Golden Shield Network Construction Plan Based on SDN Architecture

Gang Xiong, Binhui Tang

School of Computer and Software, Jincheng College of Sichuan University, Chengdu 611731, Sichuan, China

Abstract: ***This paper examines the problems exposed by traditional network architectures amid rapid network development, and introduces the new-generation architecture—Software-Defined Networking (SDN)—which breaks the vertical integration of traditional network architectures by decoupling the control and data-forwarding functions of underlying devices, i.e., control-data separation. Based on this feature, a case study illustrates the necessity of transitioning from traditional network architecture to the new SDN architecture.***

Keywords: Network architecture; SDN; Control-data separation.

1. INTRODUCTION

Since the invention of the world's first electronic computer, ENIAC, in 1946, the era of computing has begun [1]. Starting with the establishment of ARPAnet, the networked world began to flourish. Especially since the twenty-first century, the networked world has developed at high speed, connecting regions and countries across the globe and permeating every industry. While networks have brought enormous convenience, they have also exposed many problems in the current network. At this point, SDN (software-defined networking) emerged in a Harvard University laboratory, with a mission to change the existing network infrastructure that no longer fits the present situation and is difficult to expand and develop further. So why has this product born in a laboratory brought such great change to the networked world? What advantages does SDN have over traditional network architectures? This paper attempts to explore traditional network architectures and SDN architectures, analyzing their respective network structures, characteristics, current status, or development history, and uses case studies to ultimately examine the differences between the two in practical applications. Recent AI advancements span diverse domains, beginning with Peng et al. (2024) who proposed representation aggregation-segregation techniques for domain-adaptive human pose estimation [1]. Zhang et al. (2025) then explored ML-based anomaly detection in biomechanical big data environments [2]. In healthcare AI, Wang (2025) developed RAGNet, a transformer-GNN-enhanced hybrid model for rheumatoid arthritis risk prediction [3]. Enterprise-focused innovations include Qi's (2025) generative AI framework AUBIQ for automating BI requirements in resource-constrained businesses [4], Fang's (2025) adaptive cloud-edge architecture for smart water management [5], and Lin's (2025) product management approach to AI governance frameworks [7]. Spatiotemporal analysis features Li's (2025) GIS-integrated U-Net for automated land encroachment detection in protected areas [6]. Sensor data applications include Huang and Qiu's (2025) LSTM-based electricity anomaly detection in smart meters [8] and Chen's (2023) foundational work on data mining for analysis [9]. Urban emergency systems are advanced by Li's (2025) AD-STGNN for dynamic fire vehicle dispatch [10]. Computer vision contributions include Wang et al.'s (2024) YOLOv8-based road car detection [11], while causal AI is represented by Wang's (2025) joint training method for MNAR recommendation data [12]. LLM applications in biosignals are surveyed by Ding et al. (2024) [13], complemented by Restrepo et al.'s (2024) multimodal embedding alignment for low-resource healthcare [14]. NLP research includes Yang et al.'s (2025) GAN-based text summarization with reinforcement learning [15]. Industrial AI features Xie and Chen's (2025) multi-agent system Maestro for manufacturing optimization [16]. Adtech innovations encompass Zhu's (2025) reliability automation framework RAID [17], Zhang's (2025) CrossPlatformStack for high-availability deployments [18], and Hu's (2025) AdPercept for visual saliency modeling in 3D ads [19].

2. ANALYSIS OF TRADITIONAL NETWORKS

2.1 Architecture of Traditional Networks

Most existing local-area network architectures today typically adopt a three-tier architecture, especially in data-center deployments. The three-tier model consists of the following three layers:

(1) Access Layer: The access layer is the bottommost tier of the entire LAN; its role is to connect end devices while ensuring that packets are delivered after those devices join the network.

(2) Aggregation Layer: The aggregation layer sits in the middle of the three-tier network and also handles certain security controls [2].

(3) Core Layer: The core layer is the heart and backbone of the network; devices at this tier act as the gateway for all packets, tasked with high-speed forwarding and, through routing and interconnection with other networks, ensuring inter-zone communication.

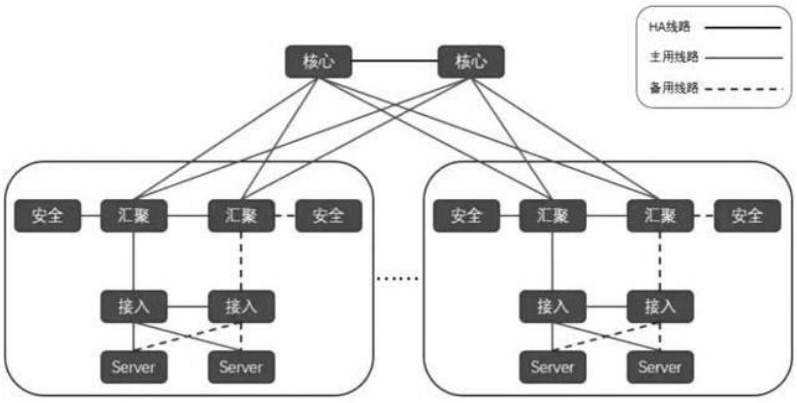

Figure 1: Diagram of the Traditional Three-Tier Network Architecture

2.2 Characteristics of the Traditional Network Architecture

The traditional three-tier network model has been in use for a long time and is widely deployed, so it naturally offers several advantages:

(1) Effective Broadcast-Domain Control: The traditional three-tier architecture can effectively limit the size of collision domains, reducing the likelihood of broadcast storms and minimizing their scope if they occur.

(2) Stable Network Structure: The three-tier design is inherently stable, with clear structural divisions and well-defined functions.

(3) Precise Policy Creation and Application: Thanks to explicit subnet segmentation, the three-tier architecture allows precise control over network policies, ensuring packets are transmitted securely and rapidly.

2.3 Current State of the Traditional Network Architecture

Although the traditional three-tier architecture has its strengths, rapid business expansion has exposed many shortcomings:

(1) Excessively Large Broadcast Domains: As business grows, a huge Layer-2 structure is often created to make computer resources more readily available.

(2) Excessive Network Latency: While scaling the business, more devices are added; as the device count rises, latency increases, ultimately degrading user experience.

(3) Unclear Traffic Patterns: During expansion, the variety of services increases, yet all packets are still forwarded by core-layer devices, piling every service onto the core instead of breaking them into separate modules.

(4) Load-Balancing Issues: Traditional three-tier networks do use load balancing, but it is essentially active-standby; most traffic still travels along a single path.

(5) Heavy Workload for Network Administrators: Scaling the network often involves mixing equipment from different vendors, posing significant challenges for administrators.

3. SDN NETWORK ANALYSIS

3.1 Origin of SDN

SDN was born in 2005 in a Stanford University laboratory, originating from the Clean Slate project funded by the U.S. GENI (Global Environment for Network Innovations) program. In 2008, Professor Nick McKeown's team at Stanford introduced the concept of the OpenFlow protocol and attempted to apply it in innovative campus-network experiments [3]. The OpenFlow concept sought to let network administrators quickly create policies via a centralized controller [4] and uniformly push those policies to all network devices, thereby achieving end-to-end policy control and secure operations. Subsequent development leveraged OpenFlow to give the entire network programmability, making business expansion far more flexible [5]. As the above shows, OpenFlow is the core of SDN, yet later developments have also seen other organizations create alternative protocols. The ultimate goal of the Clean Slate project was to reinvent the Internet, aiming to replace the existing network infrastructure that had become ill-suited to current needs and difficult to extend or evolve [3].

3.2 SDN Architecture

Today, the SDN architecture model widely recognized and adopted by the industry is likewise a three-layer model. The SDN three-layer architecture comprises:

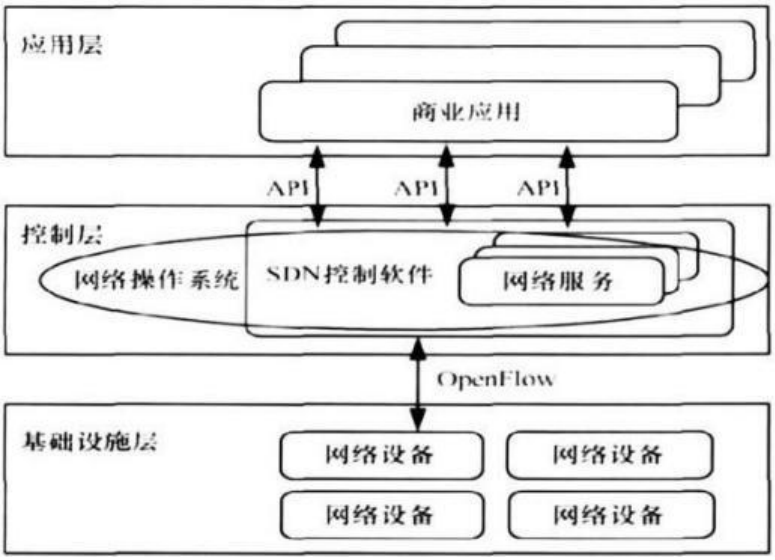

Figure 2: SDN Architecture Diagram

(1) Infrastructure layer (forwarding layer): This layer consists of numerous network devices, called network elements, whose function is to perform simple packet forwarding and data processing by examining flow tables. They exchange data with the controller via the southbound interface.

(2) Control layer: The heart of the entire SDN architecture, the control layer mainly comprises the network operating system, SDN control software, and network services. It must abstract and model the entire network to achieve global control, translate application-layer requests into instructions for infrastructure-layer devices, interact with the infrastructure layer via the southbound interface, and communicate with the application layer via the northbound interface.

(3) Application layer: Via the northbound interface, this layer interacts with the control layer, programs according to business requirements, and flexibly supports a variety of services.

Between these three layers, interfaces interconnect them. Between the infrastructure layer and the control layer is the southbound interface, for which the widely accepted protocol is OpenFlow. Its function is to deliver control information from the control layer to the underlying devices and to upload notifications or feedback from the devices upward. Between the control layer and the application layer is the northbound interface, whose mainstream design is REST API [6]. Its role is to provide an open, programmable interface that offers openness

and flexibility for various services.

3.3 Characteristics of the SDN Architecture

The SDN three-layer architecture decouples the three traditional network planes—data plane, control plane, and management plane [7]. Data-plane functions are implemented by the infrastructure layer, while control-plane functions are handled by the control layer, simplifying the underlying devices and globalizing the control layer's operations. In addition, an SDN-enabled network offers the following advantages:

(1) Centralized control: Under the SDN architecture, users can manage and configure infrastructure-layer devices through the controller by simply issuing configuration information or policies, completely changing the traditional configuration model.

(2) Clear service traffic partitioning: With the SDN architecture, a service system is divided into a separate zone, within which sub-service modules are further partitioned, making the inter-service relationships more explicit.

(3) Unlimited virtual resource changes: In an SDN-enabled network, virtualized resources can be created and migrated on any host without geographical restrictions.

(4) On-demand programmability: In traditional architectures, users have no possibility of on-demand programming; they can only purchase devices according to requirements.

(5) Ability to run software on devices: In traditional architectures, the software pre-installed on purchased devices is fixed by the vendor; users cannot add functions themselves, i.e., software cannot run on the devices.

(6) Traffic visualization: In an SDN network, when a failure occurs, the controller can provide a global view of traffic and topology, enabling accurate and timely fault location and rapid troubleshooting. In traditional networks, once a failure occurs, the large scale, multiple vendors, and complex policies make troubleshooting difficult.

(7) True load balancing: In traditional networks, the lack of global topology information prevents true load balancing and QoS (Quality of Service) control, whereas in SDN the controller can effectively achieve this.

4. CASE COMPARISON AND ANALYSIS

4.1 Public Security Golden Shield Network

The Public Security Golden Shield, as the name implies, is the construction project of the public security communication network and computer information system. The Public Security Golden Shield Network is the dedicated network that interconnects public security systems nationwide [8]. It is a typical government network architecture, divided into five levels: the Ministry of Public Security, provincial public security departments, municipal public security bureaus, district/county public security bureaus, and township police stations. Its characteristics are summarized as "three many and four large": many users, many police branches, and much collaboration; large network, large data centers, large video services, and large classified services.

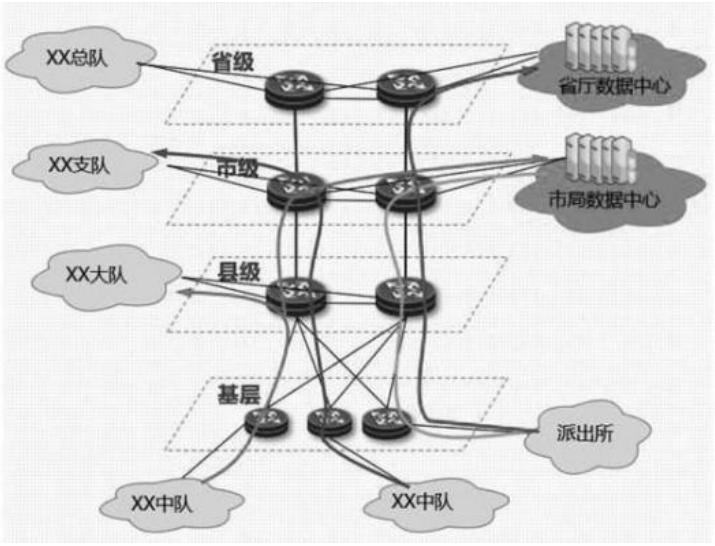

Figure 3: Public Security Golden Shield Network Architecture Diagram

4.2 Requirements Analysis

The requirements analysis for constructing the Public Security Golden Shield Network is roughly as follows:

(1) It poses three questions for business development: 1) How to provide sufficient bandwidth for the explosive growth of public security services? 2) How to guarantee the performance of critical services and improve user experience? 3) How can the network adapt to rapid business changes?

(2) It sets five requirements for network bearer: 1) reliability; 2) security; 3) service bearer capability; 4) secure isolation between special services; 5) transmission of a large volume of highly real-time, high-bandwidth services.

(3) It proposes three needs for O&M management: visibility, controllability, and manageability.

4.3 Architecture Advantage Comparison

In this case, the paper only discusses the traffic optimization solution.

(1) Traditional Network Architecture Model

Traditional network architecture thinking: 1) For data forwarding paths, it uses distributed path computation (routers compute routes independently); 2) When designing the overall network plan, it focuses more on connectivity; 3) In O&M, operators must master routing protocols such as IGP and BGP.

Effects under traditional network architecture: 1) Low network utilization due to lack of global view; 2) Manual configuration and low O&M efficiency; 3) Difficulty in launching new services; 4) Inability to perceive services and hard to adjust.

(2) SDN Architecture Model

SDN architecture thinking: 1) For data forwarding paths, it uses centralized path computation (SDN controller computes centrally) with multi-dimensional routing algorithms based on global topology, SLA, and link cost; 2) When designing the overall network plan, it focuses on path optimization on top of connectivity; 3) In O&M, SDN adopts centralized control by the controller.

Effects under SDN architecture: 1) Optimized network utilization; 2) Automated configuration and simplified O&M; 3) Easier service deployment; 4) Service awareness and real-time adjustment.

In traffic-optimization solutions, the SDN architecture has successfully resolved issues such as uneven traffic load, low bandwidth utilization, and slow routing convergence inherent in traditional networks. In the actual deployment

of the Public Security Golden Shield Network, a PCE (an intra-domain centralized path-control scheme) + SDN approach is adopted. Its advantages include: 1) traffic visualization and service awareness; 2) global-topology-based traffic optimization; 3) higher network utilization (network utilization >70%); 4) shorter service-provisioning time (services are automatically deployed by the SDN controller).

5. CONCLUSION

The Public Security Golden Shield Network has long been completed and put into operation. From its performance so far, it not only fully meets users' current needs but also supports future service growth and network expansion, demonstrating the comprehensive advantages of a next-generation network architecture. In an era when networks have become a social necessity, anything that fails to meet demand will inevitably be replaced. As the SDN architecture continues to evolve and mature, traditional network architectures will certainly be superseded. Of course, SDN still has a road of exploration ahead before this goal is fully achieved.

REFERENCES

[1] Peng, Qucheng, et al. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." arXiv preprint arXiv:2412.20538 (2024).
[2] Zhang, Shengyuan, et al. "Research on machine learning-based anomaly detection techniques in biomechanical big data environments." Molecular & Cellular Biomechanics 22.3 (2025): 669-669.
[3] Wang, Y. (2025). RAGNet: Transformer-GNN-Enhanced Cox–Logistic Hybrid Model for Rheumatoid Arthritis Risk Prediction.
[4] Qi, R. (2025). AUBIQ: A Generative AI-Powered Framework for Automating Business Intelligence Requirements in Resource-Constrained Enterprises. Frontiers in Business and Finance, 2(01), 66-86.
[5] Fang, Z. (2025). Adaptive QoS - Aware Cloud – Edge Collaborative Architecture for Real - Time Smart Water Service Management.
[6] Li, B. (2025). GIS-Integrated Semi-Supervised U-Net for Automated Spatiotemporal Detection and Visualization of Land Encroachment in Protected Areas Using Remote Sensing Imagery.
[7] Lin, Tingting. "ENTERPRISE AI GOVERNANCE FRAMEWORKS: A PRODUCT MANAGEMENT APPROACH TO BALANCING INNOVATION AND RISK."
[8] Huang, Jingyi, and Yujuan Qiu. "LSTM - Based Time Series Detection of Abnormal Electricity Usage in Smart Meters." (2025).
[9] Chen, Rensi. "The application of data mining in data analysis." International Conference on Mathematics, Modeling, and Computer Science (MMCS2022). Vol. 12625. SPIE, 2023.
[10] Li, Binghui. "AD-STGNN: Adaptive Diffusion Spatiotemporal GNN for Dynamic Urban Fire Vehicle Dispatch and Emergency." (2025).
[11] Wang, Hao, Zhengyu Li, and Jianwei Li. "Road car image target detection and recognition based on YOLOv8 deep learning algorithm." unpublished. Available from: http://dx. doi. org/10.54254/2755-2721/69/20241489 (2024).
[12] Wang, Hao. "Joint Training of Propensity Model and Prediction Model via Targeted Learning for Recommendation on Data Missing Not at Random." AAAI 2025 Workshop on Artificial Intelligence with Causal Techniques. 2025.
[13] Ding, Cheng, et al. "A Survey of LLMs on Biosignal Applications." Authorea Preprints (2024).
[14] Restrepo, David, et al. "Multimodal Deep Learning for Low-Resource Settings: A Vector Embedding Alignment Approach for Healthcare Applications." medRxiv (2024): 2024-06.
[15] Yang, Jing, et al. "A generative adversarial network-based extractive text summarization using transductive and reinforcement learning." IEEE Access (2025).
[16] Xie, Minhui, and Shujian Chen. "Maestro: Multi-Agent Enhanced System for Task Recognition and Optimization in Manufacturing Lines." Authorea Preprints (2025).
[17] Zhu, Bingxin. "RAID: Reliability Automation through Intelligent Detection in Large-Scale Ad Systems." (2025).
[18] Zhang, Yuhan. "CrossPlatformStack: Enabling High Availability and Safe Deployment for Products Across Meta Services." (2025).
[19] Hu, Xiao. "AdPercept: Visual Saliency and Attention Modeling in Ad 3D Design." (2025).