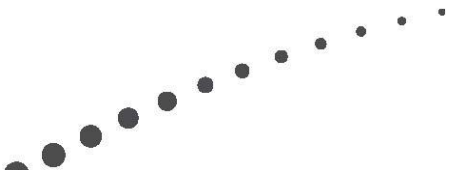




# XenDesktop Planning Guide: Provisioning Service Networking





# Table of Contents

- Overview ..... 3
- Guidelines ..... 3
  - Considerations ..... 3
  - Network Capacity ..... 8
  - Target Boot Process ..... 9
- Planning ..... 11
  - Boot Bandwidth Calculation ..... 11
  - Boot option selection ..... 12
  - Planning by Environment ..... 12
- Appendix A – Reference Documentation ..... 15
- Appendix B – Registry Settings ..... 17
  - Client-side Settings ..... 17
  - Server-side Settings ..... 17



## Overview

Citrix Provisioning Services (PVS) is a software streaming technology that allows servers and desktops to be provisioned and re-provisioned in real time from a single shared-disk image. The service is commonly integrated within a Citrix XenDesktop architecture to deliver virtual desktops efficiently.

One of the many benefits of PVS is the ability to scale, however when called upon to delivery high volumes PVS servers have significant network requirements. Therefore when planning the implementation of PVS it is important to take these requirements into consideration.

This planning guide provides Provisioning Services networking guidelines. It provides best practices, and recommendations to consider when planning to deploy PVS. It is not intended as a comprehensive guide for planning and configuring network infrastructures, nor as a networking training handbook.

The guide assumes the reader has knowledge of PVS, servers are running Windows Server 2008 R2, and clients have 1 Gigabit interfaces.

## Guidelines

Environment requirements are often balanced with financial constraints. Therefore the primary goal behind most recommendations is to provide resources necessary to deliver services without impacting user experience.

## Considerations

Layers of the internet protocol suite<sup>1</sup>, defined by the IETF, are a good model to group the network considerations when planning a PVS deployment. These include link, internet, transport (TCP/IP), and application layers:

### **Link Layer Considerations**

#### Interfaces

- Ethernet
  - 1 Gigabit (Gb), and 10Gb Ethernet are the most prevalent connection media. 1Gb typically provides enough bandwidth for targets, but it can become a bottleneck for PVS servers. 10Gb is the ideal media for PVS servers to provide sufficient network bandwidth for most environments to mitigate the likelihood of it becoming a resource bottleneck.
- Link aggregation

---

<sup>1</sup> <http://tools.ietf.org/html/rfc1122>

Link Aggregation<sup>2</sup>, also known NIC bonding or teaming, allows multiple network connections to be used in parallel as a single link. Virtualization support depends on the hypervisor, but it is a well-established method of augmenting bandwidth when single 1G interfaces are at capacity and 10G is not an option.

### NIC Settings

- Disable checksum offloading

Citrix recommends disabling Checksum Offload on the network adapter of both the Provisioning Server as well as the target devices. On many Network Interface Cards (NICs), checksum offloading can be disabled by opening the NIC properties and selecting the advanced configuration tab.

- Auto Negotiate

With 1G interfaces Auto Negotiation can cause long starting times and PXE timeouts, especially when starting multiple target devices in a PVS environment. Therefore Citrix recommends hard-coding all 1G Provisioning Server ports (server and client) on the NIC and on the switch.

10G interfaces should be set for Auto Negotiation on both NIC and switch ports.

### Switch Settings

- Disable Spanning Tree or Enable Portfast

In a switching environment the Spanning Tree Protocol (STP) places ports into a blocked state while it transmits Bridged Protocol Data Units (BPDUs) and listens to ensure the BPDUs are not in a loopback configuration. The port is not placed in a forwarding state until the network converges, which depending on the size of the network, may incur enough time to cause Pre-boot Execution Environment (PXE) timeouts. To eliminate this issue, disable STP on edge-ports connected to clients or enable PortFast.<sup>3</sup>

- Storm Control

Storm Control is a feature available on Cisco switches that allows a threshold to be set whereby, multicast, broadcast, or unicast traffic may be suppressed. Its purpose is to prevent malicious or erroneous senders from flooding an LAN and affecting network performance. PVS Servers may send a large

---

<sup>2</sup> [http://en.wikipedia.org/wiki/Link\\_aggregation](http://en.wikipedia.org/wiki/Link_aggregation)

<sup>3</sup> <http://support.citrix.com/article/CTX117374/>

amount of traffic by design that falls within a storm control threshold, therefore the feature should be configured accordingly<sup>4</sup>.

- Broadcast Helper

This switch feature is required to direct broadcasts from clients to servers that would otherwise not be routed. In a PVS environment it is necessary to forward PXE boot requests when clients are not on the same subnet as the servers.

## Internet Layer Considerations

### Packet forwarding

- Routing

A general principal of backend infrastructure design is to avoid routing. Today's high speed multi-layer switches handle inter-vlan routing with minimal latency overhead, however isolating traffic to layer 2 mitigates the risk of any service degradation from reliance on other infrastructure delivery components. When possible (small environments) PVS servers should reside on the same subnet as target hosts.

- Load Balancing

For many infrastructure services load balancing provides an effective means of providing scalability and resiliency. While load balancing can occur at any layer the internet/IP layer is most used where inter-vlan communication is required. Where PVS is concerned TFTP load balancing is a resilient option to deliver the bootstrap file to targets. Citrix NetScaler is a market leading load balancing solution.

### Subnet

Network subnets define the broadcast domain for hosts. Classless Interdomain Routing (CIDR) length determine how many bits in a 32-bit IP address apply to the network portion and ultimately determines how many hosts may be allocated on the subnet. Larger subnets allow more hosts to communicate directly through frames without incurring the overhead of routing. Smaller subnets limit the multicast and broadcast traffic overhead that must be processed by every host NIC on the subnet. Most subnets employ a /24 CIDR block, however with PVS having a broader block is beneficial since it allows more hosts to communicate directly with the servers. Citrix Consulting Services (CCS) field experience has shown that

---

<sup>4</sup> <http://support.citrix.com/article/CTX121618>

generally up to /21 CIDR blocks, which provide for  $(255 \times 4) - 2 = 1,022$  hosts, are reasonable length.

### Multihoming

Multihoming is a method to optimize the use of constrained network bandwidth by utilizing multiple server NICs to direct traffic across different network paths. Traffic is often segregated by PVS streaming, administration, and or storage.

The PVS product was initially release before server teaming or 10 Gigabit interfaces were widely deployed. Therefore to optimize use of the bandwidth provided by a 1 Gigabit Ethernet interface Multihoming was a recommended practice. Today, particularly since 10 Gigabit interfaces are widely used making the network bandwidth less of a resource constraint, Multihoming and the additional complexity that comes with it may be avoided.<sup>5</sup>

## **Transport Layer Considerations**

### TCP Large Send Offload

The TCP Large Send Offload option allows the TCP layer to build a TCP message up to 64 KB long and send it in one call via IP and the Ethernet device driver. The adapter then re-segments the message into multiple TCP frames for wire transmission. The TCP packets sent on the wire are either 1500 byte frames for a Maximum Transmission Unit (MTU) of 1500 or up to 9000 byte frames for a MTU of 9000 (jumbo frames). Re-segmenting should be disabled on all Provisioning Servers and target devices.

Disable the Large Send Offload, in the NIC properties and under the advanced configuration tab. (Some NICs do not offer this setting in the properties page).<sup>6</sup>

[See Appendix B for pertinent registry settings]

### Firewall

Firewalls can add unnecessary latency, and interface bandwidth can be a bottleneck. Therefore, when possible, firewalls should be avoided anywhere between PVS infrastructure components.

### Ports & Threads

---

<sup>5</sup> <http://blogs.citrix.com/2012/05/01/pvs-stream-traffic-isolation/>

<sup>6</sup> <http://support.citrix.com/article/CTX117374>

By default PVS is configured to service connections on 20 UDP ports with 8 threads per port or  $20 \times 8 = 160$  concurrent connections. The pool of concurrent connection across all PVS servers collectively should equate to the number of active targets at a minimum, yet for redundancy it is recommended to provide  $N + 1$  connections in the event of a server outage.<sup>7</sup>

“# of ports” x “# of threads/port” = “max clients”

## Application Layer Considerations

### Server

Server virtualization is a mainstay in most infrastructure environments and there are few cases where its use cannot be justified compared to dedicated physical servers. PVS for the most part is no exception. It is considered good practice to virtual PVS servers alongside other infrastructure components. Typically only large environments, where the sheer volume calls for dedicated resources, can justify dedicated hardware.<sup>8</sup>

### Storage

- Auto Disconnect Timeout

This setting will increase the auto-disconnect timeout above its default value of 15 minutes. This prevents the file server from closing the Provisioning Server handle after 15 minutes of idle time, which will cause the System Cache to flush.

- Direct Attached Storage - The PVS Server should use block level storage to allow maximum performance and caching of target data.<sup>9</sup>
- Network Attached Storage – CIFS or NFS may be used for image storage with certain optimizations.

CIFS optimizations:

Enable SMB2

This key does not exist by default and has an assumed value of 1. Settings this to zero will disable SMB 2 and force the server to use SMB 1.0. It is recommended that this key be set to 1 to ensure that SMB 2.0 is enabled.

---

<sup>7</sup> <http://blogs.citrix.com/2011/07/11/pvs-secrets-part-3-ports-threads/>

<sup>8</sup> <http://blogs.citrix.com/2011/07/30/virtual-provisioning-server-%E2%80%93-a-successful-real-world-example/>

<sup>9</sup> [http://support.citrix.com/servlet/KbServlet/download/24250-102-](http://support.citrix.com/servlet/KbServlet/download/24250-102-671602/Advanced%20Memory%20and%20Storage%20Considerations%20for%20Provisioning%20Services.pdf)

[671602/Advanced%20Memory%20and%20Storage%20Considerations%20for%20Provisioning%20Services.pdf](http://support.citrix.com/servlet/KbServlet/download/24250-102-671602/Advanced%20Memory%20and%20Storage%20Considerations%20for%20Provisioning%20Services.pdf)

#### Smb2 Credits Max

This key does not exist by default and has an assumed value of 1024. This value determines the maximum amount of credits a file server will allow for a single SMB session. This key should not need to be modified.

#### Smb2 Credits Min

This key does not exist by default and has an assumed value of 64. This value determines the minimum amount of credits to which a file server will forcibly limit an SMB session. This key should not need to be modified.

[See Appendix B for pertinent registry settings]

### Services

PVS relies on a cast of supporting infrastructure services. DNS, DHCP should typically be provided on dedicated service infrastructure servers, while TFTP and PXE Boot are functions that may be hosted on PVS servers or elsewhere.

## Network Capacity

PVS bandwidth utilization is mostly a function of the number of target devices and the portion of their image/(s) they utilize. Network impact considerations include:

- PVS streaming is delivered via UDP, yet the application has built-in mechanisms to provide flow control, and retransmission as necessary.
- Data is streamed to each target device only as requested by the OS and applications running on the target device.
- In most cases, less than 20% of any application is ever transferred.<sup>10</sup>
- Network utilization is most significant when target devices are booting as the OS loads. After target devices start there is minimal network utilization.

Total load time on boot can be estimated according to this formula:

$$\text{Seconds\_to\_boot} = (\text{number\_of\_targets} * \text{MB\_until\_usage}) / \text{bandwidth}^{11}$$

---

<sup>10</sup> <http://support.citrix.com/servlet/KbServlet/download/25649-102-649146/Provisioning%20Services%205%206%20Best%20Practices%20External%201.2.pdf>

<sup>11</sup> <http://support.citrix.com/article/CTX125744>



The table below lists PVS server interface options from most to least capacity.

Interface	Bandwidth	Justification
<b>Chassis 10G+</b>	80+ Gigabit	PVS servers, targets, and infrastructure servers hosted within the same blade chassis offer the maximum bandwidth potential across a common backplane.
<b>Bonded/Teamed 10G</b>	Up to 80 Gigabit	Outside of a chassis option Bonding/Teaming offers the best capacity and resiliency.
<b>Single 10G</b>	10 Gigabit	PVS servers with a 10G interface are becoming the most broadly deployed configuration.
<b>Bonded/Teamed 1G</b>	Up to 8 Gigabit	When 10G is not available Bonding/Teaming is the ideal option to bolster server bandwidth using multiple interfaces without the added complexity of Multihoming.
<b>Single 1 Gigabit</b>	1 Gigabit	Functions for small environments, but 1G targets quickly overrun 1G servers.

## Target Boot Process

A target device initiates the boot process by first loading a bootstrap program. A bootstrap program is a small program that runs before the operating system is loaded. PVS uses a special bootstrap program which initializes the streaming session between the target device and the Provisioning Server. After this session starts, the operating system begins to be streamed and loaded from the vDisk that was initiated.<sup>12</sup>

### Boot Options

There are three primary means for a target device to load the bootstrap program.

- Network, with Preboot eXecution Environment (PXE) directly
  - 1) When a target device boots from the network, DHCP sends a request to the Provisioning Server for an IP address and Scope Option settings (66 and 67). The Provisioning Server returns the information as requested.
  - 2) Using TFTP, a request for the bootstrap file is sent from the target device to the Provisioning Server. The Provisioning Server downloads the boot file on the target device.
  - 3) The target device boots the assigned vDisk image.

<sup>12</sup> <http://support.citrix.com/proddocs/topic/provisioning-61/pvs-technology-overview-boot-file-get.html>

This option requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the PVS servers to allow the PXE broadcast to be directed to them.

Methods to make this option Highly Available include:<sup>13</sup>

- DNS Round Robin Entry

With this option, a TFTP server DNS name is carried in DHCP option 66. The DNS server then would have two or more A records defined for the domain name and cycle through the list of records in round robin fashion in response to DNS queries. This provides Provisioning Services target devices with redundancy in obtaining their Bootfile.

- Provisioning Services PXE Broadcast

With this option a PXE boot server is hosted by Provisioning Services servers. After Provisioning Services target devices obtain their IP address and gateway through DHCP, they start broadcasting a TFTP boot request. Provisioning Services servers hosting PXE boot services on the same network as the target devices will receive boot requests and respond directly. For those on different subnets, routers may be configured with a IP/UDP helper address entry, which allows the router to forward the initial Provisioning Services Client PXE boot broadcasts. Without the helper address, the requests would otherwise be contained within the subnet and unable to reach the PXE service.

- NetScaler Use Source IP (USIP)

This option relies on the NetScaler to load balance the target device's initial TFTP boot request to a TFTP Server. The target devices must obtain the IP address of the NetScaler Virtual Server IP (VIP) through DHCP option 66. Once the NetScaler receives the boot request, it is directed to one of the TFTP servers from the pool by changing the destination IP address. The source IP address is not changed, therefore the TFTP server replies to the target device directly.

- NetScaler Direct Server Return (DSR)

This option is similar to the NetScaler – Use Source IP option, but it makes its load balancing decision based on the frame MAC Address

---

<sup>13</sup> <http://support.citrix.com/article/CTX131954>

and does not change the target destination IP address. Therefore the target TFTP Server must have a loopback IP address corresponding to the NetScaler VIP.

- NetScaler Global Server Load Balancing (GSLB)Storage

This option takes advantage of the NetScaler ability to integrate with DNS to control responses to queries while monitoring the availability of TFTP servers. Upon receiving a DNS query for the TFTP boot server domain name, the NetScaler dynamically responds with the best option, according to the selection algorithm configured.

- Network with PXE and DHCP options
  - 1) When a target device boots from the network, DHCP sends a request to the Provisioning Server for an IP address and Scope Option settings (option 60; PXEClient identifier). The Provisioning Server returns the information as requested.
  - 2) The target device sends a request to the Provisioning Server for the bootstrap file name and location to the PXE service (options 66 and 67). The PXE service returns the information to the target device.
  - 3) Using TFTP, a request for the bootstrap file is sent from the target device to the Provisioning Server. The Provisioning Server downloads the bootstrap file to the target device and the target device boots.
- From a boot device stored on attached media (Boot Device Manager (BDM))
 

The Boot Device Manager creates a Bootfile that PVS client can obtain through an ISO image mounted on Virtual Server from a network share. For this to be a High Availability option for delivery of the Bootfile the network share must be redundant. With this option the client may also boot through a local CD/DVD, Hard Drive, or USB yet each would be a single point of failure.

## Planning

Below are tables and figures that may aid in the planning of the network requirements for a Provisioning Services environment.

### Boot Bandwidth Calculation

The theoretical load time PVS servers collectively could provide targets as a function of network bandwidth, during initial target boot time, can be calculated by multiplying the number of targets times the portion of the image required to load the operating system in Giga (G) Bytes (B) (GB),



times 8, to produce a number in Giga (G) bits (b) (Gb), which is then divided by the bandwidth in Gigabits per second (Gbps). Using an estimate of 100 MB (the initial amount required to boot a Windows OS target varies by version), with 10 Gigabit interface, the table below provides some sample calculations:

Targets	Image (MB)	Bandwidth (Mb)	Load Time (s)
100	100	80,000	8
500	100	400,000	40
1000	100	800,000	80
10000	100	8,000,000	800
40000	100	32,000,000	3,200

## Boot option selection

Based on all of the High Availability Boot Options, the following table provides suggestions pertaining to how difficult they are to implement, how scalable they are and how fault tolerant they are (ability to identify issues and reroute requests appropriately).

Option	Difficulty	Scalability	Fault Tolerance
DNS Round Robin Entry	Low	Medium	Low
Provisioning Services PXE Broadcast	Low	Medium	Medium
Provisioning Services Boot Manager	Medium	Medium	High
NetScaler Use Source IP	Low	High	High
NetScaler Direct Server Return	Medium	High	High
NetScaler Global Server Load Balancing	High	High	High

## Planning by Environment

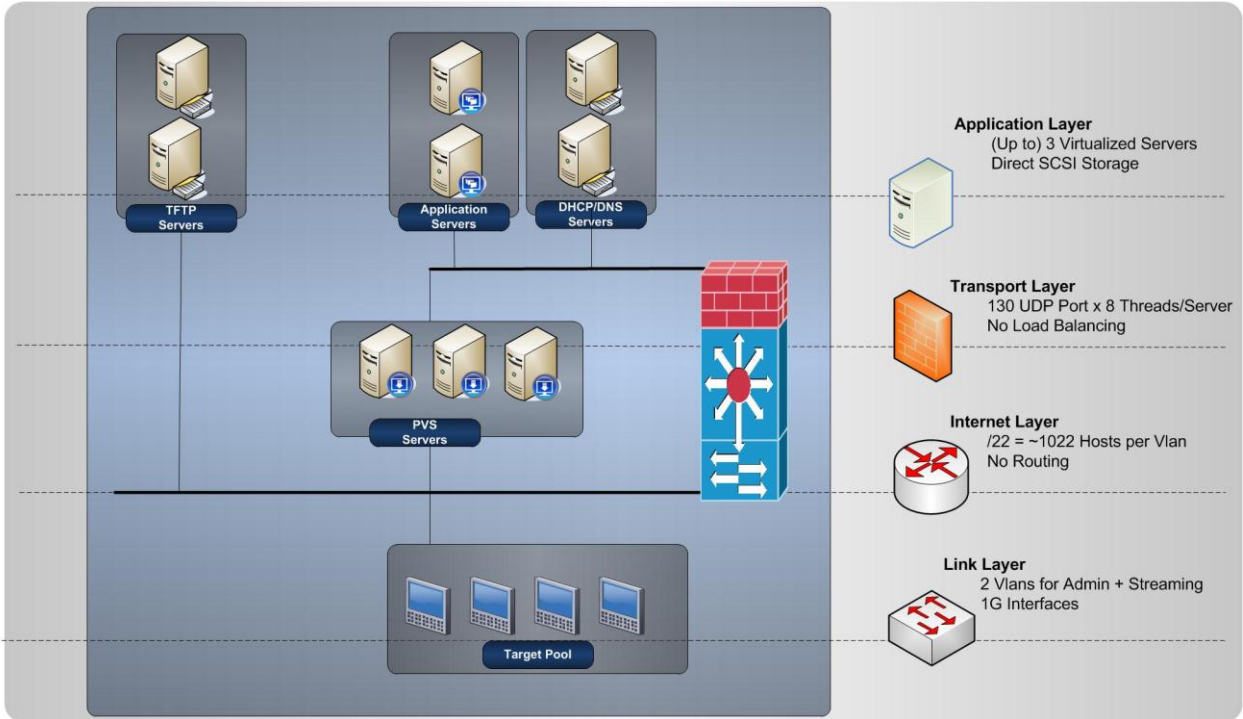
While most environments are unique a profile may be made according to typical requirements for reference purposes. The requirements of small environments are often driven by least cost, and least complexity. Medium environments are less cost driven, have greater need for resiliency, must scale, and have greater capacity for specialized administration. Large environments have the highest need for resiliency, redundancy, scalability, and are often administered by a service provider or dedicated enterprise NOC.

The following table and diagrams demonstrate considerations that may be used, “as an example”, according to the environment:

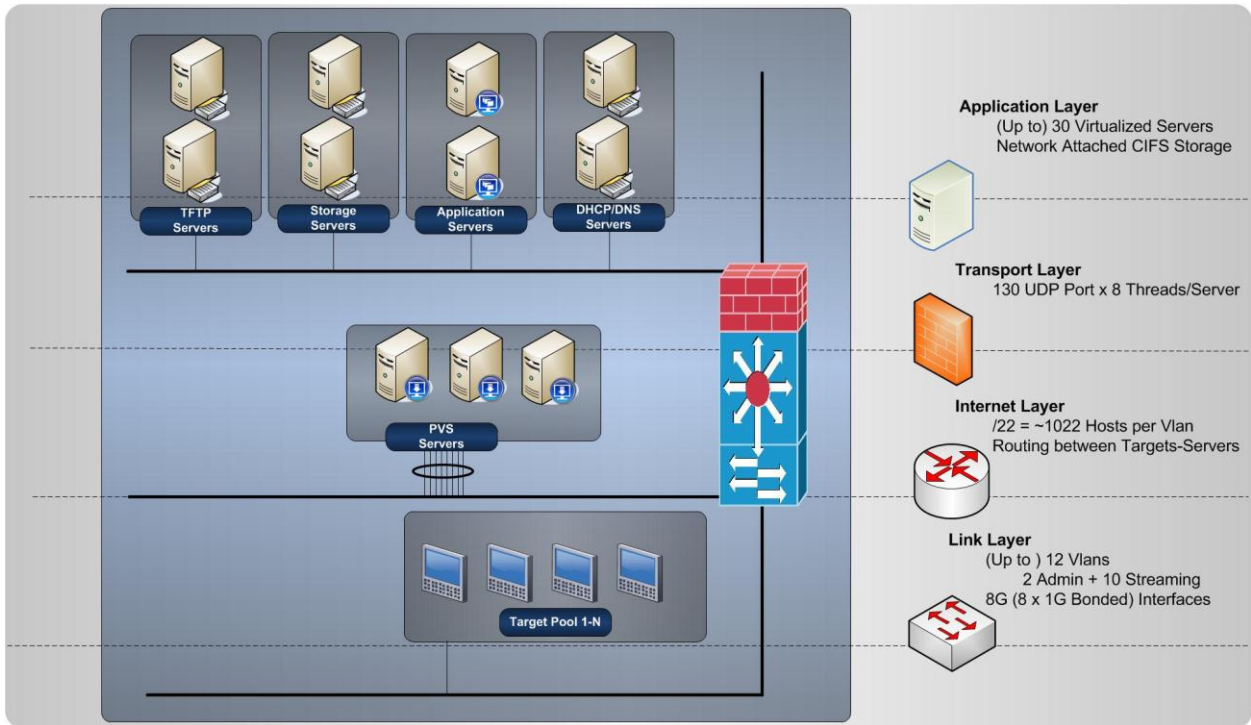
Option	Targets	Boot Option	Interface	Target IP Range	Server	Storage
Small	<1,000	Dhcp-Pxe	1G	/22	3 - Virtual	SCSI Direct
Medium	1,000 – 10,000	BDM	8G- Teamed	Up to /22 x 10	3x10=30 Virtual	CIFS Shared

Large	10,000 – 40,000	Dhcp- LoadBalance	10G	/22 x 40	3x40=120 Physical	FC Direct
-------	--------------------	----------------------	-----	----------	----------------------	-----------

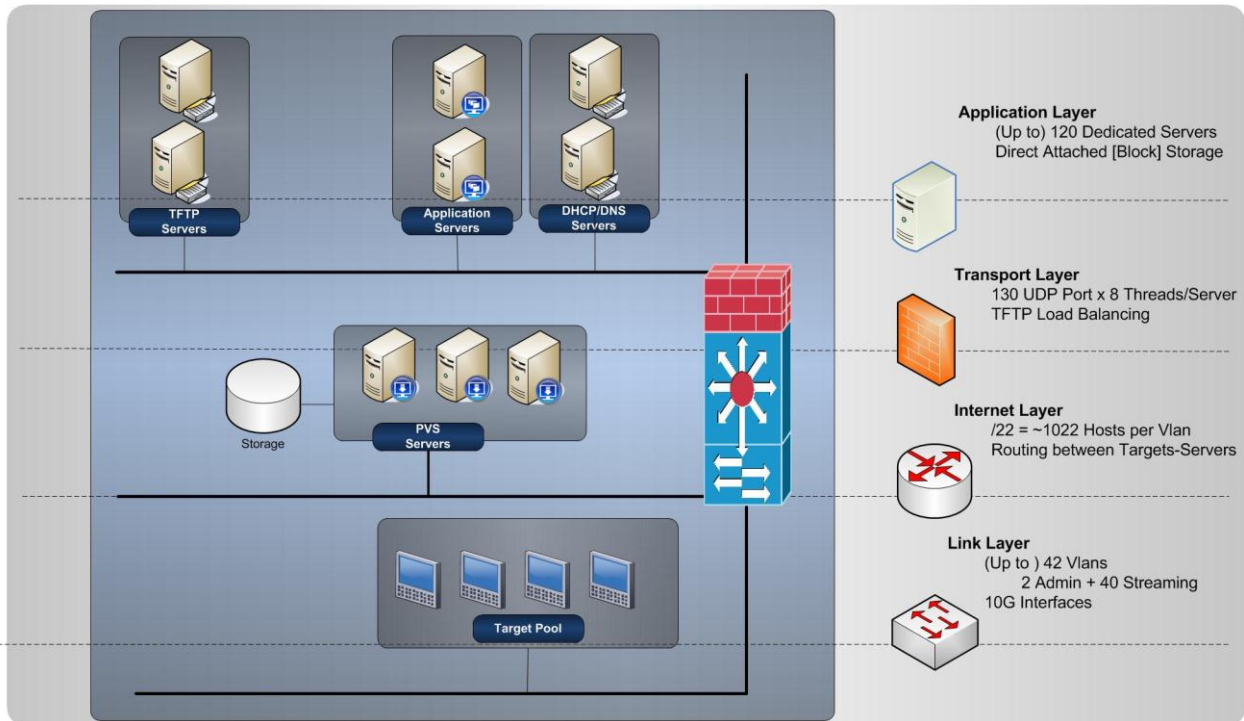
## Small Environment



## Medium Environment



## Large Environment





## Appendix A - Reference Documentation

Is Isolating the PVS Streaming Traffic Really a Best Practice?

<http://blogs.citrix.com/2012/05/01/pvs-stream-traffic-isolation/>

Virtual Provisioning Server – A Successful Real World Example

<http://blogs.citrix.com/2011/07/30/virtual-provisioning-server-%E2%80%93-a-successful-real-world-example/>

PVS Secrets (Part 1) – Selective PXE

<http://blogs.citrix.com/2011/05/31/pvs-secrets-part-1-selective-pxe/>

PVS Secrets (Part 2) – “Hidden” configurations

<http://blogs.citrix.com/2011/05/31/pvs-secrets-part-2-hidden-configurations/>

PVS Secrets (Part 3) – Ports & Threads

<http://blogs.citrix.com/2011/07/11/pvs-secrets-part-3-ports-threads/>

Advanced Memory and Storage Considerations for Provisioning Services

<http://support.citrix.com/servlet/KbServlet/download/24250-102-671602/Advanced%20Memory%20and%20Storage%20Considerations%20for%20Provisioning%20Services.pdf>

FAQ: Provisioning Services 5.1 Service Pack 2 through 5.6

<http://support.citrix.com/article/CTX125744>

Advanced Memory and Storage Considerations for Provisioning Services

<http://support.citrix.com/servlet/KbServlet/download/24560-102-647702/XD%20-%20Planning%20Guide%20-%20User%20Bandwidth%20Requirements.pdf>

How to Setup a Multi-Homed VM Separating Large Scale Traffic from ICA Traffic for XenDesktop

<http://support.citrix.com/article/CTX120955>

Best Practices for Configuring Provisioning Server on a Network

<http://support.citrix.com/article/CTX117374/>

Using PVS Boot Device Manger with XenDesktop and Xenserver

<http://blogs.citrix.com/2009/02/25/using-pvs-boot-device-manger-with-xendesktop-and-xenserver/>

Delivering 5000 Desktops with Citrix XenDesktop

<https://support.citrix.com/servlet/KbServlet/download/22662-102-645408/Delivering%205000%20Desktops%20with%20XenDesktop%204%200140.pdf%20>

Best Practices Guide for Provisioning Services and XenApp

<http://support.citrix.com/servlet/KbServlet/download/19542-102-665106/PVS%20-%20PVS%20for%20XenApp%20Best%20Practices.pdf>





Designing XenServer Network Configurations

<http://support.citrix.com/article/CTX129320>

Provisioning Services 5.6 Best Practices

<http://support.citrix.com/servlet/KbServlet/download/25649-102-649146/Provisioning%20Services%205%206%20Best%20Practices%20External%201.2.pdf>

Implementation Guide - High Availability for TFTP

<http://support.citrix.com/article/CTX131954>

Target Device Performance and Freezing Issue

<http://support.citrix.com/article/CTX121618>



## Appendix B – Registry Settings

### Client-side Settings

Description	Registry Modification (in REG format)
Disable Checksum Offloading on Network Adapter	"SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" valueName="DisableTaskOffload"
Disable TCP Large Send Offload	"SYSTEM\CurrentControlSet\Services\BNNS\Parameters" valueName="Enableoffload"

### Server-side Settings

Description	Registry Modification (in REG format)
CIFS Optimizations	"System\CurrentControlSet\Services\LanManServer\Parameters" valueName="Smb2"  "SYSTEM\CurrentControlSet\services\LanmanServer\Parameters" valueName="autodisconnect"  "SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters" valueName="EnableOplocks"  "System\CurrentControlSet\Services\MRXSmb\Parameters" valueName="OplocksDisabled"

	"SYSTEM\CurrentControlSet\services\mrxsmb\Parameters" valueName="CscEnabled"
<b>Disable Checksum Offloading on Network Adapter</b>	"SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" valueName="DisableTaskOffload"
<b>Disable TCP Large Send Offload</b>	"SYSTEM\CurrentControlSet\Services\BNNS\Parameters" valueName="Enableoffload"

## References

Footnote	Link	Author
1	<a href="http://tools.ietf.org/html/rfc1122">http://tools.ietf.org/html/rfc1122</a>	IETF
2	<a href="http://en.wikipedia.org/wiki/Link_aggregation">http://en.wikipedia.org/wiki/Link_aggregation</a>	Wikipedia
3	<a href="http://support.citrix.com/article/CTX117374/">http://support.citrix.com/article/CTX117374/</a>	Citrix Systems, Inc.
4	<a href="http://support.citrix.com/article/CTX121618">http://support.citrix.com/article/CTX121618</a>	Citrix Systems, Inc.
5	<a href="http://blogs.citrix.com/2012/05/01/pvs-stream-traffic-isolation/">http://blogs.citrix.com/2012/05/01/pvs-stream-traffic-isolation/</a>	Nick Rintalan
6	<a href="http://support.citrix.com/article/CTX117374">http://support.citrix.com/article/CTX117374</a>	Citrix Systems, Inc.
7	<a href="http://blogs.citrix.com/2011/07/11/pvs-secrets-part-3-ports-threads/">http://blogs.citrix.com/2011/07/11/pvs-secrets-part-3-ports-threads/</a>	Thomas Berger
8	<a href="http://blogs.citrix.com/2011/07/30/virtual-provisioning-server-%E2%80%93-a-successful-real-world-example/">http://blogs.citrix.com/2011/07/30/virtual-provisioning-server-%E2%80%93-a-successful-real-world-example/</a>	Dan Allen
9	<a href="http://support.citrix.com/servlet/KbServlet/download/24250-102-671602/Advanced%20Memory%20and%20Storage%20Considerations%20for%20Provisioning%20Services.pdf">http://support.citrix.com/servlet/KbServlet/download/24250-102-671602/Advanced%20Memory%20and%20Storage%20Considerations%20for%20Provisioning%20Services.pdf</a>	Dan Allen
10	<a href="http://support.citrix.com/servlet/KbServlet/download/25649-102-649146/Provisioning%20Services%205%206%20Best%20Practices%20External%201.2.pdf">http://support.citrix.com/servlet/KbServlet/download/25649-102-649146/Provisioning%20Services%205%206%20Best%20Practices%20External%201.2.pdf</a>	Citrix Systems, Inc.
11	<a href="http://support.citrix.com/article/CTX125744">http://support.citrix.com/article/CTX125744</a>	Citrix Systems, Inc.
12	<a href="http://support.citrix.com/proddocs/topic/provisioning-61/pvs-technology-overview-boot-file-get.html">http://support.citrix.com/proddocs/topic/provisioning-61/pvs-technology-overview-boot-file-get.html</a>	Citrix Systems, Inc.
13	<a href="http://support.citrix.com/article/CTX131954">http://support.citrix.com/article/CTX131954</a>	Citrix Systems, Inc.

## Product Versions

Product	Version
Provisioning Services	6.1
Windows Server	2008 R2

## Revision History

Revision	Change Description	Updated By	Date
1.0	Document Created	Matt Brooks – Principal Consultant	September, 11 <sup>th</sup> , 2012

### About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was \$1.6 billion.

©2010 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.