Research on Implementation Path and Risk Control of Large Enterprise Campus Network Upgrade and Renovation Projects

Jianying Gao*

Guangzhou Kinte Industrial Co. ,Ltd., Guangzhou, 510860, China
**Corresponding author: jygao08@139.com*

Abstract: *In recent years, with the addition of more services such as ultra-high-definition video, real-time industrial signaling, distributed storage, etc., the backplane bandwidth, forwarding capacity and the number of concurrent connections of traditional campus networks have reached their limits. At the same time, the upgrading of these networks has become increasingly complicated due to all kinds of multi-vendor protocols and irregular network topologies. The subject of this paper is the implementation path and risk control of an upgrade and renovation project, and the reasons for doing so are divided into three parts: performance decline, compatibility restrictions and change sensitivity; thus, a progressive decoupling deployment of the control and forwarding planes, a hybrid migration sequence for virtualization and physical devices, and a service-unaware cutover scheduling model are proposed, and at the level of risk control, atomic rollback boundaries are set, a real-time suppression mechanism for flapping convergence is added, and a fault injection pre-validation method is established to build an all-weather technical system for upgrade and renovation.*

Keywords: *Campus Network Upgrade, Layered Decoupling, Traffic Cutover, Risk Control, Fault Injection Testing*

Introduction

After many years of operation and several local expansions by the large enterprise, the hierarchy is often irregular. There are unreasonable loop dependencies in the redundant link configuration of the core layer, distribution layer and access layer. Multi-vendor devices have different implementations of Spanning Tree Protocol extension features, OSPF LSA flooding mechanisms, Link Aggregation Control Protocol negotiation state machines, etc., so network upgrade and renovation projects are technically very demanding. Research on the Implementation Path and Risk Control Measures for Network Upgrades and Renovations has good engineering and theoretical values. On the one hand, there are many practical technical solutions for the development of campus networks in various forms, such as traditional structures, software-defined and virtualised ones, etc. At the same time, in order to reduce the risk of service interruption and cascading failures during change operations, control measures such as atomic operation boundaries, real-time suppression mechanisms and fault injection pre-validation can be employed. First, this paper will examine the reasons for the motivation; next, it will introduce a way to implement layered decoupling; finally, a closed-loop risk-control mechanism will be put forward to provide some technical reference for similar network upgrade and renovation projects.

1. Analysis of Drivers and Constraints for Large Enterprise Campus Network Upgrades and Renovation

1.1 Degradation of Campus Network Performance and the Gap in Service Carrying Capacity

After a long period of operation of the large enterprise campus network, the backplane bandwidth of the switching architecture and the processing capacity of the distributed forwarding engines have gradually reached their design limits. With the addition of new services, such as 4K/8K ultra-high-definition video conferencing, real-time industrial control signalling, large-scale distributed storage synchronisation, etc., both the end-to-end delay jitter and the packet loss rate of the network have been rising nonlinearly. The number of concurrent connections and NAT table entries on the

egress gateway are close to their limits, and some traffic flow is causing TCP retransmission window oscillation. There are serious problems of co-channel interference and channel overlap in the areas covered by wireless access points, and the roaming handover delay for terminals exceeds the tolerance of VoIP sessions; thus, session establishment will fail or there will be audio interruption[1].

The Quality of Service network will not have deterministic forwarding after a sudden change in the traffic pattern. The original class-based weighted fair queuing has a relatively high probability of queue overflow in the event of burst traffic, and the critical traffic flow of the low-latency queue is affected by bursts in best-effort traffic; thus, priority inversion occurs and there is a sudden increase in buffer occupancy. The ageing process of NAT and firewall session table entries does not keep up with the keepalive time of long-lived connection services, and thus the connection state will be prematurely cleared. As a result of the performance decline shown above, we have reached the service-carrying capacity limit of the current campus network architecture, and thus, the upgrade and renovation should introduce high-dimensional forwarding and control resource scheduling models.

1.2 Compatibility Constraints in the Heterogeneous Environment of Multi-Vendor Devices

Large enterprise campus networks usually have many switches and routers from different vendors, and these vendors implement the protocol standards in various ways. Devices from different vendors in the Layer 2 network do not all support the extended features of the Spanning Tree Protocol, so there will be various calculations of port roles and abnormal root bridge elections. Due to the small differences in the implementation of the OSPF LSA flooding mechanism and the link-state database ageing timer at the Layer 3 routing level, the routing convergence time has not met the design goal. There are some differences in the negotiation state machines for VLAN and Link Aggregation Control Protocol among the ASICs of different chip vendors, so there may be uneven traffic distribution among the member ports in an aggregation group or link flapping.

The restrictions on the control plane and management plane are even stricter. Vendors have different structures for the management information base and various rules for encoding the return value of external interfaces; thus, there will be field parsing errors or missing data in the unified network management platform during the collection of performance indicators. Due to the different formats and event definitions of SNMP trap messages from various vendors, an alarm normalisation middleware adaptation layer needs to be developed separately. The SDN controller needs to solve the problem of adaptation for the southbound interface protocol in a multi-vendor environment; that is, different vendors have different levels of support for the match fields and action sets of OpenFlow tables, so shim logic at the abstraction layer must be added to distribute globally consistent forwarding tables. At the same time, due to the upgrade and renovation, the path of implementation must be cross-vendor interoperability-verified[2].

1.3 Vulnerability Assessment of the Existing Topology Structure to Changes

After many extensions and modifications of the local area network, an uneven hierarchy has been formed. There are redundant link configurations in the core layer, distribution layer and access layer; they may have unreasonable loop dependencies, and there may also be inconsistencies in the mapping relationship between the physical topology and the logical topology. The Bandwidth Utilisation of some trunk links is very uneven over time; a small number of backbone links have accumulated traffic that exceeds the design redundancy ratio. Operations carried out during the upgrade and renovation of an intermediate node or link may cause abnormal recursive lookups of routing next-hops or result in a temporary disconnection in the route propagation path of BGP. It is relatively likely that the probability of the single points of failure in the topology will increase due to change operations.

Another kind of vulnerability is that the old settings will not be compatible with the new ones. The configuration files of the old device have accumulated a large number of old Access Control List entries, obsolete static routes and invalid Network Address Translation mapping rules, etc., and may have an unintended effect on the network policies after the upgrade. The route leakage control policy of the Virtual Routing and Forwarding instance will be ignored during the topology change, and thus service isolation will fail. Layer 2 Networks with multiple Spanning Tree Protocols: After changing some network equipment, the original mapping of instances to VLANs will be lost, and therefore the locations of blocked ports will differ. To know how serious this problem is, we can construct a model of change impact analysis based on a configuration dependency graph and find all paths of cascading failure caused by non-atomic operations[3].

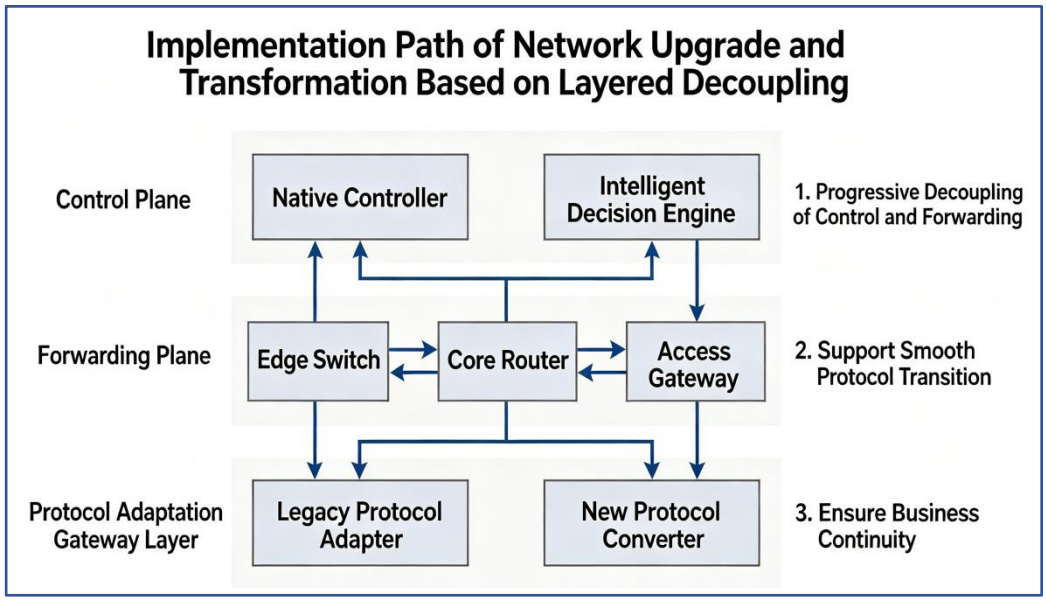
2. Implementation Path for Network Upgrade and Renovation Based on Layered Decoupling

2.1 Progressive Decoupling Deployment of the Control Plane and Forwarding Plane

The first reason for dividing the control plane and the forwarding plane is to make better use of network resources in an extended or expanded environment. Hybrid networks are still in charge of the forwarding function of the original physical devices, but the control functions of route computation, label distribution and topology discovery have been centralised or distributed to controllers. Therefore, one can gradually add control domains with lower geographic or service priorities at the aggregation node and set up a secure channel with the forwarding device via OpenFlow or NETCONF. Confirm the consistency of the state, verify that the controller's Routing Information Base and the device's local routing table are in agreement, otherwise, there will be no black-hole routing or forwarding loop after decoupling. Older devices that do not support the standard Southbound Interface can be connected to a protocol adaptation gateway, and this gateway will translate the original management protocol into a unified set of control primitives so that all control planes can be managed together.

Gradual Decoupling will solve the problem of response priority conflict in forwarding devices with multiple control sources. If the decoupling ratio is too high, some functions of the original distributed routing protocol need to be gradually removed or disabled to avoid time conflicts with the flow table entries distributed by the controller. Merge logic for the flow table has been added based on version numbers and timestamps, and entries published by the controller will be given higher priority than those created in the local routing protocol. In the fully decoupled target state, only local link-state detection and direct-connected route generation need to be done at the forwarding device; all other routes will be calculated and distributed by the controller. At the beginning of the switchover, a fallback mechanism will be used; that is to say, if too many heartbeats are lost between the controller and the forwarding device, the device will switch back to the old routing protocol and continue to operate normally.

Example:



2.2 Migration Sequence for the Hybrid Configuration of Virtualised Network Elements and Physical Devices

Virtualised Network Elements are carriers of software-based network functions that take on the roles of border gateways, firewalls, load balancers, etc., in the upgrading of campus networks. The organisation of the migration sequence is based on the principle of dependency inversion; that is to say, service-based network elements that have a lower dependency on the underlying physical link are migrated first, and then dedicated devices that are closely linked to specific hardware are moved. The three steps of the special sequence are as follows: In the first step, virtualised route reflectors and virtualised NAT instances are set up to work with the physical routers and share some of the session traffic; In the second step, access control policies and Quality of Service policies are copied from the

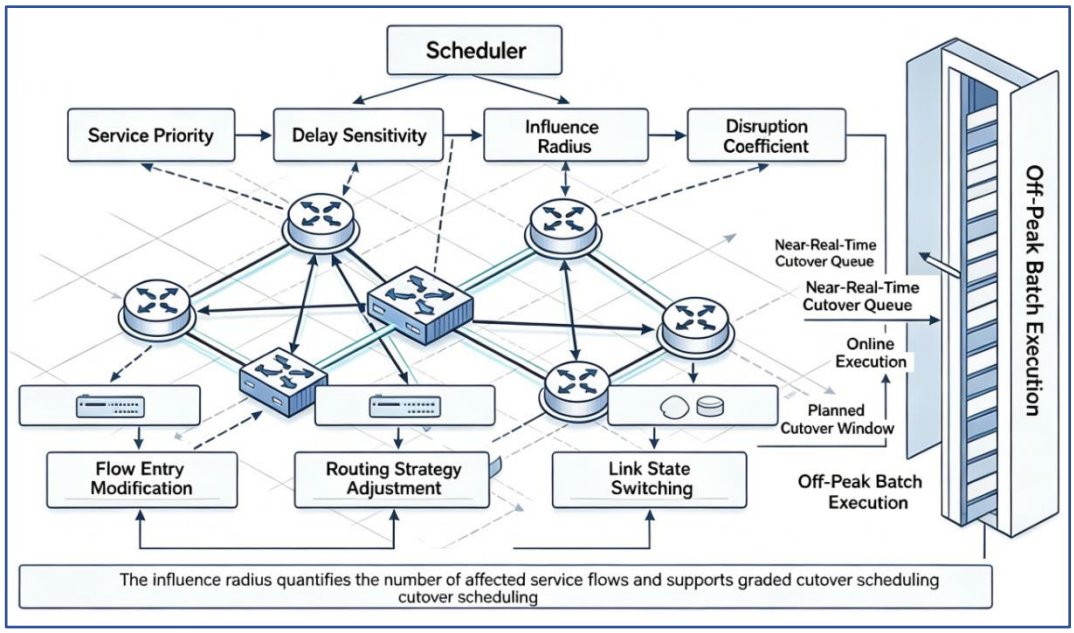
physical devices to the virtualised network elements, and a policy synchronisation mechanism is employed to ensure that the rules in both environments are consistent; finally, in the third step, the service instances in the physical devices are gradually reduced, and traffic ingress is switched to the virtualised aggregation gateway[4].

The order of migration for the hybrid environment should solve the problem of link identifier mapping of virtualised network elements and physical devices. Virtualised Network Equipment is set up on general-purpose servers or hyper-converged platforms, and the virtual network interface needs to be mapped to the ports and VLAN tags of the physical switches. VXLAN Tunnel Encapsulation Technology is used to wrap the internal communication traffic of virtualised network elements in transmission tunnels of the physical network, so it will not be affected by broadcast storms caused by the flooding of Layer 2 broadcast domains. Bidirectional health probes are placed in the migration path of the virtualised network element and the physical device, and the probe packets contain session affinity labels to ensure that the same service flow has a stable five-tuple path before and after migration. The device will enter a read-only maintenance mode, and if the migration is successful, the old settings will be saved as a rollback base.

2.3 Service-Unaware Traffic Cutover Window Scheduling Model

The Schedule of the traffic cutover window should meet the demand for continuous service and the time constraints of network modification work. According to the service priority and the urgency of the delay, a dual-parameter scheduling model has been used to divide the cutover operation into atomic task units, and each atomic unit is associated with one or a group of related modifications in the flow table entry, routing policy or link-state switch. According to the range of effect, the scheduler will set the service perturbation coefficient for each atomic task, and the range of effect is defined as the number of service flows that will experience packet loss or increased delay after the execution of the task. Atomic tasks with a coefficient below a certain threshold can be added to the near real-time cutover queue and processed online; those with a coefficient above the threshold need to be scheduled for the planned cutover window and run in batches during off-peak hours[5].

Example:



To realise service-unaware cutover, it is necessary to have prefix-independent switchover and a BFD link mechanism. Before switching to a particular link, forwarding entries need to be added in the backup path, and after the installation of the Forwarding Information Base (FIB), the metric or priority of the original link is reduced hop by hop to gradually shift traffic to the new path. At any time, there will be no whole-network Spanning Tree recalculation or full convergence of routing protocols; instead, a smooth switchover can be achieved by changing only the local metric. The Schedule Model will have a rollback timer and continuously observe the packet loss rate and round-trip delay of the critical service flow in the cutover window. If the abnormal indicators are out of the normal range for three consecutive sampling periods, then the timer will automatically start a rollback, revoke all current and

subsequent atomic tasks, and restore the original forwarding state.

3. Risk Identification and Closed-Loop Control in the Process of Network Upgrade and Renovation

3.1 Definition of Atomic Operation Boundaries Triggered by Configuration Rollback

The atomic operation boundaries of configuration rollback determine the reversible granularity and rollback scope of change operations. For configuration changes in different places or at various levels of the protocol, a two-phase commit protocol is used to coordinate the operation status of all participating nodes; the pre-commit phase carries out syntax validation and resource reservation, and then, after confirming that all nodes are ready, the formal commit phase is started.

The Definition of atomic operation boundaries should consider the asymmetry of configuration elements; that is to say, there is an inverse operation mapping between creation-type commands and deletion-type commands. Store the version difference matrix of the configuration in the system to record changes in the current running configuration compared to the target configuration, and each incremental field will be associated with a forward operation script and a reverse rollback script. When it receives the abnormal signal, the rollback trigger will execute the reverse scripts in the reverse order of the commit timestamps of the atomic units. For atomic units that have routing policies or are using tunnels, after reversal, make sure that the relationship with neighbours or the peer of the tunnel has not been broken by a recent neighbour restart or session timeout; otherwise, a secondary failure will occur. Persist the metadata of the atomic boundary and create an associated mapping relationship with the change ticket for post-mortem audit and operation review.

3.2 Real-Time Suppression Mechanism for Link Flapping and Abnormal Routing Convergence

Link flapping is a frequent change in the physical or protocol state of a link over a short period, so the routing protocol has to repeatedly calculate the shortest-path tree, and this will result in a high load on the control plane. For Layer 2 Ethernet links, the timeout parameter of the slow protocol negotiation in Link Aggregation Control Protocol is reduced to combine several state jitters into microseconds and decrease the frequency of alarm reporting to upper-layer protocols[6].

The two kinds of problems with late-stage handling of abnormal routing convergence are convergence delay and convergence oscillation. To solve the problems mentioned above, a damping algorithm can be employed; that is to say, the penalty for each time a route is withdrawn is increased, and when the total accumulated penalty reaches an upper limit, entry to that route is put in a hold-down state and temporarily excluded from forwarding decisions; it will only be reactivated after the penalty has dropped to a lower threshold according to a half-life period. Continuously monitor the oscillation status and convergence anomaly log in real time from the control plane, and if there are any abnormal events, report the information back to the management plane of the change operation.

3.3 Risk Pre-validation Method Based on Fault Injection Testing

Fault injection tests can reproduce some of the problems that generally occur in the upgrade and renovation process under simulated conditions to find any weak links and trigger conditions. Based on the historical fault database and the topology dependency graph, test cases have been developed, and the types of injection include link failures, node failures, configuration errors, control plane overload, etc. All injection cases have a general pre-failure condition, an injection time and duration, and an expected recovery behaviour after the fault has been corrected. Before carrying out a serialised migration operation, build a digital twin model of the devices or links that will be modified, continuously synchronise the running configuration and state information of the twin model in real time, and use it as the target carrier for fault injection. At the time of test execution, all the metrics of the entire network will be recorded, such as end-to-end delay, packet loss rate, jitter, routing convergence time, etc.

The results of the risk pre-validation method are in the form of a table of change operation risks. Abnormal behaviour caused by fault injection is considered a risk item, and all risk items are given a quantitative score based on the two attributes of occurrence probability and impact severity. Before the official upgrade, the current network conditions will be compared with the most recent successful pre-validation snapshot, and if the difference exceeds the set tolerance, then the fault injection test will

be repeated.

Conclusion

Research on the Implementation Path and Risk Control of Large Enterprise Campus Network Upgrades and Renovations, Analysis of Motivations and Constraints in the Three Areas of Performance Degradation and Service-Carrying Capacity Gaps, Heterogeneous Compatibility Constraints of Multi-Vendor Devices, and Vulnerability of the Existing Topology to Changes. Based on the above, a multi-level decoupling-based implementation path for upgrade and renovation has been established, which includes the progressive decoupling deployment of the control plane and forwarding plane, a hybrid configuration migration sequence of virtualised network elements and physical devices, and a service-unaware traffic cutover window scheduling model. It has an atomic operation boundary for configuration rollback, real-time suppression of link flapping and abnormal routing convergence, and a risk pre-validation method based on fault-injection testing; thus, it is a complete technical system that covers the before, during and after periods of upgrade.

The following are some research directions in the future: Machine learning can be used to study the historical development of mines and optimize the parameter adaptation of atomic operation boundary division and risk scoring models; a digital twin platform for large-scale heterogeneous campus networks will be constructed to improve the accuracy and coverage of fault injection testing; and research on state consistency and conflict resolution mechanisms among multiple controllers in cross-domain collaboration also needs to be carried out.

References

[1] Shao Yan, and Qi Jing. Synergy of Wi-Fi 7 and 10-Gigabit Optical Network Facilitates Campus Network Evolution. Communications World, 14 (2025): 25-27.
[2] Xiao Ze. Research on Full-Lifecycle Risk Management of Jinan YK Industrial Park Project. 2025. Inner Mongolia University of Science and Technology, MA thesis.
[3] Wang Jiesheng. Research on Schedule Management of YG Company's Campus Network Optimization Project. 2023. Nanjing University of Aeronautics and Astronautics, MA thesis.
[4] Ma Pianpian. Application of Network Simulation Software in Large Campus Three-Tier Network Teaching. Journal of Nanyang Normal University, 19.06 (2020): 59-66.
[5] Wang Lei. Design and Implementation of Network System and Network Security for a Digital Campus. 2019. Xi'an University of Architecture and Technology, MA thesis.
[6] Xie Wenna. Design and Simulation of Enterprise Campus Network Based on IPv4/IPv6 Dual-Protocol Stack. 2019. Xiamen University, MA thesis.