University of Colorado
Interdisciplinary Telecommunications Program
TLEN 5700

Concept Definition Document (CDD)

CLONER
CLOud NEtworking at Application LayeR

1.0 Project Information

Project Customers

Name: Jose Santos
Address:
Phone:
Email: jose.santos@colorado.edu

Team Members

Name: Pranit Yadav
Phone: 720-934-3792
Email: pranit.yadav@colorado.edu

Name: Rishikesh Adusumilli
Phone: 720-299-4732
Email: rishikesh.adusumilli@colorado.edu

Name: Pratik Lotia
Phone: 720-935-0225
Email: pratik.lotia@colorado.edu

Name: Sruthi Sneha Jose
Phone: 720-757-8068
Email: sruthi.jose@colorado.edu

Name: Prerna Tripathi
Phone: 720-499-7225
Email: prerna.tripathi@colorado.edu
2.0 Project Description

A software representation of physical hardware is the main goal of virtualization. This is implemented using hypervisors, which are simply software running on top of the physical hardware and are responsible for providing the virtual machines with their own CPU power, memory availability, and an application running environment. Networking functions such as routing, switching, and load balancing can be deployed in these environments as applications which run independently of the underlying network infrastructure. Also, virtualization provides granular security, avoiding the need for physical firewalls and processes such as hairpinning.

Traditional networks consisting of legacy routers and switches incorporate less overhead in the network, thereby efficiently using the available resources. Virtualization is the current trend in the networking field and organizations are more inclined towards it due to the services it provides like abstraction, scalability, etc., which are the needs of the data centers. The advantage of virtualization is that it simplifies networks, enhances productivity, and agility. Efficient transmission is said to take place when the total size of a packet containing the encapsulation layers and the data payload does not exceed the maximum size of MTU carried over the physical link and when the inefficiencies incorporated in this transmission are less.

In virtualized networks, more layers of encapsulation are added to the data packet when it exits the VM and hence the size available for payload decreases. This leads to an increase in the number of frame/packet transmissions. Transfer of packets between VMs in the same server will utilize only internal resources such as processing power, memory, etc. But, when this transfer takes place between VMs on different servers, inefficiencies such as overhead are incorporated. This overhead further increases when additional methods such as tunneling, VPNs, SSL, VXLAN, etc. are used as the number of encapsulation layers further increases and we need to decrease the size of the data payload to allow transmission. This is a serious problem, especially in data centers due to the amount of traffic that flows through it. It leads to increased resource utilization which further leads to increased expenses.

There is a need to evaluate these inefficiencies like overhead that are incurred when virtual network solutions are used. The CLONER project will analyze the extent of these overheads and the degradation of network performance in a virtualized architecture. The project will compare the results with a traditional network. A cost analysis comparing the two approaches will be performed.

The specific objectives of this project have been summarized into three success levels. The CLONER team will fulfill all the below mentioned levels for the highest success.

**Level 1:**
Create a virtual environment connected to external layer 2/layer 3 devices. An application like VoIP will be run on top of virtualization technologies such as VMware NSX. The goal is to implement a basic scenario to exchange traffic between VMs, servers, racks, using the emulated virtual environment. The same task will be executed in a traditional physical
network. The packets exchanged in both the environments will be analyzed and inefficiencies such as overhead, fault tolerance, etc. will be compared.

**Level 2:**
Extending the objectives in Level 1, additional applications such as bulk data, video streaming, etc. will be incorporated. All these applications will run on top of the same virtual network and traditional physical network that would be used in Level 1. Similar comparisons will be made at this level with the focus on application inefficiencies.

**Level 3:**
Extending the objectives in Level 2, a virtual network using advanced technologies like SSL VPN, VXLAN, different hypervisors, etc. will be emulated. Applications such as VoIP and bulk data will be run on top of this network. Factors such as overhead will be analyzed and the results observed will be compared with those obtained from a traditional physical network. A performance comparison between the virtual network and the traditional network will follow.

The Functional Block Diagram (FBD) and Concept of Operations (CONOPS) are shown in Figures 1 and 2 below to illustrate the vision and the scope of the CLONER project.

![Figure 1: Functional Block Diagram for CLONER](image-url)
**Functional Description**

The tasks of this project include an in-depth analysis of factors such as overhead, processor utilization, resource utilization and fault tolerance, during data transfer in a virtual network environment and comparison of these factors with those in a traditional network environment. A virtual computing environment will be set up with virtual machines hosted on one or more hypervisors. Virtualization technologies like VXLAN, VMware NSX, and SSL VPN will be implemented in this environment, and communication between the hosts (servers) and virtual machines will be enabled through logical switches, firewalls, routers and load balancers. To monitor and analyze the network, network taps will be inserted at defined points and the traffic between network nodes will be observed through packet analyzer tools. Network traffic in a traditional network environment will also be monitored and analyzed in a similar manner. After analysis and observations, the data from both the networking environments will be compared and the results will be documented.

![Figure 2: Concept of Operations for CLONER](image)

In order to ensure the success of this project, it is important to define elements that are critical for this project. The critical project elements (CPEs) that the CLONER team must consider are stated below.

**Technical C.P.E:**

**CPE.1.1:** Identify different performance parameters to measure and analyze the efficiency within different network environments (Physical and Virtualized networks). Initially, all required performance parameters to be measured should be identified and documented to correctly plan, measure, analyze, and compare the efficiency of both the
physical and virtual environments. This initial step will provide an accurate direction for the project.

**CPE.1.2:** Identify inventory, design and set up a physical and a virtual environment to run real-world simulated tests to measure parameter values. Physical hardware, software, applications, topology design, and environment setup should be carefully planned, designed and implemented to measure parameter values required by running real-world simulated tests aimed to analyze and compare physical and virtual network environments.

**CPE.1.3:** Emulate applications like VoIP, and video streaming resembling real-world scenarios using virtual and physical environments. Applications are required to test and gather parameter values such as overhead, fault tolerance, etc. Applications can be used to simulate real-world situations aimed at carefully measuring the values to analyze the advantages or disadvantages of the environments in question.

**CPE.1.4:** Analyze the simulated traffic and compare inefficiencies such as overhead, fault tolerance, etc. in traditional and virtualized networks. Utilize packet captures in different locations on traditional and virtualized topology to measure and compare values such as overhead, fault tolerance, etc. Packet analyzing tools such as Wireshark or tcpdump will be used depending on the targeted capture environment.

*Logistical C.P.E:*

**CPE.2.1:** Obtain required physical hardware, virtualization tools, and software applications to deploy on local machines. Acquire hardware components, virtualization tools, software applications required to deploy the topology for measurements, analysis, and comparison between physical and virtual environments.

*Financial C.P.E:*

**CPE.3.1:** Evaluate Operational Expenditure (OPEX) and Capital Expenditure (CAPEX). Evaluate Operational Expenditure (OPEX) involved in operating hardware and virtualized systems and evaluate Capital Expenditure (CAPEX) involved in procuring physical hardware, software, and virtualization tools.

### 3.0 Design Requirements

Functional requirements (FNC.X) as well as the design requirements (DES.X.X) are specified below to improve the clarity of the CLONER project.

**FNC.1** The architecture required for generating, capturing and analyzing data packets shall be implemented by CLONER.

**DES.1.1** Traffic shall be generated by using various applications.

**DES.1.1.1** IT Operation specific data from applications such as VoIP, web servers, file sharing, and video shall be used.

**DES.1.2** Comparison of packets captured shall be made in both traditional as well as virtualized networks.
**DES.1.2.1** Packet sniffing tools shall be used to capture packets for analysis.

**DES.1.3** Port Mirroring and Route IP Traffic Export (RITE) methodologies shall be implemented for capturing packets.

- **DES.1.3.1** Full packet capture, Netflow as well as Syslog messages shall be used for monitoring traffic.
- **DES.1.3.2** Netflow data can be used to get sampled information about packet streams.
- **DES.1.3.3** Syslog messages shall provide all types of logs, errors and warning messages.

**FNC.2** The CLONER shall be platform-agnostic.

**DES.2.1** CLONER shall implement and test the performance of multiple network virtualization platforms.

- **DES.2.1.1** Widely used platforms such as VMware NSX, Openstack shall be used for implementation.
- **DES.2.1.2** Type 1 hypervisor technologies such as ESXi and Hyper-V shall be employed to host virtual machines.

**DES.2.2** Servers compatible with the selected network virtualization platform shall be used.

- **DES.2.2.1** Dell servers supporting VMware NSX, Openstack, Hyper-V platforms and Arista switches supporting implementation of VXLAN shall be used.

**FNC.3** The CLONER shall incorporate multiple virtualization technologies

**DES 3.1** VXLAN, micro-segmentation, Layer 2 and Layer 3 overlay, VPN overlay and other virtualization features shall be used to build the virtual architecture.

**FNC.4** The CLONER shall be scalable across large traditional and virtualized network environments.

- **DES.4.1** Environments dealing with exchange of packets within VMs on the same server, multiple servers, data centers shall be emulated.
- **DES.4.2** The CLONER shall be used to monitor traffic in various network environments.
  - **DES.4.2.1** A variant of real-world data center environments shall be reproduced/created.

### 4.0 Key Design Options Considered

The basic element of the CLONER project is a system for analysis and comparison of different virtualization technologies. To achieve best results, consideration of different design options and determination of factors influencing the design options is imperative. The main design component for this project is the network virtualization platform which lays the foundation for the system. Different virtualization platforms such as VMware NSX, Openstack and Hyper-V support different network overlay features. The CLONER project requires
implementation support for virtualization technologies such as Micro-segmentation, VXLAN and SSL VPN, to perform analysis and comparison of factors like overhead and processing power. Accordingly, an extensive research was done to determine the features and capabilities in these network platforms.

The selection criteria were based on factors such as hardware support and availability, licensing, network overlay features supported, industry acceptance and familiarity, micro-segmentation support, IPv6 support and version updates in the industry. The technical specifications of various virtualization technologies that would pave us a path for selection are stated below.

**VMware vSphere**

VMware vSphere, a software suite provided by VMware, consists of ESXi, vCenter server and vSphere client. ESXi is the hypervisor server on which virtual machines are hosted. vCenter is a centralized management server which accesses and manages ESXi hosts. vSphere client, a software installed on an administrator’s machine, can access the vCenter servers and thus manage the ESXi hosts.

The main features provided by VMware vSphere suite are:

1. **Network overlays**: VMware supports all the network virtualization components that our project needs. Networking technologies supported by VMware vSphere include Virtual Distributed Switch (vDS), Microsegmentation (using VMware NSX), VXLAN, Layer 2 Tunneling Protocol, GRE tunneling and SSL VPN. Also, advanced features like Network traffic shaping, NIC (Network Interface Card) teaming, provision of dedicated default gateways for different services, ERSPAN protocol and Multicast Snooping are supported by this software suite.

2. **vMotion**: This feature facilitates movement of a Virtual Machine (VM) from one host to another [1].

3. **High Availability (HA)**: When an ESXi host fails, the HA detects it and boots the failed host’s VMs on another available host. A failed VM is restarted by default on its own host [1].

4. **Dynamic Resource Scheduling (DRS) and Distributed Power Management (DPM)**: DRS ensures load balancing between hosts, especially during peak hours. DPM saves power on a host by evacuating VMs to other hosts during its off hours [1].

5. **Support for IPv6**: VMware vSphere supports IPv6 addressing along with IPv4. Additionally, VMware vSphere is supported by Dell servers, especially PowerEdge R430 Rack Server (the server available in our lab).

The hardware requirements for VMware ESXi (version 6.0) [2] are as follows:

1. The host machine should have at least 2 CPU cores.
2. Among 64-bit x86 processors, only the ones released after September 2006 are supported.
3. Minimum required physical RAM is 4 GB. It is recommended that production environments have at least 8 GB of RAM.
4. 64-bit VMs are supported only if hardware virtualization support is enabled on x64 CPUs.
5. Only network adapters models with one Gigabit or faster rates are supported.
OpenStack

OpenStack is an open source cloud operating system used to control and manage networking and storage resources in a data center through its user-friendly web interface. The basic architecture of OpenStack has three logical components: Control, Network and Compute [3]. OpenStack web interface, Application Programming Interface (API) services, database and message bus are run by the Control. Network components are managed by the Network tier and virtualization hypervisor components are run by the Compute tier. Typically, networking and control services reside on the same server and compute services run on another server.

The several components that make up the basic architecture of OpenStack are:
1. Dashboard, the web interface component
2. Keystone, the identity management component
3. Glance, the image management component
4. Neutron, the network management component
5. Nova, the instance management component
6. Cinder, the block storage management component
7. Swift, the object storage management component
8. Ceilometer, the telemetry component
9. Heat, the orchestration component

All these components combine to form the OpenStack cloud environment.

Neutron, the networking management component manages the virtual networking services in OpenStack [3]. Open vSwitch, which is present in OpenStack by default, orchestrates the underlying virtual networking services [3]. The Neutron API provides the flexibility to integrate technologies and services such as Microsegmentation, VXLAN, GRE tunneling and SSL VPN. For example, VMware NSX can be integrated in an OpenStack environment by installing NSX plugin for Neutron. Other services provided by OpenStack include load balancing using a service known as HAProxy and High Availability (HA) using Pacemaker service [3]. The Pacemaker service monitors the networking services, resources and file systems and can move services from one node to another during times of failure.
Other benefits that OpenStack provide are, support for IPv6 and compatibility with Dell PowerEdge R430 Rack Server.

The hardware requirements for OpenStack are as follows:
1. Compute nodes should have 64-bit x86 processors with Intel 64 or AMD64 CPU extension support and AMD-V virtualization extension support. Minimum required memory is 2 GB RAM and minimum available disk space is 50 GB. NICs should support at least 2x1 Gbps rates.
2. Network nodes require a minimum of 2 GB RAM, 10 GB of available disk space and 2x1 Gbps NICs.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>No licensing requirements since OpenStack is an open source software.</td>
<td>Number of troubleshooting documents and KBs available for OpenStack is comparatively less.</td>
</tr>
<tr>
<td>Supports all major network overlay features.</td>
<td></td>
</tr>
</tbody>
</table>

Hyper-V

Hyper-V is a virtualization platform provided by Microsoft for server and network virtualization. The hypervisor comes along with Windows Server editions but its installation is optional (depending on whether administrators plan to build their infrastructure on top of Hyper-V). The standalone version of Hyper-V, called Microsoft Hyper-V Server has two essential components: Windows Server core and a PowerShell command line interface (CLI) [6]. Hypervisor configuration and OS settings can be administered through the CLI. Installation of additional services such as Hyper-V manager eases the management and monitoring processes in the system.

For network virtualization, Microsoft provides Hyper-V Network Virtualization (HNV) along with Hyper-V [7]. There are two implementations available for HNV: HNVv1 and HNVv2 [7]. HNVv1 has basic networking features, with configurations and settings managed through WMI (Windows Management Instrumentation) and Windows PowerShell [7]. HNVv2 is a virtual networking platform integrated with Microsoft Azure Stack [7]. The isolation between virtual networks is gained using NVGRE (Network Virtualization Generic Route Encapsulation) or VXLAN encapsulation [7]. Additionally, HNV supports the implementation of Micro-segmentation, Layer 2 and layer 3 tunneling methods and SSL VPN. Also, IPv6 addressing is supported by all the versions of Hyper-V Server.

The server available in our lab, Dell PowerEdge R430 Rack Server, supports Hyper-V.

The hardware requirements for Hyper-V installation include:
1. SLAT (Second Level Address Translation)-enabled 64-bit processor [8].
2. CPU support for Intel Virtualization Technology or AMD Virtualization [8].
The CLONER project would make use of different virtualization platforms and network devices available in the lab. Also, different applications such as VoIP, video and data would be used for analyzing the inefficiencies incorporated when they are implemented over a virtualized network. There involves a trade-off between the network virtualization platforms that the CLONER team would be selecting based on different networking features they support. The following table lists the various parameters that helps the CLONER team to enforce selection of a particular platform.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Weight</th>
<th>Scale (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Hardware Requirements directly affect the performance of network with respect to speed, processing power, etc. thus making it an important parameter to consider. An ideal hardware that would lead to the success of this project shall not only provide sufficient amount of CPU, Core, RAM, etc. but also would be compatible with the virtualization platform.</td>
<td>0.1</td>
<td>1: indicates high resource requirements of the tool 5: indicates efficient usage of resources</td>
</tr>
<tr>
<td>Licensing</td>
<td>This defines the product license of the software/tool required for network virtualization. A tool can be either open source, proprietary or a freemium product for educational purpose. This is the most important parameter for CLONER considering the period for which it holds valid.</td>
<td>0.2</td>
<td>1: indicates costly proprietary license 5: indicates open source version availability</td>
</tr>
<tr>
<td>Support</td>
<td>The CLONER team can face several hurdles while implementing an enterprise architecture using virtualization tools since it involves usage of several network devices from different manufacturers like Arista, Dell. This parameter defines the technical support levels received from the tool manufacturer.</td>
<td>0.05</td>
<td>1: indicates no support from the company 5: indicates quick and constructive</td>
</tr>
<tr>
<td>Network Overlay features</td>
<td>This defines the compatibility and ease of implementation of network overlay features such as Layer 2 Tunneling Protocol, GRE Tunnels, VPN/SSL support, VXLAN &amp; micro-segmentation. This decides the type of network features and traffic which can be used inside the architecture.</td>
<td>0.2</td>
<td>1: indicates low compatibility and difficulty in implementation of features 5: indicates high compatibility and ease of implementation</td>
</tr>
<tr>
<td>Industry Acceptance &amp; Familiarity</td>
<td>Often, forums on the internet are used to post configuration problems and receive answers from those who have already implemented it. A tool widely used in the industry will have proper documentation and peer support. Acceptance of tools depends on industry-specific applications and compatibility with existing infrastructure.</td>
<td>0.1</td>
<td>1: indicates low rate of industry acceptance 5: indicates high rate of industry acceptance &amp; familiarity</td>
</tr>
<tr>
<td>Micro-segmentation</td>
<td>Micro-segmentation feature enables the tool to divide the topology into logical elements and manages security policies. It integrates security into virtualized networks without the necessity of a hardware based firewall. This will help the CLONER project evaluate how secure the architecture is.</td>
<td>0.15</td>
<td>1: indicates lack of micro-segmentation feature 5: indicates proper micro-segmentation feature available</td>
</tr>
<tr>
<td>Version Updates</td>
<td>This defines how frequently bug fixes of the tool are done and inclusion of additional new features which can potentially help for better analysis</td>
<td>0.05</td>
<td>1: indicates slow version updates 5: indicates regular version updates and bug fixes</td>
</tr>
</tbody>
</table>
IPv6

<table>
<thead>
<tr>
<th>Parameters</th>
<th>VMware NSX</th>
<th>Openstack</th>
<th>Microsoft Hyper-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Requirements</td>
<td>0.1</td>
<td>3.5</td>
<td>2</td>
</tr>
<tr>
<td>Licensing</td>
<td>0.2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Support</td>
<td>0.05</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Network Overlay features</td>
<td>0.2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Industry Acceptance &amp; Familiarity</td>
<td>0.1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Micro-segmentation</td>
<td>0.15</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Version Updates</td>
<td>0.05</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>IPv6</td>
<td>0.15</td>
<td>3</td>
<td>2.5</td>
</tr>
<tr>
<td>Total</td>
<td>1.0</td>
<td>3.25</td>
<td>2.83</td>
</tr>
</tbody>
</table>

Table 2: Trade study for selection of virtualization platform

6.0 Selection of Baseline

We selected VMware and OpenStack hypervisor technologies as our project baseline based on major contributing factors like licensing, hardware support, and the network overlay features. These technologies are awarded a high trade study score due to the above-mentioned factors. The easily available student licenses make these better than the other hypervisor technologies, and also reduces the cost of obtaining them. Hardware support such as Dell, Arista, Cisco, ASA, and vMX available in the laboratories make VMware and OpenStack more preferred over the other hypervisors. Specialized hardware is required to perform the various tests to measure and understand the performance of a network, either virtual or traditional, and compared to other hypervisors in the market, VMware and OpenStack facilitate all our required network overlay features such as L2 overlay, L3 overlay, VPN overlays, VXLAN, micro-segmentation, and IPv6.

CLONER aims at analyzing traditional and virtualized environments to gather data regarding inefficiencies such as overhead, latency, fault tolerance, etc. This project analyzes the extent
of these overheads and the degradation of network performance in a virtualized architecture and compares the various required network overlay features of the traditional and the virtualized networks to further elucidate the features and limitations of both environments. According to our project, an ideal hypervisor should facilitate all these network overlay features to achieve the desired goal. VMware and OpenStack perfectly satisfy these requirements.

This project will compare the performance results of a virtualized network with a traditional network and will derive the cost analysis by comparing the two. Industry acceptance is another important contributing factor in selecting a hypervisor for our project. An industry accepted hypervisor technology will help us gather more information about a particular technology and will help us better derive the cost analysis. VMware has a good industry acceptance score of 4 in the trade study compared to other hypervisor technologies and immediately followed by OpenStack with a trade study score of 3.

On reviewing the trade study of various hypervisor technologies, VMware and OpenStack are the clear winners with scores 3.25 and 2.83 on 5 respectively. Microsoft Hyper-V closely follows OpenStack with a difference of only .08 between the two. VMware has the best score also because of available hardware and network overlay features support. OpenStack is the next best hypervisor suitable for our project considering the same major contributing factors.

We finalized VMware and OpenStack as the hypervisor technologies to measure, compare and analyze the performance and inefficiencies such as overhead, latency, fault tolerance, etc. The complete project setup would include several other components to drive the analysis. One or more hypervisors as selected by our observations and trade study will be used to build a virtual environment and we will incorporate different technologies such as VMware NSX, SSL VPN, and VXLAN. We will use hardware devices such as routers, firewalls, switches, and load balancers to enable communication between hosts present on individual servers. Network telemetry will be performed by implementing packet sniffing points using packet analyzing tools at required locations on the complete network. This same approach will be followed to gather data from the traditional network setup also for documentation, comparison, and to analyze the performance and efficiency between the two environments.

7.0 Resources


