

**Tim Malfara**

**Director, Infrastructure Solutions Group**

[**TMalfara@anexinet.com**](mailto:TMalfara@anexinet.com)

**Phone: (215) 519 1246**

**Yan Madorskiy**

**Network Architect**

[**YMadorskiy@anexinet.com**](mailto:YMadorskiy@anexinet.com)

**Phone: (412) 983 9393**

**Robert Kim**

**VP, Infrastructure Solutions**

[rkim@anexinet.com](mailto:rkim@anexinet.com)

Mobile: (610) 368-0472



**Jovin Olikara**

**Vice President\CIO – Information Technology**

[jovin.olikara@myphysio.com](mailto:jovin.olikara@myphysio.com) **Phone: (479)430-9766**

Network Remediation

**Statement of Confidentiality**

|  |
| --- |
| This document contains confidential and proprietary information belonging exclusively to Anexinet Corp. The distribution of this document shall be limited to authorized Physiotherapy employees, agents and representatives.  Said Physiotherapy employees, agents and representatives may not knowingly publicize, permit, authorize or instigate disclosure of terms, strategies, or other contents of this document to any person, firm, organization or entity of any type outside the scope of this proposal.  No part of this document may be reproduced or copied without prior written permission from an authorized Anexinet employee.  Anexinet shall not be liable to anyone for special, incidental, collateral or consequential damages that may arise out of the use of this information.  **Anexinet Corp.**  4 Sentry Parkway, Suite 300  Blue Bell, PA 19422 |

[Executive Summary 2](#_Toc431217414)

[Current Environment 2](#_Toc431217415)

[Diagram of the current network 3](#_Toc431217416)

[Diagram of Single Point of Failure 4](#_Toc431217417)

[Requirements 4](#_Toc431217418)

[Technical Requirements 4](#_Toc431217419)

[Proposed Topology 5](#_Toc431217420)

[Proposed Network Diagram 6](#_Toc431217421)

[Design Details and Requirements 6](#_Toc431217422)

[Cisco Nexus 6k/2k core 6](#_Toc431217423)

[Migration 7](#_Toc431217424)

[Phase 1 Cisco ASA 7](#_Toc431217425)

[Phase 1 Network Diagram 8](#_Toc431217426)

[Phase 2 Cisco Nexus 6ks and 2ks 9](#_Toc431217427)

[Phase 2 Network Diagram 10](#_Toc431217428)

[Phase 3 NetScalers 10](#_Toc431217429)

[Phase 3 Network Diagram 11](#_Toc431217430)

[Phase 4 ILO switches 12](#_Toc431217431)

[Phase 4 Network Diagram 13](#_Toc431217432)

[Phase 5 3825 Router Exton 13](#_Toc431217433)

[Phase 6 3825 India Router 14](#_Toc431217434)

[Phase 7 3825 IKS Router 15](#_Toc431217435)

[Phases 5-7 Network Diagram 16](#_Toc431217436)

[Phase 8 2960 Switches 16](#_Toc431217437)

[Phase 8 Network Diagram 17](#_Toc431217438)

[Phase 9 Host Migration 18](#_Toc431217439)

[Phase 10 Decommission 18](#_Toc431217440)

# Executive Summary

Physiotherapy is interested in an upgrade to its network system. Users have reported occasional downtime and slow response times when accessing the network. Physiotherapy wishes to correct these issues through an upgrade to their system, increasing redundancy and capacity.

The proposed solution involves changes to Physiotherapy’s network systems. The current hardware used throughout the network was purchased over a long period of time and uses many different technologies. New hardware will be installed to address these incompatibilities and older technologies. The result will be higher speeds, more reliability, and easier maintenance of networking components. The upgraded hardware will use up-to-date, compatible technologies that will greatly facilitate troubleshooting and maintenance.

In addition to updating the hardware, the proposed solution outlines some changes in the network configuration. These changes will provide greater reliability and security for all users of the Physiotherapy network.

# Current Environment

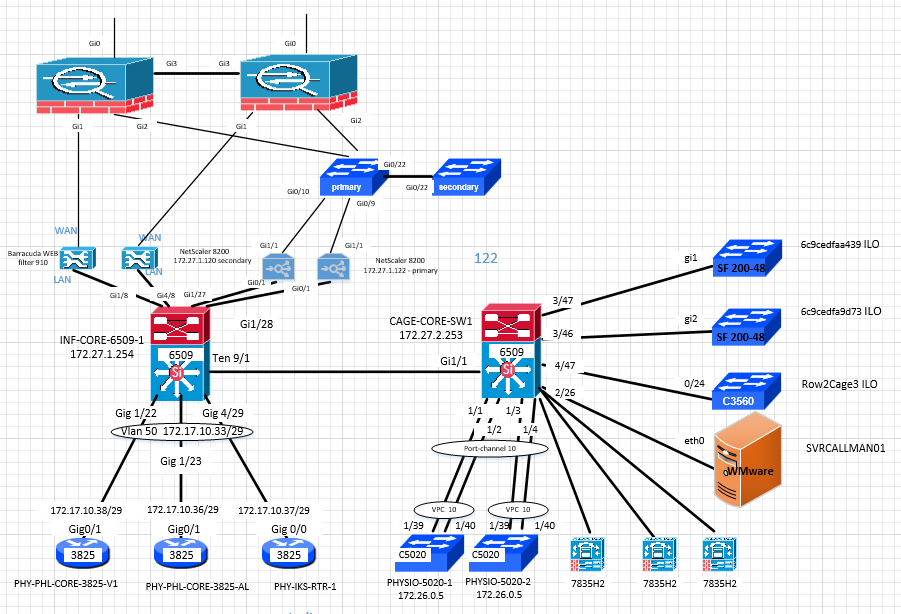
Current core switches do not offer enterprise level of reliability due to older hardware and software versions. The lack of redundancy features and misconfiguration of some key networking technologies lead to longer recovery times and network convergence in the case of an outage.

A single non-redundant connection between the core switches can lead to a long down time for Physiotherapy in case of its failure. Suboptimal routing paths created by duplicate IP addressing configured on the gateways creates slowness for applications and users.

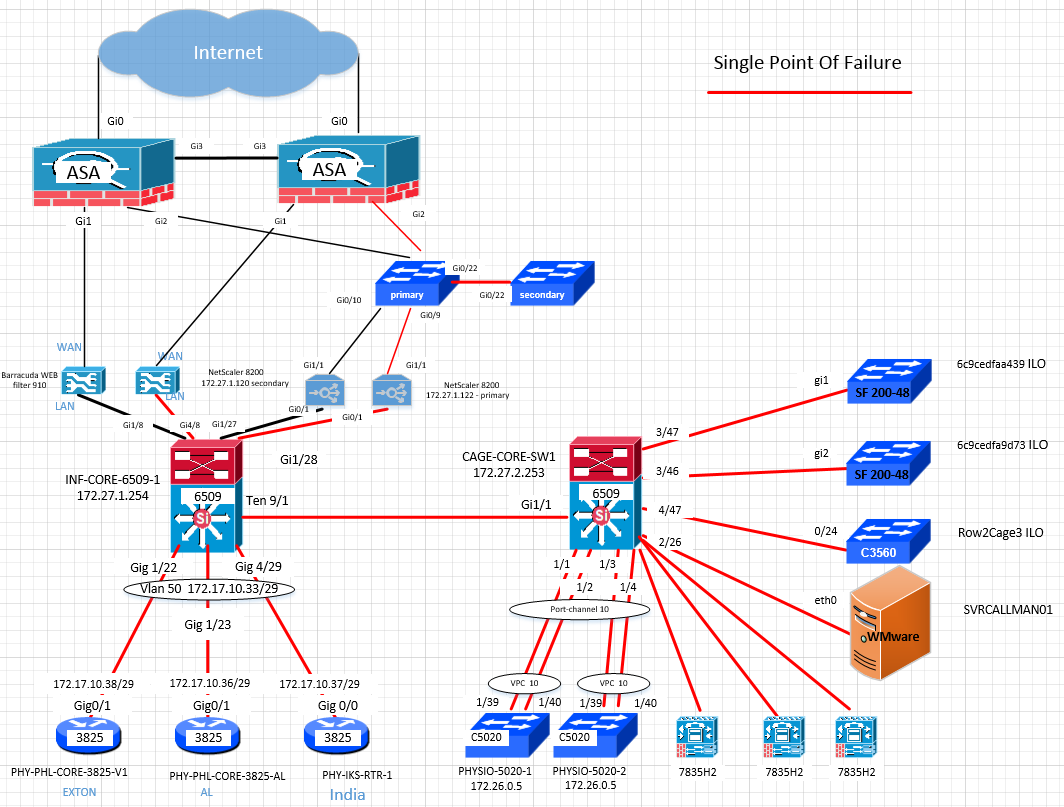
The star topology used in the current network design can lead to a full outage for any single connected device, site, server, or farm. Chassis blade servers that are dual connected to N5020 switches provide an illusion of proper design but actually will be inaccessible in case of core switch failure.

The current Internet environment has only one path to the production network and in case of a core switch outage VPN users will not be able to access any internal resources and internal users will not have access to Internet based applications.

## Diagram of the current network



## Diagram of Single Point of Failure



# Requirements

## Technical Requirements

* Migrate current SunGard Data Center network environment to new Cisco Nexus core.
* Interconnect new Cisco Nexus core switches with multiple links for needed reliability and fault tolerance
* Provide high speed and reliable access for dual connected devices
* Introduce gateway redundancy
* Improve network speed and capacity

# Proposed Topology

Cisco NX-OS Software is a purpose-built data center operating system designed for performance, resiliency, scalability, and manageability will be used on Cisco Nexus switches.

Multiple physical connections between the Cisco Nexus switches together with a Virtual PortChannel (vPC) feature of NX-OS operating system, will be used to create a fully meshed vPC domain with no single point of failure in the data center core.

A vPC will be used on Cisco Nexus switches links that are physically connected to a third device. A vPC will allow dual links to appear as a single PortChannel and provide Layer 2 multipathing which will create redundancy, enabling multiple parallel paths between nodes and traffic load balancing. Alternative physical path must exist for vPC functionality.

Hot Standby Routing Protocol (HSRP) will be implemented on all switched virtual interfaces (SVI) to provide gateway redundancy.

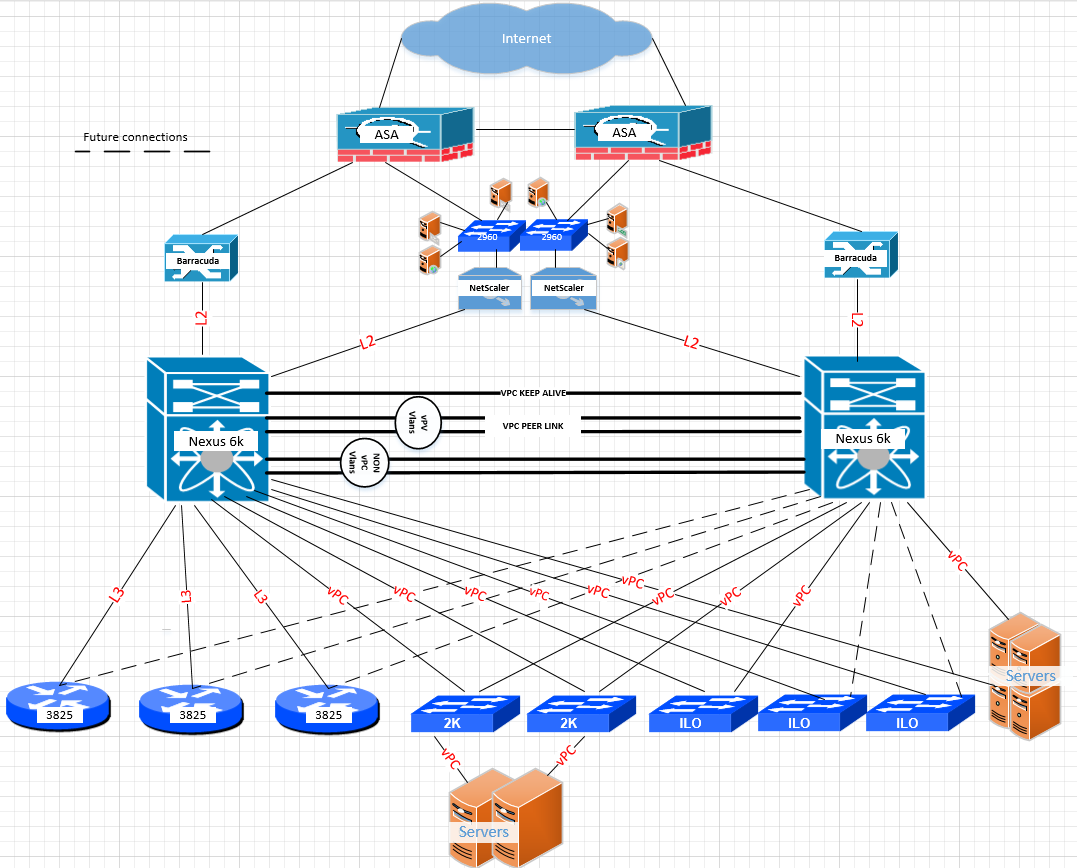
Slow to converge Border Gateway Protocol (BGP) will be replaced with Enhanced Interior Gateway Routing Protocol (EIGRP) between Cisco 3825 routers and Cisco Nexus core to provide fast convergence. Due to current hardware limitations of Cisco 3825 router, only one link will be connected to the core.

Each NetScaler and Barracuda network device interface will be connected to a different Cisco Nexus switch to provide redundancy.

Features Introduced:

|  |
| --- |
| Cisco NX-OS Software |
| Virtual PortChannel (vPC) |
| Hot Standby Routing Protocol (HSRP) |
| Secure Shell (SSH) |
| Enhanced Interior Gateway Routing Protocol (EIGRP) |
| 40 and 10 Gigabit connections |
| Multilink redundancy |

## Proposed Network Diagram



## Design Details and Requirements

### Cisco Nexus 6k/2k core

* Two links between Cisco Nexus 6ks bundled together into port-channel will create a vPC PEER-LINK required for vPC services and increase redundancy. Only vPC Vlans must be allowed on PEER-LINK.
* Two links between Cisco Nexus 6ks bundled together into port-channel for Vlans that are not present on vPC links. NON vPC Vlans must only be present.
* Single link between Cisco Nexus 6k will be in a MGMT VRF to create vPC PEER-ALIVE required for vPC.
* vPC interfaces will be used to interconnect blade chassis, servers, ILO switches, nexus 2ks
* FEX technology will be used to interconnect Cisco Nexus 6k and 2k switches. FEX will provide single management domain for Cisco Nexus 2ks.
* All L3 VLANS (SVIs) will have HSRP configured and will provide gateway redundancy. HSRP MD5 Authentication provides added security and protects against the threat from HSRP-spoofing.
* EIGRP routing protocol will be used in a core to connected L3 EIGRP devices such as 3825 routers.

## Migration

Physiotherapy data center network core migration will consist of 10 phases. Migration will begin with replacement of the current ASA firewalls, then continue with Cisco Nexus switches, NetScalers, ILO switches, Cisco 3825 routers, DMZ switches and other attached hosts with the end goal of decommissioning the current Cisco 6509 and 5020 switches. Each phase will require careful planning, scheduling, and validation. Monitoring time after each phase is also necessary to isolate any potential problems.

### Phase 1 Cisco ASA

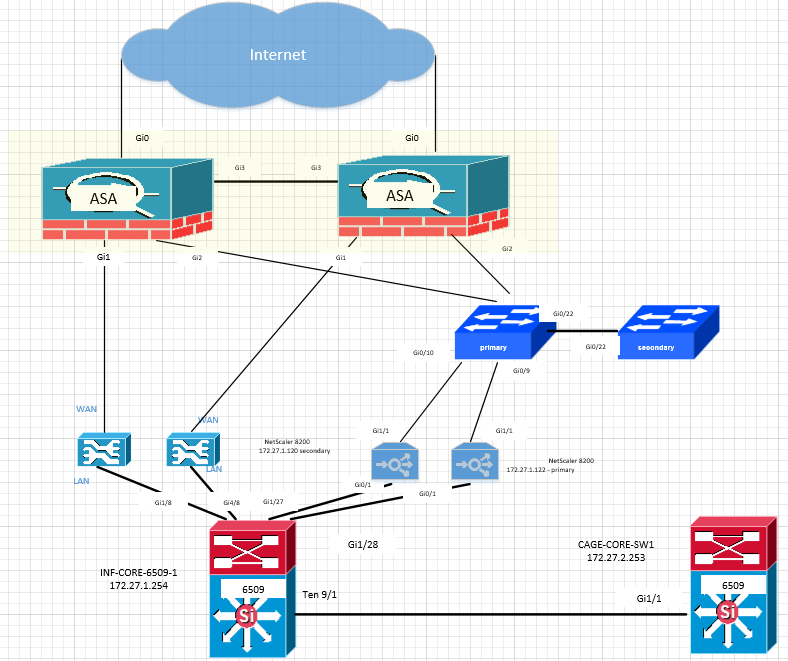
Cisco ASA firewalls provide access for external users and remote sites to internal company resources over Internet by using VPN technology. Configuration, installation, migration and testing are the necessary steps needed for migration. User testing will confirm success of the ASA migration. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure. Estimated time to completion 5 - 6 days.

1. Initial setup 8 hrs
2. Update Firmware
3. Rack and Stack
4. Configuration 16 hrs
   * + - 1. Review current configuration
         2. Implement required changes on new ASAs
5. Pre cutover validation 8 hrs
6. Hardware. ASAs will be connected to power for 5 days before migration.
7. Data path. ASAs will be connected to new Cisco Nexus switches for ICMP testing.
8. Disconnect ASAs from Cisco Nexus switches after validations.
9. Pre cutover USER validations 4 hrs
10. Users VPN access
11. Site to Site VPN
12. Internal users access to internet and DMZ servers
13. DMZ servers access
14. Cutover 4 hrs
15. Move internet connections

(b) Move DMZ connections

1. Move Barracudas connections
2. Post cutover USER validations 4 hrs
3. Users VPN access
4. Site to Site VPN
5. Internal users access to internet and DMZ servers
6. DMZ servers access
7. Back out 2 hrs
8. Move connections back to original ASA
9. After successful validations, ASAs will need to be monitored for 5 business days to proceed to the next phase.
10. Original ASAs can be powered down and removed after 30 days.

#### Phase 1 Network Diagram



### Phase 2 Cisco Nexus 6ks and 2ks

Cisco Nexus 6ks and 2ks switches are the center of new data center design and serve as an aggregation point for servers, hosts, and other devises on a network. Migration will involve multiple steps such as switch configuration, install and testing. After successful user testing of the new Cisco Nexus core environment will proceed to phases 3-9 as scheduled. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

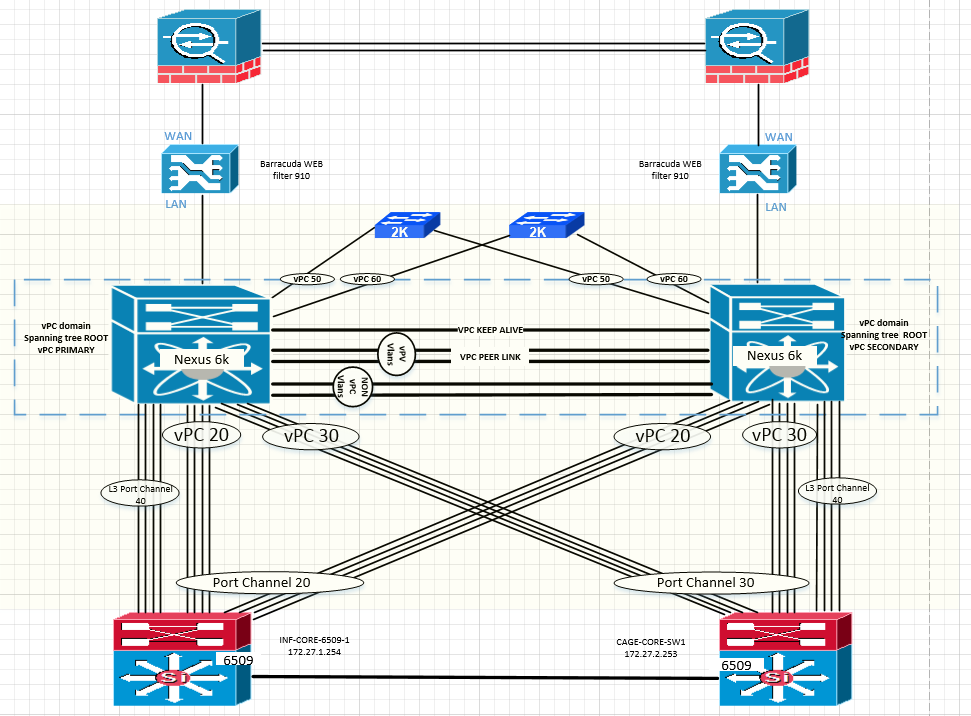
Estimated time to completion 5 - 6 days

1. Initial setup 8 hrs
2. Update Firmware
3. Rack and Stack Cisco Nexus 6ks and 2k.
4. Configuration 16hrs
   * + - 1. Review current configuration
         2. Implement required changes on new Nexus switches
5. Pre cutover validation 8 hrs
6. Hardware. Switches will be connected to power for 5 days before migration.
7. Data path. Will be performed at the time of ASA validation
8. Disconnect ASAs from Cisco Nexus switches after validations.
9. Pre cutover USER validations 4 hrs
10. VPN users access to internal resources
11. Internal users access to Internet
12. Internal users access to internal resources
13. Internal users access to DMZ servers
14. DMZ servers reachability and functionality
15. Cutover 4 hrs
16. Move Barracuda connections

(b) Connect Cisco Nexus switches to 6509s and activate connections

1. Post cutover USER validations 4 hrs
2. VPN users access to internal resources
3. Internal users access to Internet
4. Internal users access to internal resources
5. Internal users access to DMZ servers
6. DMZ servers reachability and functionality
7. Back out 2 hrs
8. Move connections from Barracudas back to 6509
9. Remove connections between Nexus core and 6509 switches
10. After successful validations environment will need to be monitored for 2 business days to proceed to the next phase.

#### Phase 2 Network Diagram



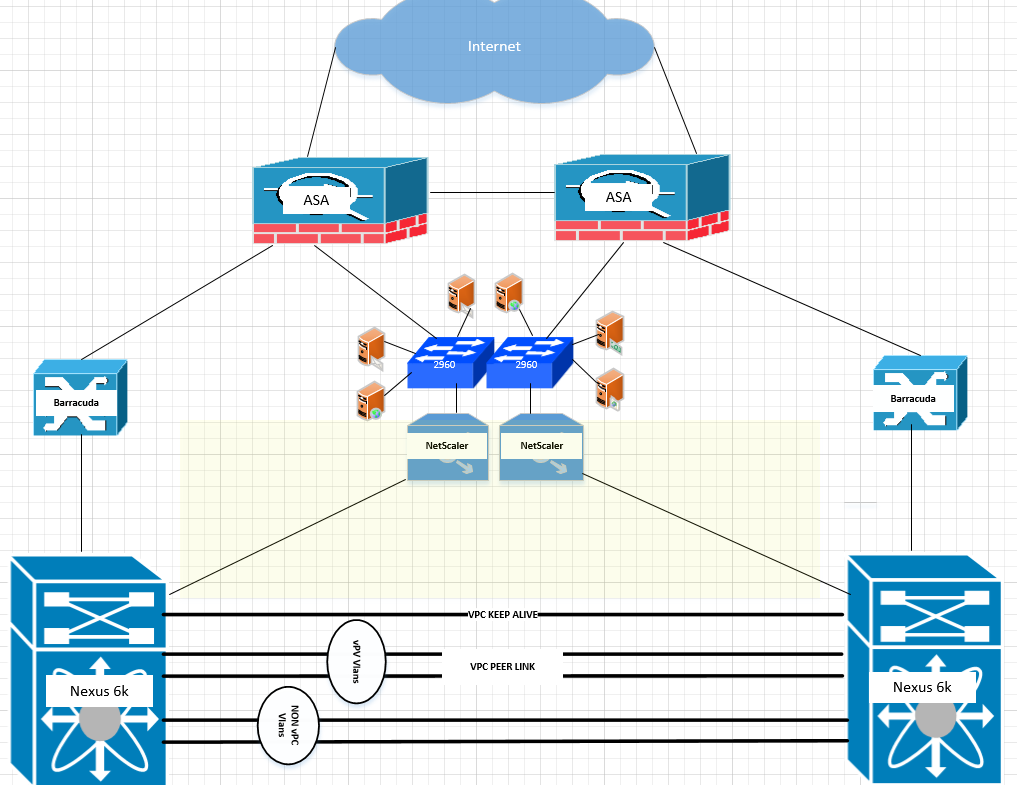
### Phase 3 NetScalers

NetScalers provide load balancing services for servers. Cutover will be completed after new Cisco Nexus core install. This will involve the configuration of Cisco Nexus core; moving cabling from existing 6509 switches and testing. After user testing completes successfully the next migration phase can be started. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

Estimated time to completion 2 - 3 days.

1. Configuration 8 hrs
   * + - 1. Review current configuration
         2. Implement required changes on NetScalers
         3. Implement required changes on Cisco Nexus core switches
2. Pre cutover USER validations 4 hrs
3. VPN users access to internal resources
4. Internal users access to Internet
5. Internal users access to internal resources
6. Internal users access to DMZ servers
7. DMZ servers reachability and functionality
8. Cutover 4 hrs
9. Disconnect NetScalers from 6509 switches
10. Connect NetScalers to Cisco Nexus core switches
11. Post cutover USER validations 4 hrs
12. VPN users access to internal resources
13. Internal users access to Internet
14. Internal users access to internal resources
15. Internal users access to DMZ servers
16. DMZ servers reachability and functionality
17. Back out 2 hrs
18. Move connections from NetScalers back to 6509
19. After successful validations environment will need to be monitored for 2 business days to proceed to the next phase.

#### Phase 3 Network Diagram



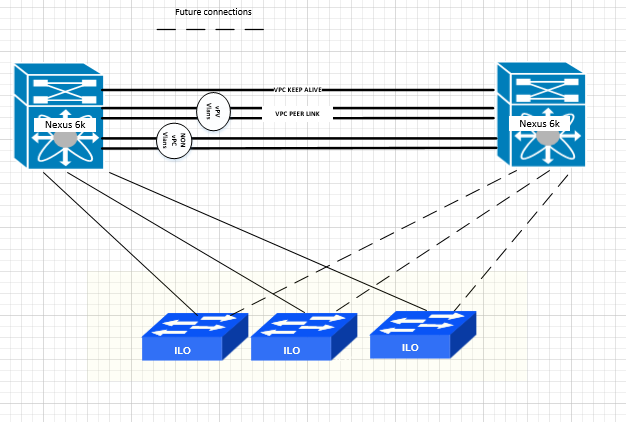
### Phase 4 ILO switches

ILO switches are used to interconnect management connections for other devices. Cutover will be completed after the new Cisco Nexus core install. This will involve configuration of three ILO switches and Cisco Nexus switches, moving cabling from existing 6509 switches and testing. After successful test completion the next migration phase can begin. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

Estimated time to completion 2 - 3 days.

1. Configuration 8 hrs
   * + - 1. Review current configuration
         2. Implement required changes on ILO switches
         3. Implement required changes on Cisco Nexus core switches
2. Pre cutover USER validations 4 hrs
3. Servers owners will validate management access
4. Cutover 4 hrs
5. Disconnect ILO switches from 6509 switches
6. Connect ILO switches to Cisco Nexus core switches
7. Post cutover USER validations 4 hrs
8. Servers owners will validate management access
9. Back out 2 hrs
10. Move connections from Nexus switches back to 6509
11. After successful validations will proceed to the next phase.

#### Phase 4 Network Diagram



### Phase 5 3825 Router Exton

The 3825 Router connecting the Exton office to the SunGard Data Center. Cutover will be completed after the new Cisco Nexus core install. This will involve configuration of the 3825 Router and Cisco Nexus switch; moving cabling from existing 6509 switch and testing. After successful test completion the next migration phase can begin. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

Estimated time to completion 2 - 3 days.

1. Configuration 8 hrs
   * + - 1. Review current configuration
         2. Implement required changes on new Nexus switches
         3. Implement required changes on 3825 router
2. Pre cutover USER validations 4 hrs
3. Access to Internet
4. Access to internal resources
5. Access to DMZ servers
6. Cutover 4 hrs
7. Move Routers connections to Cisco Nexus core
8. Post cutover USER validations 4 hrs
9. Access to Internet
10. Access to internal resources
11. Access to DMZ servers
12. Back out 2 hrs
13. Move connections from Router back to 6509
14. USER validations as in step 2
15. After successful validations environment will need to be monitored for 2 business days to proceed to the next phase.

### Phase 6 3825 India Router

The 3825 India router provides SunGard connectivity for India users. Migration will be completed after the new Cisco Nexus core install. This will involve configuration of the 3825 India router and Cisco Nexus switch; moving cabling from existing 6509 switch and testing. After successful test completion the next migration phase can begin. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

Estimated time to completion 2 - 3 days.

1. Configuration 8 hrs
   * + - 1. Review current configuration
         2. Implement required changes on new Nexus switches
         3. Implement required changes on 3825 router
2. Before cutover USER validations 4 hrs
3. Access to Internet
4. Access to internal resources
5. Access to DMZ servers
6. Cutover 4 hrs
7. Move Routers connections to Cisco Nexus core
8. Post cutover USER validations 4 hrs
9. Access to Internet
10. Access to internal resources
11. Access to DMZ servers
12. Back out 2 hrs
13. Move connections from Router back to 6509
14. USER validations as in step 2
15. After successful validations environment will need to be monitored for 2 business days to proceed to the next phase.

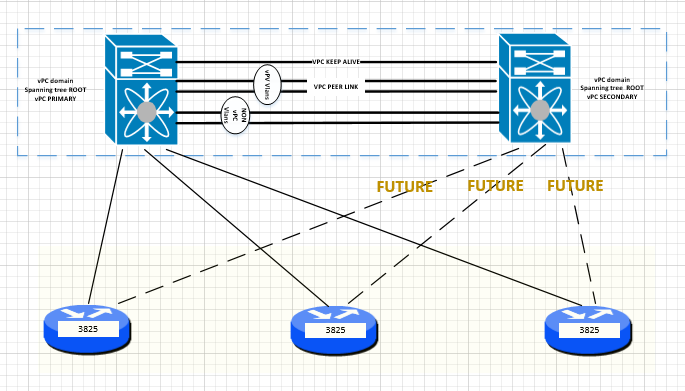
### Phase 7 3825 IKS Router

The 3825 IKS Router migration will be completed after the new Cisco Nexus core install. This will involve configuration of the 3825 IKS Router and Cisco Nexus switch; moving cabling from the existing 6509 switch and testing. After successful test completion the next migration phase can begin. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

Estimated time to completion 2 - 3 days.

1. Configuration 8 hrs
   * + - 1. Review current configuration
         2. Implement required changes on new Nexus switches
         3. Implement required changes on 3825 router
2. Pre cutover USER validations 4 hrs
3. Access to Internet
4. Access to internal resources
5. Access to DMZ servers
6. Cutover 4 hrs
7. Move Routers connections to Cisco Nexus core
8. Post cutover USER validations 4 hrs
9. Access to Internet
10. Access to internal resources
11. Access to DMZ servers
12. Back out 2 hrs
13. Move connections from Router back to 6509
14. USER validations as in step 2
15. After successful validations environment will need to be monitored for 2 business days to proceed to the next phase.

#### Phases 5-7 Network Diagram



### Phase 8 2960 Switches

The 2960 Switches provide network access for servers in the DMZ. Migration will be completed after the new Cisco Nexus core install. This will involve configuration and installation of the new 2960 switches and moving cabling from the existing ASAs and testing. Migration of DMZ servers to new switches will be scheduled at the same time as the 2960 switch install. After successful user validations next migration phase can begin. In a case of unsuccessful user testing, configuration and physical connections will be reverted back to original state. A detailed analyses would be performed and the cutover rescheduled in the event of a failure.

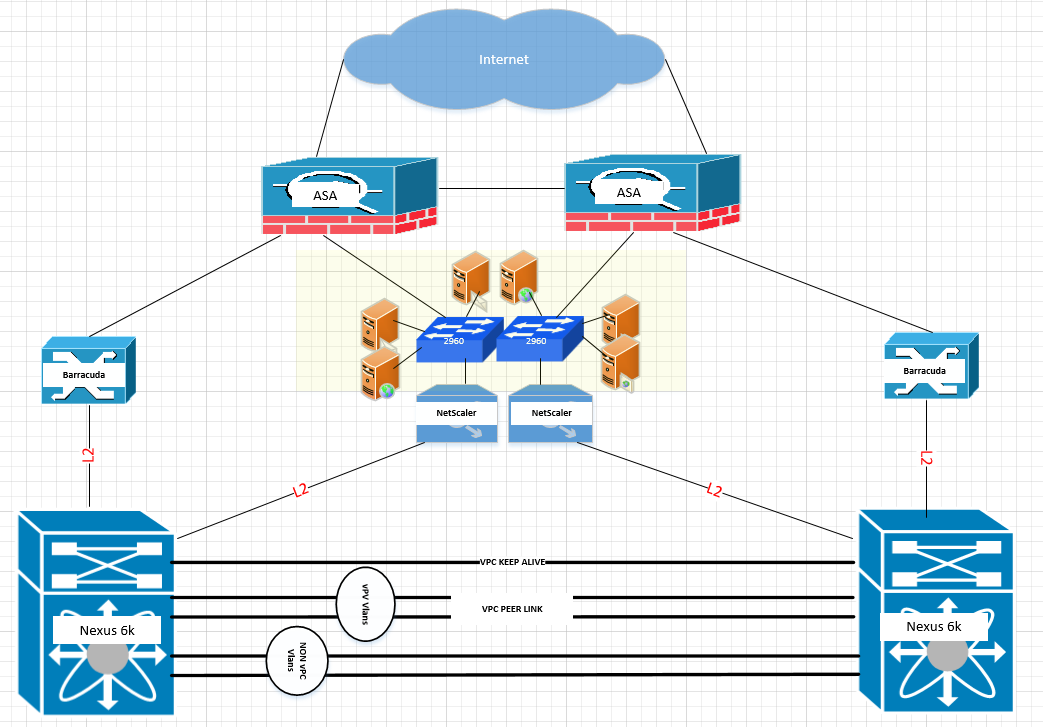
Estimated time to completion 3 - 4 days.

1. Initial setup 8 hrs
2. Update Firmware
3. Rack and Stack
4. Configuration 4 hrs
   * + - 1. Review current configuration
         2. Implement required changes on new DMZ switches
5. Pre cutover validation 4 hrs
6. Hardware. DMZ switches will be connected to power for 5 days before migration.
7. Data path. ASAs will be connected to new DMZ switches for ICMP testing.
8. Disconnect ASAs from DMZ switches after validations.
9. Pre cutover USER validations 4 hrs
10. VPN users access to DMZ servers
11. Internal users access to DMZ servers
12. DMZ servers communication with necessary resources
13. Cutover 2 hrs
14. Move ASA connections

(b) Move all DMZ servers’ connections to new DMZ switches

1. Post cutover USER validations 4 hrs
2. VPN users access to DMZ servers
3. Internal users access to DMZ servers
4. DMZ servers communication with necessary resources
5. Back out 2 hrs
6. Move connections back to ASA
7. Original DMZ switches can be powered down and removed after 30 days of completion the install.
8. After successful validations will proceed to the next phase.

#### Phase 8 Network Diagram



### Phase 9 Host Migration

After phase 1-8 successful completion, scheduled migration of servers, chassis, and remaining devices from the 6509 switches can begin to the new Cisco Nexus core.

1. Configuration per migration 4 hrs dependent on hosts
   * + - 1. Review current configuration
         2. Implement required changes on new Cisco core switches

### Phase 10 Decommission

After phase 1-9 successful completion and complete migration of all devices from Cisco 6509 switches, we can proceed with decommission.Estimated time to completion 1 day.

1. Decommission of Cisco 6509 switches 8 hrs
2. Shut down all links to 6509 switches on Cisco Nexus core.

Monitor for 7 business days

1. Remove configuration used for peering with 6509 switches from Cisco Nexus core.

Monitor for 24 hours

1. Shut down Cisco 6509 switches after successfully running on Cisco Nexus core for 14 days.