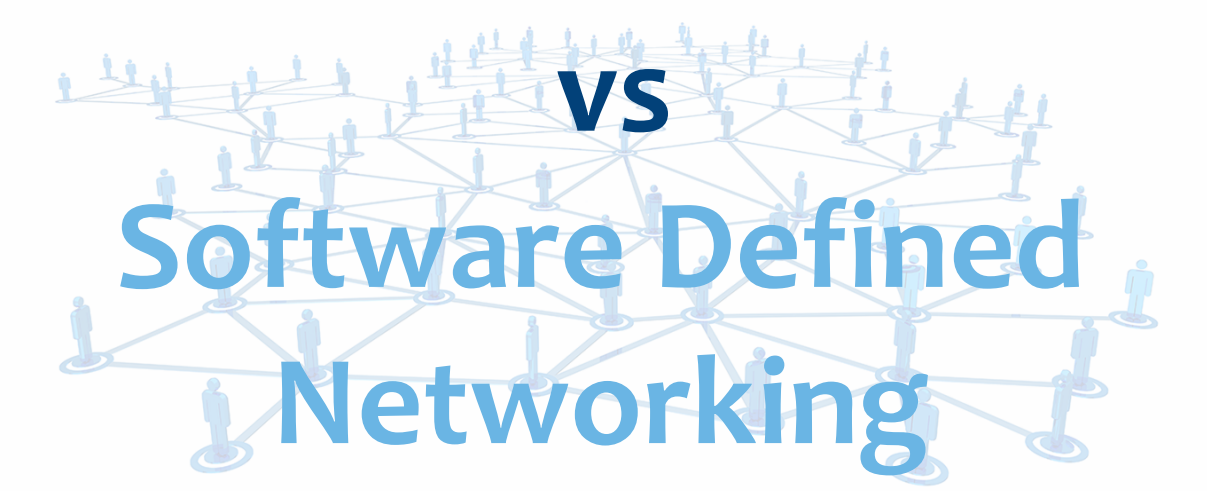
IPknowledge
We accelerate your business

Traditional



vs

Software Defined Networking

OCEDO

Why a new perspective on network management is inevitable

IT industry has enjoyed innovation such as virtualization in computing and storage. The end is nowhere in sight: technology will continue to evolve in years to come. On the contrary, networking has experienced limited innovation over the past 20 years. This stagnation has led to overly complex and inflexible networks no longer meeting current business requirements. In this white paper, we'll describe:

1) The basics of traditional networking technologies
2) Why there is need for a new perspective on network management
3) Software Defined Networking - the basics & expected benefits
4) What to look for in a SDN solution

Today, business and technical network requirements include enhancing performance and realizing broader connectivity. Companies have to meet more and more industry-specific security regulations and there is a growing demand for mobility. In order to comply with all of these criteria, networking protocols have evolved significantly over the last few decades. However, the way traditional networks are set up, deploying one protocol to realize these needs organization-wide is quite the challenge.

Traditional network configuration

The traditional approach to networking is characterized by two main factors:

1) Network functionality is mainly implemented in a dedicated appliance. In this case, 'dedicated appliance' refers to one or multiple switches, routers and/or application delivery controllers.
2) Most functionality within this appliance is implemented in dedicated hardware. An Application Specific Integrated Circuit (or: ASIC) is often used for this purpose.

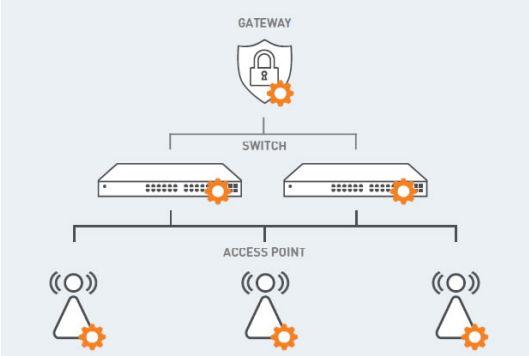


fig1 Traditional Networking

Organizations are increasingly confronted with the limitations that accompany this hardware-centric approach, such as:

- Traditional configuration is time-consuming and error-prone

  Many steps are needed when an IT administrator needs to add or remove a single device in a traditional network. First, he will have to manually configure multiple devices (switches, routers, firewalls) on a device-by-device basis (see figure 1).

  The next step is using device-level management tools to update numerous configuration settings, such as ACLs, VLANs and Quality of Service.

  This configuration approach makes it that much more complex for an administrator to deploy a

consistent set of policies. As a result, organizations are more likely to encounter security breaches, non-compliance with implications. Conclusion: the highly administrative 'hassle' that is traditional configuration interferes with meeting business networking standards.

- Multi-vendor environments require a high level of expertise

  The average organization owns a variety of equipment of different vendors. To successfully complete a configuration, an administrator will therefore need extensive knowledge of all present device types.

- Traditional architectures complicate network segmentation

  A development further complicating networking matters, is the connectivity evolution that is currently taking place. In addition to tablets, PCs and smartphones, other devices such as alarm systems and security cameras will soon be linked to the internet. The predicted explosion of smart devices is accompanied by a new challenge for organizations: how to incorporate all these devices of different vendors within their network in a safe and structured manner.
  Many traditional networks place all types of devices in the same 'zone'. In case of a compromised device, this design risks giving external parties access to the entire network. This can be hackers exploiting the internet connection of smart devices or vendors who can remotely log onto 'their' devices. In both cases, there is no apparent reason for giving them access to all network components. However, the 'administrative hassle' described earlier makes network segmentation a complex process and quickly leads to network clutter.

  In conclusion, to overcome these and other traditional networking limitations, the time has come to introduce a new perspective on network management.

Embracing change: Software Defined Networking

Networking Software Defined Networking (SDN) is rapidly becoming the new buzzword in the networking business. Expectations are that this emerging technology will play an important role in overcoming the limitations associated with traditional networking. But what exactly is SDN?

Even though a universally agreed upon definition for SDN has not yet been formulated, 'decoupling hardware from software' is often mentioned when this topic comes up. This concerns the two network device planes, i.e.:

1) The plane that determines where to send traffic (control plane)
2) The plane that executes these decisions and forwards traffic (data plane)

Decoupling these two planes involves leaving the data plane with network hardware and moving the control plane into a software layer. By abstracting the network from the hardware, policies no longer have to be executed on the hardware itself. Instead, the use of a centralized software application functioning as the control plane makes network virtualization possible. This process is similar to server virtualization:

- Server virtualization

  The process of creating various VMs (virtual machines) and decoupling them from physical servers.

- Network virtualization

  The process of creating virtual networks which are decoupled from physical network components.

SDN Business Benefits

Software Defined Networking is expected to have several business benefits, including:

- More configuration accuracy, consistency and flexibility

  As described earlier, traditional networking requires configurations to be executed on a manual, deviceby- device basis. A key characteristic of the SDN approach, is automating this process, enabling an administrator to manage the entire network as if it were a single device (see figure 2). In addition to increasing configuration accuracy and consistency, this method also boosts a networks' responsiveness. In case network conditions change, an administrator can adjust existing configurations much quicker.

- Data flow optimization

  A second expected business benefit of the SDN approach, is the optimization of data flows. Instead of having a single path from the source of communication flow to its destination, a SDN controller is able to identify multiple paths per flow. Furthermore, this approach allows the flow's traffic to be split across multiple nodes. Network performance and scalability is enhanced by optimizing the network path for a particular data flow based on the source and destination nodes[1].

What to look for in a SDN solution

Given that SDN solutions are a relatively new product category, it can be difficult to find indicators to evaluate whether the solution fits your organizational needs.
Therefore, we have formulated four focus points that should be taken into account when choosing a suitable SDN solution.
In addition, we described how SDN solution Ocedo handles these points. Ocedo is an up-and-coming Secure Automated Networking solution that offers the advantages of SDN.

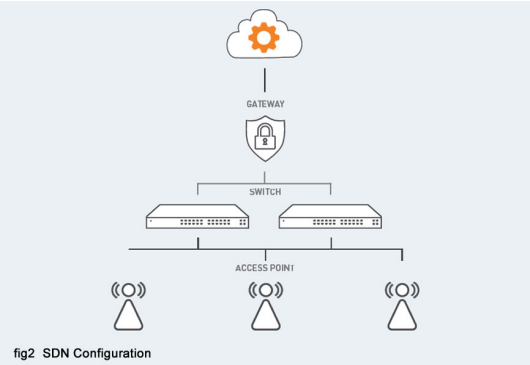


fig2 SDN Configuration

1. Integration

   A SDN solution should be able to 'play nicely' with your current network, meaning it should integrate seamlessly into existing setups. Ocedo accomplishes enterprise integration by offering the following functionalities: Hardware Instead of coercing third-party hardware into playing with the controller, Ocedo offers their own gateways, switches, and access points. These integrate seamlessly into existing setups, no matter if you want to only deploy a couple of Wi-Fi access points or use the complete solution. Directory Services The Ocedo System allows syncing Users and selected User Groups from Active Directory and Google Apps directory services. User credentials are not queried by or stored in the Ocedo Controller. In case of an on-premise Active Directory installation, the connection to the

domain controller can be securely made through any deployed Ocedo appliance, without the need for firewall rules or exposing the AD to the internet.

2. Visibility & reporting

   Despite of the many advantages SDN has to offer, the success of this technology is inextricably linked to the degree of network visibility. Before, it was only possible to get insight in individual components or 'stand-alone' logging information. A suitable SDN solution should correlate data and combine previous individual reporting in a logical manner, giving an administrator a clear overview of all network activity.
   Ocedo tracks and reports network activity across the whole enterprise network. Features include:

   Device visibility
   Ocedo keeps track of all known devices on your network, the users or groups associated with them, their most recent location, as well as the quality of their Wifi experience. Unknown detected devices are shown with available OS, vendor and owner information, if available. The Ocedo System keeps track of IP addresses used by devices. Current device location and connection information is also shown. Device traffic activity can be tracked in Traffic reporting.

   Events & alerts
   Next to device visibility, the Ocedo System offers continuous automatic monitoring and alerting/ notification on network events. The event log offers live updates on changes in the network status, as well as an ongoing audit trail for configuration changes.

   Traffic reporting
   Traffic reporting enables a full view on all generated internal and external traffic, filtered by user, site and date/time. Reporting uses the same Application Groups, Applications and web categories as the policy engine, so the reported results can directly be converted to policy rules if needed.

Security

What a SDN solution has to offer in terms of security measures should not be overlooked. For instance, does the solution provide high quality filters? Can an administrator easily isolate one network component from another? What type of authentication functionalities does the solution offer?

The Ocedo system contains several security measures, including:

Network Zoning
Administrators can easily create different zones for different device or user groups. These isolated zones provide extra layers of protection to the entire network. If a device gets hacked, an intruder does not get immediate access to the complete network. Instead, the "leak" is confined to one zone.

It is possible to assign accessing clients to different network zones. This can either be done with AD through the RADIUS/NPS server, or by setting tags on Zones and User Groups or Users.

SSID & authentication (Wifi)
The Ocedo System supports defining WPA SSIDs with password as well as enterprise authentication against RADIUS /NPS servers.

Live Threat Protection
Connectivity to hundreds of botnets or otherwise infested servers known to be in the w i l d i s blocked by the network.

Port Security
Only known and allowed devices get network access. Authentication through MAC learning or 802.1x. On-premise hosting In some cases, security policies include specific hosting requirements. Ocedo's cloud console is hosted in Ocedo's own data center, but can also be hosted on partner or customer premises.

Reliable connectivity

Finally, it is important to evaluate what measures a SDN solution offers to assure a reliable connection at all times. This can be examined by formulating different connectivity scenario's. For instance, many SDN controllers are cloud-based. Therefore, it's important to choose a solution with a data plane that is always fully operational, even when the cloud connection is temporarily down. Another aspect worth evaluating is the way internal and external traffic is distributed.

In terms of connectivity, the Ocedo concept contains several functionalities, including:

Offline measures
Executed configurations always remain active, since they run locally. So even if the cloud connection encounters some down-time, the Ocedo system does not. Also, all reporting is stored until the cloud controller is up and running again.

Uplink Balancing
Internet and WAN traffic is intelligently balanced across multiple providers, increasing bandwidth and reliability.

Traffic Priorization
State of the art Quality of Service (QoS) algorithms prioritize network users and applications, e.g. video conferencing.

Conclusion

SDN is an emerging technology that is likely to revolutionize traditional networking business. By embracing network automation, organizations will save a tremendous amount of time and significantly improve a network's flexibility. How do you prepare for this transition? Extensively evaluating which solution meets your business needs best in terms of integration, visibility & reporting, security and reliability is an important first step. Taking enough time to do this thoroughly will be an investment worthwile to prepare for this inevitable networking transition.