# Mam Tahira

**Q System network administration?**

* System network administration refers to the management and maintenance of a computer network. This includes tasks such as configuring network devices, setting up user accounts, managing network security, and monitoring network performance. System network administrators are responsible for ensuring that the network is up and running smoothly at all times, and that it is able to support the needs of the users who rely on it.
* In simple terms, system network administration is the process of managing and maintaining a computer network. This involves tasks such as setting up and configuring network devices, managing user accounts, and ensuring the security of the network. System network administrators are responsible for making sure that the network is always running smoothly and that it can support the needs of the people who use it.

Q Who are system administrator?

* A system administrator, or sysadmin, is a person who is responsible for the maintenance, configuration, and reliable operation of computer systems, especially multi-user computers, such as servers. The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers they manage meet the needs of the users, without exceeding the budget.
* A system administrator, sometimes referred to as a sysadmin, is a person who is responsible for the maintenance, configuration, and reliable operation of computer systems, particularly servers. They are typically responsible for maintaining the security and reliability of the servers, as well as monitoring their performance and making sure that they are running efficiently. System administrators often work in a team, and may be responsible for managing multiple servers and network devices. They typically have a strong background in computer science and a thorough understanding of computer networks and systems.

Q Essential of system administration

There are several essential aspects of system administration, including:

1. **Maintaining** the security of the network and the systems that it supports: System administrators are responsible for implementing and enforcing security measures such as firewalls, access controls, and intrusion detection systems to protect the network and its resources from unauthorized access and threats.
2. **Monitoring** network performance and availability: System administrators are responsible for monitoring the performance and availability of the network, and for identifying and troubleshooting any issues that may arise.
3. **Managing** user accounts and permissions: System administrators are responsible for creating and managing user accounts and permissions, ensuring that each user has the appropriate access to the resources they need.
4. **Installing and configuring** hardware and software: System administrators are responsible for installing and configuring the hardware and software that make up the network, including servers, routers, and other network devices.
5. **Providing technical support** and assistance to users: System administrators are often the first point of contact for users who have technical questions or issues, and are responsible for providing timely and effective support and assistance to resolve their problems.

Q 1. Daily operation

The daily operations of a system administrator may vary depending on the specific network and systems they are responsible for, as well as the size and complexity of the organization they work for. However, some common daily tasks that a system administrator may perform include:

1. Monitoring the performance and availability of the network and its systems
2. Troubleshooting and resolving technical issues that arise
3. Configuring and maintaining network devices such as routers and switches
4. Installing and updating software on the network
5. Managing user accounts and permissions
6. Implementing and enforcing security measures to protect the network
7. Providing technical support and assistance to users
8. Planning and implementing network upgrades and improvements
9. Keeping track of network inventory and equipment
10. Developing and maintaining documentation of the network and its systems.

Q 2. Hardware and software:-

In system administration, hardware refers to the physical components of a computer system, such as the central processing unit (CPU), memory (RAM), storage (hard drives), and input/output (I/O) devices such as a keyboard, mouse, and monitor.

Software, on the other hand, refers to the programs and applications that run on a computer. This includes both operating systems, which manage the hardware and provide a platform for other software to run on, and application software, which performs specific tasks such as word processing, spreadsheets, and web browsing.

System administrators are responsible for managing and maintaining both the hardware and software that make up a computer network. This may include installing and configuring new hardware and software, ensuring that it is kept up-to-date, and troubleshooting any issues that may arise.

Q 3. Adding and removing user account?

In system administration, adding and removing user accounts is a common task. To add a new user account, a system administrator typically performs the following steps:

1. Open the user management tool for the operating system (such as the "User Accounts" control panel in Windows, or the "Users & Groups" preference pane in macOS).
2. Click on the option to add a new user.
3. Enter the user's name and any other relevant information, such as their email address and phone number.
4. Assign a username and password for the user to use to log in to the system.
5. Select the user's permissions and access rights, such as which resources they are allowed to access and what actions they are allowed to perform.
6. Click "OK" or "Save" to create the new user account.

To remove a user account, a system administrator typically performs the following steps:

1. Open the user management tool for the operating system.
2. Select the user account that you want to remove.
3. Click on the option to delete the user account.
4. Confirm the deletion, if prompted.

It is important to note that when removing a user account, any data or files associated with that user may also be deleted, unless they are transferred to another user account or backed up before the deletion.

Q 4. Administration planning?

Administration planning is an important part of system administration. It involves identifying the current and future needs of the network and its users, and creating a plan to meet those needs. This may include identifying and prioritizing projects, allocating resources, and establishing timelines and budgets.

Some key steps in the administration planning process include:

1. Identifying the current state of the network and its systems: This involves gathering information about the network's current configuration, performance, and usage, as well as identifying any potential issues or weaknesses.
2. Identifying the needs of the network and its users: This involves gathering input from stakeholders, such as users, managers, and other IT staff, to determine their current and future needs and priorities.
3. Developing a plan to meet the identified needs: This involves creating a detailed plan that outlines the steps that will be taken to meet the identified needs, including timelines, budgets, and resources.
4. Implementing the plan: This involves carrying out the steps outlined in the plan, including acquiring and configuring the necessary hardware and software, training users, and monitoring the progress and success of the plan.
5. Evaluating and updating the plan: This involves regularly reviewing the plan and its implementation, and making adjustments as needed to ensure that the network and its systems continue to meet the evolving needs of the organization and its users.

Q 5. Documentation?

Documentation is an important part of system administration, as it provides a reference for information about the network and its systems. This can include information such as network diagrams, hardware and software inventory, and configuration details. Documentation can be helpful for new system administrators to learn about the network, as well as for experienced administrators to reference when troubleshooting or making changes to the network.

Some key elements of documentation in system administration may include:

1. Network diagrams: These show the overall structure and configuration of the network, including the location and connections of all hardware and software components.
2. Hardware and software inventory: This lists all of the hardware and software that make up the network, including details such as make, model, and serial numbers, as well as their current configuration and usage.
3. Configuration details: This includes information about the settings and configurations of the network and its systems, such as network addresses, security settings, and user permissions.
4. Procedures and policies: This includes step-by-step instructions for common tasks, as well as the policies and guidelines that the organization has established for the use and management of the network and its systems.

It is important for system administrators to regularly review and update the documentation to ensure that it is accurate and up-to-date. This can help to prevent misunderstandings and errors, and can make it easier for administrators to manage and maintain the network.

Q 6. Hardware management?

Hardware management is an important part of system administration, as it involves the installation, configuration, and maintenance of the physical components of a computer network. This includes tasks such as setting up new hardware, installing software and updates, and troubleshooting hardware issues.

Some key aspects of hardware management in system administration may include:

1. Installing and configuring new hardware: This involves physically setting up new hardware, such as servers, routers, and switches, and configuring them to work with the rest of the network.
2. Updating and maintaining hardware: This involves installing software updates and patches, as well as performing regular maintenance tasks such as cleaning and checking for hardware issues.
3. Troubleshooting hardware issues: This involves identifying and fixing problems that may arise with the hardware, such as hardware failures or connectivity issues.
4. Managing hardware inventory: This involves keeping track of the hardware that makes up the network, including details such as make, model, and serial numbers, as well as its current configuration and usage.

Effective hardware management can help to ensure that the network and its systems are running smoothly and efficiently, and can prevent disruptions and downtime.

Q 7. Troubleshooting?

Troubleshooting is a common task in system administration, as it involves identifying and resolving problems with the network and its systems. This can include issues such as hardware or software failures, connectivity issues, and security breaches.

To troubleshoot a problem, a system administrator typically follows a systematic approach that includes the following steps:

1. Identify the problem: This involves gathering as much information as possible about the issue, including symptoms, error messages, and any relevant log files or reports.
2. Isolate the problem: This involves determining the root cause of the problem, and narrowing down the possible causes to identify the specific issue that needs to be addressed.
3. Develop a plan to resolve the problem: This involves creating a step-by-step plan for fixing the issue, including any necessary research, testing, or consultation with other IT staff or vendors.
4. Implement the plan: This involves carrying out the steps in the plan to resolve the problem, including any necessary repairs or configuration changes.
5. Test and verify the solution: This involves testing the fix to ensure that it has resolved the problem, and verifying that the network and its systems are functioning correctly.

Effective troubleshooting can help to minimize disruptions and downtime, and can ensure that the network and its systems are running smoothly and efficiently.

Q 8. Data backup?

Data backup is a process in system administration that involves making copies of data so that it can be restored in the event of data loss or corruption. This is an important part of a robust data management strategy, as it ensures that important information is not lost in the event of a system failure or other unforeseen issue. There are several different ways to perform data backups, including using backup software, backing up to external storage devices, and using cloud-based services. It is important to regularly perform backups and to store the backup copies in a secure location.

Q 9. Beladys anomly?

A page fault occurs when a page is not found in the memory and needs to be loaded from the disk. If a page fault occurs and all memory frames have been already allocated, then replacement of a page in memory is required on the request of a new page. This is referred to as demand-paging. The choice of which page to replace is specified by page replacement algorithms. The commonly used page replacement algorithms are FIFO, LRU, optimal page replacement algorithms, etc.

Generally, on increasing the number of frames to a process’ virtual memory, its execution becomes faster as fewer page faults occur. Sometimes the reverse happens, i.e. more page faults occur when more frames are allocated to a process. This most unexpected result is termed **Belady’s Anomaly**.

**Bélády’s anomaly** is the name given to the phenomenon where increasing the number of page frames results in an increase in the number of page faults for a given memory access pattern.

This phenomenon is commonly experienced in the following page replacement algorithms:

1. First in first out (FIFO)
2. Second chance algorithm
3. Random page replacement algorithm

**Reason for Belady’s Anomaly –**   
The other two commonly used page replacement algorithms are Optimal and LRU, but Belady’s Anomaly can never occur in these algorithms for any reference string as they belong to a class of stack-based page replacement algorithms.

A **stack-based algorithm** is one for which it can be shown that the set of pages in memory for *N* frames is always a subset of the set of pages that would be in memory with *N + 1* frames. For LRU replacement, the set of pages in memory would be the *n* most recently referenced pages. If the number of frames increases then these *n* pages will still be the most recently referenced and so, will still be in the memory. While in FIFO, if a page named *b* came into physical memory before a page – *a* then priority of replacement of *b* is greater than that of *a*, but this is not independent of the number of page frames and hence, FIFO does not follow a stack page replacement policy and therefore suffers Belady’s Anomaly.

**Example:** Consider the following diagram to understand the behavior of a stack-based page replacement algorithm

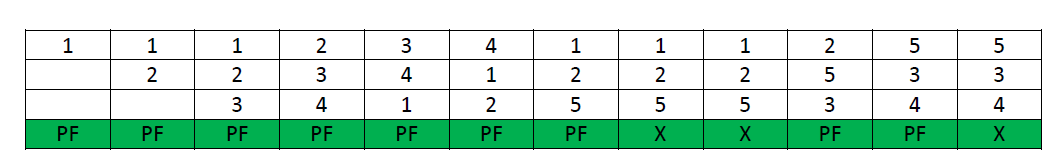


The diagram illustrates that given the set of pages i.e. {0, 1, 2} in 3 frames of memory is not a subset of the pages in memory – {0, 1, 4, 5} with 4 frames and it is a violation in the property of stack based algorithms. This situation can be frequently seen in FIFO algorithm.

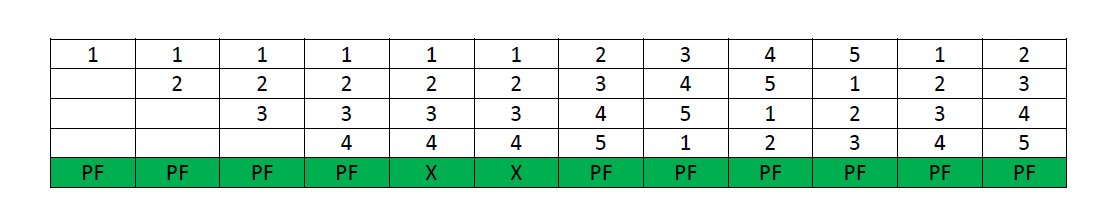
**Belady’s Anomaly in FIFO –**   
Assuming a system that has no pages loaded in the memory and uses the FIFO Page replacement algorithm. Consider the following reference string:

1, 2, 3, 4, 1, 2, 5, 1, 2, 3, 4, 5

**Case-1:** If the system has 3 frames, the given reference string the using FIFO page replacement algorithm yields a total of 9 page faults. The diagram below illustrates the pattern of the page faults occurring in the example.



**Case-2:** If the system has 4 frames, the given reference string using the FIFO page replacement algorithm yields a total of 10 page faults. The diagram below illustrates the pattern of the page faults occurring in the example.



It can be seen from the above example that on increasing the number of frames while using the FIFO page replacement algorithm, the number of **page faults increased** from 9 to 10.

**Note –** It is not necessary that every string reference pattern cause Belady anomaly in FIFO but there is certain kind of string references that worsen the FIFO performance on increasing the number of frames.

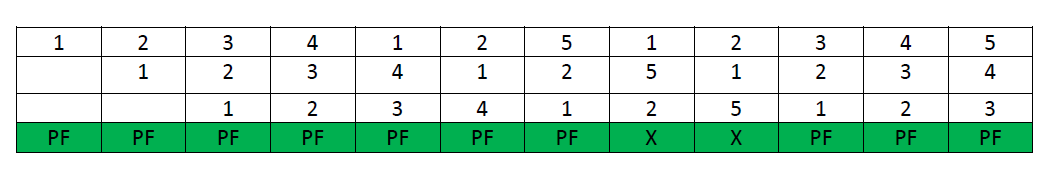
**Why Stack based algorithms do not suffer Anomaly –**   
All the stack based algorithms never suffer Belady Anomaly because these type of algorithms assigns a priority to a page (for replacement) that is independent of the number of page frames. Examples of such policies are Optimal, LRU and LFU. Additionally these algorithms also have a good property for simulation, i.e. the miss (or hit) ratio can be computed for any number of page frames with a single pass through the reference string.

In LRU algorithm every time a page is referenced it is moved at the top of the stack, so, the top *n* pages of the stack are the *n* most recently used pages. Even if the number of frames is incremented to *n+1*, top of the stack will have *n+1* most recently used pages.

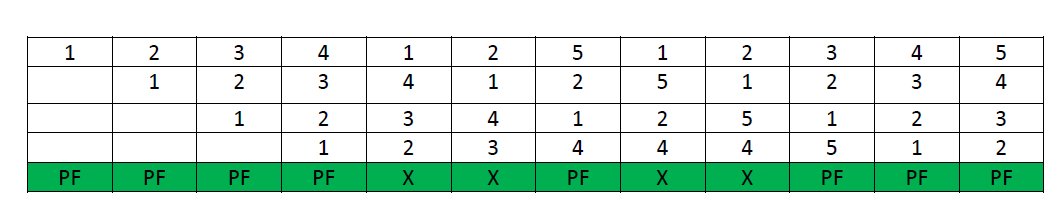
Similar example can be used to calculate the number of page faults in LRU algorithm. Assuming a system that has no pages loaded in the memory and uses the LRU Page replacement algorithm. Consider the following reference string:

1, 2, 3, 4, 1, 2, 5, 1, 2, 3, 4, 5

**Case-1:** If the system has 3 frames, the given reference string using the LRU page replacement algorithm yields a total of 10 page faults. The diagram below illustrates the pattern of the page faults occurring in the example.



**Case-2:** If the system has 4 frames, the given reference string on using LRU page replacement algorithm, then total 8 page faults occur. The diagram shows the pattern of the page faults in the example.



**How Can Belady’s Anomaly Be Removed?**

A stack-based approach can be used to get rid of Belady’s Algorithm. These are some examples of such algorithms:

* Optimal Page Replacement Algorithm
* Least Recently Used Algorithm (LRU)

These algorithms are based on the idea that if a page is inactive for a long time, it is not being utilised frequently. Therefore, it would be best to forget about this page. This allows for improvised memory management and the abolition of Belady’s anomaly.

**Conclusion –**   
Various factors substantially affect the number of page faults, such as reference string length and the number of free page frames available. Anomalies also occur due to the small cache size as well as the reckless rate of change of the contents of the cache. Also, the situation of a fixed number of page faults even after increasing the number of frames can also be seen as an anomaly. Often algorithms like **Random page replacement algorithm** are also susceptible to Belady’s Anomaly, because it **may behave like first in first out (FIFO)** page replacement algorithm. But Stack based algorithms are generally immune to all such situations as they are guaranteed to give better page hits when the frames are incremented.