NEC White Paper

SDN Component Stack and Hybrid Introduction Models

CONTENTS

ICT Issues in the Cloud and Big Data Era

Three management issues and related ICT system issues

To survive in the age of drastic changes in business environments, corporations must adapt rapidly to change. Behind the frequent mentions of the cloud and big data, there are great expectations of Information and Communication Technology (ICT) from corporations that need to adapt to change.

The management issues that a corporation has to tackle to adapt to change can be categorized into the following three types: “growth strategy execution,” “cost reduction,” and “countermeasures against risks.” An ICT system must support the resolution of these management issues rapidly and flexibly to improve the ability of a corporation to adapt to change. However, conventional ICT systems are complicated and divided into silos, exposing various issues that adversely affect adaptability to change.

Regarding “growth strategy execution,” which is intended to expand sales and revenue, if it takes more time to develop infrastructure and construct a system to execute growth strategies such as new business development and service deployment, there is the possibility of missing an opportunity to create new services. Moreover, as business expands overseas or the number of sites increases, new issues appear, such as that the network interconnecting sites may become complicated and lead to problems; for example, the line utilization efficiency could be adversely affected, and the operating costs increase.

Regarding “cost reduction”, it is important to reduce costs related to facilities and operations. If, however, the network is physically separated for each system, hardware facilities such as servers, firewalls and load balancers would be required for each network thus leading to unnecessary facility costs and redundant investment. Moreover a flexible ICT system for business change requires high skilled engineers, so the operation cost for the network management and maintenance would increase. In “countermeasures against risks,” a complicated redundant structure design and an inter-data center network for data backup are required to implement failure and disaster recovery. Moreover, as cross-industrial cooperation, open innovation, bring your own device (BYOD), etc. have become more commonplace in recent years, there are more diverse office environments in which members with various affiliations and roles bring in various devices. In such environments, security measures to protect the ICT system and information are essential.

Management issues		Related ICT systems	Issues
Growth strategy execution	New business exploitation Service development	Virtualization platform LAN (development/event NW)	Time required to build new services
	Overseas expansion Site increase	Inter-site NW	WAN line utilization is inefficient
Cost reduction	Facility cost reduction	Intra-DC NW	FW and LB servers exist individually for each physically separated network
	Operational cost reduction	Virtualization platform, intra-DC NW, LAN, inter-DC NW	Costly to modify/ maintain/manage network
		Overall system	Dependent on skilled engineers
Countermeasures against risks	Failure/recovery BC/DR	Intra-DC NW, inter-DC NW	Redundant design that considers possible failures is troublesome
	Security measures	Intra-DC NW, LAN	Cannot support various devices and open environments

NW : Network, DC : Datacenter, LAN : Local Area Network, WAN : Wide Area Network,
FW : Firewall, LB : Load Balancer
BC : Business Continuity, DR : Disaster Recovery

Virtualization of IT infrastructure to deal with changes

To solve these conventional ICT system issues and realize an ICT system that can deal with the management policies implemented to adapt to change, servers and networks must be virtualized. Creating a pool of resources consisting of virtualized servers and freely reconnecting them in a virtualized network enables the prompt building of the required services, a reduction in facility costs by sharing hardware with multiple systems and a reduction in operational costs while improving security. The latest of these network virtualization technologies, known as Software-Defined Networking (SDN), is currently gaining attention.

SDN Revolutionizing ICT

What is SDN?

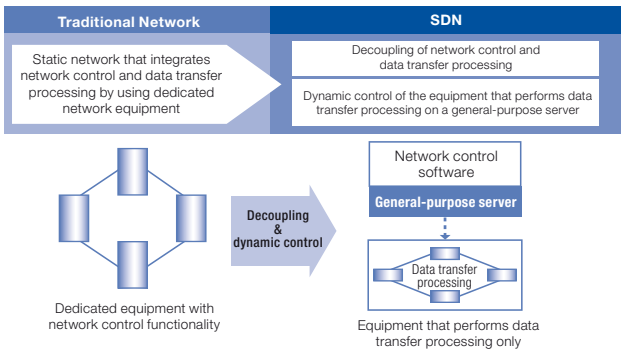
In recent years, “SDN” has been attracting attention as a network virtualization technology. However, its definition differs depending on the vendor. NEC defines SDN as the “dynamic control of a network by software, and its architecture.”

The differences between SDN and conventional networks can be summarized as: “decoupling” and “dynamic control.” In conventional networks, network-dedicated appliances such as routers, firewalls, and load balancers were placed in the paths of the packets to be used. When network control and data transfer processing were combined in these network dedicated appliances, an attempt to modify the network required manual configuration of each appliance, thus preventing smooth operation.

On the other hand, a network using SDN differs greatly in that network control and data transfer processing are “decoupled.” Data transfer processing is allocated across the network similarly to the conventional method. However, network control is centrally managed, and therefore by configuring only one location, the behavior of the entire network can be changed.

“Dynamic control” is another point that is very different from a conventional network. In dynamic control, the network behavior can be dynamically controlled from the upper-layer database and business systems using the network control software via an Application Programming Interface (API). For example, intelligent control such as changing the transfer destination of the packet based on the database content is possible.

Another keyword related to SDN is “OpenFlow.” This is one of the standard protocols of SDN that connects network control and data transfer.

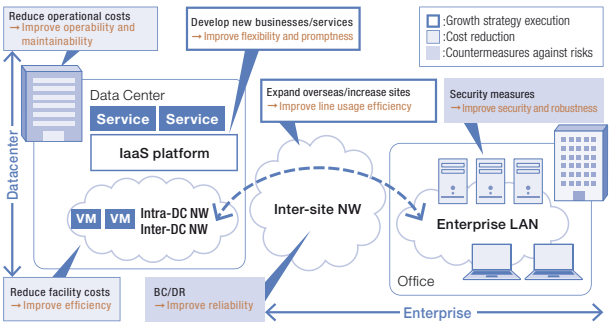


Contribution of SDN to Solve the Three Management Issues

By applying SDN, the ICT issues described earlier can be resolved. A case in which SDN is applied to a network in a data center equipped with an Infrastructure as a Service (IaaS) platform is an example of “growth strategy execution” in the development of new businesses and services. Virtualization enables provisioning server resources on demand and dynamically changing the network structure, so new services can be provided more flexibly and promptly. Moreover, by applying SDN to the inter-site network when expanding overseas and increasing the number of sites, the utilization efficiency of WAN can be improved.

For “cost reduction,” applying SDN to the network in a data center can reduce costs through the sharing of hardware facilities such as firewalls and load balancers. Moreover, operational costs can be reduced by automating the data center operation in coordination with the IaaS platform.

For “countermeasures against risk,” SDN enables disaster recovery and resource sharing between data centers via an inter-data center network. SDN also helps implement network security measures by separating members according to their affiliations and titles.



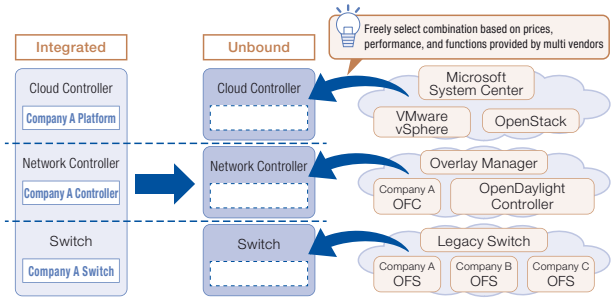
VM : Virtual Machine

Introduction Methods That Maximize the Benefit of SDN

Points to avoid pitfalls of SDN / hybrid introduction models

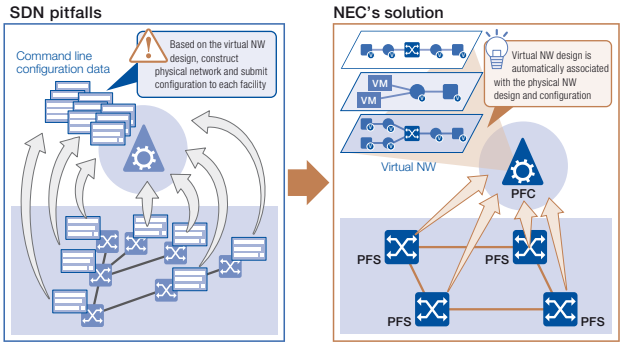
Two common questions asked about SDN introduction are “Are there any pitfalls of SDN?” and “Do we have to replace the entire existing network to introduce SDN?” In response to these questions, this section describes the points to avoid pitfalls of SDN in order to maximize its benefit, and “hybrid introduction models” in which SDN is partially introduced without replacing the entire existing network. These hybrid introduction models enable SDN to exert its value while co-existing with the existing network, and were proposed by NEC based on the company’s extensive experience in the area of SDN construction.

An important point to avoid pitfalls of SDN is the selection of SDN products and solutions using appropriate “decoupling” and “dynamic control.” “Decoupling” and “dynamic control” are the two major points that distinguish SDN from conventional networks. However, they are implemented quite differently depending on the vendor. So, what is appropriate implementation of “decoupling” and “dynamic control?” These points are determined based on whether “openness” and “abstraction of configuration structure” are fulfilled or not.



OFC : OpenFlow Controller, OFS : OpenFlow Switch

For example, even though network control and data transfer processing are “decoupled,” if the control protocol between them is strongly depend on an appliance from only one particular vendor, the user cannot select the best combination of appliances from different vendors. However, if SDN products and solutions based on standardized control protocols that assure “openness” are selected, the best combination can be selected freely based on price, performance, and functionality according to the purpose. The user can then benefit from the innovation accelerated by the openness and the cost reduction of the appliances by commoditization.



PFC : ProgrammableFlow Controller,
PFS : ProgrammableFlow Switch

Moreover, even though “dynamic control” by applications becomes possible, if that control is only accessible from the command line, it is difficult to get an overview of the entire network. For the user to grasp an overview of the entire network, the network structure must be visualized by the “abstraction of the configuration structure,” and complicated configurations must be expressed as concepts such as virtual routers, virtual bridges, and virtual links, which are intuitive and easier to understand. By guaranteeing the advantages of “decoupling” and “dynamic control,” the benefit of SDN introduction can be maximized.

Hybrid Introduction Models That Satisfy a Diverse Range of Customer Needs

SDN introduction models with a high affinity to the existing network

Introducing SDN does not require the total replacement of an existing network. Rather like targeted medical treatment in which only the amount of medicine required for treatment is administered, by adequately introducing SDN to only the required area in an existing network, the effects and benefits of SDN can be received without affecting the existing network. NEC provides SDN "hybrid introduction models" that have a high affinity to the existing network.

Hybrid introduction models can be categorized into the following three major types: "add-on type," "partial replacement type," and "overlay type."

Model		Introduction method	Main benefits of introduction
Large category	Small category		
Add-on type	Add-on model	Adds SDN Components to a specific point in the existing NW	Facility cost reduction Security measures Site increase
Partial replacement type	Edge replacement model	Replaces part of the existing NW, such as the edge and core switches, to SDN components	Acceleration of new service deployment Operational cost reduction Disaster recovery
	Core replacement model		
	Pass-through model		
Overlay type	Edge overlay model	Introduces a virtual switch to a server without changing the existing network	Acceleration of new service deployment

The add-on model, that is, an introduction model of the "add-on type," is introduced by adding SDN components such as controllers and switches to specific points in the existing network. The main benefits of the add-on model are a reduction in facility costs, better security measures, and more efficient WAN utilization when the number of sites increases.

The "partial replacement type" is further categorized into the following three types: "edge replacement model," "core replacement model," and "pass-through model." These are introduced by replacing a part of the existing network such as the edge or core switches with SDN components. The main benefits of the partial replacement type are the prompt deployment of new services, operational cost reduction, and BC/DR.

The edge overlay model, that is, an introduction model of the "overlay type," is applied by introducing virtual switches to the server and controlling the virtual switches by a controller without modifying the existing network. The edge overlay model is effective when constructing a flexible network like the IaaS platform in data centers, in which numerous virtual machines are created, moved, or removed dynamically.

Add-on model

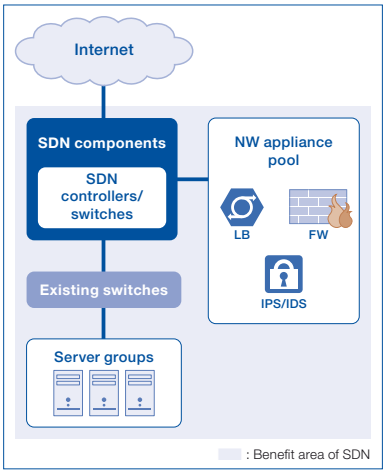
Adds SDN components to an existing network

The add-on model is used to introduce SDN components to a specific point between an existing network and the Internet, and is used to collectively utilize network appliances such as firewalls and load balancers.

In conventional network, network appliances such as firewalls and load balancers were installed separately in each silo of the network. By applying the add-on model, these network appliances can be aggregated, and shared, thus reducing facility costs.

Moreover, it is also possible to cooperate with security appliances according to traffic behavior, enabling highly flexible network security that was impossible using existing security appliances alone.

Another form of the add-on model is a method whereby an SDN switch is allocated at the WAN entrance of each site. In this case, WAN efficiency can be improved through cooperation between the SDN controller and the network monitoring system at the main data center.



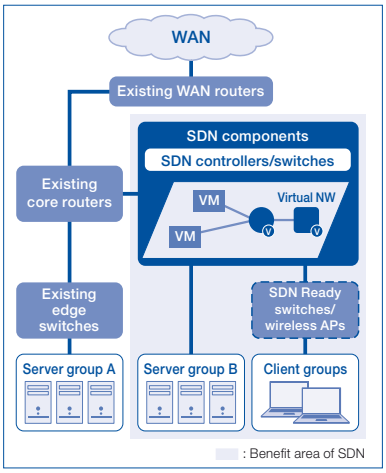
IPS : Intrusion Prevention System, IDS : Intrusion Detection System

Edge replacement model

Replaces edge switches with SDN components

The edge replacement model is an introduction model in which SDN components are introduced to an edge unit where servers and clients are incorporated into the network. The advantages of this model are that the effect of SDN can be verified in parallel with the operation of the existing network, new servers and networks can be flexibly installed according to system or organization scale-up and operational costs can be reduced in the SDN network.

An edge replacement model can also be applied by introducing, in advance, SDN Ready switches that support both the legacy (conventional) functions and SDN functions, and which will allow smooth migration later to the edge replacement model simply by adding an SDN controller.



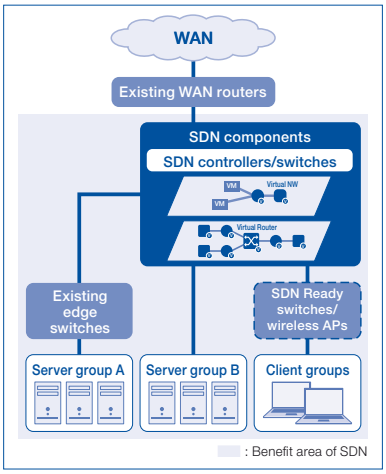
AP : Access Point

Core replacement model

Replaces the core routers with SDN components

In the edge replacement model, the existing core routers were still used as hardware equipment. In contrast, the core replacement model is an introduction model that imports the functions of the existing core routers as virtual routers on a virtual network to eliminate the existing hardware core router.

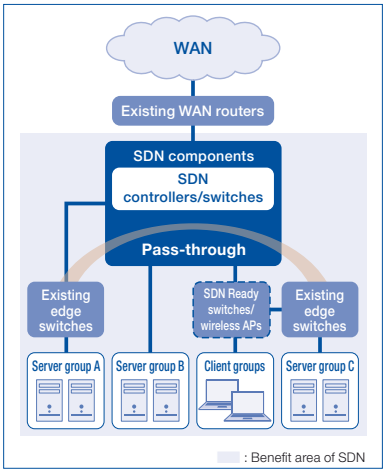
Core routers are expensive and large-scale equipment. They can be removed by the introduction of SDN, thus reducing costs related to facility installation space, power consumption, and hardware maintenance.



Pass-through model

Enables expansion while preserving the existing network

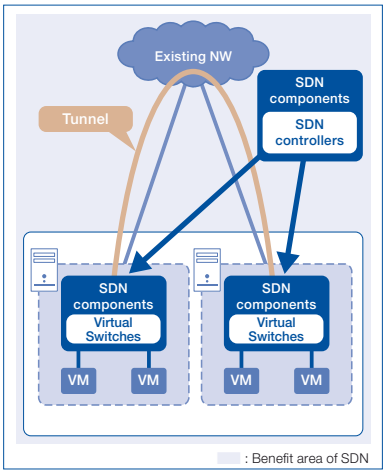
The pass-through model is an introduction model that supports the continued use of the servers and appliances connected to the existing network without changing their configuration in a hybrid environment consisting of SDN and the existing network. As the hybrid introduction of SDN advances, there are cases in which the areas of the existing network and SDN network co-exist, and the need to connect existing networks over an SDN area arises. In such a case, changing the configurations of the appliances connected to the existing network is unnecessary. Using a technology called “pass-through,” packets are transmitted through the SDN area to enable the continued use of servers and appliances connected to the existing network without having to change the original configurations.



Edge overlay model

Introduces virtual switches while remaining the existing network

The edge overlay model is a hybrid introduction model that virtualizes the physical servers and switches. An SDN controller creates a tunnel in the existing network and thus constructs an end-to-end virtual network. The main scope of this model is super large-scale data centers in which inter-virtual server communications occur often and in which virtual servers are created, moved, or removed frequently. The advantages of this model are that the physical switches installed in the existing network can remain as is while SDN is introduced, and that the network can adapt promptly and flexibly to the virtualization of the servers.

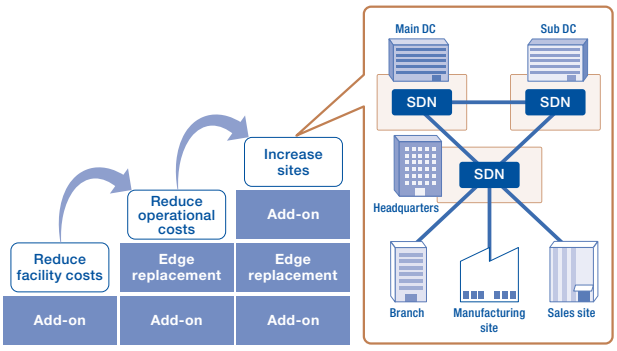


Migration scenario

The previous sections described how the five types of hybrid introduction models can realize the benefit of SDN in the different areas of the existing network. Advancing from the partial SDN introduction, NEC also proposes a path to replace the entire network with SDN. This is a migration scenario that gradually advances the hybrid introduction and draws out the positive effects of its introduction, ultimately introducing SDN to the entire existing network.

Here is an example of such a migration scenario. Firstly, the add-on models are applied to aggregate the network appliances such as firewalls and load balancers to reduce the facility costs. Secondly, by applying the edge replacement model, the network flexibility is improved and the operational costs are reduced. Lastly, applying the add-on model for the WAN enables the improvement of the efficiency of WAN utilization between data centers or between major sites. Through these steps, SDN can be introduced to the entire network.

This section has described a typical migration scenario; however, the priority order and pattern of the introduction models differ depending on your issues and situations. In actuality, various steps are considered and planned for each customer.



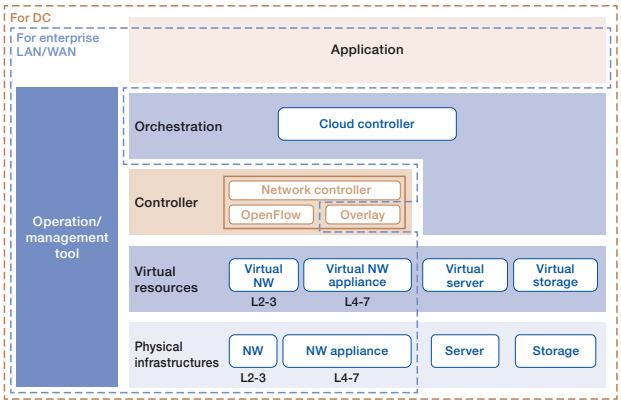
NEC's SDN Component Stack

Building blocks of SDN

This section describes NEC's SDN component stack that supports the SDN hybrid introduction models from the viewpoint of the following layers; "physical infrastructure layer," "virtual resources layer," "controller layer," "orchestration layer," and "application layer."

On the "physical infrastructure layer," there are the L2 and L3 switches that perform data transfer and routing, network appliances such as firewalls and load balancers that provide the L4 to L7 functions, physical servers, and physical storages. These physical infrastructures are virtualized and utilized as a resource pool in the "virtual resources layer." In addition, on the "controller layer" there are control modules that support OpenFlow and overlay as the methods to control switches and network appliances, and the network controller that can manage multiple network control modules in a bundle. Also, the cloud controller on the "orchestration layer" provisions server and storage resources corresponding to the user requests. By enabling cooperation between the "controller layer" and "orchestration layer," virtual servers, virtual storages, and virtual network appliances can be generated and deleted freely and connected flexibly.

The "application layer" that exists on the upper level realizes the required services by changing the virtual resources according to the Service Level Agreement (SLA) and functions/performance of applications. Moreover, an operation/management tool is provided, which operates/manages the entire system while linking these layers.



The overall image (framed by the red dotted line) visualizes an architecture for data center (DC). An architecture for an enterprise LAN/WAN may not require virtual servers, virtual storages, etc. Therefore, the blue dotted line in the SDN component stack can be applied for an enterprise LAN/WAN.

Solution stack

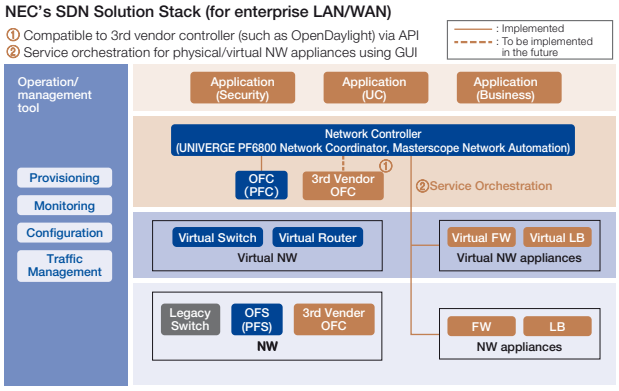
NEC's SDN solution stack maps SDN products and solutions to be released in the future on the component stack. The solution stack includes two stacks: a solution stack for enterprise LAN/WAN that focuses on network functions, and a solution stack for data centers that is the same as the enterprise LAN/WAN solution stack but with an added orchestration layer for provisioning servers and storages.

Solution stack for enterprise LAN/WAN

The solution stack for enterprise LAN/WAN is characterized by the openness and abstraction of its configuration, which are the main advantages of NEC's SDN. Specific examples include ① cooperation with controllers from third-party vendors and ② Graphical User Interface (GUI) based service orchestration.

① In cooperation with a third-party vendor controller, OpenDaylight can be involved in our solution. We have contributed source code for Virtual Tenant Networks (VTN) to the OpenDaylight project that enable configuration abstraction and visualization of the network. Moreover, in the future we will strengthen our cooperative relationship with other vendors, to enable the selection of the most suitable controller from an extensive ecosystem.

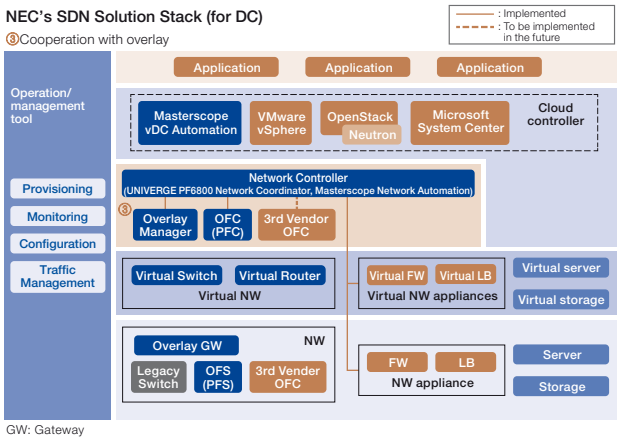
② The service orchestration of both physical/virtual network appliances using a GUI is already realized to some extent by cooperation of UNIVERGE PF6800 Network Coordinator (UNC) and Masterscope Network Automation (NWA). In the future, we plan to further integrate UNC and NWA, and increase our network appliance partners.



UC: Unified Communication

Solution stack for data centers

The solution stack for data centers is characterized by the existence of elements actualizing the cloud controller and overlay. As an NEC product for the cloud controller, we provide Masterscope vDC Automation. It is also possible to cooperate with other vendor products such as VMware vSphere and Microsoft System Center, as well as OpenStack that has a track record as an open source cloud controller. To enable cooperation with overlay, know-how is already being accumulated by employing the edge overlay method in the virtualization of the BIGLOBE data center and the NEC Kanagawa data center.



GW: Gateway

Advantages of NEC's SDN component stack

In this white paper, we have described NEC's SDN hybrid introduction models and the SDN component stack that enables the introduction models. NEC's SDN component stack is superior in the following three points.

(1) Openness: Flexibility of combination and innovation achieved by openness can be fully utilized
(2) Abstraction of configuration: By abstraction of configuration, the network status can be grasped easily, thus lowering the operational cost
(3) Variety of adapted models: High-throughput and Quality of Service (QoS) by physical switches and scalability/ flexibility by virtual switches can be selected and used according to the user environment and demands

When introducing NEC's SDN, the existing network does not need to be replaced entirely, because partial hybrid introduction is possible. Even after partial introduction, in the future it will be possible to pursue (1) cooperation with third-party controllers, (2) service orchestration using GUI and (3) cooperation with overlay. SDN provided by NEC is characterized by the ability to choose the best combination for the future business environment changes.

Use Cases

Case 1
Security gateway

Introduction model :
[Add-on]

Introduction scope :
[Intra-data center network/office LAN]

By introducing SDN to DeMilitarized Zone (DMZ) and making it operate as an intelligent tap, security can be improved while keeping costs low.

■ *Issues*

- The functions of existing security appliance products are segmented, making it difficult to select the best one.
- Security appliances with a high throughput are expensive.

Cyber attacks that are becoming increasingly sophisticated each year. Expensive security appliances with high throughput are required to check all traffic coming into in-house network from outside. Moreover, the functions of conventional security appliance products are segmented, making it difficult for users to select the most suitable one for their requirements.

■ *Solutions*

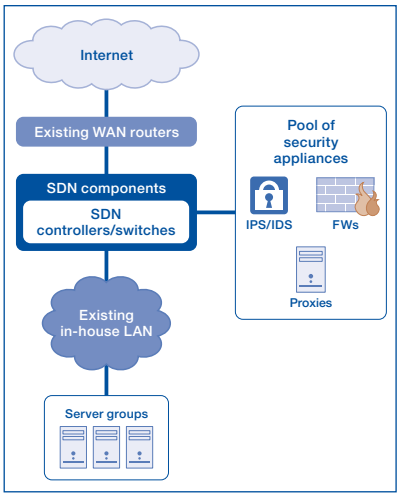
- Introduce SDN to DMZ by applying the add-on model to realize an intelligent tap function.
- Select suspicious traffic selectively based on its behavior.

SDN is introduced to DMZ (the boundary line between an external network and an office LAN or intra-data center LAN) by using the add-on model, and functions as an intelligent tap that automatically allocates traffic to each security appliance according to traffic behavior.

■ *Benefits*

- Security is improved
- Facility costs are reduced

The intelligent tap function is implemented by SDN, which eliminates the need to check all traffic by using security appliances. The existing expensive, high-throughput intelligent tap is no longer required, which realizes facility cost reductions and, at the same time, improves security.



Case 2
DoS/DDoS attack countermeasures

Introduction model :
[Add-on]

Introduction scope :
[Intra-data center network/office LAN]

The combination of SDN and a Denial of Service (DoS) / Distributed Denial of Service (DDoS) defense device can improve security while preventing the degradation of network throughput because only suspicious traffic of malicious communication is redirected and inspected by the DoS/DDoS defense device.

■ *Issues*

- Threat of cyber attacks caused by the spread of easy-to-use DoS/DDoS attack tools and sophisticated attack methods
- Degradation of network throughput caused by the introduction of a DoS/DDoS defense device because all packets need to be inspected

In recent years, damage from DoS/DDoS attacks has been increasing, and the need to counteract illegal traffic is growing. However, when a DoS/DDoS defense device is implemented in the network, the necessity of inspecting all traffic causes degradation in network throughput.

■ *Solutions*

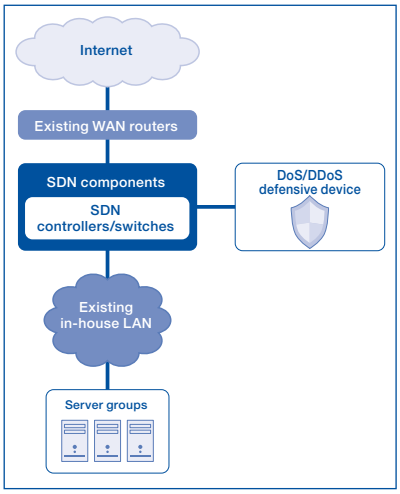
- Have only packets with suspicious fluctuation of communication volume redirected to and checked by the DoS/DDoS defense device
- Discard the packets at the entrance to SDN once they are identified as attack traffic by the DoS/DDoS defense device.

Introduce SDN to the boundary zone of the external network and in-house LAN or intra-data center LAN by using the add-on model, and coordinate it with the DoS/DDoS defense device. Traffic is monitored by the SDN controllers and switches, and if suspicious communication is detected, it is redirected to the DoS/DDoS defense device and inspected. If it is determined to be illegal traffic, the DoS/DDoS defense device instructs the SDN controller so that huge volumes of attack packets can be discarded at the entrance of network.

■ *Benefits*

- Security is improved.
- Throughput is improved.

By detecting suspicious traffic with SDN and inspecting it selectively with a DoS/DDoS defense device, illegal traffic can be eliminated efficiently, and security can be improved without degrading network performance.



Case 3
Consolidation of network appliances

Introduction model :
[Add-on]

Introduction scope :
[Intra-data center network]

An SDN component is introduced between the existing network and the Internet. Facility and operation costs can be reduced by consolidating and sharing network appliances such as firewalls and load balancers that were allocated for each silo of the network.

■ *Issues*

- Network appliances are installed for each silo of the network.
- Facility investments are duplicated.

In many cases, numerous network appliances such as firewalls and load balancers are installed for each organization and business system. In such a siloed network, facility investment is duplicated, increasing facility and operation costs.

■ *Solutions*

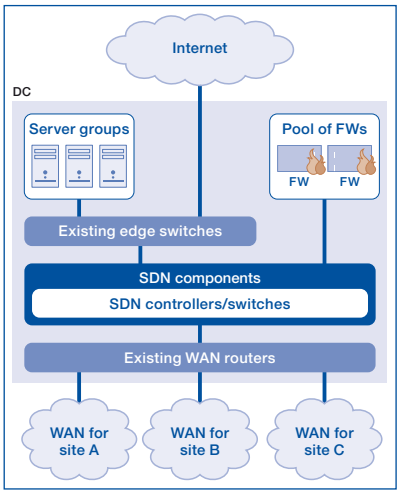
- Consolidate physical network appliances.
- Share virtual network appliances and create a resource pool.

The SDN components are introduced between the existing network and the Internet by adopting the add-on model. The firewalls for each organization and business system are integrated and aggregated. Centralized management of the communication route can share physical/virtual network appliances as a resource pool.

■ *Benefits*

- Facility costs are reduced by consolidating network appliances.
- Operational costs are reduced, and networks creation and configuration changes can be more prompt and flexible.

Network appliances can be pooled as shared resources. In some cases firewalls have been consolidated to less than one tenth of the original number, and annual operational costs reduced to approximately one third. Moreover, centralized network management has allowed to change configuration more promptly and flexibly.



Case 4
Optimization of inter-data center connections

Introduction model :
[Add-on]

Introduction scope :
[Inter-data center network]

Introducing SDN to inter-data center connections enables an Active-Active operation of redundant lines.
Moreover, the maximum transmission capacity at peak times can be covered by aggregating the bandwidths of all the lines, reducing both operational and line costs.

■ *Issues*

- The operation of inter-data center connections becomes more complex as the number of data centers increases.
- A redundant configuration is required to ensure the reliability of inter-data center communications.
- Processes for investigating the cause of failures such as burst traffic have become complex.
- Line and operational costs have increased.

When using an Active-Standby configuration to ensure the reliability of inter-data center communications, there will be unused bandwidth most of the time. Because standby line resources are usually unused and the bandwidth per line is determined based on the maximum transmission volume at peak times. As the number of lines increases between data centers, the rate of failures such as burst traffic also increases, and investigating the cause and applying countermeasures is complicated. Given this background, issues of both line and operational costs arise for inter-data center communications.

■ *Solutions*

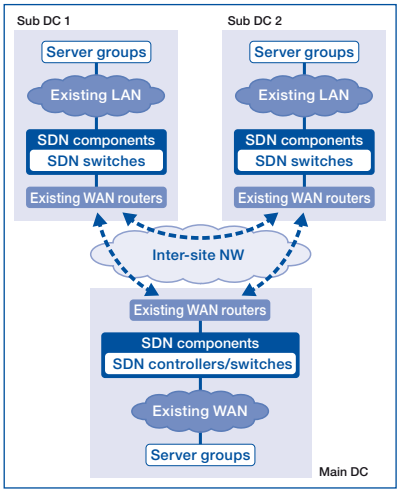
- Introduce SDN between existing LAN and WAN routers.
- Monitor traffic at the existing WAN routers and control flow based on the traffic volume.

To use redundant inter-data center networks as an Active-Active configuration, SDN components are allocated between the existing LAN and WAN routers in each data center. The process for preventing failure caused by burst traffic is automated by the coordination of network monitoring tools and SDN controllers.

■ *Benefits*

- Line costs are reduced.
- WAN operability is improved.

SDN enables the efficient use of line capacity and reduces the line costs. Moreover, automating failure prevention improves the operability of the WAN line.



Case 5
Virtualization of the server network

Introduction model :
[Edge]

Introduction scope :
[Virtualization platform]

Introducing SDN to a virtualized environment improves the flexibility of ICT systems because not only servers but also network resources can be provisioned on demand.

■ *Issues*

- Each time a new user environment is created, operations for adding and configuring network appliances occur, thus increasing the costs and required number of man-hours.
- Network configuration and failure recovery require high-level skills, so the operation depends on individual expertise.

Demands for on-demand development environments are increasing. Server resources can be provided more promptly by server virtualization technology. However, the time required to add and configure network appliances still prevents prompt resource provision. Moreover, reducing operation costs and responding quickly to failures are issues of vital importance.

■ *Solutions*

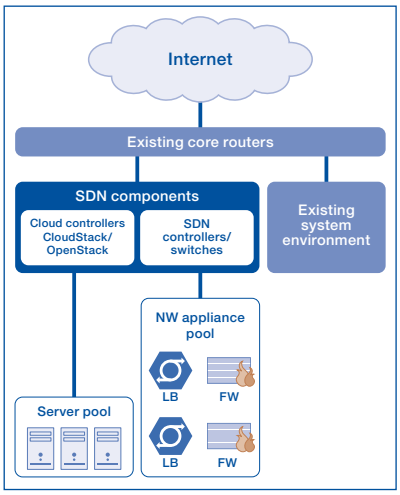
- Semi-automate creation of development environments by the cloud platform and SDN controller.
- Network visualization provides easy understanding of the current situation and intuitive operations.

Open-source cloud platform software such as OpenStack and CloudStack are used to create a virtual server environment. Applying SDN switches and controllers can enable visualization of the network topology and status. Network visualization makes the assessment of the current situation easier and the network operation more intuitive.

■ *Benefits*

- The lead time for development environment construction is reduced.
- Network operation does not depend on individual expertise.
- Faster failure recovery.

Almost all construction work related to servers and networks can be automated. The lead time for constructing a development environment can be shortened from one month to several hours. Visualization of the network configuration and modifications reduces the difficulty of configuration work, and eliminates dependency on individual expertise. At the same time, failures can be recovered more quickly and efficiently.



Case 6
Gradual migration of intra-data center network to SDN

Introduction model :
[Edge]

Introduction scope :
[Intra-data center network]

To introduce SDN without stopping data center operations, it is possible to use a gradual migration method whereby virtual servers are migrated from the main site to a backup site where SDN has already been introduced.

■ *Issues*

- Network modifications take longer than the time required to provide a virtual server.
- Outsourcing network configuration changes incurs additional costs.

Even if IT resources are provisioned flexibly, it is still takes time to configure and modify the network; therefore it is difficult to provide the entire infrastructure promptly. If network operations in data centers are outsourced, each time IT resources are provisioned, configuration modification fees are charged, thereby increasing operational costs. SDN can effectively solve these issues in an intra-data center network. However we need a way to introduce SDN without stopping the overall operation.

■ *Solutions*

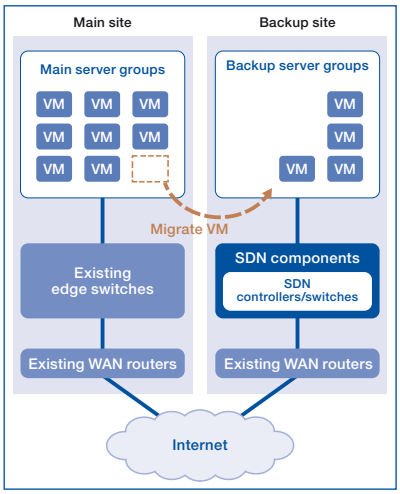
- Introduce SDN to the backup site LAN by using the edge replacement model.
- Verify SDN while gradually migrating the virtual servers in the main site to a backup site.

A backup site is built in the data center, and SDN is introduced by using the model in which the edge switches are replaced by the SDN components. SDN can be introduced and verified in the backup site during migration without affecting the data center operation in the main site.

■ *Benefits*

- Infrastructure construction lead time is reduced.
- Operational costs are reduced.

The lead time required to provide IT infrastructure, which is normally 1 to 2 months, can be reduced to several days. Outsourcing costs can be eliminated because configuration changes can be performed in-house.



Case 7
Expansion of new services in data centers

Introduction model :
[Edge]

Introduction scope :
[Intra-data center LAN]

Virtual server environments in data center business have become common and can be provided by almost any providers.
Data center providers can provide more competitive services by adding the advantages of network virtualization by SDN to virtual server environments.

■ *Issues*

- When providing hosting services, even though a virtual server environment can be prepared quickly, it still takes time to prepare the network.
- Mistakes in network configuration may affect other users, a verification test requires significant man-hours.

In a virtual hosting service, even though virtual servers can be provisioned quickly, it still takes time to construct the network. Moreover, prior infrastructure verification test requires significant man-hours to prevent affecting other users. The lead time for network construction and verification is too long to realize the full benefit of server virtualization.

■ *Solutions*

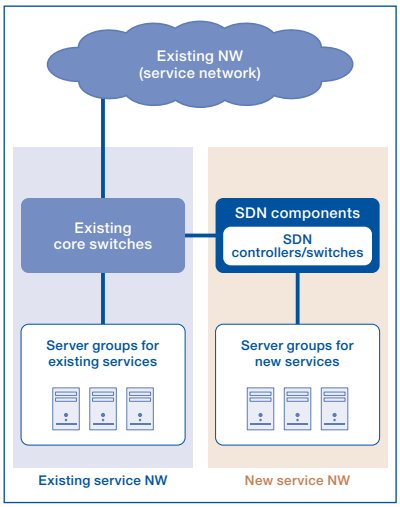
- Apply the edge replacement model to create a new service network and connect to the existing service network.

SDN components can be introduced to create a new service network at the edge of the network. The existing core switches remain in the existing service network and connects to the SDN components in the new service network. In this way, SDN advantages can be enjoyed without stopping the existing hosting service.

■ *Benefits*

- A network can be added without affecting other users.
- The lead time for providing the infrastructure is reduced.
- Operational cost reduction delivers highly competitive services.

VTN can construct isolated networks safely, and can eliminate the need to verify network interference. The virtual hosting service can provide infrastructure on the same day, because the manual labor required to construct and modify the network is significantly reduced. The reduced operation and management costs can be reflected in the service price, therefore IT services become more competitive both in terms of price and quality.



Case 8
Business continuity and disaster recovery between data centers

Introduction model :
[Edge]

Introduction scope :
[Intra-data center network]

By utilizing the SDN components, resource sharing and bi-directional backup between two data centers can be realized.
An efficient disaster recovery can be realized without large scale investment.

■ *Issues*

- Large scale investment is required to share ICT resources and enable bi-directional backup between two data centers.
- Significant manual configuration changes are required to add and move virtual servers.

Dedicated software and devices are required to share ICT resources and enable bi-directional backup between two data centers. If disaster recovery is also considered, a huge investment is required. Moreover, even for operations under normal conditions, significant man-hours are required to change configuration of routers and switches for creation and migration of virtual servers.

■ *Solutions*

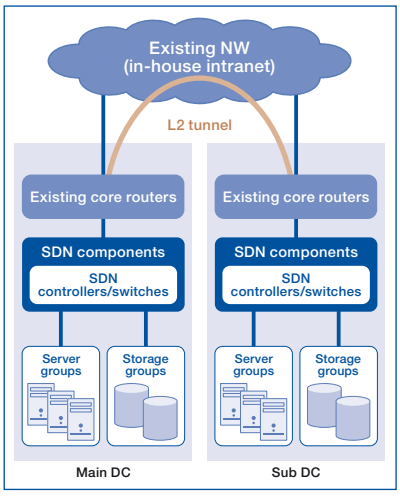
- Apply the edge replacement model in both the main and backup data centers.
- Form an Layer 2 (L2) tunnel in the in-house intra-network as a bridge between the data centers.

Instead of replacing all the data center network appliances at once, only the edge of network is replaced with SDN components. Virtual servers connect to SDN switches, and the existing core routers can be used continuously. Moreover, an L2 tunnel is formed in the in-house intra-network as a bridge between the data centers. Load balancing and disaster recovery can be realized by moving resources such as virtual servers between data centers. Users does not need to consider resource location because of a transparent operations provided by SDN.

■ *Benefits*

- A mutual backup disaster recovery environment is realized while suppressing facility investment.
- Shared resources can be used from anywhere.
- The number of manual network configuration changes is significantly reduced.

By exploiting the network visualization of VTN, the communication situation is displayed by the GUI to enable consolidated management of resources in each data center. Configuration and policy can be easily changed, thus significantly reducing the operation cost. When the data center resources are strained or undergoing maintenance, or if the data center is struck by a large-scale disaster, virtual servers can easily and quickly be provisioned at another data center. This method can be applied for load balancing between data centers, non-disruptive maintenance any time, and efficient disaster recovery systems.



Case 9
Aggregating network management for multiple departments

Introduction model :
[Edge/core]

Introduction scope :
[Office LAN]

If networks are constructed and expanded by each department, the operational and management costs of the overall corporate network will continue to increase.
Replacing existing core and edge switches with SDN components enables the logical design of a network connecting the servers, clients, and the network appliances of each department, significantly reducing the cost of adding to or modifying the network in the future.

■ *Issues*

- Grasping an overall image of the network is difficult because each department has constructed and expanded its own network as required.
- Adding a new network requires verification of connectivity between individual departments and complicated configurations, thus increasing the costs of network management.

Many corporations find themselves facing issues of not being able to grasp the overall structure of their network, as a result of continuously constructing and expanding the network for each department. Moreover, if the addition and modification of networks occurs frequently under such conditions, verification of the connectivity between individual departments and complicated configurations are required, thus increasing the costs of network management.

■ *Solutions*

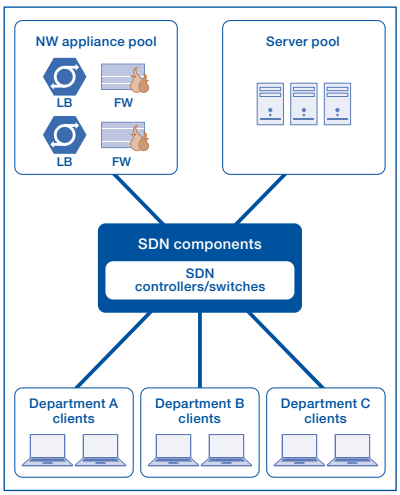
- Introduce SDN to both core and edge switches and integrate the networks that were individually managed by multiple departments.

By introducing SDN to the core and edge of networks, the networks individually managed by each department are integrated and aggregated under the SDN component. Appliances are grouped and physically allocated, forming pools of network appliances, servers, and clients for each department. Logical networks can then be configured freely later.

■ *Benefits*

- Operational costs are reduced.
- Security is improved.
- The number of appliances is reduced.

Operational costs are reduced, because the SDN components reduce the number of network appliances and the number of man-hours required for network configuration. Access to the appropriate network per device can be controlled after constructing virtual networks for each department. Both flexibility and security of network can be achieved by this model.



Case 10
Visualization of existing network traffic

Introduction model :
[Core]

Introduction scope :
[Office LAN]

By introducing SDN to the core part that connects the external network to the intra-data center LAN, traffic between external and internal network is visualized without touching the existing network, thus improving operability.

■ *Issues*

- When integrating data centers, changes in the existing network should be avoided.
- The network traffic of the entire system, including the existing system, needs to be visualized to improve the operation efficiency.

When integrating data centers, conventionally configurations in the existing network needed to be changed, causing the migration costs to increase. Moreover, to visualize the network traffic, it was necessary to introduce a dedicated device.

■ *Solutions*

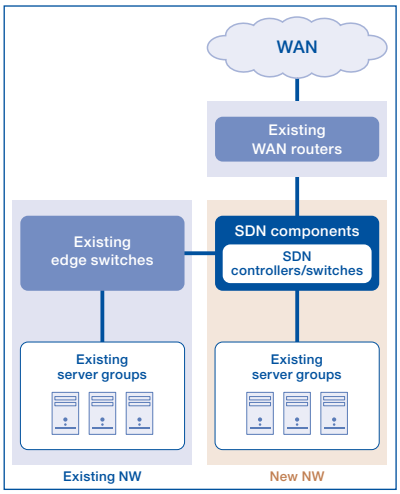
- Introduce SDN to the core part between the external network and intra-data center network.
- Maintain the existing network as is, enabling co-existence with SDN and visualization.

When data centers are integrated, a new network utilizing SDN is introduced by the core replacement model. The existing network can co-exist with the new network without any configuration changes. Moreover, traffic from the existing and new networks always passes through the core network constructed by SDN; therefore the traffic can be visualized without using a dedicated device.

■ *Benefits*

- Operability is improved.
- Scalability is improved.

Operability is improved because data center network integration and visualization of traffic are possible without changing the configuration of the existing network. Moreover, scalability is improved because servers and network appliances are easily added and changed in the new network.



Case 11
Integration of multiple service networks

Introduction model :
[Pass-through]

Introduction scope :
[Office LAN]

There are many cases in which multiple networks with different policies exist in-house. For example, there is one network for general operations and another broadband network used for data transfer. Even if network configuration changes are required as a result of office layout changes or site relocation, the costs of configuration changes can be reduced if SDN is applied. In addition, by utilizing the pass-through method, communication between two existing networks is possible via SDN without requiring special configurations.

■ *Issues*

- Addition and configuration changes of edge switches occur as a result of frequent office layout changes.
- Networks are constructed for each service, therefore wiring is required individually.
- A variety of networks of affiliate companies co-exist.

When there are numerous networks with different policies, such as information networks for the Internet, file servers and email, or business infrastructure networks for connecting dedicated appliances and communication networks to link with affiliate companies, the network administrator has to handle the individual wiring and as well as the heavy workload of changing switch configurations to respond to frequent office layout changes. This made it hard to connect ICT resources according to purpose, ensure bandwidth flexibly for business infrastructure networks, and assure security between affiliate companies.

■ *Solutions*

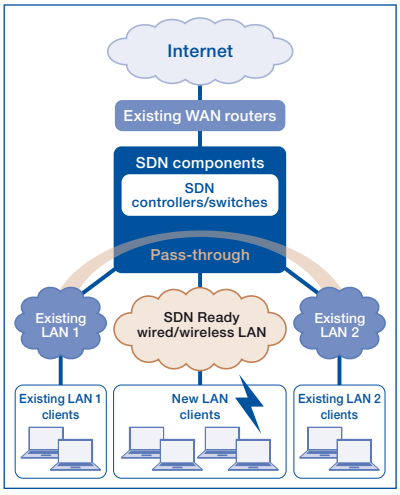
- Introduce SDN to the core network.
- Form a pass-through between the existing LANs to allow duplicated Virtual Local Area Networks (VLANs) remaining as is.

An SDN controller and switches on the core side enable the logical design of an L2/L3 network, while edge switches in existing LANs can be used without any changes. At the same time, by utilizing pass-through technology between existing LANs, the networks can be operated with duplicated VLANs remaining as is.

■ *Benefits*

- The flexibility and promptness of network creation and configuration changes are improved.
- Security in a multi-device environment is improved.

The freedom and speed of network construction and operation are improved, because the physical design and construction of a network can go ahead first, followed by the logical design. Moreover, multiple firewalls with different policies can be installed, and logical network design becomes independent from physical location through SDN. Network security in a multi-device environment can be assured by providing a multi-tenant-like service in the data center.



Case 12
SDN platform for IaaS

Introduction model :
[Edge overlay]

Introduction scope :
[Virtualization platform]

By virtualizing the physical servers and forming tunneling using an overlay gateway, a virtual network can be constructed promptly and flexibly, while keeping the existing network configuration as is. Moreover, the customer environment can be migrated to the data center easily without changing the IP addresses.

■ *Issues*

- A long lead time is required to construct and change infrastructure.
- The IP addresses must be changed when the user environment is migrated to the data center.

In conventional data centers, it takes several weeks to construct and change the infrastructure for physical installation and manual configuration. Moreover, when the user environment is migrated from on-premises to the data center, network configuration changes are conventionally required to avoid the duplication of IP addresses.

■ *Solutions*

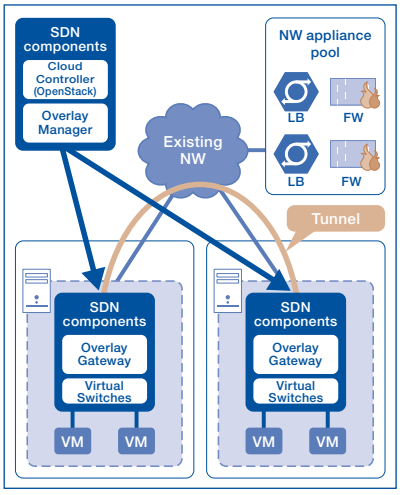
- Virtualize the physical servers and install a virtual switch.
- Construct a virtual network using an overlay gateway.

Each physical server on the edge of network is virtualized and a virtual switch is installed, and tunneling is formed using an overlay gateway to construct a prompt and flexible virtual network without changing the existing network. Tunneling technology can also handle duplicated IP addresses for different tenants.

■ *Benefits*

- The lead time required to provide the infrastructure is reduced.
- Migration to a data center is possible without changing the IP addresses.

The lead time required to provide the infrastructure can be reduced because the virtual network can be constructed both promptly and flexibly. Moreover, duplicated IP addresses can be handled safely, enabling the customer environment to be migrated to the data center easily.



NEC's SDN solutions

For detailed information, please refer to the following:

Domestic website : *http://jpn.nec.com/sdn/index.html*
International website : *http://www.nec.com/en/global/solutions/sdn/*

For inquiries, please contact the following:

NEC SDN Strategy

E-mail : inquiry@sdn.jp.nec.com

7-1 Shiba 5-chome, Minato-ku, Tokyo 108-8001 JAPAN

NEC