 | 10.10.12.1/30 | On | Uplink |

Point-to-Point Links

Device1	Interface	IP	Device2	Interface	IP	Explanation

BASE1	Gi1/0/3	10.10.18.1/30	DSW1	Gi1/0/3	10.10.18.2/30	Redundant to 10.10.19.0
BASE2	Gi1/0/1	10.10.19.1/30	DSW1	Gi1/0/2	10.10.19.2/30	ECMP pair
BASE2	Gi1/0/3	10.10.20.1/30	—	—	10.10.20.2/30	Peer not shown
BASE3	Gi1/0/1	10.10.22.2/30	—	—	10.10.22.1/30	Likely to BASE2

Unconfigured Links: Route table shows 10.10.21.0/30, 10.10.22.0/30 via BASE2; assume additional Gi ports on BASE2.

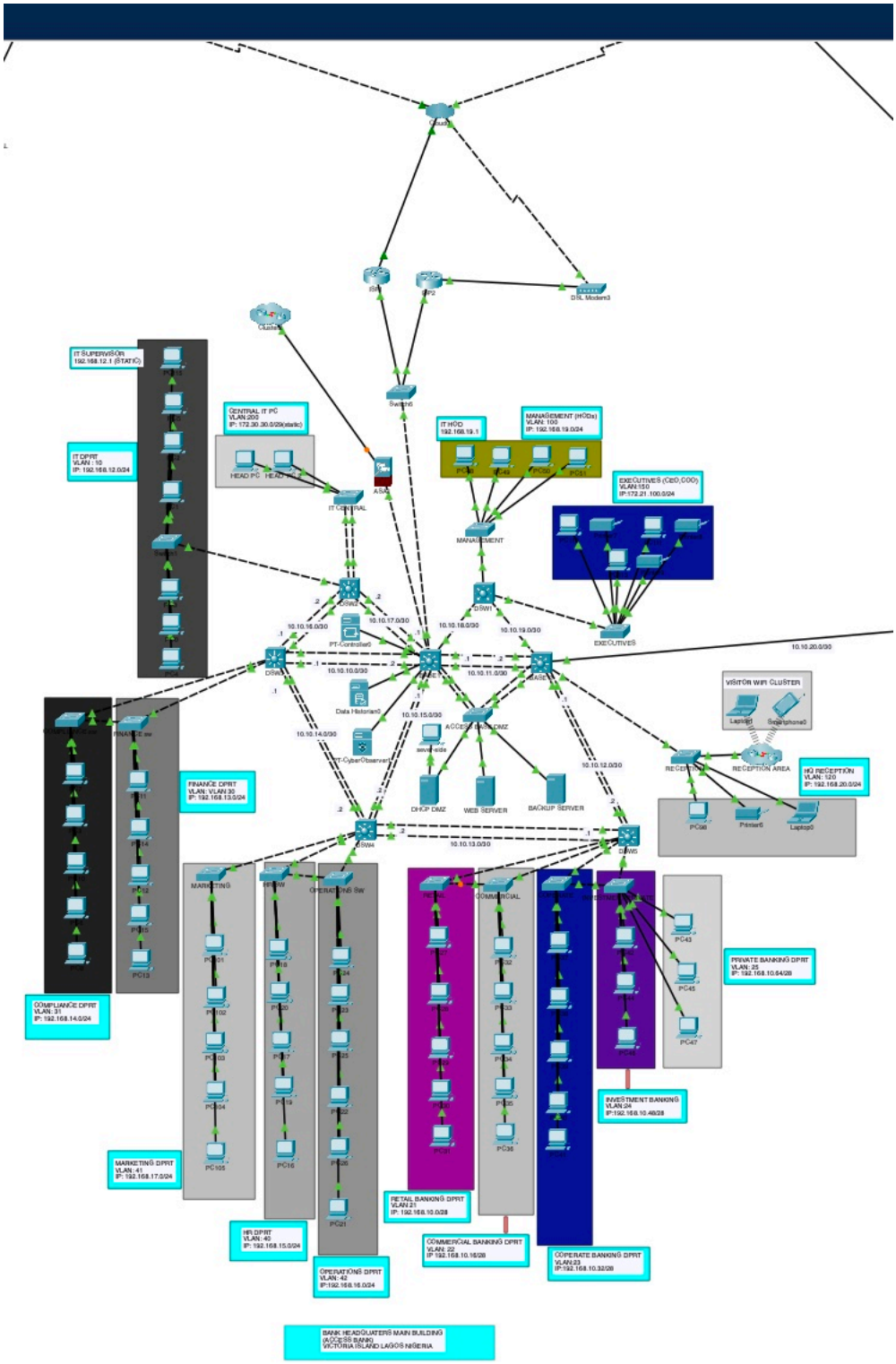
6. VLAN & SVI Summary

All SVIs have MAC overrides. DHCP relay to central servers (e.g., 203.1.100.1 at HQ, which serves both DHCP and syslog functions). Branches have localized relays.

Core Services VLANs (HQ)

VLAN	Purpose	IP Subnet	Device	Gateway
500	Core Services	203.1.100.0/24	BASE1	203.1.100.254
501	Backup Services	203.1.200.0/24	BASE1	203.1.200.254
1	Management	192.168.1.0/24	BASE1	192.168.1.254
1	Management	192.168.2.0/24	BASE2	192.168.2.254

Departmental VLANs (HQ)

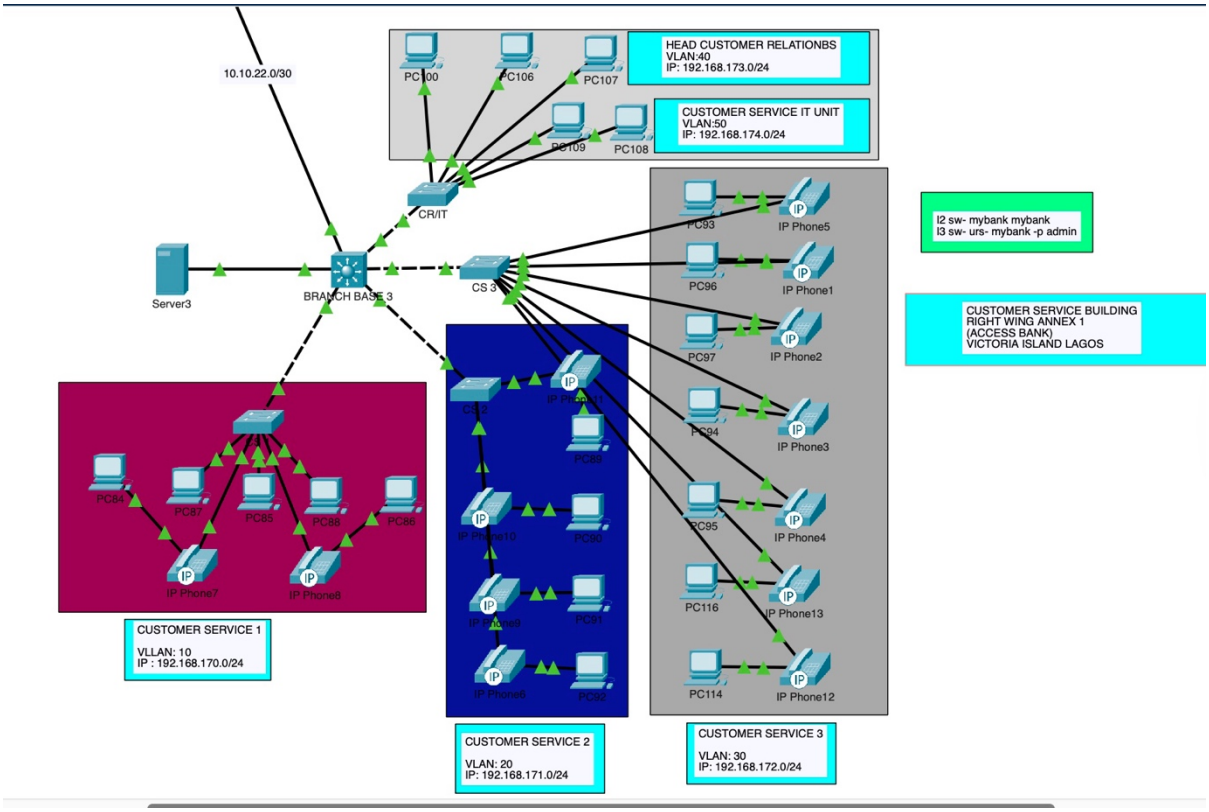


VLAN	Department/Purpose	IP Subnet	Device	Gateway	DHCP Helper
100	Management/HR	192.168.19.0/24	DSW1	192.168.19.254	203.1.100.1
150	IT/Guest	172.21.100.0/24	DSW1	172.21.100.254	203.1.100.1
10	Finance/IT	192.168.12.0/24	DSW2	192.168.12.254	203.1.100.1
200	Servers/Security	172.30.30.0/29	DSW2	172.30.30.6	N/A
30	Operations	192.168.13.0/24	DSW3	192.168.13.254	203.1.100.1
31	Marketing	192.168.14.0/24	DSW3	192.168.14.254	203.1.100.1
40	Administration	192.168.15.0/24	DSW4	192.168.15.254	203.1.100.1
41	Executive	192.168.17.0/24	DSW4	192.168.17.254	203.1.100.1
42	Board	192.168.16.0/24	DSW4	192.168.16.254	203.1.100.1

DSW5 Subnet Division (192.168.10.0/24)

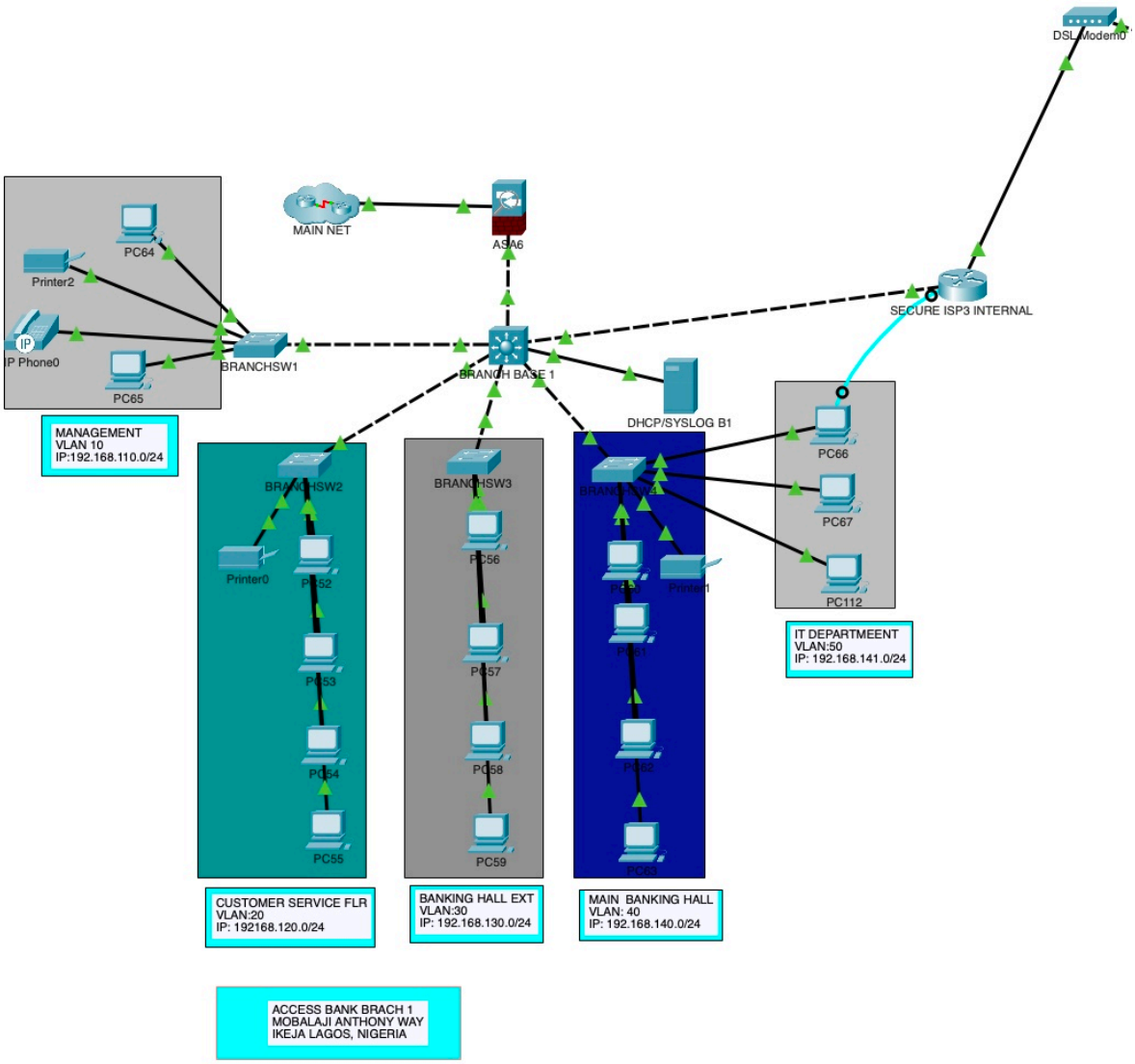
VLAN	Subnet Range	Usable IPs	Gateway	Purpose
21	192.168.10.0/28	192.168.10.1–14	192.168.10.14	Subnet 1
22	192.168.10.16/28	192.168.10.17–30	192.168.10.30	Subnet 2
23	192.168.10.32/28	192.168.10.33–46	192.168.10.46	Subnet 3
24	192.168.10.48/28	192.168.10.49–62	192.168.10.62	Subnet 4
25	192.168.10.64/28	192.168.10.65–78	192.168.10.78	Subnet 5

Branch Office VLANs (BASE3 - Customer Service)



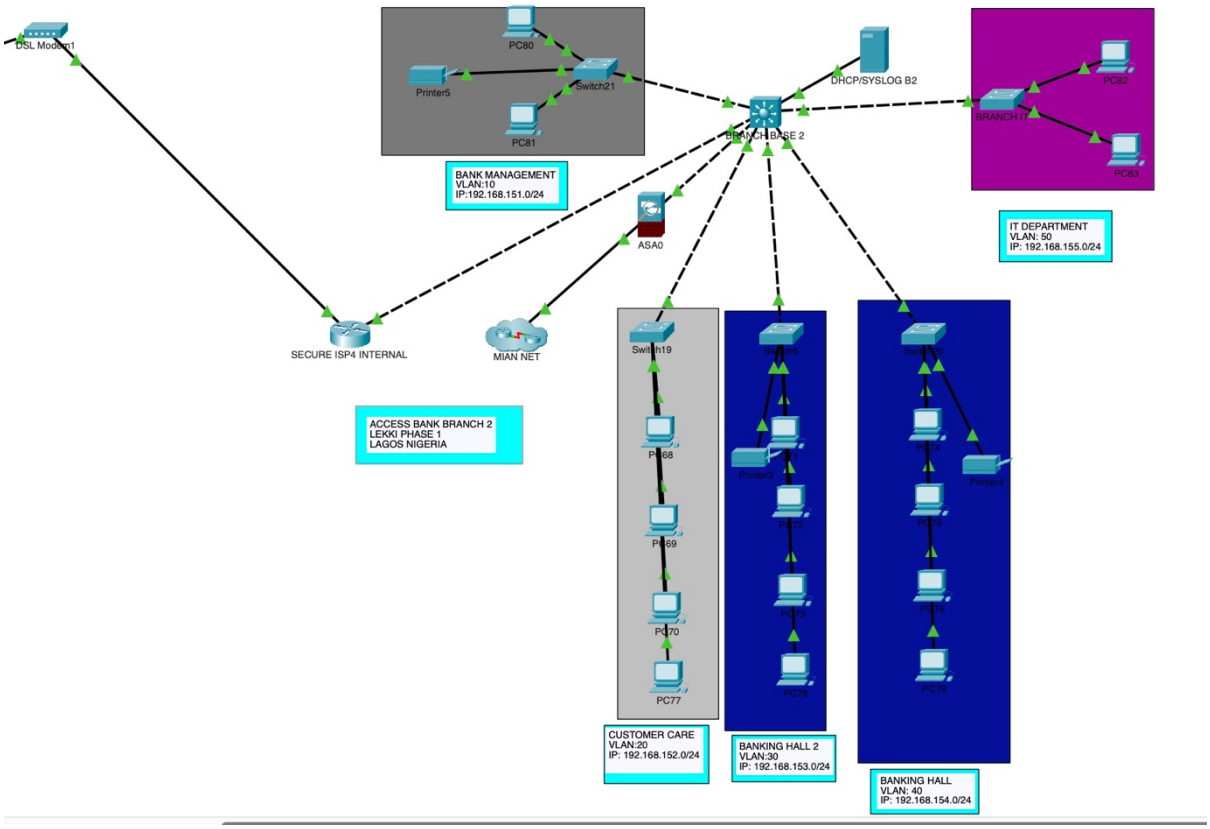
VLAN	Department	IP Subnet	Gateway	DHCP Helper
10	Dept 1	192.168.170.0/24	192.168.170.254	192.168.190.1
11	Dept 2	192.168.175.0/24	192.168.175.254	192.168.190.1
20	Dept 3	192.168.171.0/24	192.168.171.254	192.168.190.1
30	Dept 4	192.168.172.0/24	192.168.172.254	192.168.190.1
40	Dept 5	192.168.173.0/24	192.168.173.254	192.168.190.1
50	Dept 6	192.168.174.0/24	192.168.174.254	192.168.190.1
100	Management	192.168.190.0/24	192.168.190.254	N/A

Branch Office VLANs (Ikeja - BRANCH1)



VLAN	Department	IP Subnet	Gateway	DHCP Helper
10	Dept 1	192.168.110.0/24	192.168.110.254	192.168.100.1
20	Dept 2	192.168.120.0/24	192.168.120.254	192.168.100.1
30	Dept 3	192.168.130.0/24	192.168.130.254	192.168.100.1
40	Dept 4	192.168.140.0/24	192.168.140.254	192.168.100.1
50	Dept 5	192.168.141.0/24	192.168.141.254	192.168.100.1
100	Management	192.168.100.0/24	192.168.100.254	N/A

Branch Office VLANs (Lekki - BRANCH2)



VLAN	Department	IP Subnet	Gateway	DHCP Helper
10	Dept 1	192.168.151.0/24	192.168.151.254	192.168.160.1
20	Dept 2	192.168.152.0/24	192.168.152.254	192.168.160.1
30	Dept 3	192.168.153.0/24	192.168.153.254	192.168.160.1
40	Dept 4	192.168.154.0/24	192.168.154.254	192.168.160.1
50	Dept 5	192.168.155.0/24	192.168.155.254	192.168.160.1
100	Management	192.168.160.0/24	192.168.160.254	N/A

Trunk Ports: e.g., Gi1/0/23–24 on DSW3/4 (trunk mode); carry all VLANs.

7. Routing & Reachability

OSPF Details

• Neighbors: Formed over L3 links; no authentication (add MD5 for security).

• Routes from BASE1 (excerpt): Direct (C), OSPF intra (O), inter-area (O IA), external (O E2). ECMP on paths like to 7.7.7.7 [110/3] via two nexthops.

• Convergence: Multi-area reduces flood; log-adjacency for changes.

BGP for Branches

• Peering: HQ (BASE1) peers with Ikeja (203.3.3.1) and Lekki (203.2.2.1) over ISP.
• Advertisements: Branches advertise local subnets (e.g., 192.168.110.0/24) to HQ AS; HQ advertises summary (192.168.0.0/16).
• Default Route: Branches static to ISP, redistributed via BGP. HQ uses local-pref 200 for primary path.

Key Technical Points

1. Multi-Area Design: Scalable hierarchy with Area 0 as backbone.
2. Route Summarization: Not explicitly configured; potential optimization area.
3. Passive Interfaces: Loopback interfaces passive in distribution layers.
4. Equal-Cost Multi-Path (ECMP): Load balancing evident in routing table.
5. Route Redistribution: Branches redistributing default static routes into OSPF.
6. Area Border Routers: DSW1, DSW2, DSW3, DSW4 acting as ABRs.

Resilience Features

1. EtherChannel Bundles: Multiple physical links aggregated for redundancy.
2. Dual Homed Distribution: Distribution switches connected to both core switches.
3. Multiple Paths: ECMP routing provides automatic failover.
4. Loop Prevention: Spanning-tree mode PVST with trunk redundancy.

This documentation provides a comprehensive view of the Access Bank enterprise network, demonstrating a well-designed, resilient infrastructure capable of supporting critical banking operations with high availability and security.

Static Routes

• Branches: ip route 0.0.0.0 0.0.0.0 ISP_GW (203.x.x.254).
• No classless routing (ip classless); all explicit.

8. High Availability Features

Feature	Implementation	Explanation
Link Aggregation	EtherChannel (LACP mode "on") on all core/distribution links (2 members per Po)	Doubles bandwidth (2 Gbps per Po), automatic failover if one link fails. Load-balances using src-dest IP hash.
Routing Redundancy	OSPF ECMP (Equal-Cost Multi-Path) + BGP multi-path (for branches)	Multiple equal-cost paths (e.g., to DSW5 via BASE2 and DSW4). BGP allows path preference via local-pref/med.
Spanning Tree	PVST+ (Per-VLAN Spanning Tree Plus) enabled globally	Prevents L2 loops on trunks. Recommend configuring BASE1 as root bridge (priority 4096).
Device-Level HA	Dual core switches (BASE1 + BASE2), no stacking	Manual failover. Recommend HSRP/VRRP on SVIs (e.g., Vlan1: BASE1 priority 110, BASE2 priority 100).
Management Access	SSH v2 only, VTY access restricted via ACL 1	Only 172.30.30.0/29 (Security) and 192.168.12.0/24 (IT) allowed. No Telnet.
Monitoring Redundancy	SPAN Session 1 (VLANs 500/501) + Session 2 (all Po) → Gi1/0/6	Mirrored traffic to NMS at 203.1.100.1 for IDS/analyzer.

9. Security & Access Control

ACLs

- VTY Access (access-class 1): Permit from 172.30.30.0/29, 192.168.12.0/24; applied inbound on vty 0-15.
- Extended ICMP ACLs: e.g., DSW1 'icmpexe' permits specific pings, denies others, ends with permit ip any any. Applied implicitly to interfaces/VLANs (not shown; assume in/out). Controls DoS via echo limits.
- Branches: Similar 'icmpit' denies unsolicited ICMP.

Other

- No Password-Encryption: Plaintext; enable 'service password-encryption'.
- Logging: Trap debugging to 203.1.100.1 (syslog server, combined with DHCP functions).

• Monitor Sessions: BASE1 SPAN VLANs 500/501 and port-channels to Gi1/0/6 for IDS/NMS.
• Threat Monitoring: Cyber Observer provides detailed threat intelligence, including automated scans for CVE vulnerabilities, behavioral analysis for insider threats, and integration with Network Controller for real-time link health alerts and anomaly detection on traffic patterns.

10. External Connectivity

Device	Interface	IP Address	Subnet Mask	Gateway (ISP)	Protocol Used	Explanation
BASE1 (HQ)	Gi1/0/7	203.1.1.1	255.255.255.0	203.1.1.253	Static + OSPF (Area 0)	HQ primary ISP uplink. Default route injected via OSPF E2.
Ikeja Branch	Gi1/0/8	203.3.3.1	255.255.255.0	203.3.3.254	BGP (eBGP to HQ)	Public IP. BGP peer with HQ (AS 65000). Local subnets advertised.
Lekki Branch	Gi1/0/9	203.2.2.1	255.255.255.0	203.2.2.254	BGP (eBGP to HQ)	Public IP. BGP peer with HQ. Default route via ISP, redistributed.

11. Monitoring & Logging

• SPAN: Session 1 (VLANs 500/501), Session 2 (all Po) → Gi1/0/6 (BASE1).
• NetFlow: v9 export (no destination; configure 'ip flow-export destination').
• Logging: Debugging to syslog; add timestamps. The syslog server at 203.1.100.1 also handles DHCP services for centralized management.
• Advanced Monitoring: Network Controller monitors link utilization, jitter, and packet loss in real-time, generating reports and alerts. Cyber Observer complements this with threat-specific details, such as identifying phishing attempts or DDoS patterns through log correlation and machine learning-based predictions.

12. IP Addressing Plan

Expanded with all subnets from configs/routes.

Subnet	Mask	Purpose	Gateway	Device
10.10.10.0–22.0	/30	Core/Dist Links	.1/.2	Core/Dist

172.16.10–13.0	/24	Internal Services	.254	BASE1
172.21.100.0	/24	Guest	.254	DSW1
172.30.30.0	/29	Security	.6	DSW2
192.168.1–8.0	/24	Management	.254	All
192.168.10.0/16–80	/28–/24	Dept VLANs	Varies	DSW5
192.168.12–20.0	/24	IT/Servers	.254	DSW2/BASE2
192.168.13–17.0	/24	Depts	.254	DSW3/4
192.168.19.0	/24	Local	.254	DSW1
192.168.100/160/190.0	/24	Branch Mgmt	.254	Branches/BASE3
192.168.110–175.0	/24	Branch Depts	.254	Branches/BASE3
203.1.1.0	/24	HQ ISP	.1	BASE1
203.1.100/200.0	/24	Monitoring/Backup	.254	BASE1
203.2.2.0	/24	Lekki ISP	.1	Lekki
203.3.3.0	/24	Ikeja ISP	.1	Ikeja

13. Future Scalability

- BGP Expansion: Add iBGP between cores; peering for cloud.
- VLANs: 50+ available; VTP for propagation.
- IPv6: Disabled; enable cef for dual-stack.
- SD-WAN: Overlay on BGP links.
- Monitoring Enhancements: Expand Cyber Observer for AI-driven threat hunting and integrate Network Controller with orchestration tools for automated scaling.

End of Document
AB-NEXUS: Secure. Scalable. Future-Ready.