Problems of Reliable and Timely Delivery of Information on the Servers

Dadamuxamedov Alimjon

Senior Lecturer at the Department of "Modern information and communication technologies" of International Islamic Academy of Uzbekistan

ABSTRACT

The article analyzes the advantages and disadvantages of reliable and timely delivery of information to the servers of religious educational institutions. Religious educational institutions are a special type of organization that requires reliable and timely delivery of information to their servers. This article discusses the main directions of ensuring the reliability and timely delivery of information to servers.

Keywords: network protocols, multipath redundant transmissions, UDP, delivery time limits, delivery probability, real-time systems Replication, database, connection, blocking, synchronous replication, asynchronous replication, disk array

Kirish

Indeed religious educational institutions' servers and online programs are important tools designed to facilitate student exchange of information and study material. Through these programs, students of religious educational institutions can learn religious information and participate in the educational process.

These online programs offer the following opportunities:

Provision of educational material: The servers of religious educational institutions are used to provide lessons, articles, books, videos and other educational materials for students. These online programs aim to provide an easy way to find and learn religious information according to students' aptitude and level of study.

Learning Control: Programs allow students to control their own learning. Students can test their knowledge through quizzes, quizzes, hands-on activities and other interactive tools, or complete tasks to achieve set goals.

Enhancing student-to-student communication: These online programs work to foster student-to-student communication. This communication can be done through the programs using forums, online chats, tables and links. This creates an opportunity for students to exchange ideas, ask questions, help each other and cooperate.

Student monitoring: Students submit assignments and test results through the program to monitor and evaluate their progress. This allows students to change the lessons that have expired, and to carry out independent study with ease.

Information and resources for teachers: Religious education servers are also useful for teachers. The programs help teachers with information, teaching materials, preparing lesson plans, organizing tests and facilitating assessment processes.

Religious education institutions' servers and online programs also provide services for students to study and discuss student interests and personal development. These provide opportunities for rethinking and developing learning styles.

These servers provide important information for students (https://hemis.iiau.uz/, https://estudy.iiau.uz/). Database replication is generally not the easiest task to tackle when developing distributed systems. The issues of reliable and timely delivery of information on the servers of religious educational institutions are based on several important concepts.

First of all, it is very important to protect the personal data of users on the servers of religious educational institutions. This information includes personal details about the user (name, address, phone number and other information) and must follow important guidelines to ensure their security. There are several important methods of data protection: Encryption, Authentication, Data Storage, Security Testing, Security Updates, User Permissions. These methods are the basic security principles recommended for protecting users' data on the servers of religious educational institutions. There should also be international and local data protection compliance requirements appropriate to each issue.

Secondly, it is important to deliver information on time on the servers of religious educational institutions. This allows for timely and quick delivery of available information to users in the system. Institutions provide users with the ability to quickly exchange ideas and exchange information related to their students and teachers.

The need to reliably store data in a server system is of great importance. This is important because readers store text, photos, video material, and other data on servers. This information should be saved so that it can be retrieved again in case of any problems. Therefore, servers must perform timely data maintenance. These measures include protecting personal data, protecting servers from viruses, and serving other important purposes [13:17].

There are also disadvantages for servers. The first reason may be that fast services are required for servers. This eliminates the hassle for students and teachers to secure shares with servers at unexpected times. The second reason is that since the servers can only be accessed over the network, it may affect students' access to the servers in areas where internet connections are not available.

Also, servers are not designed to solve the unique problems that exist in other online systems. This may require awareness and solutions specific to your data environment. Therefore, it is necessary to make local adjustments in the system of institutions to solve the desired problem. Databases are increasingly becoming a part of our lives.

Method

Methods such as scientific description, comparative, and component analysis were used to illuminate the research topic.

Main Part

Computer networks have several methods and mechanisms that help increase the likelihood of reliable and timely data delivery. Below are some of them:

Checksum is a method of checking the integrity of data transmitted over a computer network. Before the data is sent, a checksum is calculated and then added to the data packet. When receiving data, the receiver also calculates a checksum and compares it with the sent checksum. If they do not match, this indicates a data transfer error (Figure 1).

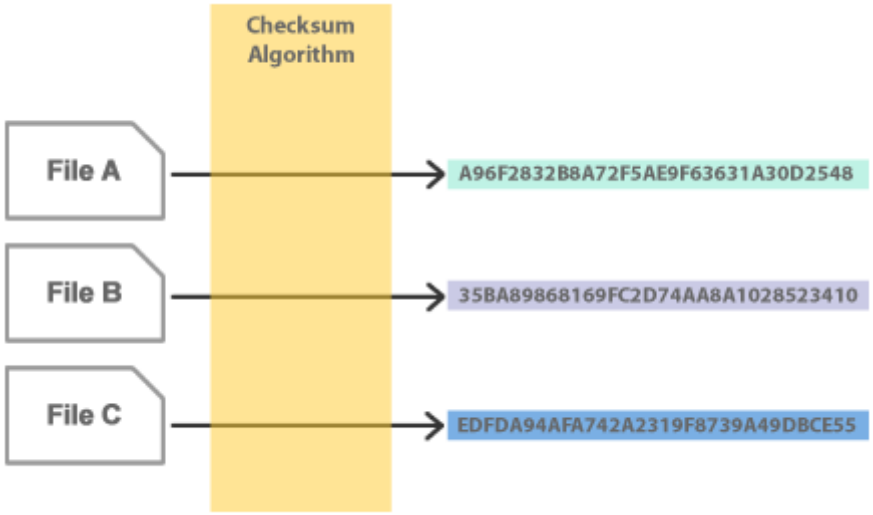


Figure 1. How Checksum works.

Checksum is a data integrity check method used in data transmission. It is used to detect errors that occur when transferring data from one device to another. To calculate the checksum of the data, an algorithm is used that scans all the data bits and calculates the sum of their values. This sum is then compared to a known checksum value. If the sum of the values of the data bits equals the value of the checksum, then the data is considered intact and is said to be intact during transmission [1:18].

When transmitting data, the sender calculates a checksum and includes it in the message along with the data. The receiver also calculates a checksum using the same information and compares it with the checksum received from the sender. If both checksums match, then the data is transmitted successfully, otherwise an error occurs and the data must be sent again [3:42].

Checksums are widely used in many communication protocols such as TCP, UDP, Ethernet, etc. They are a reliable way to detect errors in data transmission and help ensure the integrity of data transmitted over the network.

Retransmission is a method of retransmitting data that is lost or corrupted during transmission. If an error is detected, the sender can resend the packet so that the data is fully delivered (Figure 2).

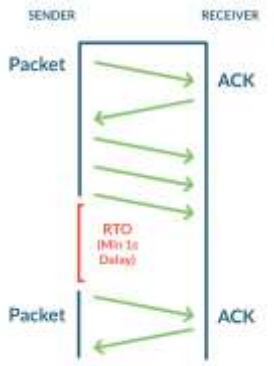


Figure 2. Appearance of retransmission.

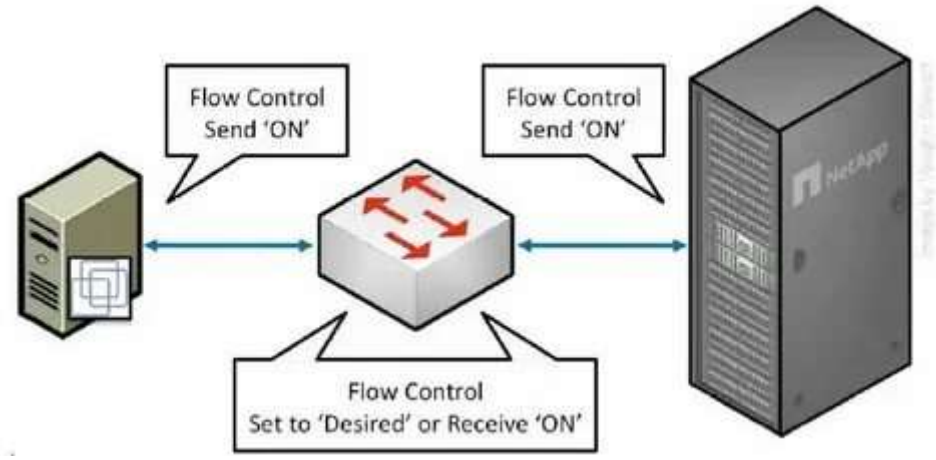
Retransmission is a transmission recovery method used to ensure data transmission reliability in networks where data transmission errors may occur. This method is used to ensure high data reliability in protocols such as TCP.

In the process of data transmission, the sender divides the data into packets and sends

them to the receiver. The receiver checks the integrity and correctness of the packets and then sends an acknowledgment (ACK-(Aknowledgement) - Acknowledgment token) to the sender to inform the sender that the packets have been successfully received [4:74].

If the sender does not receive a confirmation within a certain time, he assumes that one or more packages were lost in transit. In this case, the sender will resend the lost packets. The receiver receives the retransmitted packets and sends an acknowledgment (ACK) to the sender to indicate that the packets were successfully received. This process is repeated until all packets are successfully submitted. Thus, retransmission ensures reliable data delivery in networks where data transmission errors may occur.

Flow Control - Flow control protocols are used to control the amount of data that can be transferred between a sender and a receiver at a given time. This helps prevent network congestion and ensures reliable data delivery (Figure 3).



3-rasm. Flow Control ishlash holati.

Flow control is a method of controlling the flow of data used in data transmission. It is used to control the data rate between sender and receiver to prevent data loss due to buffer overflow or packet loss [5:12].

In the process of data transmission, the sender sends data packets to the receiver, which receives them and sends an acknowledgment (ACK) to the sender. However, if the sender sends packets too fast and the receiver cannot process them at the same rate, a buffer overflow problem occurs.

Flow Control Flow control solves this problem by allowing the receiver to tell the sender how much data it can receive at one time. The receiver sends windows (windows) indicating to the sender how much data it can send before waiting for an acknowledgment [6:18].

For example, if the receiver can only receive 100 bytes of data at a time, then it will send a 100-byte window to the sender. The sender can send data, but only within the window size specified by the receiver. After the receiver receives and processes the data in the current window, the sender sends a new window of the new size so that it can continue transmitting data [7:55].

Thus, Flow Control allows you to control the data transfer rate to prevent buffer overflows or data loss due to data loss. This technique is used in protocols such as TCP to ensure reliable data transmission across networks.

Error Control — error control protocols are used to detect and correct errors in data transmitted over a computer network. This may include data retransmission, use of checksums, and other methods (Figure 4).

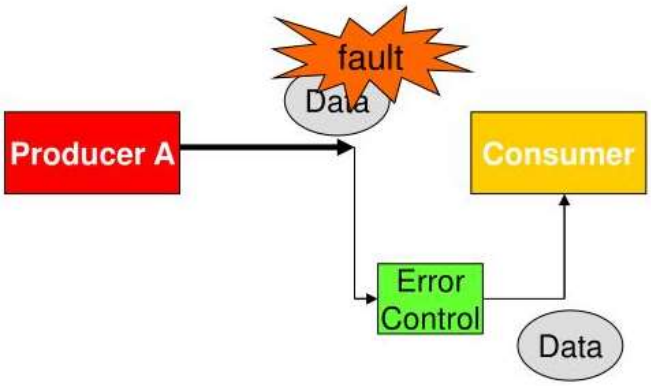


Figure 4. Schematic representation of Error Control.

Error Control is a method of eliminating errors used in data transmission. Used to detect and correct errors in transmitted data. This method is used in protocols such as TCP to ensure data delivery with high reliability [8:13].

During data transmission, the sender divides the data into packets and sends it to the receiver. The receiver checks the integrity and correctness of the packets and then sends back (ACK) to inform the sender that the packets were successfully received.

However, if the packets contain errors, the receiver will not send an acknowledgment (ACK) back to the sender. In this scenario, the sender resends the lost packets. The receiver receives the angry packets and checks their integrity and correctness. If the packets still contain errors, the receiver drops the packets and sends a request to transmit the packets (Figure 5).

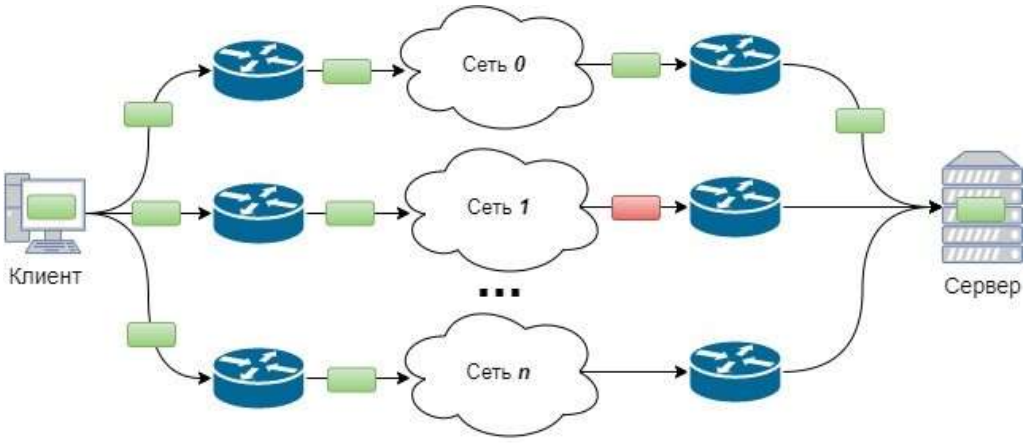


Figure 5. The process of sending packages.

In addition, error checking techniques such as checksums are used to detect errors in the transmitted data. Checksum is a value calculated based on the contents of a data packet. The receiver calculates the checksum for each received packet and compares it with the checksum sent with the packet. If the values do not match, the packet is considered [9:28].

If the packet is considered corrupt, the receiver sends a request to transmit the packet. The sender resends the corrupted packet and the process repeats until the packet is successfully delivered.

Thus, Error Control ensures reliable data transmission in networks where data transmission errors are possible, by detecting

and correcting errors in transmitted data [10:14].

Multicast — Multicast is used to send data to multiple devices simultaneously. This helps reduce network load and ensures fast and reliable data delivery (Figure 6).

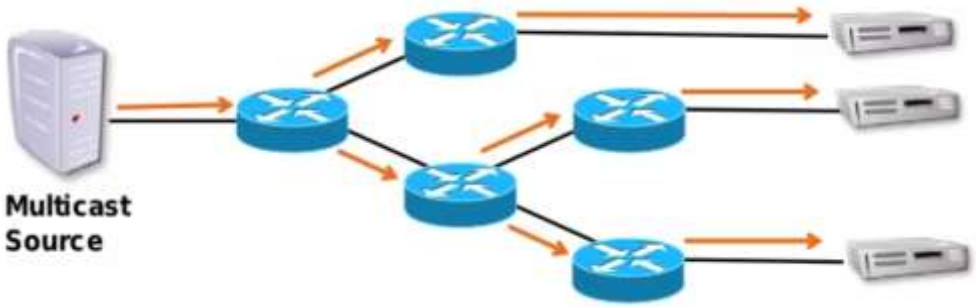


Figure 6. Overview of the multicast system.

Multicast is a method of data transmission in computer networks that allows data to be transmitted from one source to multiple receivers simultaneously. This reduces network traffic and reduces the load on the network, especially when multiple devices need to receive the transmitted data at the same time. Multicast is a method of distributing data arriving at one destination to multiple receivers. This protocol is mainly used in IP networks. Multicast allows data packets to be distributed frequently to multiple receivers by sending them to a single destination (multicast destination).

The following process ensures that the multicast protocol is used:

Providing additional multicast addresses: You will need to provide multicast addresses, which include addresses in the range 224.0.0.0 to 239.255.255.255 in IPv4.

Configuring multicast support: Network-based routers and switches must be configured to support multicast. This includes receiving multicast packets, distributing them directly, and managing multicast addresses.

Distribution of multicast addresses to users: Data is sent to a multicast address and it is distributed to multicast receivers frequently. When a multicast address is received by users, the data sent to the multicast address is distributed to them.

Using IGMP (Internet Group Management Protocol): IGMP is used to directly select and join multicast addresses. Users work with IGMP services to join multicast groups, lose multicast, and accept multicast addresses [13:48].

Multicast protocol allows to distribute massive data to multiple receivers quickly and efficiently. This protocol is widely used for data distribution in video and audio networks, mobile television, interactive games and other networks.

When using multicast, a source sends data to a multicast address, which specifies the group of receivers interested in receiving that data. Devices interested in receiving this information must subscribe to a multicast address to receive this information. When a source sends data to a multicast address, the network sends a copy of the data to all devices subscribed to that multicast address.

Multicast can be used in a variety of applications, including video and audio broadcasting, distributed databases, multimedia applications, and more. It should be noted that multicast does not guarantee data delivery, as it depends on the network condition and the availability of receivers [11:41].

When using multicast, a source sends data to a multicast address, which specifies the group of receivers interested in receiving that data. Devices interested in receiving this information must subscribe to a multicast address to receive this information. When a source sends data to a multicast address, the network sends a copy of the data to all devices subscribed to that multicast address [12:27].

These are just some of the techniques and mechanisms that help increase the

likelihood of reliable and timely data delivery across computer networks. Depending on your specific situation, you may need to use one or more of these methods.

Conclusion

The general conclusion of this article is that Checksum, Retransmission, Flow Control, Error Control and Multicast are all important components of network layer protocols that ensure the reliability and efficiency of data transmission in networks. In general, these mechanisms are essential to ensure the reliability, integrity, and execution of data transmissions on the network. They are used in various networking procedures and technologies to ensure optimal network performance. The information stored on the servers of religious educational institutions is important personal and confidential information. It is necessary to increase the protection of this information and establish better security areas in the systems of religious educational institutions. Also, user-provided terms of use and privacy policies in religious educational institutions' systems help serve these purposes.

References

1. Irgashevich D. A. Development of national network (tas-ix). ACADEMICIA: An International Multidisciplinary Research Journal, 10(5), 144-151. (2020).
2. Шувалов В.П. Егунов М.М., Минина Е.А. Обеспечение показателей надежности телекоммуникационных систем и сетей. — М.: Горячая линия — Телеком,— 168 с. (2015).
3. Bogatyrev V.A. Parshutina S.A. Redundant distribution of requests through the network by transferring them over multiple paths // International Conference on Distributed Computer and Communication Networks. - Vol. 601. 199–207 p. (2016).
4. Bartoli A., Jiménez-Peris, R., Kemme, B., and all: Adapt: towards autonomic web services. In: Distributed Systems Online (2015).
5. Bochkov M.V. Proektirovanie avtomatizirovannix sistem obrabotki informatsii i upravleniya / M. V. Bochkov, Ye. I. Novikov, O. V. Tarakanov; pod red. M.V. Bochkova. – Orel: Akademiya FSO Rossii,–406 s.. (2017).
6. Wallace T.D. Shami A. Concurrent Multipath Transfer Using SCTP: Modelling and Congestion Window Management // IEEE Transactions on Mobile Comput- ing. Vol. 13, no. 11. — Pp. 2510 – 2523. (2014)
7. Cardellini V., Casalicchio, E., Colajanni, M., Yu, P.S.: The state of the art in locally distributed Web-server systems. ACM Comput. Surv. 34(2), 263–311 (2018).
8. Chen J., Soundararajan, G., Amza, C.: Autonomic provisioning of backend databases in dynamic content web servers. In: Int. Conf. on Autonomic Computing (ICAC) (2006).
9. Noskov I.I, Bogatyrev V.A, Slastikhin I.A. Simulation of computer network with switch and packet reservation // CEUR Workshop Proceedings. -Vol. 2344. (2019).
10. Коннолли, Т. Бази данних. Проектирование, реализация и сопровождение [пер. с англ.] / Т. Коннолли, К. Бегг, А. Страчан. – 3-е изд. – М. : Издателский дом "Вилямс", 2003. – 1440 с.
11. Ахо А. Структури данних и алгоритми [пер. с англ.] / А. Ахо, В. Хопкрофт, Д. Улман Д. Джеффри. – М. : Вилямс,– 384 с (2001).
12. Баденко В. Л. Високопроизводителние вичисления : учеб. пособие / В. Л. Баденко. – СПБ. : Изд-во Политехн. ун-та, – 180 с (2010).
13. Баранова И.В. Управление предприятием на основе интегрированних средств поддержки распределённих баз данних / И. В. Баранова // Вестник южно-российского государственного технического университета Новочеркасского политехнического института.. – № 1. –С. 110-118. (2013).