io by HFCL

io.hfcl.com

Whitepaper

Designing Secure and Scalable Banking Networks

A Policy-Driven Architecture Approach

Real-World Banking Use Cases across Wired, Wireless, and Access Control

Table of Contents

1. Executive Summary

The banking and financial services sector is undergoing a structural transformation driven by rapid digitization, evolving customer expectations, and increasingly stringent regulatory requirements. While much of the industry focus is placed on digital applications and services, the underlying network infrastructure remains the foundational layer that enables secure, reliable, and continuous banking operations across geographically distributed environments.

Banking networks are fundamentally different from conventional enterprise networks. They are **compliance-driven, highly distributed, integration-intensive, and operationally mission-critical.** Banks must ensure uninterrupted connectivity across their centralized IT environments, zonal and regional offices, and thousands of branch locations. All this while simultaneously maintaining strict adherence to regulatory mandates such as **Reserve Bank of India's cybersecurity directives, Mandatory Testing and Certification of Telecommunication Equipment** (MTCTE) certifications, and audit readiness requirements.

In this context, network infrastructure must address several critical challenges:

Always-on availability
Banking operations require near-zero tolerance for downtime across all network layers

Scalable branch connectivity
Large-scale deployments across hundreds or thousands of branches demand standardized repeatable architectures

Security and access control
Strong enforcement of user (both banking staff and visitors), devices, and network policies aligned with CISO frameworks

Seamless interoperability
Integration with existing banking systems such as NAC, AAA, directory services, and centralized monitoring platforms like Network Management Systems (NMS)

Regulatory compliance and audit readiness
Continuous alignment with RBI, CERT-In, and telecom certification mandates

IO by HFCL addresses these challenges through a purpose-built, end-to-end networking solution portfolio tailored for banking environments. The solution is designed around a multi-tier architecture that aligns with how banks operate today, which spans into centralized IT environments, Local Head offices as aggregation layers, Regional operational centers, and Distributed branch networks.

The IO by HFCL approach focuses on delivering:

Secure wired and wireless infrastructure, including enterprise-grade access points and switching platforms

Robust access control and authentication frameworks, leveraging AAA and standards-based integration with existing NAC systems

Policy enforcement and network security, through multi-tier firewall and gateway solutions

Centralized visibility and operational control, enabled via network management systems and unified wired/wireless controllers

Scalable deployment models, supporting zero-touch provisioning and hierarchy-based, template-driven rollouts across large networks

Importantly, IO by HFCL's solution is designed to integrate seamlessly into existing banking environments, without disrupting established systems or workflows. The focus remains strictly on strengthening the network infrastructure layer, ensuring that banks can operate securely, efficiently, and at scale.

This whitepaper provides a comprehensive view of banking network requirements in the Indian context, outlines the regulatory landscape, and presents HFCL's approach to building secure, compliant, and scalable network infrastructure for modern banking operations.

Introduction

2. Banking Connectivity Trends

2.1. Evolution of Banking IT and Connectivity Requirements

The banking sector has undergone a fundamental transformation over the past decade, driven by the rapid adoption of digital services, evolving customer expectations, and the need for operational efficiency across distributed environments. While much of the industry focus has been on customer-facing platforms, the underlying shift has significantly impacted the **network infrastructure that supports internal banking operations.**

Modern banking environments are no longer confined to isolated branches or centralized systems. Instead, they operate as **highly interconnected, multi-layered ecosystems,** where employees, devices, and applications rely on continuous and secure connectivity. This transformation has elevated the role of network infrastructure from a supporting utility to a **critical enabler of operational continuity, security, and scalability.**

Several key trends are shaping this evolution

1. Branch Modernization and Digital Enablement
Bank branches have evolved from transactional centers into **digitally enabled service hubs**. Employees now rely on continuous access to centralized applications, digital onboarding systems, Video-based remote customer interactions and collaboration tools to deliver efficient services. This shift has significantly increased the demand for **high-performance, always-on connectivity,** both wired and wireless, within branch environments. As a result, network infrastructure must support seamless access to centralized systems while maintaining consistent performance and security across all locations. The ability to deliver reliable connectivity in these environments directly impacts the efficiency of day-to-day banking operations.

2. Rise of Multi-Device and IoT Environments
Modern banking networks today support a diverse and growing range of connected devices. In addition to traditional endpoints such as desktops and laptops, environments now include IP phones, video conferencing systems, surveillance cameras, biometric systems, POS terminals and kiosks and other operational devices. This increase in device density introduces new challenges related to **network capacity, power requirements, and access control.** To address this, network infrastructure must be capable of supporting **PoE-based deployments, device-level segmentation, and policy-driven access mechanisms.** The ability to manage and secure a heterogeneous device environment has become a fundamental requirement for modern banking networks.

3. Shift Toward Distributed IT Architectures
Banking networks are inherently distributed, spanning centralized IT environments, zonal or aggregation offices, regional operational units & a large number of branch locations. Each of these layers serves a distinct purpose while remaining tightly integrated with centralized systems. This hierarchical structure necessitates a network design that can deliver **consistent policy enforcement, centralized visibility, and seamless interoperability** across all layers. Infrastructure must be capable of supporting both centralized control and distributed execution, ensuring that operational consistency is maintained regardless of scale.

4. Increased Emphasis on Zero Trust Network Architecture (ZTNA)
With growing cybersecurity threats and regulatory expectations, banks are increasingly adopting **identity-driven access models** based on Zero Trust Network Architecture. Network access is no longer granted based solely on connectivity but is governed by user and device identity, roles, and predefined policies. This approach requires network infrastructure to support advanced authentication mechanisms such as **802.1X, role-based access control, and integration with centralized AAA and NAC systems.** As a result, the network becomes an active enforcement layer for security policies rather than a passive transport medium.

5. Demand for Centralized Management & Automation
The scale and complexity of modern banking networks make manual operations impractical. Managing thousands of devices across distributed locations requires a shift toward centralized management and automation-driven operations. Banks increasingly rely on capabilities such as template-based configurations, zero-touch provisioning, and real-time monitoring to ensure consistency and reduce operational overhead. These approaches enable faster deployment, improved visibility across the network, and efficient troubleshooting.

2.2. Unique Requirements of Banking Networks

While the trends are shaping connectivity across industries, banking networks, unlike general enterprise networks, operate under a strict operational, regulatory, and architectural constraints. These unique requirements define how network infrastructure must be designed and deployed.

1. 24×7 Availability with Zero Tolerance for Downtime
Banking operations are highly sensitive to disruptions, and network availability is critical to maintaining operational continuity. Employees across branches and offices depend on uninterrupted access to centralized systems to perform daily tasks. As a result, network infrastructure must be designed with high availability, redundancy, and failover mechanisms to ensure consistent performance across all layers.

2. Large-Scale, Distributed Branch Connectivity
Banks typically operate across hundreds or thousands of locations, making scalability a fundamental requirement. Network infrastructure must support **standardized and repeatable deployment models,** enabling institutions to maintain consistency while expanding their footprint.
This requires architectures that can scale efficiently without introducing complexity, ensuring that new deployments can be integrated seamlessly into the existing network.

3. Multi-User and Multi-Role Segmentation
Banking environments involve multiple categories of users and devices, each with distinct access requirements. Employees, administrators, contractors, and operational devices must be governed through clearly defined access policies.
This necessitates the implementation of **segmentation mechanisms such as VLANs, role-based access control, dynamic ACLs and multi-factor authentication,** ensuring that access is restricted on need-basis, as per defined roles and policies.

4. Integration with Existing Banking Infrastructure
Banks operate within well-established IT ecosystems that include NAC platforms, directory services, authentication systems, and centralized monitoring tools. Any new network infrastructure must integrate seamlessly with these systems without disrupting existing workflows. This requirement emphasizes the importance of **interoperability, standard protocols, and flexible integration frameworks,** enabling network components to function cohesively within the broader environment.

5. Compliance and Audit Readiness
Regulatory requirements impose strict expectations on banking infrastructure, particularly in areas related to security, logging, and configuration management. Network environments must be designed to ensure **continuous audit readiness,** enabling institutions to demonstrate compliance at any point in time rather than relying on periodic validation.

A key aspect of this requirement is the need for **alignment with RBI directives and internal CISO-led** security policies, which define the baseline for secure network design, access control, and operational governance. This alignment ensures that network infrastructure is not only technically robust but also compliant with the broader security and risk management frameworks mandated within banking institutions.

To support this, network infrastructure must provide **comprehensive logging, configuration traceability, and visibility into user and device activity.** Systems should be capable of maintaining detailed audit trails, enabling institutions to track changes, investigate incidents, and validate adherence to defined policies. Additionally, support for **secure configuration management, patch enforcement, and rollback capabilities** is essential to ensure that infrastructure remains compliant throughout its lifecycle.

By embedding these capabilities into the network layer, banks can ensure that compliance is not treated as a periodic exercise but as a **continuous and integral part of network operations,** aligned with both regulatory expectations and internal security governance.

The evolution of banking IT has transformed network infrastructure into a **strategic enabler of operations rather than a supporting function.** Modern banking networks must deliver **secure, scalable, and highly available connectivity** across a distributed architecture, while ensuring seamless integration with existing systems and strict adherence to regulatory requirements.

3. Indian Regulatory & Compliance Landscape

The regulatory environment governing banking infrastructure in India is both comprehensive and continuously evolving. Unlike conventional enterprise IT environments, banking networks are subject to **multi-layered regulatory oversight,** where cybersecurity, infrastructure integrity, and operational resilience are tightly controlled. Institutions are required not only to implement secure systems but also to demonstrate **continuous compliance, auditability, and governance alignment** across their entire technology stack. Within this framework, network infrastructure plays a foundational role. It is not merely a connectivity layer, but a *control plane through which security policies, access enforcement, and audit visibility are operationalized.* As a result, network design decisions must be aligned with directives issued by regulatory bodies such as the Reserve Bank of India (RBI), CERT-In, and telecom authorities including TEC and the Department of Telecommunications (DoT).

3.1. RBI Cybersecurity Framework

The RBI's Master Directions on IT Governance, Risk, Controls, and Assurance Practices (2023), effective from April 2024, represent a consolidation of earlier cybersecurity guidelines and establish a unified framework for banking institutions. These directives emphasize a governance-driven approach, where accountability is clearly defined and security is embedded into operational processes rather than treated as an overlay. From a network infrastructure standpoint, the framework necessitates the ability to enforce centralized policies while maintaining distributed control. Access to network resources must be governed through structured mechanisms such as role-based access control and identity-driven authentication. This aligns with the RBI's expectation that access privileges be tightly managed and auditable. Equally important is the requirement for continuous monitoring and incident response readiness. Banking institutions must be capable of detecting anomalous behavior, generating alerts, and maintaining detailed logs that can support forensic analysis. This places a direct requirement on network devices and management systems to provide real-time visibility, event logging, and seamless integration with centralized monitoring platforms. Another critical dimension of the RBI framework is the emphasis on secure configuration and lifecycle management. Systems must be hardened against vulnerabilities, regularly updated, and capable of reverting to known-good configurations when required. For network infrastructure, this translates into the need for secure management interfaces, controlled configuration changes, and structured firmware upgrade processes.

Finally, the RBI mandates periodic audits and compliance validation, which require organizations to demonstrate traceability across their infrastructure. Network systems must therefore support comprehensive audit trails, configuration history, and policy enforcement records, ensuring that compliance is not only achieved but also verifiable.

3.2. RBI Cybersecurity Framework

In parallel with RBI directives, the Information Technology Act (Amendment 2008) and guidelines issued by CERT-In establish baseline expectations for cybersecurity practices across critical sectors, including banking.
CERT-In Directions (April 28, 2022) mandate cybersecurity practices including incident reporting, log retention, and infrastructure monitoring.

Additionally, CERT-In's Guidelines on Information Security Practices for Government Entities provide detailed implementation controls across network security, access management, and monitoring. These regulations focus on ensuring that organizations implement "reasonable security practices" and maintain the capability to respond effectively to cybersecurity incidents. A key requirement under CERT-In directives is the timely reporting of security incidents, which necessitates the presence of robust monitoring and logging mechanisms. Network infrastructure must therefore be capable of capturing detailed event data and forwarding it to centralized systems for analysis and reporting.

This includes support for standardized logging protocols and integration with security information and event management (SIEM) platforms. Access control is another critical area addressed under these guidelines. Organizations are expected to implement strong authentication mechanisms and monitor access to critical systems. In the context of network infrastructure, this requires support for identity-based access control frameworks, including 802.1X authentication, integration with AAA systems, and compatibility with existing NAC deployments. Such capabilities ensure that both users and devices are authenticated before being granted access to network resources. CERT-In guidelines also emphasize vulnerability management and system hardening, requiring organizations to conduct regular assessments and apply timely patches. Network devices must therefore support secure firmware management, patch deployment processes, and configuration compliance mechanisms, enabling institutions to maintain a consistent security posture across all locations.

3.3. Telecom and Device Certification uirements (DoT/TEC/MTCTE)

In addition to cybersecurity regulations, banking networks must comply with telecom and equipment certification requirements defined by the Department of Telecommunications (DoT) and enforced through the Telecommunication Engineering Centre (TEC). Under the Mandatory Testing and Certification of Telecom Equipment (MTCTE) framework, network devices such as access points, switches, and gateways must undergo certification before being deployed in operational environments.
These requirements ensure that all networking equipment meets defined standards for safety, interoperability, and performance. For banks, this introduces an important consideration during procurement and deployment: only certified and compliant devices can be integrated into the network infrastructure. Non-compliance can lead to regulatory challenges and operational risks.

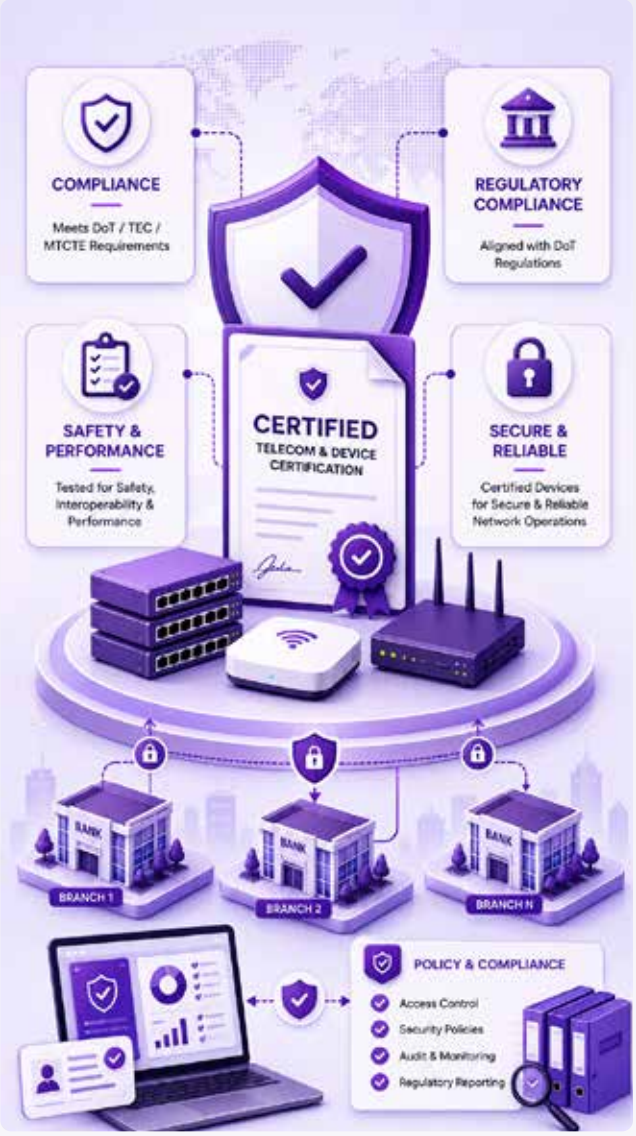
From an architectural perspective, this reinforces the need for standardized and validated infrastructure components, reducing variability and ensuring consistency across deployments. It also aligns with broader regulatory expectations around reliability and long-term maintainability of critical systems.

3.4. Additional Policy and Compliance Considerations

Beyond formal regulatory frameworks, banks must also align with broader policy directives related to data sovereignty, procurement practices, and operational security. Data localization requirements, for instance, necessitate that sensitive information remains within national boundaries. This has implications for how network management systems and control planes are deployed, often favoring on-premises or tightly controlled environments.

Similarly, government initiatives such as Make-in-India policy defined by DPIIT influences vendor selection and procurement -process. Banks are increasingly expected to adopt solutions that align with domestic manufacturing and compliance norms, ensuring both regulatory alignment and supply chain reliability.

Operationally, RBI circulars and internal security policies also mandate network segmentation, secure communication channels, and strict access controls. These requirements must be enforced consistently across all layers of the network, from centralized environments to distributed branches. Network infrastructure must therefore support granular segmentation mechanisms, policy-driven access control, and secure communication protocols, enabling institutions to isolate and

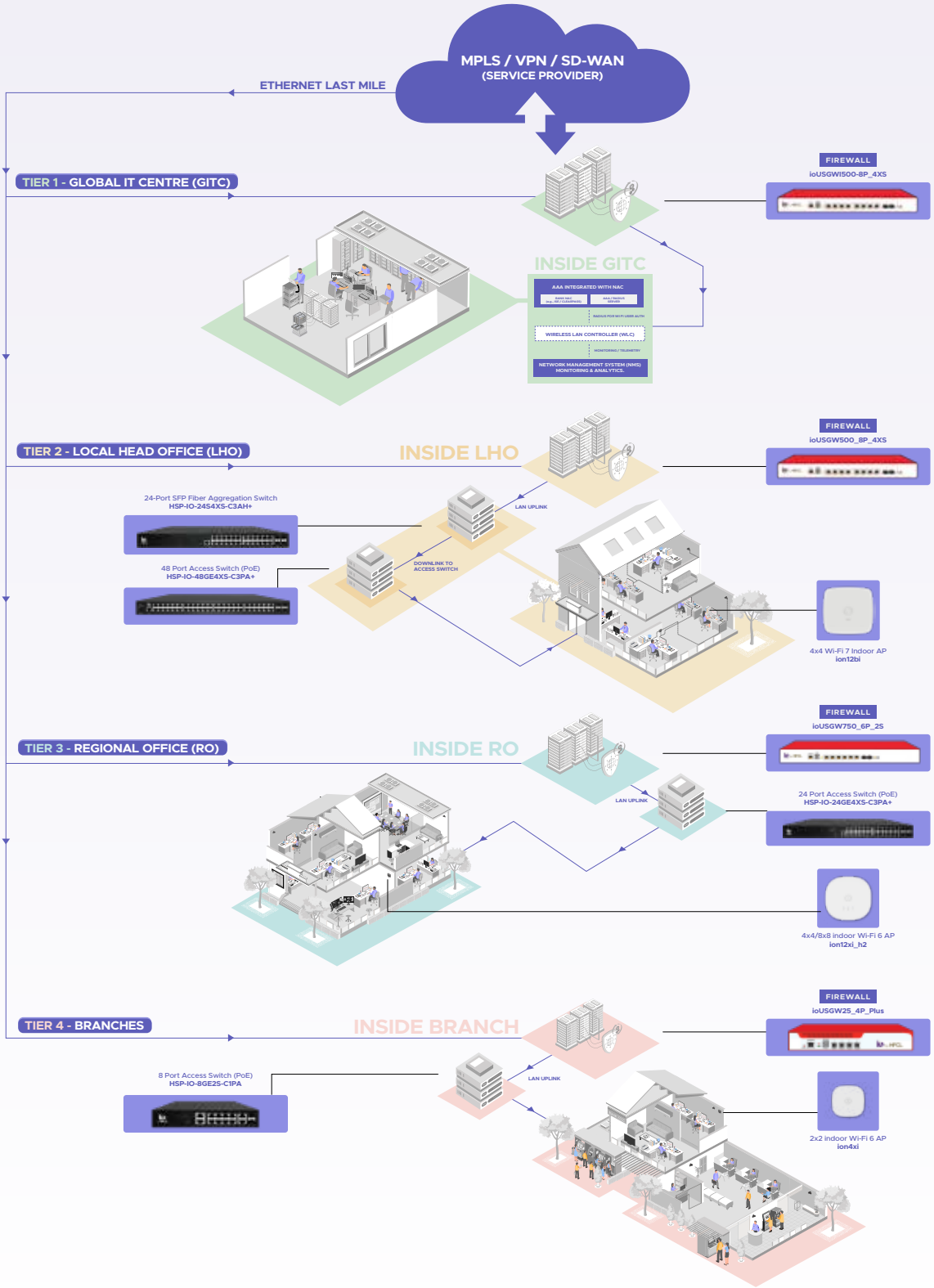


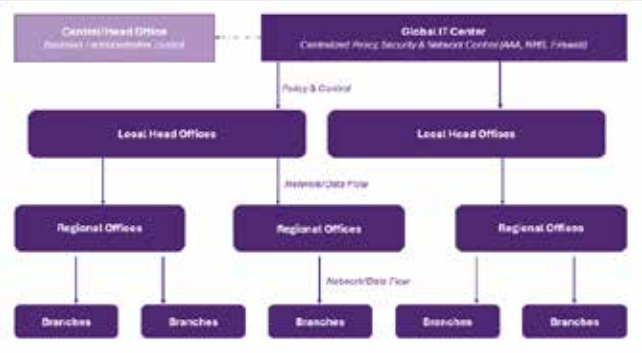
protect different categories of users and devices. The regulatory landscape for banking networks in India establishes a clear expectation: infrastructure must be secure, compliant, and continuously auditable by design. Network systems are expected to go beyond basic connectivity and serve as enablers of governance, security enforcement, and operational transparency.

This places a strong emphasis on capabilities such as identity-based access control, centralized visibility, secure configuration management, and integration with existing security frameworks. Additionally, compliance with certification mandates and policy directives ensures that infrastructure is both reliable and aligned with national standards.
In this context, the design and deployment of network infrastructure become critical to meeting not only operational requirements but also regulatory obligations. The following section outlines how HFCL's networking solution is structured to address these challenges while aligning with the architectural and compliance needs of modern banking environments.

4. IO by HFCL Banking Network Solution

Modern banking networks require an infrastructure approach that is not only scalable and secure but also closely aligned with the multi-tier operational structure of banking institutions. Rather than adopting a one-size-fits-all model, network design must reflect the hierarchical nature of banking environments, spanning centralized IT locations, zonal aggregation layers, regional offices, and distributed branches, each with distinct roles and requirements.





IO by HFCL's banking network solution is built around this principle of architecture-aligned deployment, where each layer of the network is equipped with purpose-built components that address its specific operational, security, and scalability needs.

The solution focuses exclusively on the network infrastructure layer, enabling secure connectivity, access control, and operational visibility without interfering with application or core banking systems.

Layer-specific infrastructure design, aligned with banking network hierarchy

Seamless integration with existing heterogenous banking environment, including NAC, AAA, NMS and directory services

Compliance-driven architecture, supporting regulatory and audit requirements by design

4.1. Reference Architecture Approach

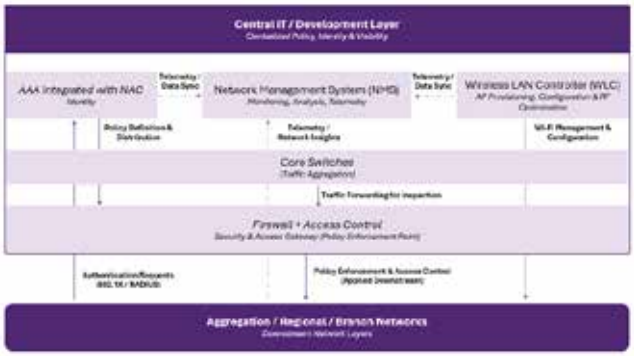
A well-designed banking network must reflect the inherently hierarchical and distributed nature of banking operations. Rather than treating the network as a flat connectivity layer, it is essential to structure it across clearly defined tiers, each responsible for a specific set of functions while remaining tightly integrated with centralized control systems.

The reference architecture presented here follows a multi-tier model, where centralized systems provide policy, authentication, and visibility, while distributed layers execute these policies closer to users and devices. This separation enables scalability, ensures operational consistency, and simplifies deployment across large and diverse banking environments.

4.1.1. Central IT / Development Layer

The central IT environment functions as the control and governance layer of the network. It is responsible for defining access policies, authenticating users and devices, enforcing security controls, and maintaining visibility across all connected locations. This layer does not directly handle user access but instead orchestrates how access is granted and managed across the network. Within this environment, authentication services validate identities and enforce role-based access policies, while security gateways inspect and regulate traffic entering and exiting the network. Wireless control functions manage access points deployed across distributed locations, ensuring consistent configuration and performance. In parallel, management systems provide real-time monitoring, logging, and integration with existing banking infrastructure through standard interfaces.

By centralizing these functions, the network ensures that policy decisions remain consistent, regardless of where users or devices connect from. This model is particularly critical in banking environments where regulatory alignment and audit readiness are mandatory.



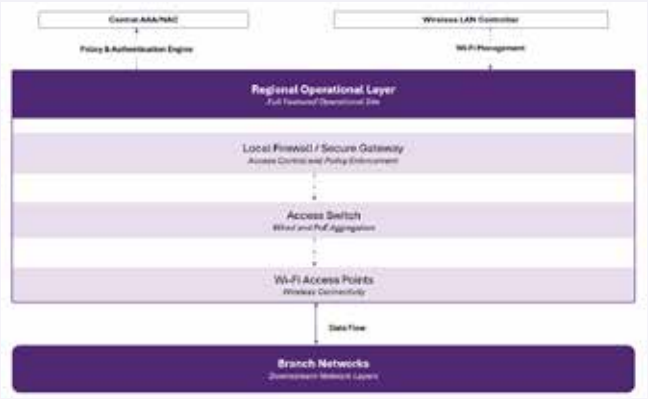
4.1.2. Zonal / Aggregation Layer

The aggregation layer acts as the intermediate consolidation tier, bridging centralized systems with distributed operational environments. It is designed to aggregate traffic from multiple regional locations while extending centralized policies closer to the edge. At this layer, high-capacity aggregation switches consolidate traffic flows and ensure efficient forwarding toward central systems. Security enforcement continues through appropriately scaled firewall deployments, enabling segmentation and controlled communication between different network zones. In addition, access control enforcement points ensure that identity-driven policies defined at the central layer are consistently applied as traffic traverses the network. This layer plays a critical role in maintaining network stability and scalability, as it isolates faults, optimizes traffic distribution, and ensures that large volumes of data can be handled without impacting performance. It also enables controlled expansion of the network by acting as a buffer between core systems and regional deployments.

4.1.3. Regional Operational Layer

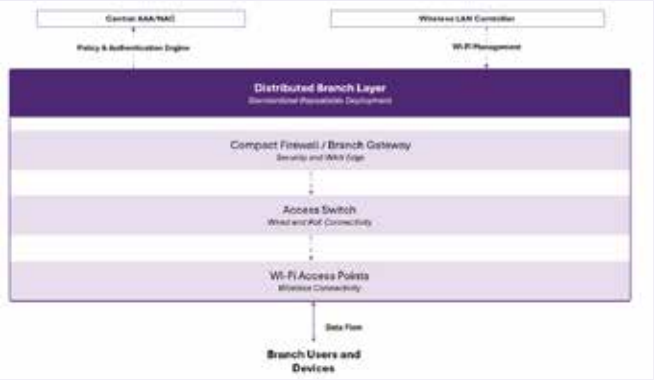
Regional offices represent operational network environments where both connectivity and policy enforcement converge. These locations support employees, operational systems, and wireless users, requiring a balanced approach to performance, security, and manageability. Access switches provide wired connectivity for users and devices, while PoE capabilities enable the deployment of access points and other powered endpoints. Wireless infrastructure delivers secure connectivity for employee devices, with centralized control ensuring uniform configuration across all sites. Security enforcement is maintained through firewalls and gateways, which regulate traffic and enforce access policies locally while remaining aligned with centralized definitions. This layer ensures that users experience consistent and secure connectivity, regardless of their location, while enabling the network to scale efficiently across multiple regional sites. It also serves as an important checkpoint where centralized policies are translated into real-world access control decisions.

At this layer, high-capacity aggregation switches consolidate traffic flows and ensure efficient forwarding toward central systems. Security enforcement continues through appropriately scaled firewall deployments, enabling segmentation and controlled communication between different network zones. In addition, access control enforcement points ensure that identity-driven policies defined at the central layer are consistently applied as traffic traverses the network.
This layer plays a critical role in maintaining network stability and scalability, as it isolates faults, optimizes traffic distribution, and ensures that large volumes of data can be handled without impacting performance. It also enables controlled expansion of the network by acting as a buffer between core systems and regional deployments.



4.1.4. Branch Layer (Distributed Edge)

The branch layer is characterized by high scale, geographical spread and operational simplicity, as banks typically operate across hundreds or thousands of such locations, distributed across the country. The network design at this layer prioritizes ease of deployment, minimal configuration overhead, and consistent policy enforcement. Each branch deployment typically includes access switching for wired connectivity, optional PoE capability for powering wireless access points and surveillance devices, and a compact firewall or gateway for security enforcement. Wireless access points provide connectivity for employees and operational use cases, with configurations centrally managed to ensure uniform behavior across all branches. Despite its simplicity, this layer remains fully integrated with centralized systems. Authentication requests are validated through central AAA systems, policies are inherited from the control layer, and monitoring data is continuously fed back to management platforms. This ensures that even at scale, the network maintains uniform security posture and operational visibility.



4.1.5. End-to-End Network Behavior

While each layer performs a distinct role, the network operates as a single, unified system, where multiple types of flows traverse the architecture simultaneously. User traffic originates at the edge and moves upward through the hierarchy, while authentication, policy enforcement, and management functions are orchestrated centrally and applied across all layers. Authentication requests initiated at branch or regional levels are validated centrally, ensuring identity-driven access control. Security enforcement is applied at multiple points across the network, creating a layered defense model. At the same time, telemetry and operational data flow continuously toward centralized systems, enabling real-time visibility and proactive management. This interplay between centralized intelligence and distributed execution ensures that the network remains secure, scalable, and operationally consistent, even as it expands across large and diverse environments.

The reference architecture establishes a clear separation between centralized control functions and distributed access layers, enabling banking networks to scale efficiently without compromising on security or operational control. By aligning infrastructure deployment with the hierarchical structure of banking environments, the design ensures consistent policy enforcement, seamless integration with existing systems, and high levels of visibility across all locations.

4.2. IO by HFCL Banking Product Portfolio

HFCL's portfolio for banking networks spans key infrastructure domains required to build and operate secure, scalable, and distributed environments.

The wired infrastructure layer is anchored by a range of Layer-2 and Layer-3 switches, comprising of PoE and Non-Poe models, along with SFP-based aggregation switches designed to support connectivity across different network tiers. Access switches provide reliable connectivity for user devices and operational systems, while PoE capabilities enable the deployment of access points, IP cameras, and other powered devices. Aggregation switches, particularly SFP-based platforms, are positioned at higher network layers to consolidate traffic and provide high-throughput uplink connectivity.

Complementing the wired infrastructure is HFCL's wireless networking portfolio, which includes enterprise-grade indoor and outdoor access points designed for high-density environments. These access points support latest Wi-Fi standards and are managed through a centralized wireless controller platform (io Canvas), enabling configuration, monitoring, and policy enforcement specifically for wireless networks. This ensures consistent performance and secure access across distributed locations.

In addition to the connectivity and management layers, HFCL's portfolio also incorporates critical security, identity, and access control components, which are fundamental to banking network architectures. This includes next-generation firewalls deployed across data center, regional, and branch environments to enforce perimeter security, support advanced threat protection, and enable secure segmentation of network zones. These firewalls are designed to handle high-throughput traffic while supporting features such as deep packet inspection, VPN termination, and policy-based access control.

To strengthen identity-driven access, the portfolio includes AAA (Authentication, Authorization, and Accounting) systems, available in both on-premises and cloud-based deployment models. These systems integrate with enterprise directories and enable centralized control over user and device access across wired and wireless networks. Capabilities such as RADIUS-based authentication, user profiling, and integration with NAC frameworks ensure that only authorized users and compliant devices gain access to network resources.

The solution also includes network management capabilities that provide visibility into network operations. While wireless networks are centrally managed through the controller, broader network visibility and monitoring are enabled through network management systems that support logging, analytics, and integration with existing monitoring platforms via standard interfaces.

Together, these additional components complement the existing wired, wireless, and management layers by introducing end-to-end security, identity enforcement, and policy control, enabling banks to build a secure, compliant, and centrally governed network architecture across all tiers.

5. Banking Use Case Scenarios

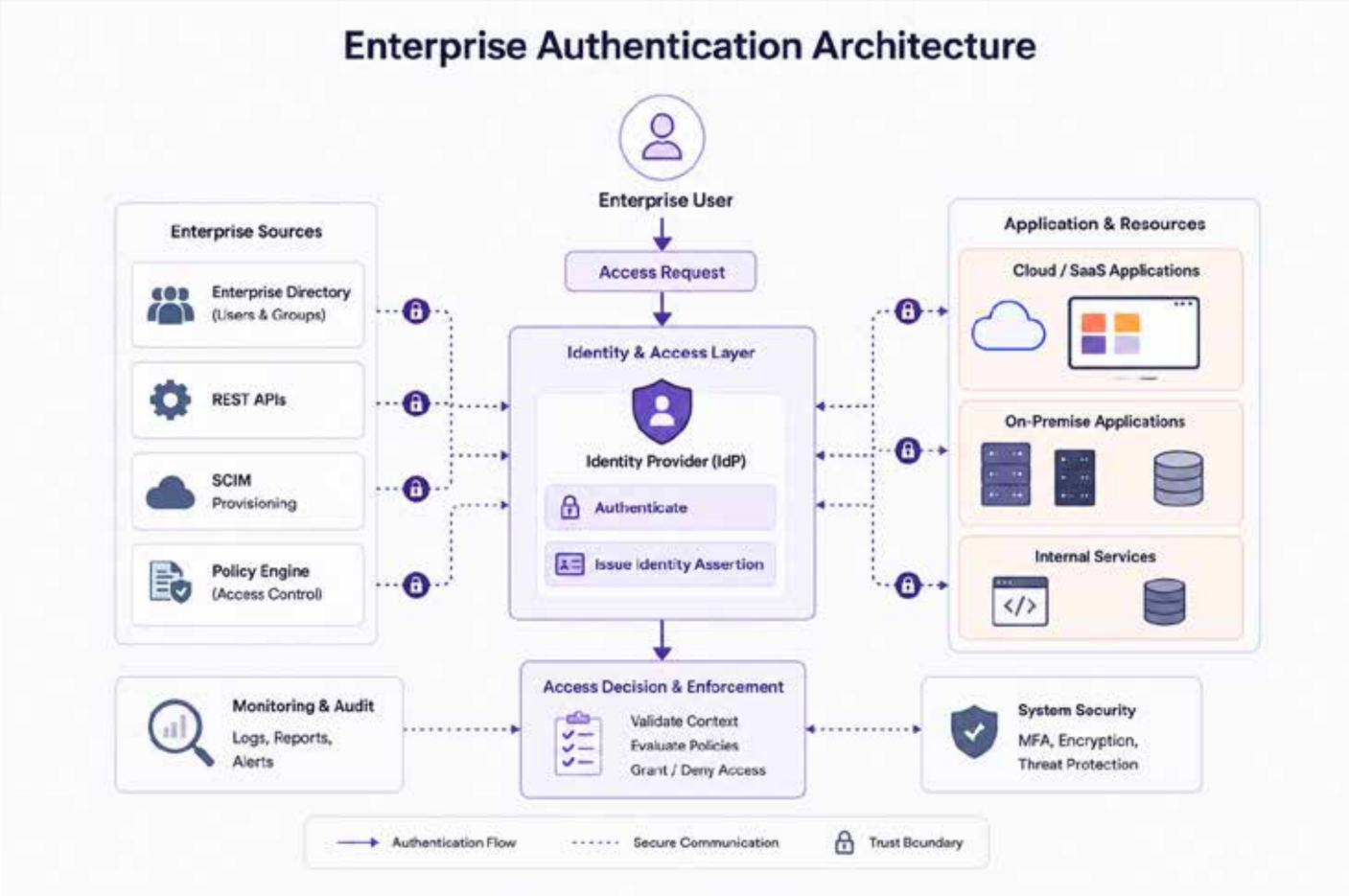
Banking networks are not designed in abstraction, in fact, they are built to support specific operational workflows across branches, regional offices, and centralized IT environments. While the underlying architecture defines how connectivity, security, and policy enforcement are structured, its effectiveness is ultimately determined by how well it enables real-world banking operations.

In practice, each layer of the network must support distinct use cases

- Secure wired connectivity within branches
- High-density wireless access for employees, developers and guests
- Controlled onboarding of users and devices, and
- seamless integration with centralized policy and authentication systems

These requirements are not isolated, they operate simultaneously within the same environment, often at large scale and under strict regulatory expectations.

The following sections examine key banking use cases in detail, focusing on how these scenarios are implemented within the network. Each use case is described in terms of its operational context, the flow of traffic and control, and the role of the network in enforcing security, segmentation, and reliability. The objective is to provide a clear, practical view of how a well-architected network supports day-to-day banking operations across distributed environments.



5.1. Wired Access and Segmentation Across Banking Locations

Across banking locations ranging from central offices to regional sites and branches, multiple systems operate simultaneously. These can be teller terminals, back-office desktops, IP phones, surveillance cameras, biometric devices, and sometimes kiosks. While these systems coexist within the same physical environment, they must not share the same network behavior or security posture. The network at this layer must therefore ensure that connectivity is not just available, but controlled, segmented, and predictable, without adding operational complexity at the branch level.

For example, a teller system handling customer operation cannot be exposed to the same network segment as a CCTV camera or a visitor-facing device. At the same time, all these endpoints must function reliably without introducing operational delays.

5.1.1. How It Works

At the branch, the access layer is built around a PoE-enabled access switch, which serves as the primary aggregation point for all wired endpoints.

Each device/user category is mapped to a dedicated logical segment (VLAN). This ensures that even though devices share the same physical infrastructure, their traffic remains isolated and governed by policy.

A typical flow operates as follows

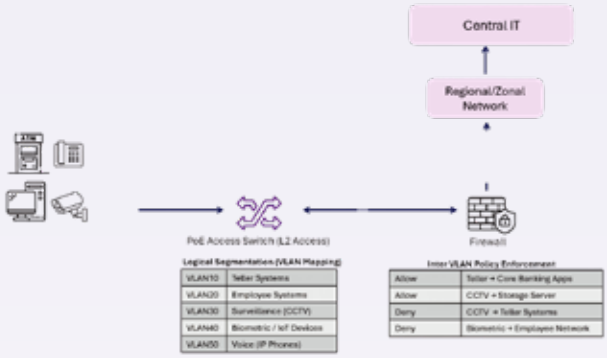
- End devices (e.g., teller systems, desktops, cameras) connect to the access switch
- The switch assigns each connection to a predefined VLAN (or dynamically via policy)
- Traffic is tagged and isolated at Layer-2 within the branch
- All traffic is forwarded upstream to the branch firewall for inspection

At the firewall

- Inter-VLAN communication is controlled based on defined policies
- Only authorized traffic between segments is permitted
- All other traffic is restricted, ensuring isolation between device categories

From here, validated traffic is forwarded towards upstream layers (regional or central systems) over secure links.

For example, a teller system handling customer operation cannot be exposed to the same network segment as a CCTV camera or a visitor-facing device. At the same time, all these endpoints must function reliably without introducing operational delays.



5.1.2. Network Behavior and Enforcement

This design ensures that the network enforces segmentation and control inherently, rather than relying on endpoint-level security.

Key behaviors enabled at this layer include

Logical isolation of devices
Teller systems, surveillance devices, and employee endpoints operate in separate segments, reducing the risk of unauthorized access.

Controlled inter-segment communication
Any communication between VLANs is explicitly governed by firewall policies, ensuring that only required traffic flows are allowed to cross VLAN boundaries.

Consistent policy enforcement across branches
Since VLAN structures and firewall policies are standardized, the same behavior can be replicated across all branch deployments.

Resilience through redundant design
Features such as dual uplinks, link aggregation, and loop prevention mechanisms ensure that connectivity is maintained even in case of link or device failures.

5.1.3. Why This Matters in Practice

In a real branch environment, this architecture enables predictable and secure operations without manual intervention

- A new device can be added and automatically placed into the correct network segment
- A compromised endpoint remains isolated and cannot access sensitive systems
- Network disruptions are minimized due to built-in redundancy
- IT teams can deploy identical configurations across hundreds or thousands of branches

The result is a network that behaves as a controlled access environment, where connectivity, security, and segmentation are enforced by design and supports the operational and compliance requirements of modern banking environments.

5.2. Secure Wireless Access for Employees and Guests

Wireless connectivity within banking environments must support two fundamentally different access models operating on the same infrastructure. Employees require seamless, secure access to internal systems, while guest users such as visitors, auditors, or third-party contractors require limited, controlled connectivity with no access to internal resources.

The challenge lies in enabling both access types simultaneously while ensuring that:

- Security is not compromised
- User experience remains seamless
- Policies are enforced consistently across all branches

This is achieved through a combination of **SSID-based segmentation, centralized authentication, and policy-driven access control.**

5.2.1. How It Works

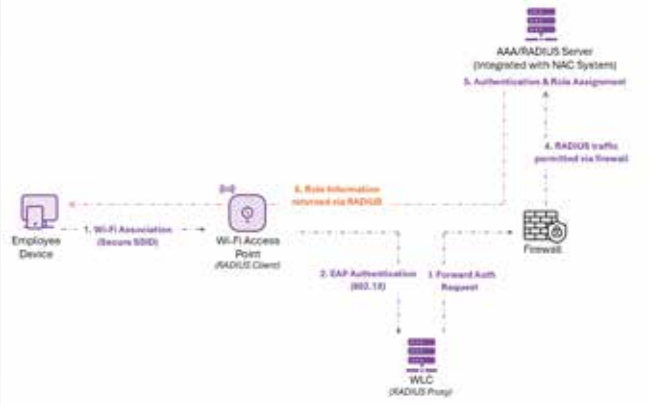
Across banking locations, Wi-Fi access is delivered through enterprise-grade access points, centrally managed via a wireless controller. Multiple SSIDs are broadcast, each mapped to a specific access model.

Employee Access (Secure, Identity-Based)
Employees connect to a dedicated secure SSID configured for enterprise authentication.

The flow operates as follows:

- The employee device connects to the **secure SSID**
- The access point forwards the authentication request upstream via the network
- The request is validated against the **central AAA system integrated with the bank's NAC**
- Upon successful authentication
  - The user is assigned a role or profile
  - Corresponding network policies (VLAN, access rules) are applied
- The user gains access only to permitted internal resources

This ensures that access is not just granted but contextually controlled based on identity.



Guest Access (Captive Portal-Based)

Guest users connect to a separate SSID designed for controlled, temporary access.

The flow is as follows

- The guest device connects to the **guest SSID**
- The user is redirected to a **captive portal (hosted via AAA system)**
- Authentication is performed using predefined methods (e.g., OTP, credentials, or sponsor-based access)
- Upon successful login:
  - The user is granted internet access
  - Access is restricted from internal banking systems
- Session policies such as **time limits and bandwidth controls** are enforced

This ensures that guest access is **isolated, auditable, and temporary by design.**

5.2.2. Network Behavior and Enforcement

The wireless network enforces strict separation between different user categories, even though they share the same physical infrastructure.

SSID-based segmentation ensures logical separation
Employee and guest traffic are isolated from the point of association.

Identity-driven access control for employees
Access is dynamically assigned based on authentication outcomes from AAA/NAC systems.

Complete isolation of guest traffic
Guest users are restricted to internet access and are prevented from accessing internal networks.

Centralized policy enforcement across branches
Wireless configurations and policies are managed centrally, ensuring consistency in user experience and security posture.

5.2.3. Why This Matters in Practice

In a real banking environment, this model ensures both usability and control:

- Employees experience seamless and secure connectivity without manual configuration
- Guest users can access the internet without risking exposure to internal systems
- Access policies remain consistent across all locations, regardless of scale
- IT teams retain full visibility and control over user sessions and access behavior

This approach transforms wireless connectivity from a convenience layer into a **controlled access framework,** where every connection is authenticated, segmented, and governed in alignment with banking security requirements.

5.3. User Role-Based Access and Segmentation

Banking environments operate with multiple categories of users, i.e., employees, administrators, auditors, third-party vendors, and temporary staff etc. Each requires different levels of access to network resources. These users often connect through both wired and wireless networks across different locations, but their access **must remain strictly governed by identity and role,** not by where they connect from. A teller accessing internal systems, an auditor performing compliance checks, and a vendor connecting for maintenance must all be treated differently by the network, even if they are connected to the same access point or switch.

This requires the network to move beyond static segmentation and adopt a **dynamic, identity-driven access model.**

5.3.1. How It Works

User access is enforced through integration between the network infrastructure and centralized **AAA systems aligned with the bank's NAC framework.** Authentication and authorization decisions are made centrally, while enforcement happens at the network edge.

A typical flow operates as follows:

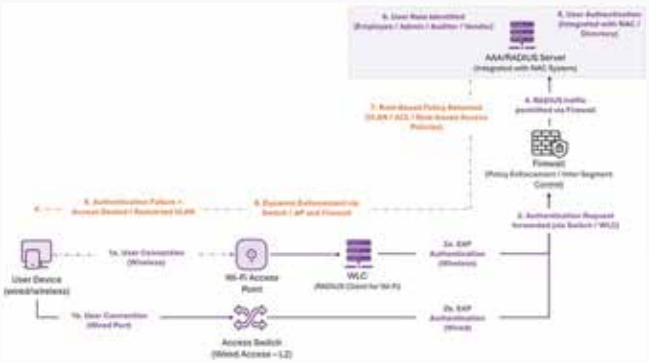
- A user connects to the network (via wired port or Wi-Fi SSID)
- The access device (switch or access point) initiates an authentication request (802.1X)
- The request is forwarded to the AAA system, which is integrated with the bank's NAC and identity systems
- The user's credentials are validated against centralized directories or NAC policies

Upon successful authentication:

- The user is mapped to a role/profile (e.g., employee, admin, auditor, vendor)
- The network dynamically applies:
  - VLAN assignment
  - Access control policies
  - Network privileges based on role
- Traffic from the user is then enforced through the firewall and access control systems, ensuring that only permitted resources are accessible

If authentication fails:

- Access is denied or restricted to a limited network segment



5.4.2. Network Behavior and Enforcement

This model ensures that access decisions are made based on **who the user is**, rather than **where they are connected from.**

Non-802.1X onboarding mechanisms
Headless devices that cannot perform username-based authentication are still identified and onboarded using alternative methods.

Device-level segmentation
Each device category operates within its own isolated network segment, preventing lateral access.

Restricted communication paths
Devices are allowed to communicate only with predefined systems (e.g., camera to NVR), reducing attack surface.

Scalable onboarding across locations
Policies are centrally defined and automatically applied, enabling consistent deployment across thousands of sites.

5.4.3. Why This Matters in Practice

In real banking environments, this approach enables controlled integration of operational devices without compromising security:

- A newly installed CCTV camera is automatically placed into a restricted network segment
- A biometric device can communicate only with authentication servers and nothing else
- A compromised IoT device cannot move laterally within the network
- Large-scale deployments can be executed without manual configuration at each site

This ensures that all connected devices, whether user-driven or system-driven, operate within a **secure and policy-governed framework,** aligned with the broader network architecture.

5.5. Centralized Policy Enforcement and Visibility

Banking networks operate across multiple layers and locations, but must behave as a **single, controlled system.** Policies related to user access, device behavior, and security enforcement cannot be defined independently at each site; they must be centrally governed to ensure consistency, compliance, and audit readiness.

At the same time, operations teams require continuous visibility into network behavior, across wired and wireless environments, to monitor performance, detect anomalies, and respond to issues in real time.

This creates a dual requirement:

- **Centralized control** of policies and configurations
- **End-to-end visibility** across distributed infrastructure

5.5.1. How It Works

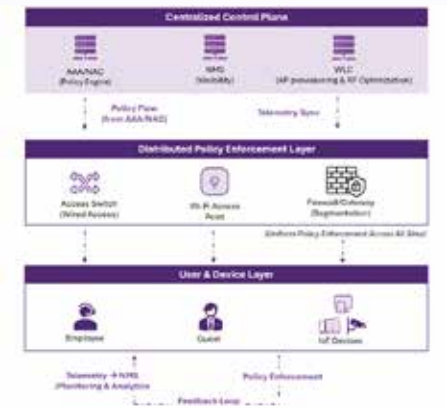
The network operates on a model where **control is centralized,** while **enforcement is distributed across the network layers.**

From a policy perspective:

- Access and security policies are defined within centralized systems such as AAA/NAC platforms
- These policies determine:
  - Who can access the network?
  - What level of access is granted?
  - Which resources are permitted?
- Once defined, these policies are enforced across the network through:
  - Access switches (for wired connections)
  - Access points (for wireless connections)
  - Firewalls and gateways (for traffic control and segmentation)

From a visibility and management perspective:

- Network devices continuously generate telemetry related to:
  - Device status
  - Client connectivity
  - Traffic behavior
- This information is collected by centralized management platforms, which provide:
  - Real-time monitoring of network health
  - Historical insights for troubleshooting and optimization
  - Visibility across all locations from a single interface
- Wireless infrastructure is managed through a dedicated controller, which ensures:
  - Consistent configuration of access points
  - RF optimization and performance tuning
- The controller and management systems can exchange data to provide a unified operational view, without overlapping control functions.



6. From Rollout to Run: Network Operations and Lifecycle

6.1. HFCL's 4-Stage End-to-End Network Services Framework

HFCL delivers banking network modernization through a structured 4-stage professional services framework designed specifically for financial institutions. This service-led approach provides single-point accountability from initial assessment to audit-ready handover, eliminating fragmented partner ecosystems. The framework ensures regulatory compliance, zero-downtime deployments, and seamless integration with existing NAC and security infrastructure.

Stage 1

Network Assessment & Gap Analysis

OBJECTIVE
Establish the bank's target network model, security posture, and service priorities before any deployment begins.

Key Activities

- Review the current network estate across GITC, LHO, RO, and branch locations.
- Assess existing network, segmentation, NAC, and security dependencies.
- Identify gaps in availability, policy consistency, and compliance readiness.
- Validate control requirements for Zero Trust and secure remote operations.

Deliverables

- Network segmentation blueprint for GITC, LHO, RO, and branch environments.
- QoS design for traffic prioritization across banking segments.
- Zero Trust policy framework covering dACLs, CoA triggers, and RADIUS integration.
- SASE and unified security architecture design.

Stage 2

Zero-Trust Security Design & Reference Architecture

OBJECTIVE
Translate the approved policy and segmentation model into deployable site standards and configurations.

Key Activities

- Conduct site surveys at representative locations.
- Capture RF conditions, switch-port requirements, cabling readiness, and power availability.
- Define branch archetypes by size and function.
- Map AP density, switch placement, and controller placement by site type.
- Prepare standard configuration profiles for repeatable rollout.

Deliverables

- Site survey reports with heat maps and switch and AP placement recommendations
- Standard profiles for branch, LHO, and RO, including small, medium, and large site types.
- Configuration templates for SSIDs, VLANs, ACLs, QoS, and security policies.
- Bill of Materials for switches, access points, and on-premises controllers per site type.

Stage 3

Deployment, Migration and Cutover

OBJECTIVE
Execute rollout in controlled phases with minimal disruption to branch operations.

Key Activities

- Prepare staged rollout from pilot branches to regional rollout and then nationwide deployment.
- Configure zero-touch provisioning through the on-premises controller.
- Plan coexistence with legacy switches, older Wi-Fi, and existing firewalls.
- Prepare migration runbooks with rollback procedures.
- Execute weekend or after-hours cutovers for customer-facing sites.
- Validate connectivity, policy enforcement, and service continuity after cutover.

Deliverables

- Staged rollout plan from pilot branches to regional rollout to nationwide deployment.
- Zero-touch provisioning configuration via on-premises controller.
- Coexistence plan for legacy switches, old Wi-Fi, and existing firewalls.
- Branch migration runbooks with rollback procedures.
- Weekend or after-hours cutover execution for customer-facing locations.
- Post-deployment validation reports covering performance, security, and compliance checks.

Stage 4

Audit-Ready Handover & AI-Driven Optimization

OBJECTIVE
Move the network into steady-state operations with governance, visibility, and improvement built in

Key Activities

- Monitor the estate through centralized management and AI-driven analytics.
- Tune performance, capacity, and policy behavior based on live usage.
- Finalize documentation and operational handover.
- Train internal IT teams for ongoing management and troubleshooting.
- Establish escalation workflows and support procedures.

Deliverables

- AI analytics-driven optimization report covering performance tuning and capacity planning.
- Complete network documentation including policies, VLANs, ACLs, and RADIUS configurations.
- Audit-ready compliance artifacts including RBI evidence and change logs.
- IT team training on network management, troubleshooting, and policy updates.
- Operational runbooks and escalation procedures.

7. Deployment Highlights and Case Studies

India's Largest Public Sector Bank: GITC Wi-Fi Modernization

Scan the QR Code to
Download the Case Study

One of India's oldest government-owned banks needed to modernize wireless connectivity at its Global IT Center to support accelerated digitalization across front-end and back-end systems. The existing network could not meet the density, security, or visibility demands of the bank's growing IT operations. HFCL deployed 165 Wi-Fi 6 indoor access points across the GITC campus, managed centrally through a cloud network management system. The solution incorporated WPA3 and AES encryption, AAA-based authentication, firewall enforcement, and an SMS gateway for regulatory-compliant user authentication.

The results were measurable. Employee complaints about network slowness reduced by 2x, customers served per session increased by 3x, and the deployment delivered an 80% reduction in infrastructure investment costs. Security was strengthened through WPA3, AES, and TPK encryption, and the stable network foundation enabled the IT team to extend IoT device adoption across the campus. This deployment demonstrates how a centralized banking operations environment can be modernized without disrupting live workloads, and directly supports the GITC-layer architecture described in Section 4.1.1 of this whitepaper.

Large Public Sector Bank: Seamless Switch Transformation Across 1,600+ Branches

Scan the QR Code to
Download the Case Study

One of India's oldest public sector banks, processing more than 604 million UPI transactions monthly, needed to replace foreign-manufactured switches across its entire branch network to comply with the government's Make in India initiative. The primary challenge was executing this at scale without disrupting live banking operations, while also ensuring that the new switches integrated cleanly with the bank's existing NAC system and maintained branch-level security continuity. HFCL supplied 2,800 Make-in-India 24-port L2 managed switches across 1,600+ branches. Each switch was configured with a robust authentication mechanism for secure user access and a local security feature that ensured uninterrupted branch operations even in the event of a disconnect from the central system. Integration with the bank's existing NAC ensured that only authorized devices could access branch networks.

The transition was completed without any downtime across the bank's network. Branch connectivity remained uninterrupted throughout the cutover, security protocols were strengthened against cyber threats, and the local security capability provided an additional layer of resilience at the branch edge. This deployment demonstrates how a large-scale branch switch refresh can be executed with zero operational disruption, and directly supports the branch-layer architecture and Stage 3 migration approach described in Sections 4.1.4 and 6.1.3 of this whitepaper.

India's Largest Insurance Provider: Branch Network Modernization at Scale

Scan the QR Code to
Download the Case Study

India's largest government-owned insurance institution operates across 8,000+ offices, serving 290 million policies with a 1.3 million-strong agent network. Its infrastructure must support uninterrupted access to policy management systems, CRM platforms, and centralized financial databases.
The challenge: replace End-of-Life and End-of-Sale L2 switches across branch offices nationwide, within strict timelines, without disrupting live operations, and with full integration into existing infrastructure. HFCL deployed 2,000+ units of fully managed 24-port non-PoE switches and 500+ units of 8-port non-PoE switches across the branch estate. The switches, with a switching capacity of were configured with dynamic ACLs, dynamic VLAN assignment, L2/L3/L4 ACLs for policy enforcement, and SNMP integration for centralized monitoring and proactive fault detection.

The deployment was completed on schedule with zero operational disruption. Outcomes included expanded port density for growing device populations, optimized bandwidth for financial transactions, strengthened access controls, and proactive fault detection via SNMP-enabled monitoring.
This deployment illustrates the branch-layer architecture covered in Section 4.1.4, where standardized switching at scale must balance security enforcement, operational continuity, and centralized visibility.

India's Apex Rural Development Institution: Network Modernization at Scale

Scan the QR Code to
Download the Case Study

HFCL modernized the nationwide network infrastructure of India's apex institution for agriculture and rural development, helping strengthen connectivity across a distributed rural finance environment. The institution needed to replace a legacy wired environment that was limiting bandwidth, causing frequent disruptions, and constraining the delivery of digital services and training programs. The upgrade also had to support secure access, centralized visibility, and continuity across a large and geographically dispersed operational footprint. HFCL deployed 156 Wi-Fi 6 indoor access points and 8 fully managed 24-port switches across the premises. The solution used an on-premises controller integrated with the existing NAC and firewall environment, along with two SSIDs, one for authenticated users and one for guest access. AI-powered analytics provided centralized monitoring, proactive issue detection, and better operational control.

The result was improved employee productivity, reduced downtime, and faster digital transaction processing. The new network also supported training, collaboration, and digital inclusion initiatives across rural communities. This deployment reflects the multi-tier architecture and on-premises management model described in Sections 4.1 and 4.2 of the whitepaper, where distributed financial institutions require centralized policy control without compromising security or data sovereignty.

8. Conclusion

Modern banking networks are no longer passive connectivity layers, they have evolved into active **enforcement systems** that govern how users, devices, and applications interact across a highly distributed environment. As banks expand across centralized IT hubs, regional offices, and large-scale branch networks, the need for a network that delivers **consistent control, security, and operational visibility** becomes critical. This whitepaper has outlined how a structured, multi-layered network architecture can address these requirements by separating **centralized control from distributed enforcement**. By integrating authentication, policy definition, and monitoring within centralized systems, while enabling enforcement at the edge through switches, access points, firewalls, and gateways, the network becomes both scalable and resilient. The use cases explored demonstrate that real-world banking operations—ranging from secure wired connectivity and wireless access to identity-driven user segmentation and IoT device onboarding—can be effectively supported through a **policy-driven networking approach.** In such a model, access is determined by identity and role rather than location, ensuring that security and compliance requirements are consistently met across all environments. Equally important is the ability to maintain **operational simplicity at scale**. Centralized visibility, standardized deployment models, and automated policy enforcement allow banks to manage thousands of sites without introducing complexity at individual locations. This ensures faster deployments, reduced operational overhead, and improved responsiveness to network events. From a regulatory standpoint, the architecture aligns with the expectations of banking institutions by enabling **continuous audit readiness, traceability, and policy consistency,** supporting adherence to RBI directives and internal CISO-led security frameworks. Ultimately, the network becomes a **strategic enabler of banking operations**—providing the foundation for secure access, seamless connectivity, and scalable growth. By adopting an architecture that is aligned with operational realities and built on standardized, interoperable components, banks can ensure that their network infrastructure remains robust, adaptable, and future-ready.

9. References and Standards

This whitepaper is aligned with established networking standards, security frameworks, and regulatory guidelines relevant to enterprise and banking environments. Key references include:

Networking Standards

IEEE 802.1X – Port-Based Network Access Control
https://standards.ieee.org/standard/802_1X-2020.html

IEEE 802.11 (Wi-Fi Standards)
https://www.ieee802.org/11/

Security and Authentication

RFC 2865 – Remote Authentication Dial-In User Service (RADIUS)
https://datatracker.ietf.org/doc/html/rfc2865

RFC 3580 – IEEE 802.1X RADIUS Usage Guidelines
https://datatracker.ietf.org/doc/html/rfc3580

https://www.cisco.com/c/en/us/solutions/enterprise-networks/campus-network.html

Industry Best Practices

Wi-Fi Alliance – Enterprise Security (WPA3)
https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.5.pdf

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

Regulatory and Compliance (India – Banking Context)

Reserve Bank of India – Cyber Security Framework for Banks
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/107MDITGOVERNANCE3303572008604C67AC25B84292D85567.PDF

Information Technology Act (2008)
https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=

Telecommunication Engineering Centre (TEC) – MTCTE Certification
https://www.tec.gov.in/standards-specifications (TEC 48060:2026 - LAN Switches, TEC 38020:2021 – Access Points)

Cert-in Guidelines
https://www.cert-in.org.in/ (Guidelines - Guidelines on Information Security Practices for Government Entities)

https://www.cert-in.org.in/Directions70B.jsp (Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet)

10. Glossary

Authentication, Access & Security	
AAA	Framework that controls user/device access **A**uthentication for identity verification, **A**uthorization for access rights and **A**ccounting for session logging
NAC	**N**etwork **A**ccess **C**ontrol is a system that enforces security policies by validating users/devices before granting network access. It integrates with AAA and directory services.
802.1X	IEEE standard for port-based network access control using EAP over LAN (EAPOL).
RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice is a protocol used by AAA systems for authentication and authorization.
ZTNA	**Z**ero **T**rust **N**etwork **A**rchitecture is a security model where no implicit trust is given and access is continuously verified based on identity, device posture, & context.
MFA	**M**ulti **F**actor **A**uthentication is an authentication method requiring two or more verification factors (password + OTP, biometrics, etc.).

Networking & Segmentation	
VLAN	**V**irtual **LAN** is a logical segmentation of a network at Layer 2 to isolate traffic.
Dynamic VLAN Assignment	Automatic VLAN allocation based on user/device identity via RADIUS attributes
ACL	**A**ccess **C**ontrol **L**ist are the rules that permit or deny traffic based on IP, port, or protocol.
Micro segmentation	Fine-grained segmentation at workload/user level (beyond VLANs).
PoE	**P**ower **o**ver **E**thernet is the technology that delivers power and data over Ethernet cables.

Identity, Access & Policy	
RBAC	**R**ole-**B**ased **A**ccess **C**ontrol is a method of restricting system access based on predefined user roles. Users are granted permissions based on their role (e.g., admin, stuff, auditor).
EAP	**E**xtensible **A**uthentication **P**rotocol is the framework used in 802.1X authentication to support multiple authentication methods (EAP-TLS, PEAP, etc.).
Directory Services	Centralized repositories (LDAP/AD) that store user identities and credentials, used for authentication and policy enforcement.

Security Infrastructure	
NGFW	Next-Generation Firewall is a security device that inspects and controls traffic.
DPI	**D**eep **P**acket **I**nspection is the scrutiny of packet payload (Layer 7) to detect threats or enforce policies.
VPN	**V**irtual **P**rivate **N**etwork is a secure encrypted tunnel for communication over untrusted networks.

Networking & Architecture	
L2 Switching	Switching based on MAC addresses. Used for local network communication within a VLAN.
L3 Switching	Switching based on IP addresses. Enables inter-VLAN communication and routing between networks.
SFP	Small Form-factor Pluggable module used for fiber or high-speed uplinks in switches.
Loop Prevention	Protocols (STP, MSTP etc.) used to prevent network loops in Layer 2 environments.
Link Aggregation	Combining multiple physical links into a single logical link for increased bandwidth and redundancy.
SSID	Name of a Wi-Fi network.
WPA3	**W**ireless **P**rotected **A**ccess – 3 is the latest Wi-Fi security standard providing stronger encryption and authentication.
Captive Portal	Web-based authentication mechanism for guest users.

Regulatory & Compliance (India)	
RBI	The **R**eserve **B**ank of India central banking authority of India defining cybersecurity and IT governance standards.
CERT-In	Indian **C**omputer **E**mergency **R**esponse **T**eam is a National agency for cybersecurity incident response that creates mandates for Incident reporting, Log retention and Monitoring
MTCTE	**M**andatory **T**esting and **C**ertification of **T**elecom **E**quipment is the certification by TEC ensuring telecom/network devices meet Indian standards.
DoT	**D**epartment **of T**elecommunications is the regulatory authority governing telecom infrastructure in India.
TEC	**T**elecommunication **E**ngineering **C**entre is the technical body under DoT responsible for standards and certification.
CISO	**C**hief **I**nformation **S**ecurity **O**fficer is a senior executive responsible for an organization's information security strategy.

Network Operations & Management	
NMS	The Network Management System is a platform for monitoring, managing, and troubleshooting network devices.
SIEM	Security Information and Event Management is a platform that aggregates logs and provides real-time security analytics.
Telemetry	Real-time data collected from network devices for monitoring and analytics.
ZTP	Zero Touch Provisioning is a process of automated deployment of devices without manual configuration.
Audit Trail	Chronological record of system activities used for compliance and forensic analysis.
Data Localization	Requirement that data must be stored within national boundaries (critical in Indian banking).
Log Retention	Storage of logs for a defined period (e.g., 180 days as per CERT-In).

Get Your Network Assessment Done Today

Email: sales@iobyhfcl.com
Phone: 8792 701 100
Visit: io.hfcl.com/solutions/banking-network