# CS551: Homework 2

1) Consider data center networking. One of the challenges arises from the need to respond quickly when reconfiguring the network after an outage occurs.

a) Conventional routing protocols do help recover after an outage. Describe how such protocols work and give the name of the property that characterizes their approach.

Data center networking uses conventional routing protocols like OSPF (Open Shortest Path First) and BGP(Border Gateway Protocol). The OSPF makes use of a routing table storing the best path for the packet using BGP. The BGP and the OSPF get the shortest path between the destination of the data center and the internet. They save these forwarding rules in switches and whenever the switch fails, they dynamically change the routing table to use a different route for the packet. This process is called dynamic routing and convergence is the property.

b) Why aren't conventional routing protocols sufficient in a data center?

Conventional routing protocols aren’t sufficient at times in a data center since they take approximately 10 seconds to converge. They adapt after the change has occurred and this makes the latency high. Hence this isn’t enough in a data center.

c) What is the name of an alternative method used to configure and reconfigure network switches?

The alternative method used to configure and reconfigure network switches is called Software Defined Networking (SDN). It makes use of a controller and allows monitoring and configuring of these switches.

2) a) What do switches that support P4 offer that conventional switches do not?

Switches that support P4 are more powerful since instead of conventional match-action rules and criteria, these switches have a processor that allows more programmability. Using the P4-enabled switch allows the controller to download custom programs directly into the switch. This helps in having an adaptable switch that can handle VXLAN encapsulation and de-encapsulation or packet encryption on the fly for security purposes.

The addition of a chip and the use of P4 provide these switches advantages that go beyond basic flexibility. The central controller is not overloaded with exceptions making these switches way better. The tasks can be handled locally in the switch which also improves speed and ensures scalability.

b) Consider the networking technologies used in a data center and find an example of a technology that could benefit from having P4 switches.

VXLAN (Virtual Extensible LAN) is a networking technology in data centers where we layer virtual networks on top of real networks, addressing scalability concerns in big cloud computing installations. P4 switches can help this VXLAN's encapsulation and de-encapsulation processes. Their programmability enables customized VXLAN management, including improved load balancing and faster encapsulation operations. We can also use these P4 switches for detecting anomalies in VXLAN flows ensuring faster incident responses.

3) a) What are the advantages of using Docker containers compared to virtual machines?

As we know the biggest disadvantages of a VM are startup overhead and processing overhead. Docker solves these problems since Docker containers can start up in seconds while VMs take around 10 seconds to start since they have to boot up an entire OS, as given in the slides. The second biggest advantage is Docker containers have less processing overhead since they share the host OS, rather than needing their OS. This also improves speed and efficiency.
Apart from these 2 advantages, Docker containers encapsulate all the dependencies and the application in a single unit making it easier to move across different environments. Lastly, many containers can run simultaneously without the overhead of multiple OS instances.

b) What are the disadvantages?

Some disadvantages include handling persistent data storage. They manually have to be started and stopped which might make it more complex than VM's. The other biggest challenge is security. Since Docker containers share the same OS kernel, a vulnerability in the kernel might expose all your containers as well endangering data in containers. VMs provide isolation of data, even on a hardware level. So, with that aspect, VMs provide better isolation than Docker containers don't. Also, some public containers might have vulnerabilities, as we saw in our assignment, which might bring malicious content into our systems if not monitored correctly.

4) Consider a containerized application writing files to the container's file system. Suppose either the container or the physical server running the container crashes while the container is running.
a) Will any of the data be preserved or will it all be lost? Explain.

**Data will be lost in both cases.**
When it comes to the container crashing, the server will still be running. When we restart the container, the data will be lost since the containers are ephemeral. The file system exists only up until the point when the container is running.
Now, when we look at the other case of the server crashing, the same rule will apply since when the servers crash the container will also stop and upon restarting the container will lose the data.

b) Answer the same question for data written to an object store.

An object store like Amazon S3 manages data like objects and **data will not be lost if we use this object store.**
If the container crashes, data is already written to the object store which provides isolation from the container and the server. This is an external storage space that is not tied to any file or operating system.
If the server crashes, similarly, the data will not be lost, and it will be preserved since we will be able to retrieve the data from the object store by restarting the server/container.

5) a) Can a NAS system store arbitrary digital objects? Explain.

**Yes**, NAS(Network Attached Storage) can store arbitrary digital objects since it is essentially a remote file system at a data center. It is very flexible as it supports all standard file types which can be represented in binary. This allows diverse data storage in terms of arbitrary digital objects and the storage system groups these objects into buckets similar to folders or directories.

b) If a data center has both NAS and SAN available, why would an object store also be needed?

If a data center has both NAS and SAN, then all traditional storage needs are met where even an arbitrary digital object can be stored. This can be done through a remote file system, but it depends on the particular OS. File translation to make them compatible with another system may result in unexpected changes. Neither SAN nor NAS supports the scale-out approach, which is critical for dealing with large data sets. This constraint, along with the dangers associated with content change during conversion, makes object storage also needed, which provides scalability while maintaining data integrity across platforms.

6) Are there any circumstances in which SAN storage is better than NAS storage? Explain.

   There are many circumstances where SAN is better than NAS. Since NAS doesn't suffice for VM disk storage, SAN can work with any VM. This makes SAN better for VM storage since it can provide VMs with virtual disks of arbitrary sizes. Furthermore, a SAN can act as a boot device for VMs allowing them to boot an OS. Lastly, the quickness with which a SAN system converts a client's block number to a physical disk position is better than a NAS. This guarantees peak performance, particularly in data-intensive applications. Another advantage is the utilization of storage capacity, as SAN configurations leave no unutilized gaps on traditional drives. This is unlike some NAS file systems, which may leave fragmented or empty regions. So, the main circumstances are: High-Performance Applications, Virtualized Environments, Uniformity when it comes to different OS, and efficient storage utilization.

7) When cloud tenants discuss the use of automation, they usually think of automating the applications their company uses internally or services the company sells to its customers. What are the costs and benefits of applying automation at each of the 5 levels of the model in the textbook?

   **Level 0: No Automation**
   This is characterized by a complete lack of automation, and it requires a high manual effort for every operation, which inevitably increases labor costs. The absence of automation leads to prolonged times to detect, analyze, and rectify problems causing increased expenditures. This level also carries a higher likelihood of human errors, creating inconsistencies and elevating costs further. However, the benefit is in direct human oversight for all tasks, preventing machine errors, and offering flexibility to manage unforeseen situations that machines can't.

**Level 1: Automated Preparation and Configuration**
Level 1 includes automation in preparation and configuration, mitigating the costs of initial setup and implementation of automation tools, along with the costs involved in training staff to use them. The benefits at this level are faster and more consistent configurations, reduction in human errors during setup, and considerable time savings in performing repetitive configuration tasks.

**Level 2: Automated Monitoring and Measurement**
At Level 2, automation tends to be monitoring and measurement, imposing investment in advanced tools and systems, and training staff to interpret their outputs. The advantages at this level are significant; faster problem detection, continuous environmental health checks, and enabling decision-making which is backed up by data due to constant checks of system parameters.

**Level 3: Automated Analysis of Trends and Prediction**
Level 3 involves automated analysis of trends and predictions. This level involves integration costs for advanced analytics and possibly machine learning systems and requires expertise in data analytics. The benefits are many; issues can be detected proactively before getting worse, allowing for ideal resource planning and capacity management, and providing an improved understanding of system behavior over time.

**Level 4: Automated Identification of Root Causes**
Level 4 includes the automation of identifying root causes. It needs advanced tools and systems, and also ongoing training to stay up to date on tools. The benefits at this level are lots; troubleshooting time is drastically reduced, identification of problems is consistent and objective, and better problem identification.

**Level 5: Automated Remediation of Problems**
At Level 5, automation reaches a point where it can fix problems automatically. This stage involves the integration of complex automation workflows and carries potential risks if the automation goes wrong or applies incorrect remedies. It requires a continuous review and update of automation rules. The benefits are many, with reduced downtime, significant cost savings due to lesser manual intervention, and the consistent application of solutions across different environments.

8) a) When cloud providers discuss the use of automation, what do they generally think of automating?

1. **Creation and Deployment of New Virtual Resources**:
   - Setting up new virtual machines and containers.
   - Creating virtual storage facilities, including virtual disk images like SAN and NAS.

2. **Workload Monitoring and Accounting**:
   - Measuring the load on servers, storage devices, and networks, tracking each tenant's use of resources, and calculating the associated charges.
   - Identifying areas of high demand or load.

3. **Optimizations**:
   - Fine-tuning both initial deployments and any subsequent modifications.
   - Reducing the latency between applications and storage.
   - Diminishing network traffic and migrating virtual machines, either to boost performance or cut down on power consumption.

4. **Safety and Recovery**:
   - Planning regular backups of tenant data.

- Keeping an eye on servers, network equipment, and storage equipment. This also includes spotting failures in redundant power supplies and disks in RAID systems.
- Automated rebooting of virtual machines and containers and auditing machines.

5. **Software Update and Upgrade**:
    - Ensuring applications and operating system images are kept up to date.
    - Upgrading to the latest software releases as specified by a tenant.
    - Helping in the continuous deployment of tenant applications.
6. **Administration of Security Policies**:
    - Implementing network security throughout the data center.
    - Protecting each tenant's data and computational tasks.
    - Offering management tools for secrets and encryption keys.

b) Give an example of how providers use automation at each level of the model presented in the textbook

**Level 1: Automated Preparation and Configuration**

**Example**: Scripts automatically prepare the necessary infrastructure before deploying a new application stack. This could mean provisioning VMs, setting up necessary networking configurations, etc.

**Level 2: Automated Monitoring and Measurement**

**Example**: Cloud providers offer monitoring services that continuously monitor resources, collecting data about CPU, memory usage, network traffic, etc. If it goes above threshold numbers, alerts are created.

**Level 3: Automated Analysis of Trends and Prediction**

- **Example**: Using machine learning and analytics on collected data, a system might predict that given the current growth

rate, a database will run out of storage in the next two months or any other metric. This allows the data center owner to add storage or any other provision proactively.

2. **Level 4: Automated Identification of Root Causes**
    - **Example**: If there's an unexpected spike in error rates for an application, this level might correlate with a recent deployment or a change in network configurations. The system might then deduce that the recent deployment to that microservice is the most probable root cause of the errors.

3. **Level 5: Automated Remediation of Problems**
    - **Example**: If a virtual machine in a cluster crashes or becomes unresponsive, a system might automatically try to restart it. If a network link fails, automated processes could reroute the traffic through an alternative path without human intervention.

9) Suppose that instead of using full virtualization, cloud providers use another form. From a tenant's perspective, what disadvantages would result if a provider used:

a) Software emulation?
The biggest disadvantage would be the high-performance cost of emulation, which necessitates more processing power and results in slower program execution from the tenant's perspective. Slower response times can hurt user experience and could lead to higher costs since tenants could need more resources to operate at the needed levels. Software emulation makes it simpler to transfer software across computers, but because of its inefficiency and increased resource utilization, it might not be the best option.

b) Para-virtualization?
One notable drawback of para-virtualization is the requirement that the operating system's source code be modified before deployment. This is because para-virtualization asks for replacing all privileged instructions with calls to hypervisor functions. This change may limit the tenant's options for operating systems, which may raise the complexity and resource requirements in para-virtualized settings. It may also cause stability and compatibility concerns. Although para-virtualization can enable native execution of instructions, which results in high-speed execution, the necessary changes and potential restrictions on software options can be significant negatives for tenants.

10)
a) Given what you know about data center networking, will it be easier to place a leaf switch or a spine switch while the data center continues to run? Explain.

In contrast to a spine switch, replacing a leaf switch would often be simpler while the data center is still operational. Replacing a leaf switch normally has less of an impact on the network as a whole since it typically connects to servers in a single rack or a small group of racks. The connectivity of many systems can be impacted if the spine switch, which is connected to several leaf switches, goes offline.

b) Once the "easy" replacements from part (a) have all been made, what steps will you need to take to handle the more difficult replacements?

1. Develop a plan to replace spine switches one at a time, ensuring network redundancy to minimize downtime.
2. Before the replacement, configure the network to use alternative paths, allowing data to flow through other spine switches while one is being replaced.

3. Monitor the network continuously for any anomalies or disruptions during the switch replacement process and analyze the traffic to ensure no congestion is occurring on alternative paths.
4. Back up the configuration of the existing spine switch before replacement to easily restore settings on the new switch.
5. After replacement, evaluate the network performance and resolve any identified issues.

11) (Hyperconverged Infrastructure) You are a site reliability engineer setting up an embedded system to monitor the overall health of a data center. Each rack contains a small sensor that monitors temperature and periodically sends a message to a centralized monitoring station. Suppose each sensor sends an average of 500 KB per second. If the data from all sensors in the data center must pass over the 1 Gbps network to the monitoring station, how large can the data center become before the link to the monitoring station becomes saturated?

Step 1: Convert 1 Gbps to Bytes per second. 1 Gbps equals 10^9 bits. Since 1 Byte equals 8 bits, then 1 Gbps in Bytes per second is calculated as follows: 1 Gbps = (10^9 bits) / (8 bits/byte) = 125 x 10^6 Bytes per second.
Step 2: Calculate the number of racks the data center can support. Each sensor sends an average of 500 KB per second. 500 KB equals 500 x 10^3 Bytes. So, 500 KB in Bytes per second is 500,000 Bytes per second.
To find out the number of sensors (racks) the network can support before becoming saturated: Number of sensors (racks) = (125 x 10^6 Bytes per second) / (500,000 Bytes per second per sensor) = 250 sensors (racks).
So, the data center can have up to 250 racks before the link to the monitoring station becomes saturated.