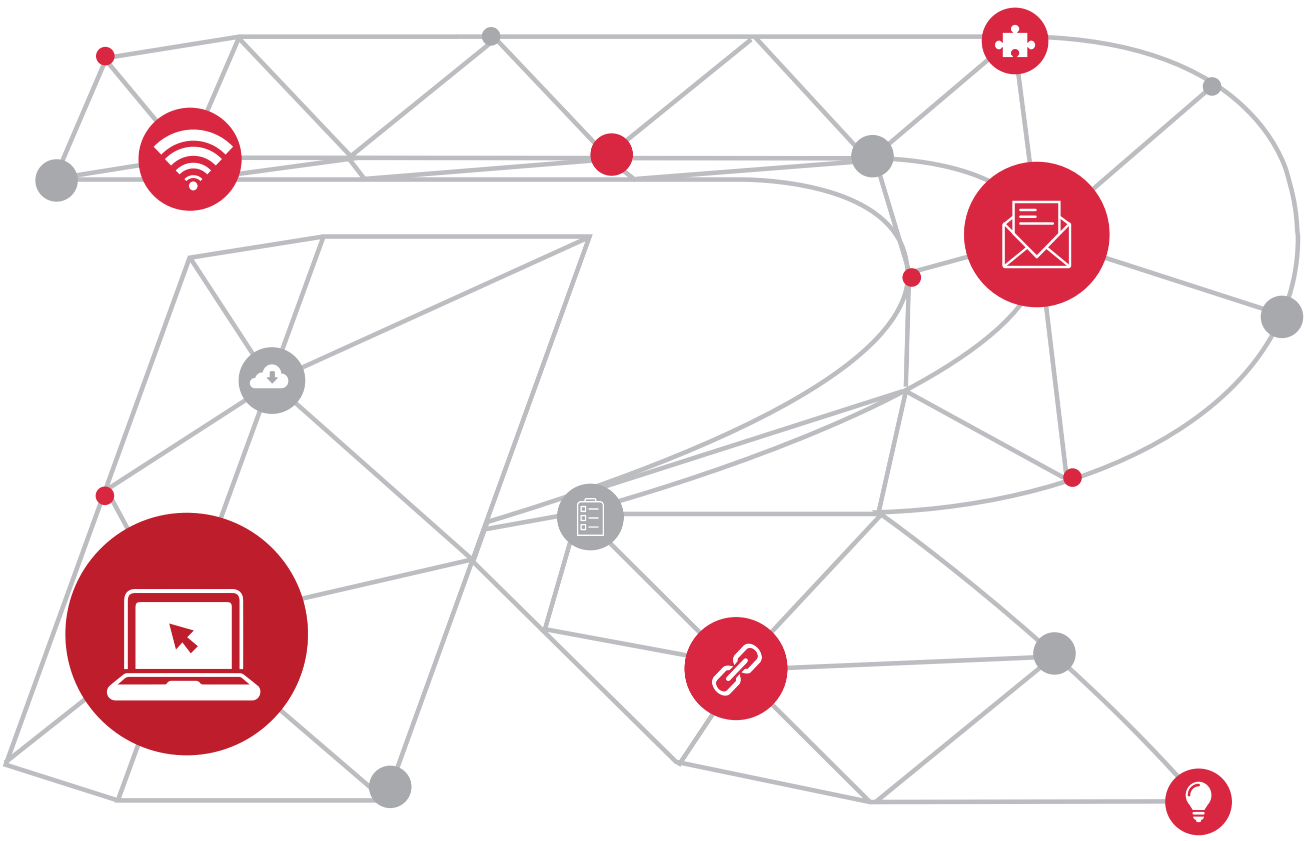
Ruijie Virtual Switch Device

White Paper



Contents

Introduction 3

Background 3

Summarization 10

Technical Principle 10

Basics 10

Virtualization Solution 12

Typical Application 17

Application Solutions 17

Conclusion 19

Introduction

• Background

With expansion of information and communications technology (ICT) networks, especially data center networks, and increasing diversity of service types, network management become more complicated. Besides, the requirements on network attributes such as service isolation, security, and reliability become stricter. In addition, as hardware capacity are rapidly growing, and multi-frame, clustered, and distributed routing switch system become mature, the service processing capacity of a single physical network device has reached a new height. Therefore, how to make full use of the service processing capacity of a single physical device to flexibly adapt to current service requirements and provide future-proof scalability has become a primary concern.

Specifically, customers face the following network problems and appeals.

Problem 1: Contraction between huge investment and low utilization of network devices

With the flourish of data center services, the growing ICT infrastructure results in high maintenance costs; and the growing number of network devices significantly increases the investment in the network devices. In addition, as the network infrastructure is growing, O&M costs, such as power consumption and footprint, greatly increase.

To meet the data service requirements in the future, customers have to select network devices that exceed the current service requirements to ensure the network expansion capability. Therefore, the load of the current network devices is probably unbalanced, lowering utilization of some devices.

In this case, how to solve the contradiction between high investment (high CapEx) and low utilization of devices become a primary concern of the customers.

Problem 2: Contraction between centralized multi-user bearing and management isolation and O&M simplification

As large and centralized data centers develop, enterprise customers are likely to establish unified data centers and networks to bear the services of multiple user groups, including various internal and external customer groups, different departments, and organizations. Network devices generally bear the services of different user groups simultaneously, such as production department, R&D department, and marketing department. The services of these user groups differ in network attributes such as security, performance, and reliability. Therefore, they should be separated for better management. That is, different departments need to separately deploy, manage, and maintain their services on a same device. Therefore, though centralized bearing of the network brings convenience, problems still remain, such as management separation and O&M (high Opex) simplification.

Problem 3: Contradiction between centralized multi-service bearing and reliable isolation security of network devices

With development of the next generation data centers, new network technologies emerge one after another, including technical solutions such as layer-2 Transparent Interconnection of Lots of Links (TRILL), Fiber Channel over Ethernet (FCoE), and multi-data center interconnection. In addition, customers expect the network to bear diverse external services. As a result, the technologies and services born by the data center networks become more abundant. How to ensure independent operation of these technologies and services is an urgent problem for the next generation data centers. More services need to be migrated to the cloud computing data centers. This imposes higher requirements on reliability and security isolation of the network devices.

The following examples describe how to address the above problems by using Ruijie core switches.

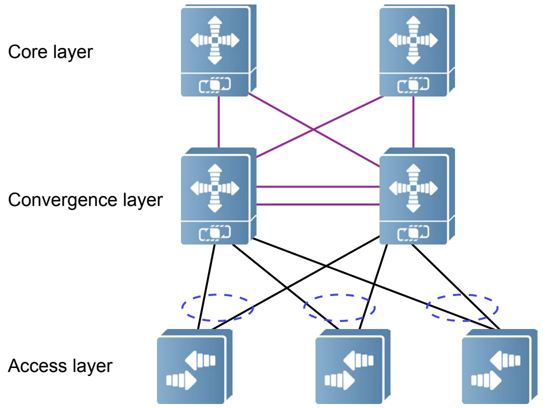
Problem 1

Scenario 1: Network Deployment

Cause

Currently a data center adopts a hierarchical architecture, including: access layer, convergence layer, and core layer, as shown in the figure:

Figure 1 Hierarchical Architecture



During the construction of a small network, enterprises do not want to invest much due to finance restriction and little demand for access devices. However, to meet the rapid business growth in the future, enterprises must ensure scalability of network architecture. Therefore, the core network inside the enterprise must be classified into the core layer, the convergence layer, the access layer, and so on, so as to ensure stability, robustness, and scalability of the network for business development.

If the network is strictly classified as required, the customers will face the following problems:

* **The devices at the convergence layer and the core layer will not be fully utilized within a certain period of time. Besides, the devices will be depreciated in several years. This is unacceptable to the customers.**

* **The added devices require footprint in equipment room, lighting, air-conditioning, maintenance, and so on. This increases the costs.**

However, if the network is not classified into layers, it will be difficult to expand the network in the future.

Expectation

The customers expect a solution that requires a small number of devices during the initial construction phase and follows the network hierarchy to ensure high scalability.

Scenario 2: Utilization of a VSU Control Engine

Cause

The Virtual Switch Unit (VSU) feature is added to the core switches, bringing advantages such as simplified management, fault recovery, reliable redundancy, and simplified network topology. Currently the devices in the VSU system work in active-standby (AS) mode with one active unit and one standby unit deployed. When the active unit fails, the standby unit takes over the services of the active unit. Therefore, it is possible that the active unit has high CPU usage but the standby unit is idle. The current chassis of the Ruijie core switches only supports the VSU composed of two devices, which will grow to four devices. In this case, Four devices have eight supervisor engines, and only one of them has high CPU usage, whereas the other engines are idle.

Expectation

The customers expect that the devices they have purchased can be fully utilized. Especially, in VSU mode, the load of all the supervisor engines is balanced.

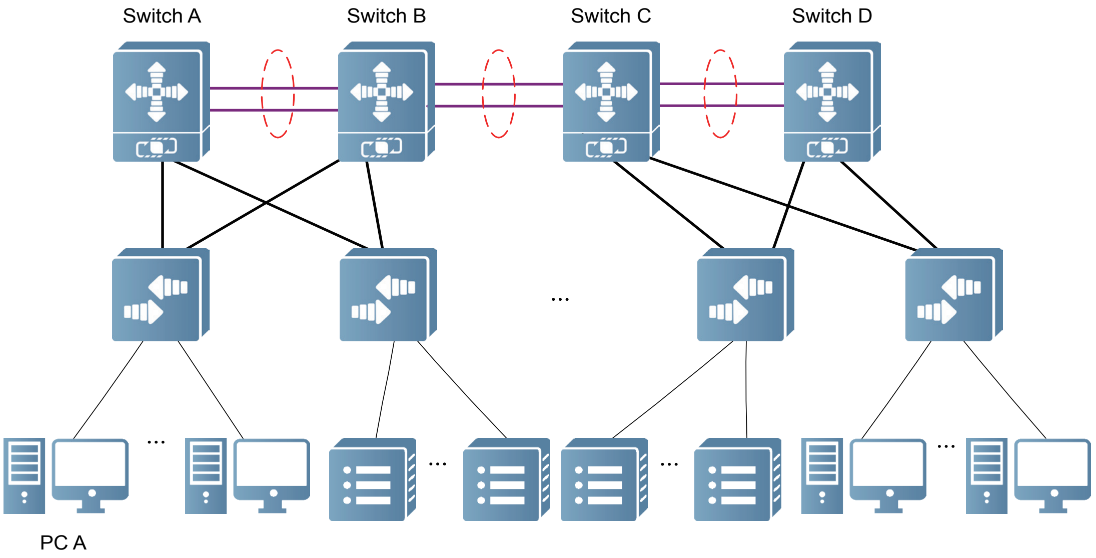
Scenario 3: VSU Capacity

Cause

After the VSU feature is added to the core switches, the port density increases, so more devices can be connected. However, because the table for storing device entries does not increase in size, the number of connected devices is limited.

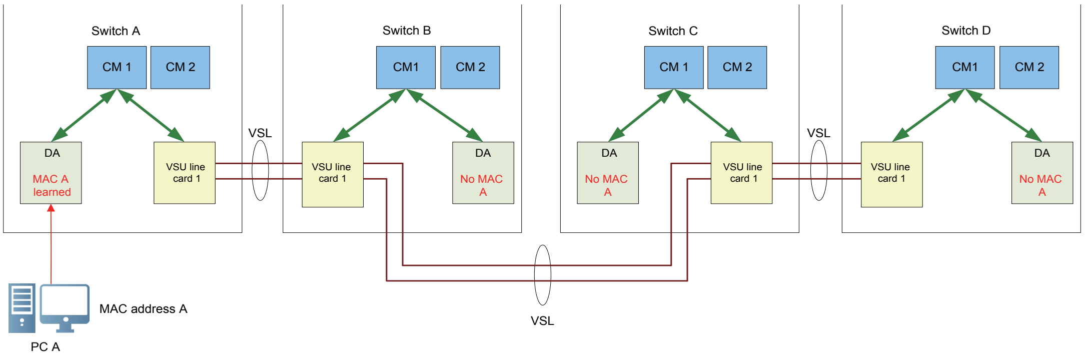
In Figure 2, four core switches are deployed at the convergence layer to form a VSU system.

Figure 2 VSU Capacity (1)



When the Ruijie core switches do not support the VSU feature, the maximum capacity of the MAC address table is 128 K. After the VSU feature is supported, the capacity of the MAC address table remains unchanged. However, because the port density increases, more devices can be connected, and more MAC addresses can be learned. As a result, the number of the MAC addresses learned from the line cards and the MAC addresses synchronized from other line cards exceeds the capacity of line cards. In this case, the capacity of the MAC address table is insufficient, as shown in Figure 3:

Figure 3 VSU Capacity (2)



In Figure 3, due to capacity insufficiency, the DA line cards on switches B, C, and D fail to learn the MAC address of PC A, or the DA line card on switch A fails to learn the MAC addresses of other switches. In this case, the MAC address table is updated frequently.

Expectation

The customers expect that when the number of devices that form the VSU increase, the capacity of the system table also increases, so that more devices can be added to the VSU and the VSU can be put into full use.

Problem 2

Scenario 1: Dependent Network Management

Cause

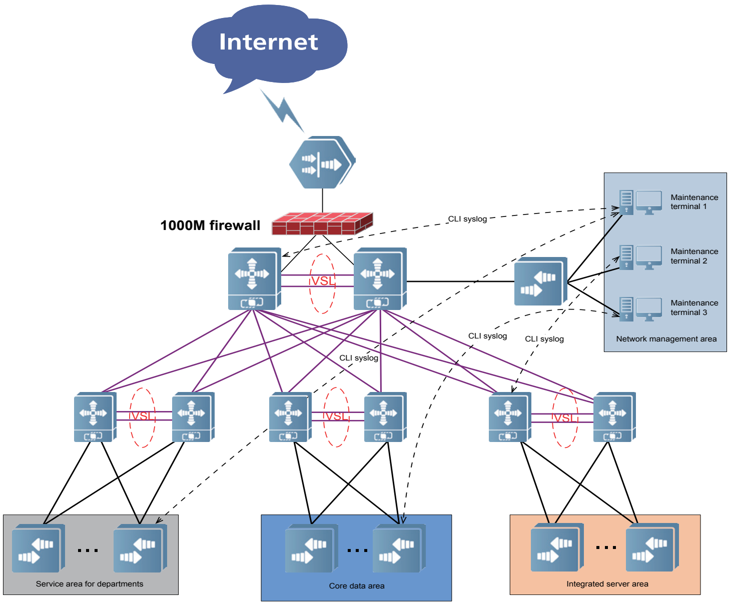
As data centers become more complex, network areas are functionally divided to implement service isolation, as shown in figure 4:

Figure 4 shows the network topology of a data center for a government network. The administrator can access any switch in the data center to maintain and modify the configuration. This management mode has the following defects:

* **The network devices bear abundant services, and these services differ remarkably in security, performance, and reliability. Therefore, the administrator must be familiar with these services before maintaining the devices, thereby imposing a high requirement on the administrator.**

* **The network maintenance is not independent. The network is functionally divided into multiple areas, so the service servers of multiple departments are located in a same area. However, for the sake of security and confidentiality, each department does not want other people to know its service configuration. Therefore, the network management should be properly separated.**

Figure 4 Network Management



Expectation

The customers expect that the data center is provided with a solution that manages different services separately, so that administrator only needs to focus on the maintenance of his own services.

Scenario 2: Isolation Between a Production Area and a Training Area

Cause

The data centers become more complex, imposing increasingly higher requirement on the administrator. However, newly recruited administrator must spend much time receiving training. To ensure operation of the data center networks, it is impossible for the new comer to operate the physical networks. Therefore, the new administrator cannot get much useful experience.

Expectation

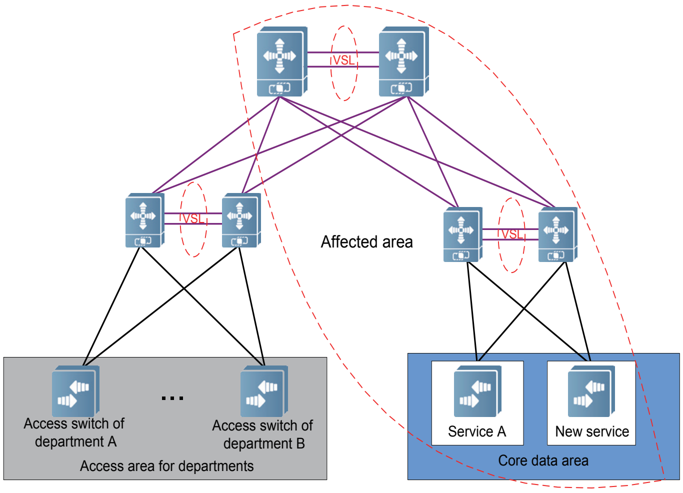
The customers expect that a simulated environment is provided for the new administrator to get training.

Scenario 3: Deployment of a New Service

Cause

New services are developing rapidly. If the deployment of a new service fails, the existing services will be affected. Therefore, a new service is generally deployed when the data center is idle, for example, at midnight. If the deployment fails, the configuration should be rolled back. The deployment process takes a long time with much effort, as shown in Figure 5:

Figure 5 Deployment of a New Service


VSL
VSL
Affected area
VSL
Access switch of department A
...
Access switch of department B
Access area for departments
Service A
New service
Core data area

In Figure 5, if a new service fails to be added to the core data area, the entire network will fail.

Expectation

The customers expect that a new service is deployed during work hours without affecting the existing network whether the deployment succeeds or not.

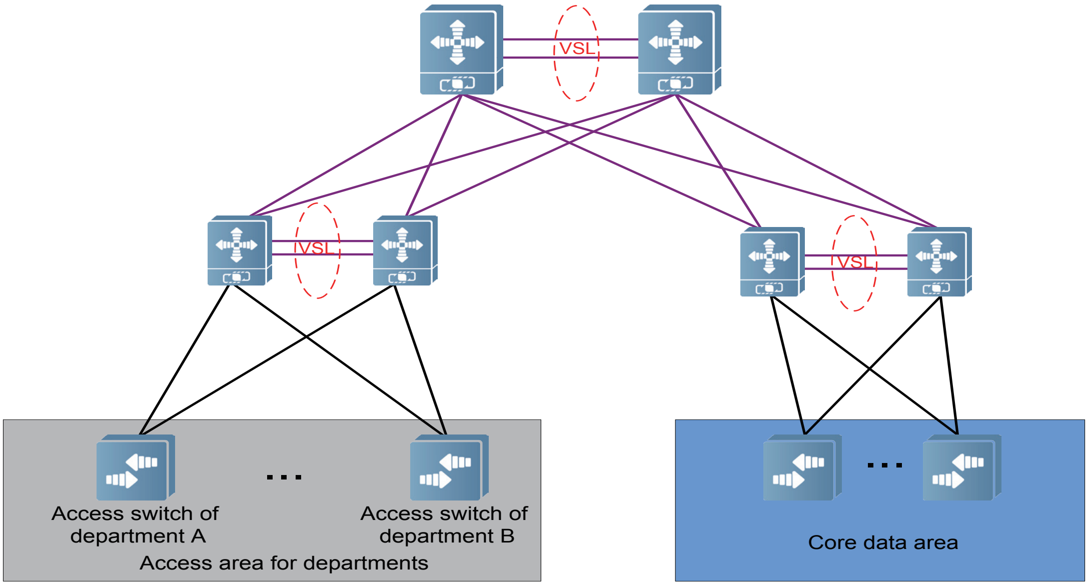
Problem 3

Scenario 1: Network Isolation

Cause

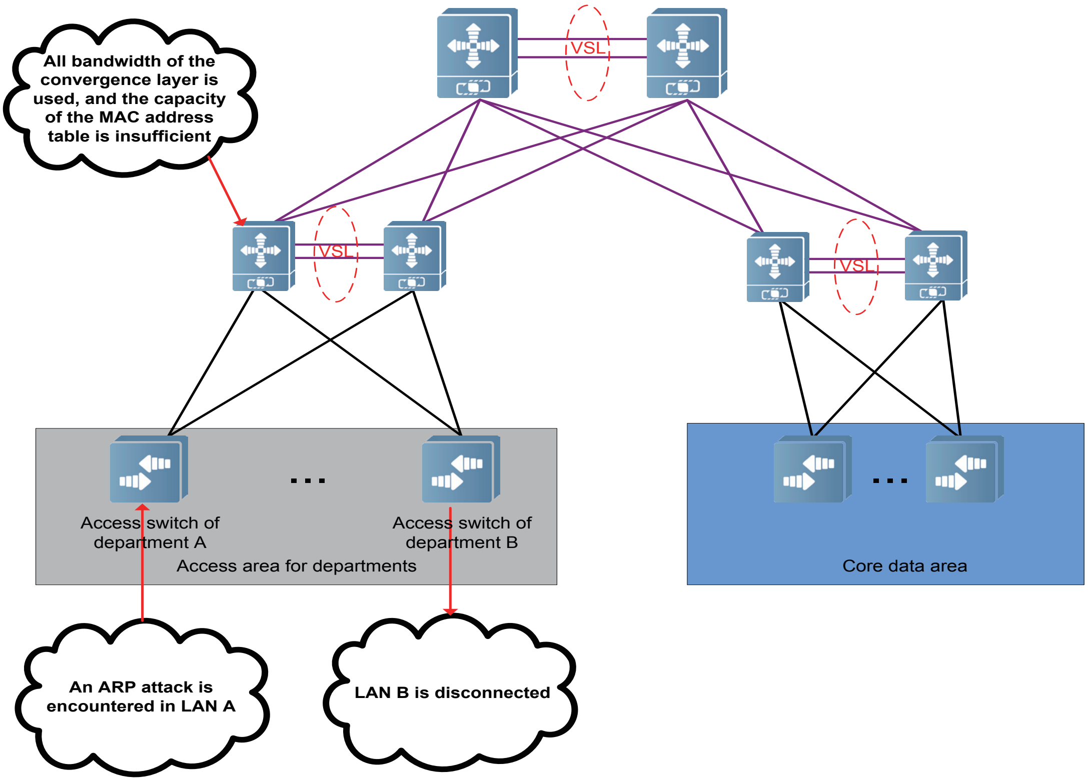
In a data center, users of a same department are connected to a same access switch; and all the access switches are converged at the convergence switch. As shown in Figure 6, the access switches of department A and department B are converged at a same network device.

Figure 6 Network Topology of a Company


VSL
VSL
VSL
Access switch of department A
...
Access switch of department B
Access area for departments
...
Core data area

If an ARP attack occurs in department A, the capacity of the MAC address table of its access switch will become insufficient, and the convergence switch will continuously receive ARP requests and responses. In this case, much bandwidth will be wasted, and the network of department B will be affected. Therefore, once the virus is spread, peripheral networks will be affected, and it is difficult to troubleshooting the problem, as shown in Figure 7:

Figure 7 ARP Attack


All bandwidth of the convergence layer is used, and the capacity of the MAC address table is insufficient
VSL
VSL
VSL
Access switch of department A
Access switch of department B
Access area for departments
Core data area
An ARP attack is encountered in LAN A
LAN B is disconnected

Expectation

The customers expect a solution is provided to prevent a virus from being spread to external networks without increasing the investment in the network devices, so that the virus does not affect operation of other networks and it is easy to troubleshooting the problem.

Scenario 2: Fault Isolation

RGOS 11.X supports modular components. Each component is independently compiled, and fault recovery must be taken into consideration when each component is designed.

As the network services grow, the data center networks become more complex, and the inter-service interference increases. Figure 8 shows the network topology of the access area in the data center of a municipal government. The access switch of the municipal government is connected to the convergence switch. The convergence switch is a piece of provider equipment (PE), and the access switch is a piece of customer equipment (CE). The municipal government needs to access four types of VPN services, but only one physical link is available. Therefore, sub-interfaces must be enabled on the uplink interface of the access router to access the VPN Routing and Forwarding (VRF) instances of different VPNs at the PE, so as to isolate the traffic of different services. The PE allocates four VRF instances for access from the CE so as to isolate the traffic.

Figure 8 Access Area in the Data Center of a Municipal Government

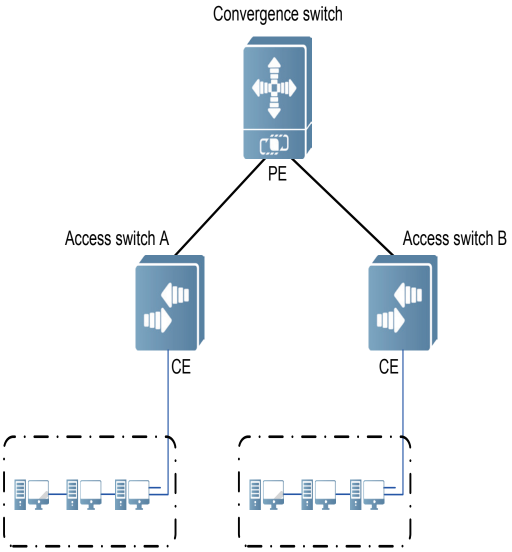


Figure 9 Abstract VRF Instance

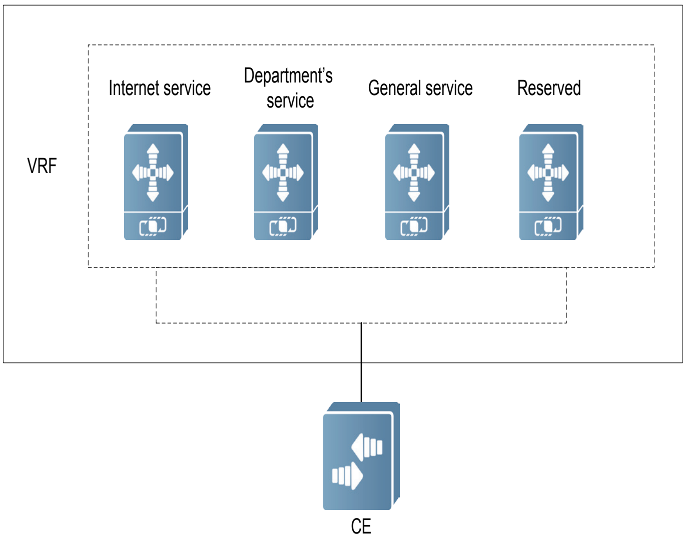
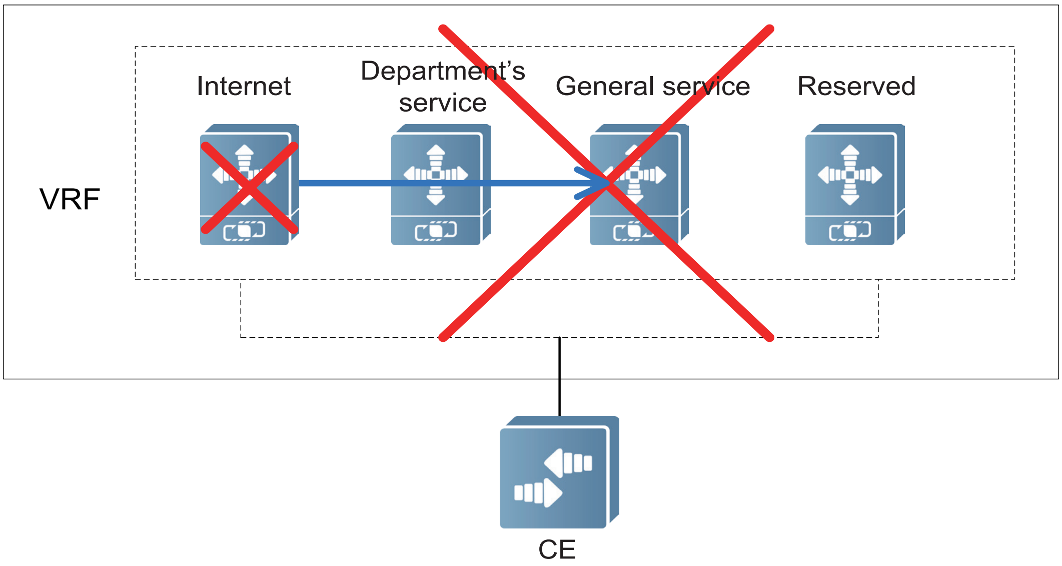


Figure 9 shows an internal VRF instance of the convergence switch.

In Figure 9, all the VRF services are processed by one process. Therefore, if one VRF service fails, all the VRF services fail, and the entire network is affected, as shown in the following figure:

Figure 10 VRF Failure



Expectation

The customers expect that without adding devices, a solution is provided to ensure that when one service fails, the other services are not affected.

• Summarization

According to the foregoing analysis, the users mainly report the following problems:

*** Fault isolation: The current device cannot isolate a faulty module, and the entire system must be restarted to restore the functions of the system or the faulty module; and the network that is not related to the faulty module is also disconnected.**

*** Network isolation: When multiple departments share a same device, if the network of a department fails, the networks of other departments may fail. This does not facilitate network isolation, and users are willing to increase investment in new devices.**

*** User management: The configuration of Ruijie devices cannot be independently managed. Especially in schools, when multiple offices share a same set of device, there are multiple administrators, which will lead to poor management.**

*** Low utilization rate of network devices: As networks are developing, more money is invested in the network infrastructure. As a result, the network devices are not fully utilized, and the network maintenance costs increase. When the economy is sluggish, enterprises are cutting their investment in network devices. Therefore, the device suppliers must figure out a network integration solution to reduce the network maintenance costs.**

*** Insufficient capacity of system table: In a VSU system, especially in a VSU system composed of multiple devices, when the number of line cards and ports increases, the capacities of some system tables will become insufficient.**

*** Unbalanced load of control engine: When the VSU system is deployed, the port density increases, but the energy efficiency decreases. The supervisor engines of some devices are not fully utilized, but consume much power.**

The foregoing problems are common in data centers. Data centers are broadly applied in schools, government, and enterprises, so the foregoing problems must be solved.

Technical Principle

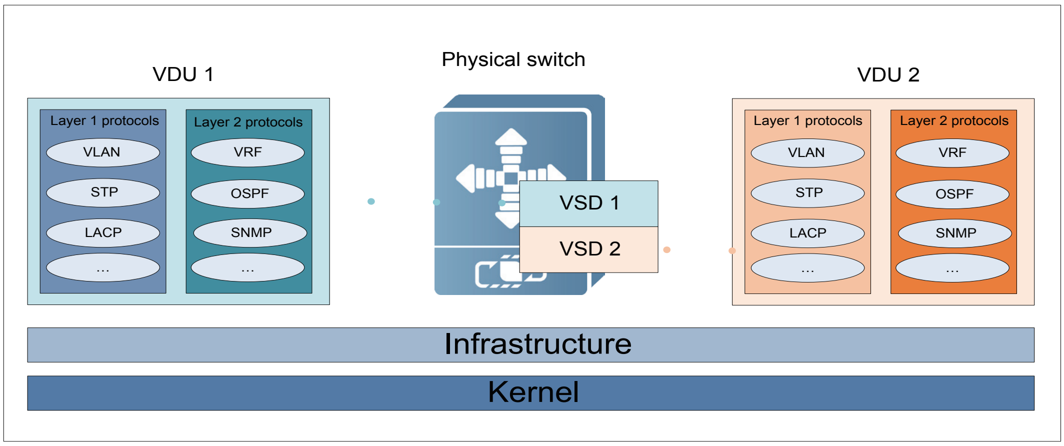
• Basics

A simple and convenient virtualization solution must be deployed to solve the foregoing problems. Therefore, a system-level virtualization solution is required, that is, network device virtualization. The network device virtualization solution is not specific to a service or a channel. Instead, it provides device-level virtualization.

Based on the current core switches, Ruijie has proposed a virtualization solution, that is, Virtual Switch Device (VSD). A VSD is a logical device that is virtualized on a physical device. In terms of functionality, the VSD is the same as a physical switch.

One physical device can be virtualized into multiple switches, as shown in the following figure:

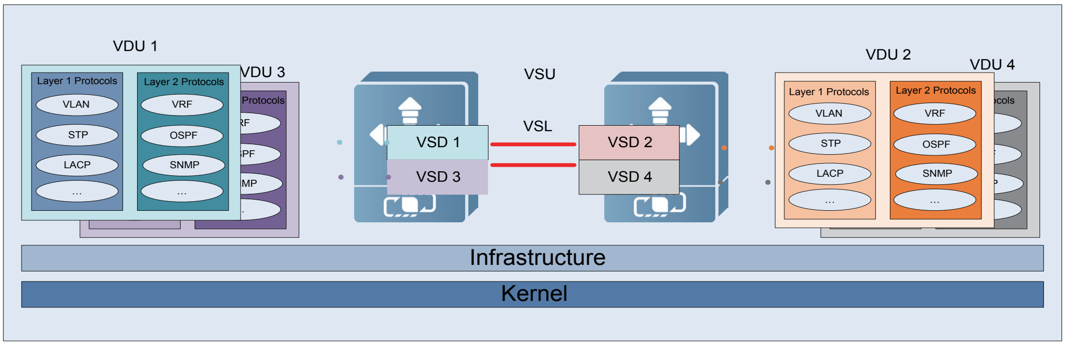
Figure 11 VSD model on a physical switch



A single chassis-type switch contains one or two supervisor engines and multiple line cards. One single physical device can be virtualized into multiple network devices: Each virtual device has corresponding resources, such as several line cards, or several ports of one line card. However, these resources belong to one VSD.

One VSU can be virtualized into multiple switches, as shown in the following figure:

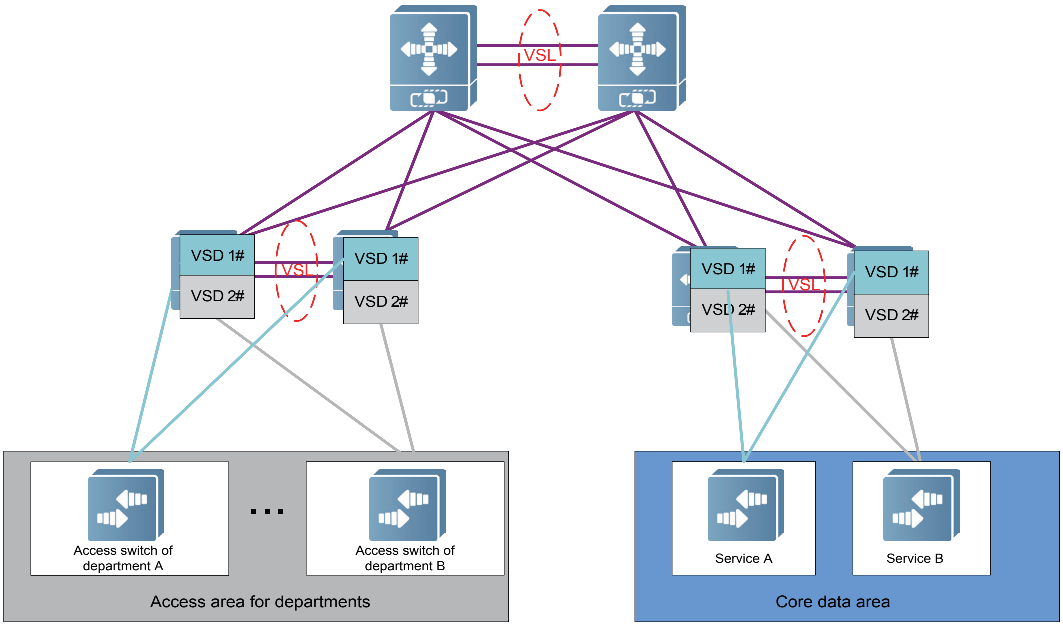
Figure 12 VSD Model on a VSU



Ruijie VSU system consists of multiple devices that are connected by virtual switch links (VSLs). Similar to a single physical device, one VSU can be virtualized into multiple VSDs. Each VSD has corresponding resources, such as one line card, or several ports of one line card.

Figure 13 shows the simple VSD networking.

Figure 13 Simple VSD Networking



In Figure 13, the convergence switch is virtualized into two VSDs, and each VSD is separately connected to one access switch. The VSDs are not dependent upon or associated with each other. Each VSD implements its own services. Some resources on the physical switch, such as ports, are divided into two parts and allocated to the two VSDs respectively. The resources allocated to one VSD cannot be accessed by the other VSD.

Therefore, the VSD technology solves the following problems:

*** Fault isolation: When a service fails, the networks not associated with the service are not affected.**

*** Network isolation: When a LAN fails, the other LANs are not affected.**

*** Low utilization rate of network devices: The VSD technology provides a network integration solution to optimize the network and increase utilization of network devices.**

*** Power consumption: The idle supervisor engines participate in the device or system operation.**

*** Insufficient capacity of system table: When the number of ports increases, the capacity of the physical device also increases.**

*** User management: A reasonable solution is proposed to provide proper and convenient configuration management.**

• Virtualization Solution

If one physical device is virtualized into multiple devices, one of the users' primary concerns is whether the virtual devices can provide the service functions as required. Therefore, the service and protocol modules are separated so that they run as an independent process, which is called VSD. To provide the required service functions, a certain hardware resources such as chips are allocated to the VSD. Each virtual device corresponds to one VSD. Each VSD has a certain hardware resources to implement its service. Each VSD is independent and does not affect other VSDs. Figure 14 shows the principle of the solution.

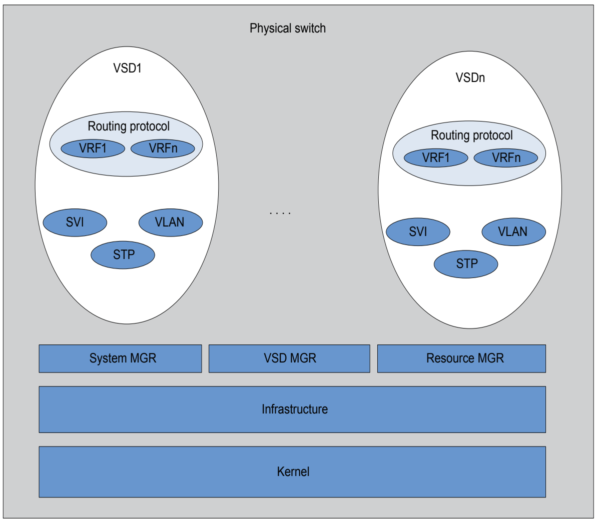
In Figure 14:

1) The VSD user cares about the services within his own network and the resources allocated to the user. A VSD is deemed as a virtual logical device.

2) Resource management and VSD management ensure that each VSD has a logically independent data forwarding plane, service control plane, and management plane. They ensure that all data are forwarded within the VSD, but not forwarded to other VSDs.

3) Because each VSD is a logical device, communication between two VSDs is realized by data forwarding through upstream and downstream devices or connected physical ports.

Figure 14 Virtualization solution



User Management Solution

Currently, the user management is not hierarchical. As a result, on one hand, the operators need to master more knowledge to avoid improper operations; on the other hand, the configuration may be modified by other operators.

Each VSD can be deemed as an independent switch. The user permissions can be configured based on VSDs. Therefore, the creation of independent management environment for each virtual device is the key to simplifying the operation and management of various virtual environments. Hierarchical user management requires that some operators can use only specified management environments or a subset of these management environments.

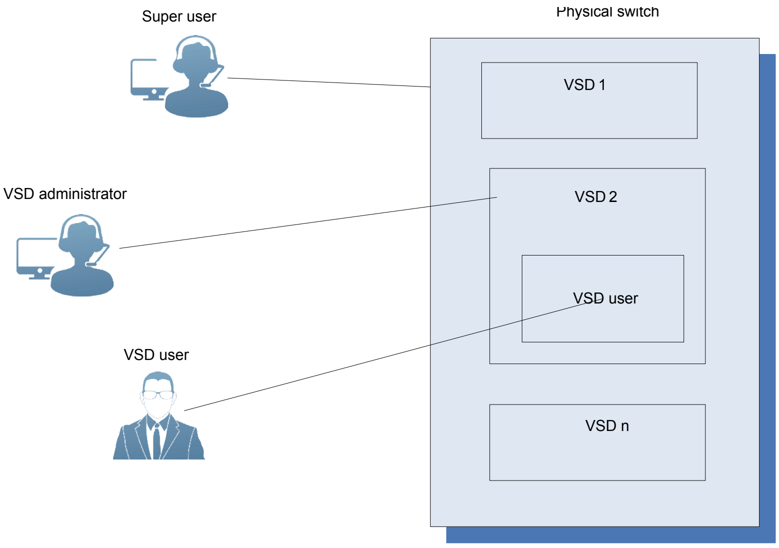
In the VSD framework, hierarchical management is implemented on switches and VSDs. the users at each layer are allowed to run certain CLIs commands. If the user runs an unauthorized command, an error will occur. This management mode brings the following advantages:

* **Each user is granted minimum permissions. This prevents the configuration from being modified, thereby facilitating user management.**

* **With hierarchical user management, the users at each layer are only allowed to manage authorized configuration, thereby ensuring proper configuration management.**

* **With hierarchical user management, the users at each layer only see only authorized commands, so the user can easily master the commands.**

Figure 15 VSD User Management



As shown in Figure 15, in the user management based on the VSD framework, users are divided into three classes: super user, VSD administrator, and VSD user.

1) Super user

As the highest-layer node in the user tree, a super user has the maximum permissions of the switch. In the VSD framework, a super user can:

* **Create or delete a VSD.**

* **Specify a physical port for a VSD.**

* **Restart a physical switch and a VSD.**

* **Modify some commands so that they are globally visible.**

* **Operate a VSD.**

2) VSD administrator

When a VSD is created, a VSD administrator is automatically created. As a layer-2 manager in the VSD system, the VSD administrator can:

* **Modify and save VSD configuration.**

* **Configure VSD protocol, services, entries, and so on.**

* **Restart VSDs.**

3) VSD user

As a layer-3 manager in the VSD framework, a VSD user can only run certain configuration commands and query commands. A VSD user can inherit the permissions of a VSD administrator.

Resource Allocation Solution

In the virtualization solution, each VSD can be deemed as a logical switch. Therefore, each VSD has its resources, and these resources cannot be shared by other VSDs. This feature is essential to fault isolation and network isolation. A VSD user can only see his own VSD resources. Therefore, in a VSD system, the resources of a physical switch must be reallocated.

Hardware resources must be flexibly divided so that they can be allocated to specified virtual devices. Fault prevention largely depends on the capability to isolate different virtual devices and the capability to allocate hardware resources for them. A VSD is created with resources allocated to it. Not all resources of the switch can be allocated to the VSD, as shown in the following figure:

Table 1 Switch Resources

Allocatable Switch Resources	Unallocatable Switch Resources
Physical ports, VLANs, APs, and switched port analyzer (SPAN) sessions	CPU, memory, and forwarding information base (FIB)

Only the globally visible and disposable resources can be allocated. In the current system, resources such as CPU and memory are not disposable.

1) Allocation of physical ports

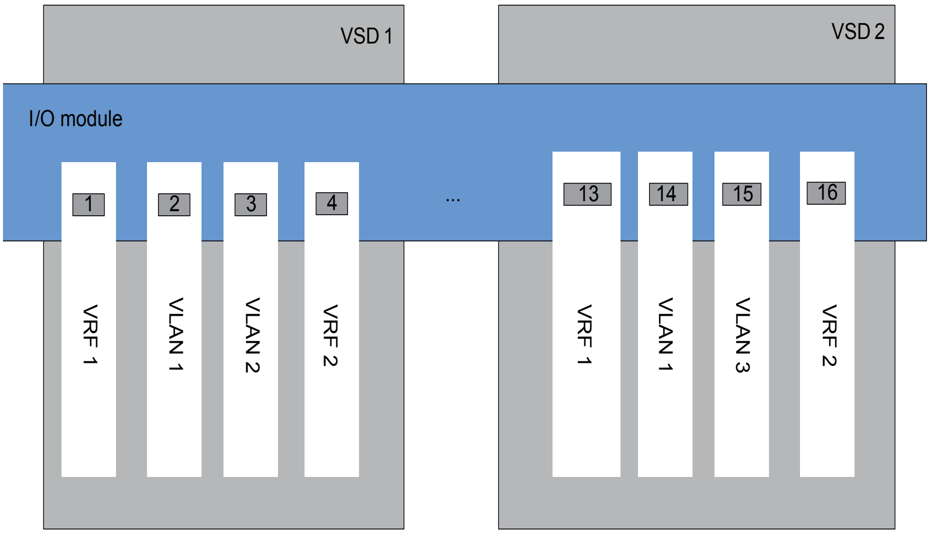
Rules for allocating physical ports

* **Each port can be allocated to only one VSD.**

* **After a port is allocated to a VSD, it cannot be used by the other VSDs.**

* **Different VSDs are different logical devices, so they can have the same protocol identifier. For example, VLAN 1 may exist on both VSD 1 and VSD 2.**

Figure 16 Allocation of Physical Ports



In Figure 16, ports 1, 2, 3, and 4 are allocated to VSD1, and ports 13, 14, 15, and 16 are allocated to VSD 2. These ports cannot be allocated to the other VSDs; that is, the other VSDs cannot use these ports. The VSD can be configured with related services. The services configured for the ports on VSD 1 will not affect other VSDs. For example, the MAC addresses learned by port 1 on VSD 1 will not be synchronized to VSD 2.

2) SPAN sessions

Due to the limitation of the switching chip, before virtual devices are divided, the maximum number of SPAN sessions that can be created is limited. After the VSD feature is introduced, the maximum number remains unchanged. For example, a maximum of two SPAN sessions can be created on a physical switch. When three VSDs are created on the switch, VSD 1 and VSD 2 are allocated one SPAN separately. No SPAN session will be allocated to VSD3. VSD 1 and VSD 2 serve as different logical switches, so their SPAN sessions can have the same identifier, that is, SPAN 1.

3) APs

Due to the limitation of the switching chip, the number of APs that can be created on a switch is limited. Therefore, the total number of APs on all the VSDs must not exceed the limit. For example, 128 APs can be created on a S12000 switch. Assuming that three VSDs are created on the physical switch, VSD 1 can be allocated 64 APs, and the remaining 64 APs are evenly allocated to VSD 2 and VSD 3. Different VSDs serve as different logical switches, so their APs can have the same identifier.

4) VLANs

Due to the limitation of the related protocol, a switch can support a maximum of 4096 VLANs. Similarly, a maximum of 4096 VLANs can be created on each VSD. After the protocol is extended and the QinQ technology is used, more than 4096 VLANs can be created on a switch with the VSD feature. Assuming that four VSDs are created on the physical switch, 4096 VLANs can be created for each VSD, so the total number of VLANs is 16,384. The VLANs on each VSD are numbered 1–4096.

VSD Deployment Solution

According to the analysis in the foregoing sections, VSD must be supported by a single device and the VSU system. A single device can be deemed as a special VSU system. The following analysis is based on the VSU system.

In the VSU system, the supervisor engine in a secondary switch/VSD has a low utilization rate.

The VSU system consists of one switch or multiple stacked switches. The VSU system can be divided into multiple virtual switches. In this case, the following problems must be considered:

* **Does the VSD run on one or multiple virtual switches? If the switch is a chassis device, which supervisor engine should the VSD run on?**

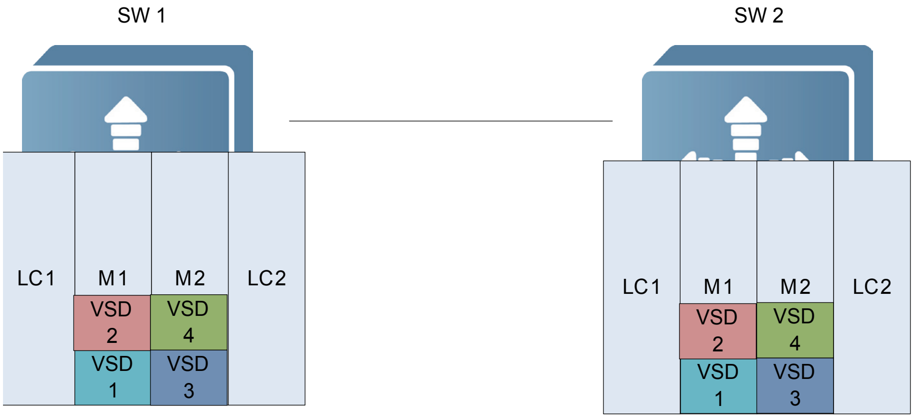
* **Because each VSD can be deemed as an independent logical switch, do the VSDs need to form a VSU?**

The following discusses the VSD deployment. For the discussion about VSU support, see the next section.

A chassis device features multiple supervisor engines and line cards. Based on the supervisor engines on which the VSD runs, the following solutions are available.

Figure 17 shows the distributed hot backup.

Figure 17 Distributed Hot Backup



In Figure 17, on SW 1, M1 contains primary VSDs including VSD 1 and VSD 2, and M2 contains secondary VSDs including VSD 3 and VSD 4; on SW2, M1 contains secondary VSDs including VSD 1 and VSD 2, and M2 contains primary VSDs including VSD 3 and VSD 4.

The foregoing solution brings the following advantages:

* **The load of a primary VSD can be allocated to different switches.**

* **The VSD backup is supported.**

VSD Hot Backup

In a VSU system, or on a chassis device that contains primary and secondary supervisor engines, VSDs can be deployed in a distributed or centralized manner. In either manner, VSD hot backup must be supported. If the VSD hot backup is not supported, once a VSD fails, the network on the VSD will be disconnected, and will not recover until the VSD is restarted.

Management of VSD Physical Ports

After the user logically divides a physical device into multiple VSDs, the following problems will occur: Taking the first scenario of problem 1 as an example, the user first needs to allocate the physical ports on the physical device; for example, the user needs to allocate some ports to VSD 1 so that VSD 1 works as a core switch, and allocate some ports to VSD 2 so that VSD 2 works as a convergence switch. As we all know, there are physical links between a core switch and a convergence switch. Therefore, the user needs to establish a connection between VSD 1 and VSD 2; that is, the user needs to physically connect the corresponding ports on the physical switches. If the number of logical switches or physical connections between logical switches increases, loops will occur when the logical switches are incorrectly connected. Besides, it will be difficult for the user to identify the VSD to which a port belongs (the user must log in to the switch and view the related configuration).

This problem can be solved with two approaches. One is to display the VSD to which a port belongs by using hardware, such as an LCD. This solution requires hardware support. The other solution is to allow the user to query the VSD to which a port belongs by using software, for example, to provide a command to display the physical ports of each VSD, or add a port attribute that indicate the VSD to which the port belongs. Based on the current hardware design of the CA, the solution that visually displays the VSD to which a port belongs is not available. Instead, related commands are added or modified to allow the user to query the VSD to which a port belongs. However, this mode depends on the planning of switch resources. If the switch resources are properly planned, this problem can be mitigated to a certain degree.

Typical Application

• Application Solutions

Network Node Virtualization

In this solution, virtual systems are created based on network nodes. For example, core-layer and convergence-layer virtual systems are created vertically, so that one physical device implements the functions of two physical devices; or two parallel virtual systems are created horizontally, so that the number of network devices decreases by half.

Figure 18 shows two vertical virtual systems.

Figure 18 Vertical Integration

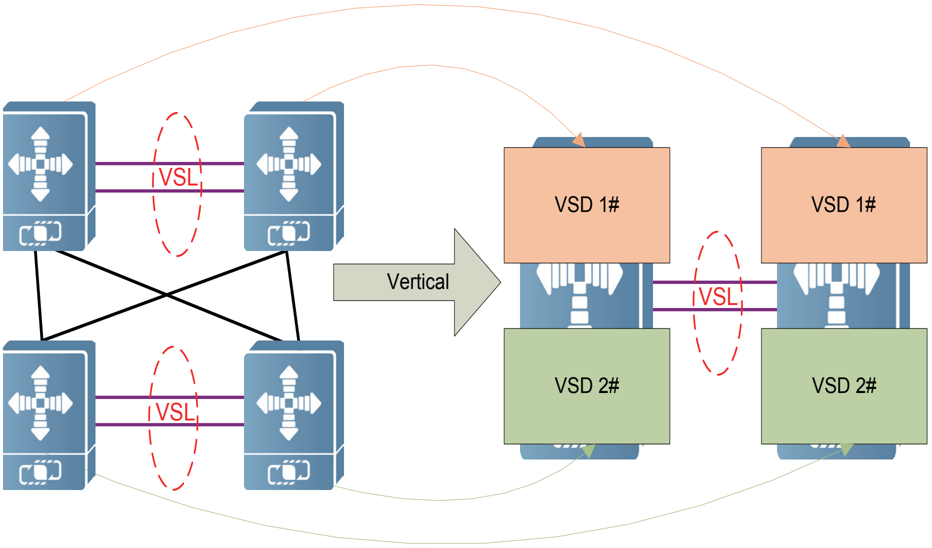
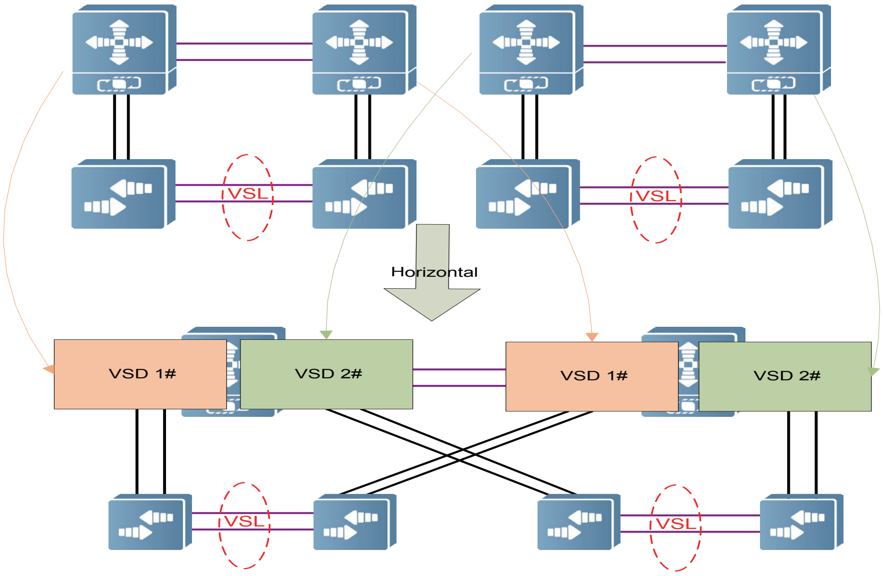


Figure 19 shows two horizontal virtual systems.

Figure 19 Horizontal Integration

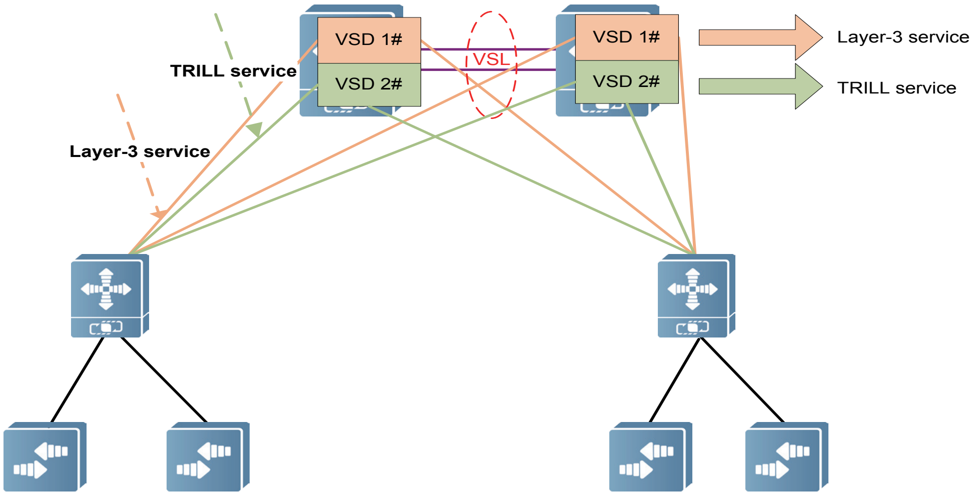


Benefits of the application scenario: The network topology remains unchanged, but the number of physical network devices decreases. This reduces the costs of the devices, improves the utilization of the devices, and lowers the power consumption of the devices (power supply, fans, and so on), auxiliary devices (equipment room, air-conditioning system, and so on), and resources, without degrading service experience and management experience.

Service Virtualization

Virtual systems are created based on services. For example, layer-3 services are deployed on VSD 1, and new service TRILL is deployed on VSD 2. Because the new service is deployed on a separate VSD, the potential impact of the new service on the existing services is reduced.

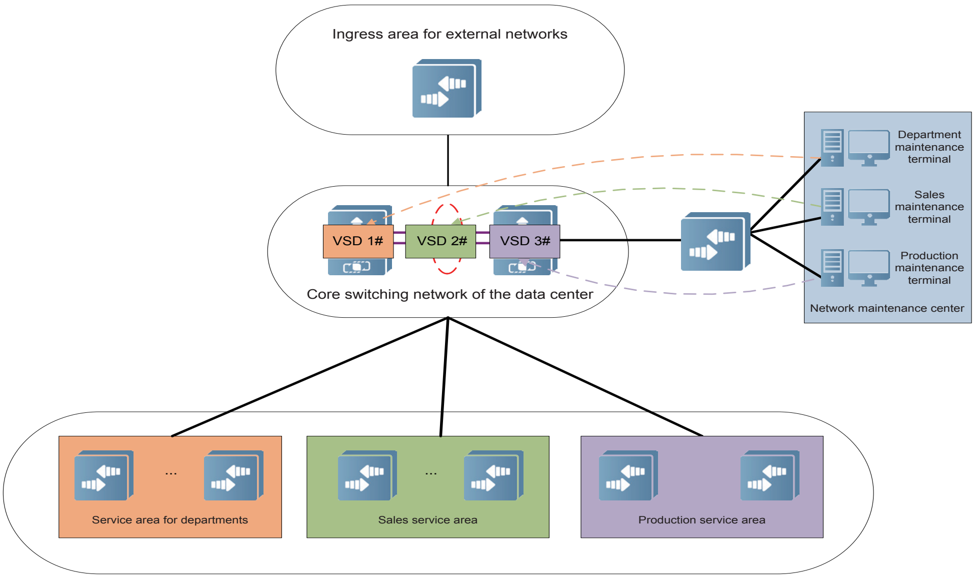
Figure 20 Service Virtualization



Benefits of the application scenario: Different services are isolated by VSDs. In this way, each service operates independently as if deployed on different devices. This protects the service resources and improves the reliability.

User Group Virtualization

Figure 21 User Group Virtualization


Ingress area for external networks
VSD 1#
VSD 2#
VSD 3#
Core switching network of the data center
Department maintenance terminal
Sales maintenance terminal
Production maintenance terminal
Network maintenance center
...
Service area for departments
...
Sales service area
Production service area

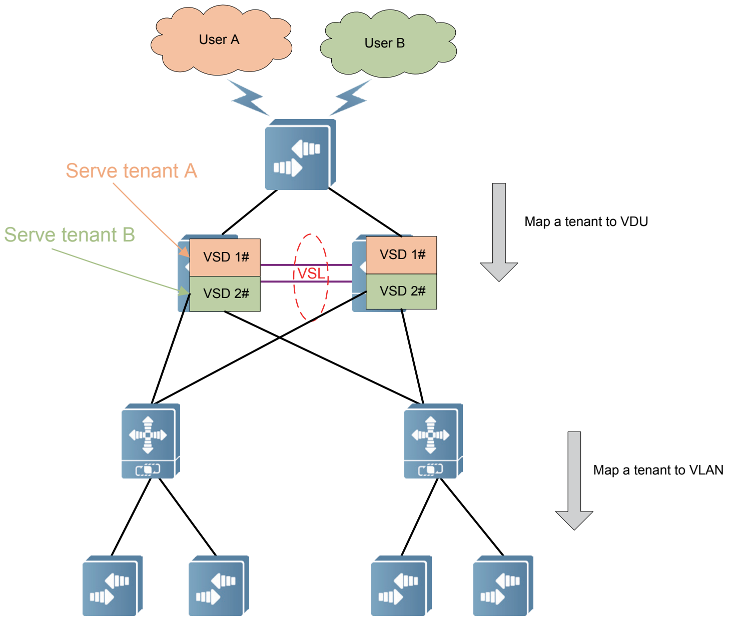
Virtual systems are formed based on network user groups, which can be user's business departments (such as production, R&D, marketing, service, and network management), user attributes (such as Intranet, DMZ, and Extranet), or user categories (such as internal office operation, online banking, and credit card service).

Benefits of the application scenario: Virtual systems are created to isolate the network service traffic and faults in different user groups, thereby improving the security and reliability. In addition, independent network management is implemented on different user groups, thereby avoiding the information security risk.

IDC Multi-tenancy

Virtual systems are formed based on different VIP customers. For example,

Figure 22 IDC Multi-user



Benefits of the application scenario: Compared with the VRF isolation, VSDs are used to flexibly deploy services for multiple users. It has advantages in network management, reliability, and security isolation, meeting the requirements of VIP customers.

Conclusion

As a new generation "one virtualized into multiple" architecture, Ruijie VSD technology enables more customers to flexibly create virtual switches for data centers, simplifies user management, and improves the reliability and security of services. It also ensures that network device resources are fully utilized, thereby saving costs for customers. In addition, with the "multiple virtualized into one" technology, namely, VSU, the network devices can be flexibly deployed as required, providing flexible and scalable service experience. In a word, it turns the data center into a highly flexible and scalable virtualization cloud network, helping customers experience the cloud network.

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**