LANCOM™ White Paper
Network virtualization

Introduction

Virtualization is a hot topic on the IT market right now. Along with widespread solutions such as server virtualization, this approach is of increasing interest in other areas of information technology as well. The reasons for this trend are obvious: Experts expect efficiency gains in the exploitation of company resources, better flexibility and security, as well as reductions in investment costs and management overhead. This white paper outlines the technology and potential applications for network virtualization, and the components which are required to achieve this.

Objectives of virtualization

In information technology, the term "virtualization" generally refers to the separation of an IT application from the underlying hardware. This separation aims to meet various objectives, including:

- Optimal exploitation of company resources
- Security
- Cost reductions

Server virtualization is already widespread. This involves relocating the server application (e.g. a file server), including its operating system, onto a virtual machine. Multiple virtual server processes, each with different operating systems, can be implemented in parallel on a single physical machine, which serves to optimize the exploitation of the company's resources. If a problem arises with the hardware, the virtual server processes are simply transferred to backup hardware and operations can continue without interruption. This enables servers to be managed centrally on standardized hardware, which significantly reduces operating costs and maximizes the availability of the processes.

The objectives of client-side virtualization are similar. Hardware at the workplace is reduced to the input/output equipment, i.e. monitor, keyboard and mouse. Each workstation works with its own instance of the operating system running on the server. Users each have their own personal configuration. Along with easier administration and simplified data-backup options, the lack of local storage media increases data security.

Network virtualization

Virtualization is an option not only for servers and workstations, but also for the network itself (LAN and WLAN). Whereas client and server virtualization primarily offer centralized management and cost savings, virtual networks offer completely new applications which "normal" networks are incapable of. Methods of network virtualization used until now relate to the path used for transmission:

- VPN uses a WAN connection as if it were a LAN connection.
- VLAN allows multiple secured network connections to operate on a single shared transmission medium.
- Access points which have a single wireless LAN module can operate multiple radio cells (SSIDs). This allows different encryption settings to be operated in parallel (Multi-SSID).

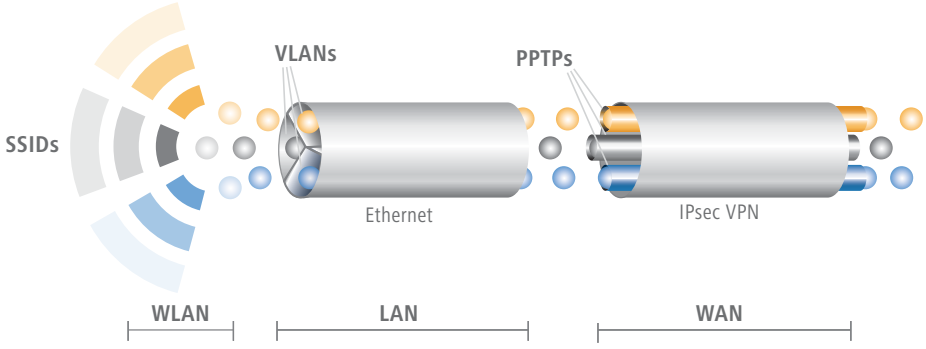
These three techniques allow completely separate networks to be operated in parallel over the different transmission paths (IPsec VPN for WAN, VLAN for Ethernet cabling, Multi-SSID for WLAN). However, the services available with these techniques are limited, as they are generally restricted to just one transmission path. Economical and effective end-to-end virtualization requires these techniques to be logically linked. A further factor is that VPN and VLAN are generally used to extend internal network structures. In

LANCOM™ White Paper
Network virtualization

contrast to this, there is an increasing need to interconnect completely different external users: IP-based collaboration is increasingly orientated towards the tasks carried out by the employees, meaning that it is no longer limited to the barriers of the organization itself. In the simplest case, guests on the company premises require network access. In complex scenarios, external service providers can use the Internet to access certain services in the local network. Consequently, the next stage is to implement a complete logical virtualization of the entire network, irrespective of any particular access nodes: To achieve this, the different transmission paths and the virtualization technologies they use also have to be inter-linked by virtual routing between them. Comparable to server virtualization, a hardware router supports multiple virtual routers. Each virtual router is configured for its own network. These higher levels of virtualization allow existing infrastructure to support different applications in parallel, each with dedicated router settings and access rights.

Multi-VPN: Tunnel-in-tunnel

IPsec has become the established industry standard for high-security connections via the WAN. Professional routers with a VPN gateway offer various options for secure authentication and encrypted data transmission. Using certificates as a basis for authentication effectively prevents any third-party device from establishing a connection to the central VPN gateway by deception. Even if transmitted data is intercepted, AES encryption makes it completely illegible. This makes IPsec VPN the ideal method for virutalizing an Internet-based transmission path between two sites. IPsec has the disadvantage that transmission on the TCP/IP level (layer 3 in the OSI reference model) is restricted to one defined network, i.e. it cannot operate between two separate networks with overlapping IP address ranges. Network virtualization requires flexibility in meeting the specific requirements of different networks. To achieve true end-to-end network virtualization, the IPsec tunnel must be able to encapsulate further inter-gateway tunnels which are independent of the IP address ranges of the networks being connected. The PPTP protocol is a technology which has long been used for various types of dial-up Internet connection. Similar to VLAN in the LAN, a PPTP tunnel is established for each virtual network. Working through the IPsec tunnel, the PPTP tunnel connects the corresponding VLANs at the various locations to form a consistent network. This innovative tunnel concept enables the secure transportation between sites even of protocols for the dynamic control of IP routing within a virtual network, such as RIP. A further



LANCOM Systems

LANCOM™ White Paper
Network virtualization

advantage of this concept, as opposed to separate tunnels with authentication and encryption for each network, is that authentication and encryption is only required for the enveloping IPsec tunnel. Even though the levels of security are identical to scenarios with separate IPsec tunnels, the computing-intensive authentication and rekeying processes (cyclic changes of the encryption key) can be dispensed with. The result is transparency and routing equivalent to that of MPLS VPN, but with higher security and with the advantage that the VPN is under the control of the company operating it, and not the Internet provider. There is no longer any reason not to base the backup connections for a site on a variety of different communications technologies such as ADSL, SHDSL, fiber-optic cable, or UMTS. Independence from any one provider allows network virtualization to be internationalized and based on different types of network access.

Advanced Routing and Forwarding (ARF)

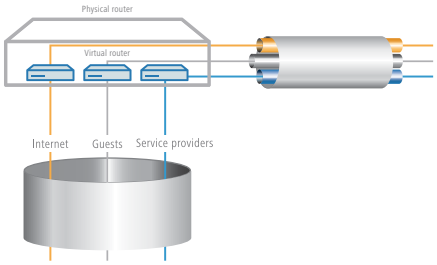
How can existing physical networks be used to meet the latest requirements in modern communications and collaboration? Modern network virtualization goes beyond the static configuration of VPNs and VLANs and relies on advanced functions such as ARF (Advanced Routing and Forwarding). The essence of this technology is the option to set up a central physical router with separate IP networks dedicated to different applications (e.g. one network for the employees with their workstation PCs or notebooks, one for WAN guest accounts, one for an external service provider who services the alarm system). Basic services for each of these networks can be configured separately (e.g. DHCP server services). Data packets arriving at the physical router are assigned to one of the networks according to different, predefined or even automatically learned criteria. Exactly how these data packets are routed, and where they are routed to, is decided by rules which are valid for the virtual network. Overall these networks behave like a collection of independent virtual routers, each with its own definitions, properties, services and criteria for data-packet assignment. The criteria and properties for this type of virtual network may be:

- Access via a specified network port on a switch, if necessary with authorization, and inclusion into the VLAN for employees in the LAN. The VLAN directs packets intended for the employees into the relevant network. Consequently, users have access to all of the applications and resources which are available to employees.
- Access from a mobile PC by means of VPN client, including authentication and encryption. By means of the VPN, the user is assigned to the network for employees, including its resources and applications.
- Access via WLAN with the SSID for employees. This SSID operates with authentication and high-security encryption. After logging in, the user is in the network for employees.
- Access via WLAN with the SSID for guests. Here, no authentication and only a lower standard of

LANCOM™ White Paper
Network virtualization

encryption is required. The user accesses the guest network by entering the SSID and is granted access to the Internet and a selection of printers only. Strictly speaking, the other resources are not blocked; however, on an IP level, the other networks, services and resources simply do not exist.

- Service-provider access via VPN with authentication and encrypted data transmission. Based on the VPN being used, the user is assigned to the network for service providers. Only the devices in this network can be accessed, i.e. those belonging to the alarm system. No other resources exist in this network.



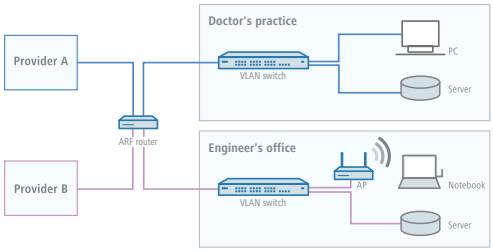
Hardware requirements

To achieve this type of virtualization, the routers must be capable of supporting Advanced Routing and Forwarding, i.e. of managing and providing services to multiple, completely independent IP networks in parallel. In addition, the routers must support the assignment of IP networks to interfaces, VLANs, SSIDs, remote peers, WAN connections, and also the detection of packet properties by the firewall. In order for the virtual networks to be extended across structured cabling and into the wireless LAN, all of the switches and access points must also support VLANs.

Example: Joint offices doctors' practices

Virtual network structures offer significant advantages to smaller companies. Doctor's practices, accounting firms, or engineering consultants need to be networked with their business partners. Many office buildings simply do not have the amount of cabling required to offer a dedicated network to every tenant.

In cases like this, a separate IP network can be set up for the doctors' practice and for the engineering consultant company. Both networks are completely separate, making it impossible to gain unauthorized access to patient's files or construction plans. The engineering company can additionally set up WLAN access for its guests who require access to the Internet only.



Example: Networked chain stores

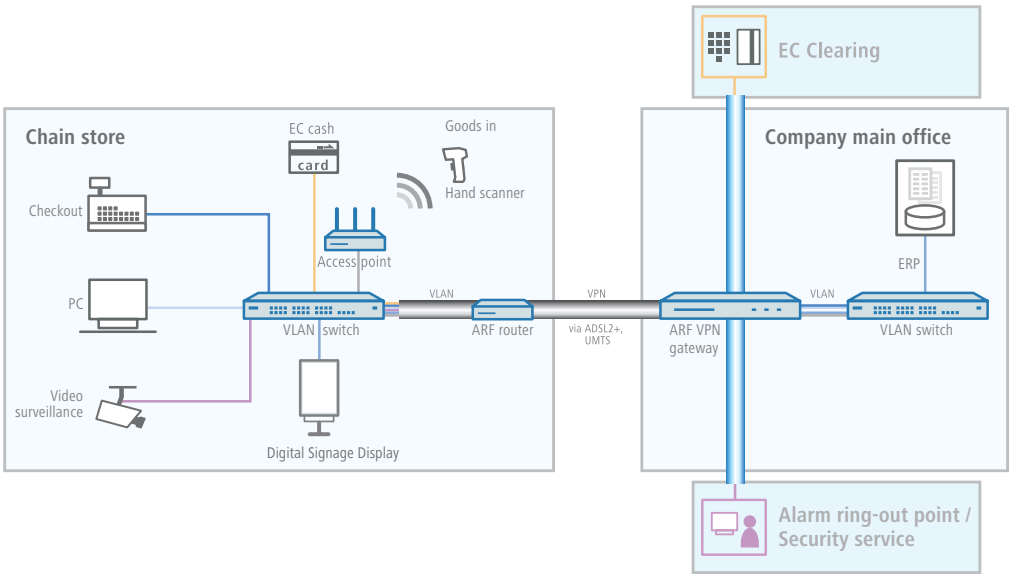
The first example deals primarily with the separation of internal data streams. However, a major advantage of virtual network structures is the integration of external users into internal networks. The example of a completely network chain store (e.g. a supermarket) demonstrates the potential of ARF in combination with VLAN. Along with the store manager's PCs which are connected to the main office via VPN (shown here in blue), the bar-code scanners (networked via an access point) used for inventorizing incoming goods can con-

LANCOM™ White Paper
Network virtualization

tinuously exchange data with the ERP system. Apart from that, various external service providers are integrated into the network: A large bakery controls its automated ovens and continuously queries the status information (light blue), the security company can monitor video from the surveillance cameras around the clock in the store (purple), and the electronic cash tills are directly connected to the clearing house (yellow). Each application has its own virtual IP network with a specific IP address range and its own routing settings. The network segment for cash-till accounting can be adapted to the IP addresses used by the VPN structure at the clearing house. In the internal LAN, the IP networks are additionally marked by corresponding VLANs which are separated by a VLAN-compatible switch. Other users cannot access this network. By working with network components which support TACACS+ for authentication, authorization and accounting, important requirements of the PCI (Payment Card Industry) can also be fulfilled.

Summary

Tried-and-trusted virtualization technologies such as VPN, VLAN and Multi-SSID greatly improve the exploitation of existing physical data-transmission media (Internet connection, network cabling, WLAN) in networks. Advanced Routing and Forwarding enables the technologies for the virtualization of different transmission paths to be interlinked, and it also virtualizes router functions. This enables the parallel operation of multiple secure, separate IP networks which can operate across geographical network limits. Network virtualization which is based on ARF-based routers, VLAN-capable switches, and access points with Multi-SSID opens up a range of completely new applications based on a single, shared infrastructure – as well as greatly reducing costs.



LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Wuerselen I Germany I E-Mail info@lancom.de

LANCOM Systems