A Systematic Quality Analysis of Virtual Desktop Infrastructure Technologies

Arman Sheikholeslami[1] and Kalman Graffi[2]

[1] University of Paderborn, armanpts@gmail.com
[2] Technology of Social Networks Lab, University of Düsseldorf, graffi@hhu.de

Abstract. The Virtual Desktop Infrastructure is a promising technology hosted by powerful servers or within the cloud that allows remote and potentially weak devices to run their virtualized desktop environment on a powerful machine. Mainly used in commercial environments, i.e. enterprises, also private users might be interested in this functionality. The benefits are given through customizable (virtual) hardware resources on the fly while maintaining a long lasting desktop environment. Hardware failures, resource limitations and risks due to damages to the physical hardware are omitted with desktops running upon a Virtual Desktop Infrastructure. Currently, many Virtual Desktop Infrastructure solutions are available, most important of which are XenDesktop by Citrix, Horizon View by VMware, and VDI by Microsoft. In this article, we deploy and systematically evaluate the quality of these solutions in terms of streaming quality under the workload of popular application types and under the influence of various network conditions. We conclude that XenDesktop by Citrix is performing best, Horizon View by VMware is close, but provides less features, while VDI by Microsoft is both limited in its quality and its functionality.

1 Introduction

Nowadays, with huge quantity of computers in the world, the administration of computers has become cost- and effort-intensive. This is due to the constant attention that computers require. Maintaining the computer hardware is both an expensive and work-intensive task. Most consumer computers are only used a few to several hours a day, but not day and night, the utilization of these devices is even not ideal. To reduce the operating costs and efforts of computers, an efficient use of computers is proposed.

In the traditional approach, software (operating system, applications, etc.) is placed on top of a dedicated hardware infrastructure, which eventually are not fully utilized, meaning that their resources, to some extents, remain idle. Hence, the costs of ownership also must cover the resources of the computers that are not actually used most of the time. A good example is a user who only performs low-level computer tasks (online shopping, music streaming, etc.) on a high-tech laptop. While the computer is used a few hours a day, after 2-3 years, the computer might be outdated and not anymore suitable for high-end calculations. A new computer is bought. Both, from a private user's view as well as from an enterprise user's view, this is not an ideal hardware utilization.

Ideally, the computing resources made available to a desktop environment and applications in it should always meet the desired quality, even after years. For that we differentiate between the operating system and connected applications, a input/output device (such as a notebook or monitor/keyboard) as well as the computing unit with sufficient computational power, memory and storage. Basically, the concept of efficient use of computers proposes that the underlying hardware infrastructure can be separated from the input/output device and shared among multiple computer users and applications (including the operating system) such that the hardware resources can be fully exploited. In this way, users only pay for the extent of the resources that they consume. On the other hand, deploying multiple computers on one hardware infrastructure (i.e. pooling) reduces operating costs and administrative tasks. This is in particular very useful for organizations with numerous standalone computers as Converged Infrastructure [1]. This way, an administrator gets a holistic view on the status of one single hardware infrastructure and the applications deployed on it through an administration platform instead of having to deal with all standalone computers separately. This new concept of pooling hardware resources among multiple applications is known as Virtual Desktop Infrastructure (VDI) technology.

This is a technology in which a user's operating system as well as data and applications are stored in a data-center which is a shared hardware infrastructure, as displayed in Figure 1. Then, a user can remotely connect to the data-center and access his/her operating system, applications and data as if they are on his/her own local machine. These remotely hosted virtual desktops can be both used by individual users but also in order to enable collaborative desktop sharing, with team members accessing the same desktop, and coordinating their work within this desktop environment. Virtual desktops enable teams to easily coordinate the knowledge available for them, by using one common desktop. Cloud-hosted VDIs introduces several advantages, the most important are on demand resource provision and enhancement [4], reduction of costs [3], device and location independence [4], virtualization, central maintenance and management, boost of cooperation and collaboration, and reliability and security [5] [6]. An open question is with regard to the quality of the available VDI solutions.

Our contributions in this paper are the following. In Section 2, we introduce the three most popular VDI technologies namely: XenDesktop by Citrix, Horizon View by VMware, and VDI by Microsoft. In Section 3, we present our implementation of virtual desktops on top of each these three VDI technologies in a local network environment. We benchmarked these three VDI solutions in Section 4 using the workload of the seven dominant desktop applications identified in [2] and varying challenging network characteristics. Through the dynamics of the network conditions and the different usage patterns we are able to exactly identify the suitability of the three solutions for the use case of virtual desktops. In Section 5, we summarize the test results of each solution and we point out that both the benchmarks as well as the user test identify the XenDesktop by Citrix as best choice with Horizon View by VMware being almost on par. Microsoft's VDI on the other side falls back both in the streaming performance under any network condition but also in terms of user experience. In the following, we in-

troduce first in the VDI as option to host virtual desktops. Besides a general overview on the requirements for such a technology, we also introduce the three most popular VDI technologies namely XenDesktop by Citrix, Horizon View by VMware, and VDI by Microsoft.

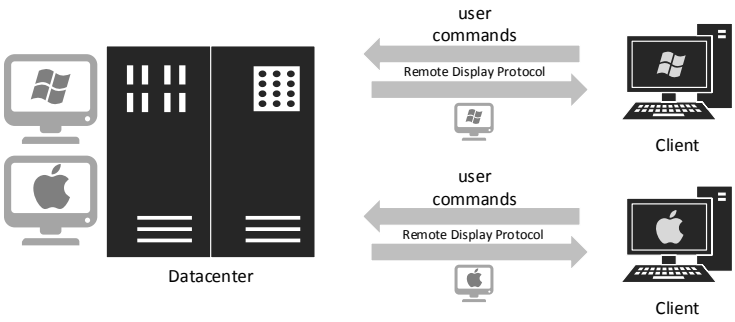


Fig. 1. Functioning mechanism of Virtual Desktop Infrastructure

2 Considered Virtual Desktop Infrastructures

VDI is can be run by server pools, such as in Cloud environments and also on dedicated powerful servers. See Figure 1 for this. Such an environment benefits companies as an existing infrastructure is shared and paid accordingly [3], allowing organizations to avoid huge upfront infrastructure costs. A virtual desktop is a technology that has a lot in common with VDI technology. The main differences are the type of users, user tasks and the network type over which they operate. Thus, a quality analysis of the current VDI technological solutions can provide useful insights about the current technological situation that can be used to implement the concept of VPC. Next, we introduce the three dominant VDI solutions: Citrix XenDesktop, VMware Horizon View and Microsoft VDI.

2.1 Citrix XenDesktop

Citrix, founded in 1989, is a Microsoft alliance that provides different virtualization products and services. The most famous product of Citrix is the Xen family, which consists of open-source products, mainly consisting of XenDesktop, XenServer, and XenApp. XenDesktop is a VDI by Citrix which is designed specifically for commercial environments (i.e. organizations), and delivers Windows-based Desktop and Server operating systems.

Figure 2 shows standard architecture of Citrix XenDesktop, virtual desktops are installed on virtual machines in form of desktop or server operating systems. An operating system must have a Virtual Delivery Agent installed on it, and it may contain many applications. All virtual machines are hosted by a native Hypervisor, which can be of different types as mentioned before. To access a virtual desktop, a user connects to the StoreFront Server using a Citrix Receiver or a web browser. The StoreFront Server redirects the inbound connections to the Delivery Controller Server and after authentication, assigns a virtual desktop to it. The authentication is performed based on the knowledge base of Active Directory Server. Ultimately, all operations are recorded in the Database Server.

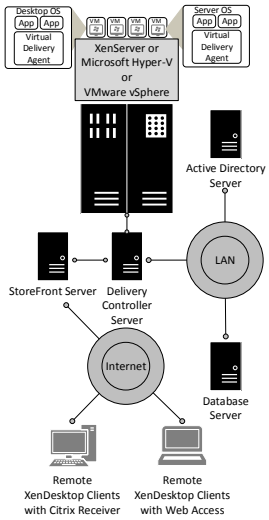


Fig. 2. Citrix Xen Desktop

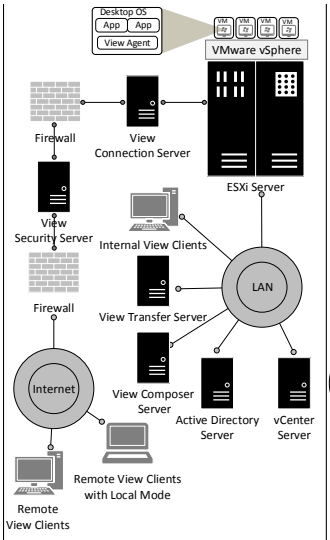


Fig. 3. VMware Horizon View

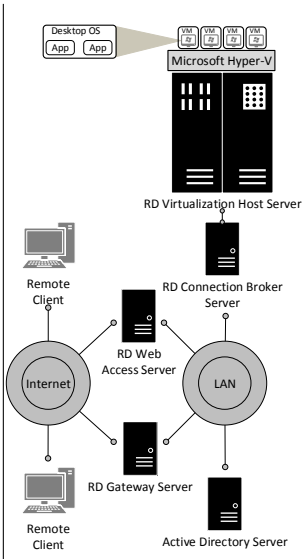


Fig. 4. Microsoft VDI

2.2 VMware Horizon View

Horizon View is a VDI solution for Windows-based desktop and application virtualization in organizations. With Horizon View, VMware claims to extend the power of data centers to devices. All virtual desktops and applications can be accessible through one single platform, making it easy for users to access the resources they need. Using automated desktop setup and provisioning, considerably less administrative effort is required for initial deployment of desktops. Additionally, the management console gives a view of the VDI mechanics and fascilitates to trace and fix the problems [7]. Horizon View is constructed upon several components that work together to deliver virtual desktops. Among all, in Figure 3, we display the most important components based on [8].

One of the most crucial components of the architecture is vSphere Server (i.e. the ESXi Server). The vSphere should be deployed on a dedicated server to store virtual desktops. More concretely, vSphere creates an individual virtual machine for each remote desktop. Then, on top of each virtual machine, the virtual desktop (guest operating system) is installed. The virtual desktop, then, can contain data and applications, like a regular desktop. Furthermore, to control the status of virtual desktops and manage resources, View Agent should be deployed on each virtual desktop. However, since the View Agent should exist in the parent image of the virtual desktop, and that virtual desktops are copies of the parent image, the View Agent will automatically be replicated among the virtual desktops. The Composer Server and vCenter Server can co-exist on one dedicated server. Furthermore, the Active Directory server can be deployed on a virtual machine. This server does not only provide Active Directory services, but also DNS and DHCP services. The other components like Connection Server, Transfer Server and Security Server should be assigned to dedicated servers each.

Figure 3 displays the architecture of a fully configured VMware Horizon View. In this architecture, clients can use virtual desktops on the premise, using LAN or through the Internet. Based on the requirements of the organizations, a variety of network architectures can be considered for implementation of Horizon View VDI. Here, we consider the most basic architecture in which one single LAN connects different servers to each other. On the premise clients can use the same LAN to access their virtual desktops. First, they access the Connection Server and then the Connection Server connects them to their virtual desktops. The same holds for clients reaching virtual desktops through the Internet, but with an additional level of security. First, they need to pass through two firewalls with the Security Server in the middle. Then, the Connection Server connects the clients to their virtual desktops.

2.3 Microsoft Virtual Desktop Infrastructure

Remote Desktop Services (RDS) is a feature of Microsoft Windows Server, which allows to access a computer remotely. In 2012, when Windows Server 2012 R2 was published, this service was extended to include Microsoft VDI. Microsoft VDI is a desktop virtualization technology, which virtualizes an operating system and allows users to remotely take control of it. Obviously, Microsoft VDI only supports provisioning of Windows-based operating systems and applications.

Microsoft VDI is comprised of many components depicted in Figure 4, each having a responsibility in the chain of service delivery. However, some components are optional and, depending on the specification of the VDI service, may not be deployed. For example, if web access to virtual desktops is not required, Remote Desktop Web Access component will not be deployed.

Figure 4 shows an abstract architecture of Microsoft VDI. In this architecture, users accessing through a Web Browser are directed to the RD Web Access Server and users accessing through RemoteApp are forwarded to RD Gateway Server. These two servers authenticate the users using the credential storage of Active Directory Server and, then, redirect the inbound connections to the RD Connection Broker Server. RD Connection Broker Server, then, finds the appropriate virtual desktop on the RD Virtualization Host Server. Finally, the RD Virtualization Host Server prepares the corresponding virtual machine as well as virtual desktop to be used. As soon as the virtual desktop is prepared, the access to virtual desktop is given to the connection, hence, the user can utilize it. The RD Virtualization Host Server is a service provided by Windows Server 2012 R2. As mentioned before, the RD Virtualization Host is integrated with Hyper-V, which is a virtualization service of the same operating system. As shown in Figure 4, the Hyper-V on the RD Virtualization Host Server hosts virtual machines. On each virtual machine, a (guest) operating system is deployed, which is the virtual desktop that users connect to.

3 Technology Implementation and Evaluation Setup

In this section, we briefly discuss our VDI architecture deployment of these three technologies. First, we abstractly describe the deployment environment. To im-

plement the three VDI technologies, based on our demand, four desktop computers were used, with following specifications: CPU - Intel Core i7-2600@3.40 Ghz, 8GB memory, 460 GB disk space, NIC - Intel 82579LM Gigabit Ethernet Adapter. The machines are termed VDI-1, VDI-2, VDI-3 and VDI-4. Some optional components (e.g. Security Server) that have no effect on the quality of the final service delivery were not implemented. Best efforts are made to prevent these limitations to degrade the quality of service. In VDI technologies, usually a machine plays the role of a connection broker, which middles the connections oriented from LAN or the Internet requesting a virtual desktop service. For this means, one of the machines (in our case VDI-1) should have two Network Interface Cards (NICs); a LAN NIC with private IP address to connect VDI-1 to the internal LAN in which other servers reside; and an Internet NIC with a public IP address to connect to the Internet. We interconnected the four machines in a dedicated small local area network and tuned the network quality with a tool named "Clumsy". In the following, we describe, how we used these four machines to implement the VDI reference architecture of the corresponding solutions, which are presented in Figure 2, Figure 3 and Figure 4.

Citrix XenDesktop In this technology, VDI-1, which acts as the a connection broker, has two NICs since it is connected to the Internet as well as to the LAN. The four servers are used as follows: VDI-1: StoreFront Server Server, DNS Server, NAT Server. VDI-2: Delivery Controller Server, XenCenter, Database Server. VDI-3: Active Directory Server, DHCP Server, DNS Server. VDI-4: XenServer Server. To access a virtual desktop, a user connects to the StoreFront Server using a Citrix Receiver or a web browser. The StoreFront Server redirects the inbound connections to the Delivery Controller Server and after authentication, assigns a virtual desktop to it. The authentication is performed based on the knowledge base of Active Directory Server. Ultimately, all operations are recorded in the Database Server.

VMware Horizon View For VMware Horizon View, each of VDI-1 to VDI-4 provides a specific service, as follows: VDI-1: View Connection Server, DNS Server, NAT Server. VDI-2: vCenter Server, View Composer, SQL Server. VDI-3: Active Directory Server, DNS Server. VDI-4: ESXi Server. Depending on the type of servers, in some cases, one machine can host one or several servers. For instance, VDI-4 is only dedicated to ESXi Server since ESXi Server stores all virtual desktops and it requires high Disk, Memory and CPU capacity. On the other hand, VDI-2 can host vCenter Server, Composer Server, and MS SQL Server at the same time since its hardware capacity allows it and that these three servers can share the same host machine with no conflict of functionality.

Microsoft VDI We only focus on the deployment of the essential virtual desktop services and exclude the components providing non-functional services (e.g. Security Server). The hardware infrastructure used to deploy Microsoft VDI technology includes VDI-1, VDI-2, and VDI-3. The only exception is that the VDI-1, which acts as the RD Connection Broker, has two NICs since it is connected to the Internet as well as to the LAN. The role of each machine is shown

in the following: VDI-1: RD Connection Broker Server, RD Web Access Server, RD Gateway Server, DNS Server, NAP Server, NAT Server. Obviously, this is not the best approach for large scale projects, for benchmarking with a limited number of virtual desktops, it does not lead to quality degradation. VDI-2: Active Directory Server, DNS Server, DHCP Server. VDI-3: RD Virtualization Host Server, Hyper-V Server, IIS Server. In our deployment, regardless of using a web browser or Remote Desktop application, a user living on the LAN or on the Internet first is connected to the VDI-1. Then, after the user is authenticated and is assigned to the right virtual desktop by VDI-1, the user connection is redirected to VDI-3 where the virtual desktops are stored. When learning about the desktop request, VDI-3 prepares the virtual desktop for service provisioning. In the following we comparatively benchmark these setups with respect to the quality of service of the desktop streaming.

4 Benchmarking of the VDI Solutions

In this section, we measure the quality of the implemented technologies. We perform a comparative measurement of the streaming quality in terms of frames per second following a benchmarking approach [9] The main metric we use are the *frames per second* (FPS) displayed to the user. While there is no hard quality limit, values below 20 are considered to lose more and more of appeal. The frames per second show how quickly and smoothly the desktop environment is presented to the user and how quickly potential input is recognized. Our test setup consists of three parts. First, the VDI solution which is tested. Second, the application use case performed in the virtual desktop, and third, the network conditions under which the solutions are tested. In subsection 4.1, we specify the test workload, which is defined by the task types that a user performs on a PC. To specify the test workload, we present the potential users of a VDI.

Our set of tests consists of seven computer tasks (i.e. test workload) performed on a virtual desktop. The purpose of this test set is to investigate the capability of virtual desktops in performing the typical tasks performed on a PC. In addition, task-based testing measures the Quality of Service of a virtual desktop in performing each task is also measured. To evaluate the Quality of Service of a virtual desktop, we specify nine test cases. In the first five test cases, the purpose is to find the effect of each network quality factor on the Quality of Service of a virtual desktop. For the first five test cases, we only focus on one test object, the Web Browsing test object. For this, each network quality factor is tested separately in the absence of other factors. Since VPCs may be used in different network qualities, we examine the performance of VDIs in the remainding four test cases using four network qualities.

4.1 Setup: Activities based on identified User Types

We categorize users into three main groups based on [2], namely Power Users, Office Users, and Home Users. Each group performs countless number of tasks on PCs, each needing a different set of requirements. However, there are some tasks that are common among users of each user type. We define in Table 1 a

Table 1. Computer Tasks for Home Users, Office Users and Power Users

Home User Tasks		
Task 1	Web Browsing	Web surfing and flash content rendering using Google Chrome.
Task 2	A/V Streaming	Playback of a 1080p HD video file in the format of MKV in this task.
Office User Tasks		
Task 3	Presentation Design	Designing presentation slides using Microsoft PowerPoint 2013.
Task 4	Data Analyzing	Data processing using Microsoft Excel 2013.
Task 5	Word Processing	Creating textual documents using Microsoft Word 2013.
Power User Tasks		
Task 6	Code compiling	Implementation, compilation and execution of an Android project using Eclipse ADT.
Task 7	Image Processing	Processing graphical elements using Inkscape application.

few task types for each user type that represent that user type. Note that, this classification does not necessarily dictate a task type to a user type since a user type may be assigned to different, and possibly all, task types in the real world. In total, we test seven computer tasks, which we introduce and explain next.

Having the tasks needed to be performed to test a virtual desktop, in the next subsections we explain the Application-Task-based Testing and User-based Testing, these two test sets we perform to assess the quality of virtual desktops.

4.2 Setup: Network Variations

The quality of the network has a large influence on the delivered quality of service. Our aim is to identify how the various network factors influence the quality individually as well as how the performance is under various levels of networking quality. The five network factors that we consider are the following. `Delay:` Latency in the packet delivery. `Drop:` Packet loss. `Throttle:` Insufficient bandwidth. `Out of Order:` Packets delivery in different order than they were sent. `Duplicate:` Receiving a packet twice since the sender thinks that the first packet is not delivered due to packet loss and retransmit the packet.

We define four categories of network quality, displayed in Table 2, namely best network quality, normal network quality, average network quality, and worst network quality. Each category is comprised of the five above mentioned network factors and each factor affects the network quality with a specific ratio. For instance, as is shown in Table 2, in a network with normal quality the delay is about 20ms, the Drop is 1%, the Throttle is 5%, etc. We use an application named "Clumsy" (http://jagt.github.io/clumsy) to simulate the four network qualities listed in the table and to test the quality of Web Browsing test object with each network quality factor separately.

4.3 Video Streaming Quality: Impact of individual Network Factors

In Table 3 we investigate the impact of each individual network factor on the resulting frame rate. Therefore we consider the use case of Web Browsing and

Table 2. Network Types based on differing Quality Factors

Quality Type	Delay	Drop %	Throttle %	Out of order %	Duplicate %
Type 1: Good	1 ms	0	0	0	0
Type 2: Normal	20 ms	1	5	1	3
Type 3: Average	50 ms	2	8	5	7
Type 4: Worst	200 ms	5	15	15	18

Table 3. Effect of Network Quality Factors at the Use Case of Web Browsing

Quality Type	Delay	Drop %	Throttle %	Out of order %	Duplicate %
Good Network	1 ms	0	0	0	0
Technology	Frames per Second				
Local PC	24.79	24.79	24.79	24.79	24.79
Quality Type	Delay	Drop %	Throttle %	Out of order %	Duplicate %
Normal Network	20 ms	1	5	1	3
Technology	Frames per Second				
Citrix XenDesktop	23.57	9.20	17.96	19.03	15.87
VMware Horizon	14.56	11.05	14.06	24.31	21.52
Microsoft VDI	2.44	2.55	2.39	4.71	3.92

first analyze the frame rate at a local PC. For this, the frame rate is 24.79. Next, we modify each single network factor individually and analyze the effect on the three solutions. For this, in the initial state, Delay is set to 1ms, the drop rate to 0%, the bandwidth throttle to 0%, the ratio of out of order packets is 0% and the ratio of duplicate packets is 0% as well. In each step, only one factor is modified, while the rest stays the same, i.e. either 1ms or 0%. We tested the three VDI solutions under these conditions and list the results in Table 3 with the corresponding frame rates. In this context, the higher the frame rate is, the better quality will be.

The first observation is that both the selected solution as well as the network factor has an influence on the resulting frame rate. Citrix XenDesktop shows very high resilience against Delay, and very low resilience against Drop. This technology also relatively shows a good performance in case of other degraded network quality factors, such as Throttle, Out of Order, and Duplicate. VMware View Horizon is considerably resilient against Out of Order and Duplicate packets. On the other hand, Delay, Packet Loss (Drop), and Throttle have the most negative effects on the QoS of virtual desktops by reducing the frame rate of Web Browsing task from a frame rate of 24.79 to 14.56, 11.05, and 14.06, respectively. Microsoft VDI is very sensitive to low quality of any network factors. This is such that the frame rate in this task is dramatically degraded compared to 24.79 on a PC. This technology does not show any resilience to degradation of any network quality factors since in any of five network quality factors, the frame rate is dropped under 5. The largest impact of the networking factors on for the solution by Citrix and VMware is the loss of packets. Both solutions drop to a frame rate of around 10 with a drop rate of 1%. With respect to the capabilities of a human brain, a frame rate of 10 should be still acceptable, while a frame rate of below 5 is not acceptable.

4.4 Streaming Quality of Solutions in various Network Conditions

In this section, we performed each user task (as listed in Subsection 4.1) on each network condition (as listed in Subsection 4.2) with each VDI solution as well as a local PC. First, we execute the tasks on a PC and measure the resulting frame rate for each task (Table 4). In this ideal state, the frame rate is around 25 for Web browsing, audio/video streaming, presentation editing, word processing and code compiling, while the frame rate is around 12-15 for data analysis and image processing. This due to the few changes in the figure or screen lag due to calculations in the background.

Table 4. Effect of Network Quality on Application Use Cases in Frames per Second

Local PC - Measure in Frames per Second							
Network	Browse	Stream	Word	Analysis	Slides	Image Proc.	Compile
Ideal	24.79	25.86	25.99	12.27	25.96	27.37	15.5
Citrix XenDesktop							
Network	Browse	Stream	Word	Analysis	Slides	Image Proc.	Compile
Type 1	22.97	24.00	5.86	12.23	4.67	11.50	3.71
Type 2	20.22	17.73	4.90	9.66	4.77	11.12	9.15
Type 3	9.56	3.97	2.01	10.61	1.60	2.89	7.38
Type 4	3.70	2.36	1.94	4.44	0.90	3.63	6.61
VMware Horizon - Measure in Frames per Second							
Network	Browse	Stream	Word	Analysis	Slides	Image Proc.	Compile
Type 1	20.00	23.00	12.44	7.49	18.90	24.67	13.00
Type 2	12.22	2.33	3.43	4.15	12.00	17.70	10.55
Type 3	9.36	2.18	10.57	4.08	10.05	16.15	14.08
Type 4	3.50	0.30	4.24	4.42	4.37	2.39	6.55
Microsoft VDI							
Network	Browse	Stream	Word	Analysis	Slides	Image Proc.	Compile
Type 1	20.87	13.17	4.30	5.69	5.48	13.51	6.32
Type 2	3.70	3.40	3.84	4.69	3.76	5.07	4.30
Type 3	3.04	2.15	5.27	2.78	1.44	2.69	1.86
Type 4	0.54	0.62	2.04	1.03	0.94	0.82	1.24

Results for Citrix XenDesktop In both best and normal network quality, Web Browsing and Video/Audio Streaming have the best performance. Surprisingly, the quality of these two tasks in best network quality is only slightly lower than the quality that a PC can deliver. However, their quality crashes in average network quality and reaches to the lowest level in worst network quality. Word processing, data analyzing, presentation designing, and image processing keep their frame rate relatively stable in best and normal network quality. Their frame rate decreases in average network quality, leading to the lowest frame rate in worst network quality. In general, XenDesktop performs these tasks with much lower frame rate than a PC. Although code compiling has the worst frame rate in the best network quality, compared to other tasks, it considerably improves in the normal network quality, but again slowly loses frame rate in the average and worst network quality.

Results for VMware Horizon View In the best network quality, image processing has the best performance with 24.672fps and data analysis has the lowest frame rate with 7.493fps. Since the quality of the data analysis task does not deviate much in the other network qualities, we believe the cause of low frame rate is resulted from the nature of this task and the fact that the state of a user's screen is usually static and does not change very frequently. Therefore, the performance of this task is might be regardless of the network quality and can be acceptable in any network quality. Word processing, however, has a relatively erratic behavior. Starting from 12.44fps in the best network quality, it crashes in 3.43fps in the normal network quality, climbs up to 10.57fps again in average network quality and, finally, crashes into 4.24fps again. In each network quality, the same test case for each task is performed, however, the speed of executing the a task (e.g. scrolling speed) may differ in each network quality, which consequently affects the frame rate. The same behavior can also be observed for code compiling, however, with higher frame rate and less variance in each

network quality comparing to word processing. Among other tasks, video/audio streaming has the highest quality degradation. Dramatically falling from 23fps in the best network quality to, first, 2.33fps in the normal network quality and, finally, 0.30fps in the worst network quality, a minimum level of quality is only achievable in the best network quality with Horizon View technology. Compared to a PC, the VMware Horizon View cannot establish a similar level of quality in any of the tasks. Finally, other tasks, such as Web browsing, presentation designing (Slides), and image processing, have an expected decrease in frame rate and, consequently, the quality of services id degraded as the network quality is degraded. However, the frame rate of the image processing task crashes dramatically in the worst network quality, making it almost impossible to perform the task. The reason to this behavior is that Image Processing, as a task dealing highly with graphical features, requires high frame rate and, therefore, is more vulnerable to poor network quality.

Results for Microsoft VDI Focusing on the results in Table 4, next we discuss the results of testing the seven tasks in four network qualities using Microsoft VI. In the best network quality, Web browsing has the best performance with 20.87 fps, image processing (13.51fps) and video/audio streaming (13.17fps) also has a relatively high frame rate. Word processing (4.3fps) together with code compiling (6.32fps), presentation designing (Slides) (5.48fps), and data analyzing (5.69fps) show a very poor performance. These four tasks also maintain low frame rate in normal, average, and worst network qualities. In the transition between the best network quality and the normal network quality, the quality of Web browsing, video/audio streaming and image processing dramatically falls. After that, all the tasks lose frame rate until the worst network quality, in which, with regard to their frame rates, no task can be performed. Microsoft VDI also performs the tasks with a high difference in QoS (i.e. frame rate) compared to the quality of these tasks on a PC.

Based on the benchmarking that we performed on these three VDI technologies, we can conclude that Microsoft VDI falls back compared to Citrix XenDesktop and VMware Horizon View in Quality of Service and Quality of Experience. Furthermore, compared to VMware Horizon View, Citrix XenDesktop proves to be more stable in delivery of suitable Quality of Service and Quality of Experience, as the table indicates by having more votes on normal behavior or acceptable behavior for the Citrix XenDesktop in comparison to VMware Horizon View. Additionally, the user-based testing that we performed also exposes that users are, in general, more satisfied with the quality of Citrix XenDesktop.

5 Conclusions

Introducing Virtual Desktop Infrastructure (VDI) technology as a commercial desktop virtualization approach, we believe that there should be a counterpart technology, which provides desktop virtualization for personal users, namely Virtual Personal Computer (VPC), allowing users to access their desktop environment from any place and device at any time. In this paper we chose, elaborated and implemented the architectures of three dominant VDI technologies, namely

Citrix XenDesktop, VMware Horizon View, and Microsoft VDI. After a careful parameter study a setup of each technology, we defined and performed a set of test cases and which allows us to identify the impact of the network on the quality of the VPCs. We tested each technology with task-based testing. The results of the two tests gave useful insights about the QoS of each technology. Finally, we compared the three technologies from different aspects to determine a fair rating for the quality of the services that they provide. In the comparison of the feature list, Citrix XenDesktop is rated best with the other two solutions being slightly less powerful. In the comparison of the impact of the individual Network Factors VMware Horizon View proves to be robust against various single work modifications. In the combination of limited network factors, i.e. in various network conditions, Citrix XenDesktop turns out to be more able to maintain a stable frame rate. While VMware Horizon View shows also good results, Citrix XenDesktop is slightly better while Microsoft VDI is very limited and provides only a small frame rate. We conclude that Citrix XenDesktop surpasses VMware Horizon View and Microsoft VDI in terms of Quality of Service and the variety of features that it offers. Thus, we believe that Citrix XenDesktop is the most qualified VDI technology, upon which the VPC concept can be established. In future work, the type and quality of the tasks tested will be extended to match more use cases. Also we aim at conducting a user-based study measuring the quality of experience as well as at indentifying the options for peer-to-peer service provision [10] [11].

References

1. K. Oestreich: Converged Infrastructure, CIO & Leader (2010)
2. S. Sierra: The Three Types of Computer User, Digital Digressions (2006)
3. K. Subramanian: Recession Is Good For Cloud Computing Microsoft Agrees, Cloudave (2009)
4. C. Gong, J. Liu, Q. Zhang, et al.: The Characteristics of Cloud Computing, Int. Conf. on Parallel Proc. Workshops (ICPPW), Volume 39, pp.275 - 279 (2010)
5. L. M. Kaufman: Data Security in the World of Cloud Computing, IEEE Security Privacy, Volume 7, pp.61 - 64 (2009)
6. Y. Simmhan, A. G. Kumbhare, B. Cao, and P. Viktor: An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds, IEEE Int. Conf. on Cloud Computing (CLOUD), pp.582 - 589 (2011)
7. Horizon Advantages, www.vmware.com/products/horizon-view/features.html
8. J. Ventresco, Implementing VMware Horizon View 5.2, Packt Publishing Ltd, 2013
9. A. Kovacevic, K. Graffi, S. Kaune, C. Leng, and R. Steinmetz: Towards Benchmarking of Structured Peer-to-Peer Overlays for Network Virtual Environments, in Proc. of the IEEE Int. Conf. on Parallel and Dist. Systems ICPADS08, 2008.
10. N. Liebau, K. Pussep, K. Graffi, S. Kaune, E. Jahn, A. Beyer, and R. Steinmetz: The Impact Of The P2P Paradigm on the New Media Industries, in Proc. of Americas Conf. on Info. Sys. AMCIS, 2007.
11. K. Graffi, C. Groß, D. Stingl, H. Nguyen, A. Kovacevic, and R. Steinmetz: Towards a P2P Cloud: Reliable Resource Reservations in Unreliable P2P Systems, in Proc. of the IEEE Int. Conf. on Parallel and Dist. Systems ICPADS10, 2010.