REMOTE REPLICATION METHOD AND APPARATUS BASED ON DUPLICATED DATA DELETION

A de-duplication-based remote replication method and an apparatus are provided. The de-duplication-based remote replication method is applied to a remote replication system, where the system includes a primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the method includes: obtaining, by the primary end device, a second snapshot of the primary end device (101); determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot (102); and when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, sending the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device (103). The method and the apparatus improve performance of remote replication of disaster recovery backup.
Description

TECHNICAL FIELD

[0001] Embodiments of the present invention relate to the field of computer technologies, and in particular, to a de-duplication-based remote replication method and an apparatus.

BACKGROUND

[0002] De-duplication is a data reduction technology designed to reduce a storage capacity used in a storage system. Duplicate variable-sized data blocks in different locations in different data are searched for, and these duplicate data blocks are replaced with indicators, so as to reduce a stored data volume. A highly redundant data set (for example, backup data) benefits greatly from the de-duplication technology, and a user may implement a reduction ratio from 10:1 to 50:1. Remote replication is a disaster recovery technology, which refers to replicating data of a primary end device to a remote disaster recovery end device. When the data of the primary end device is corrupted, the data may be recovered using the disaster recovery end device.

[0003] If the de-duplication technology is applied to the remote replication, a data transmission volume may be reduced, bandwidth may be reduced, and a replication window may be reduced. In a de-duplication-based remote replication solution in the prior art, a fingerprint of differentiated data between to-be-replicated data and last-replicated data of a primary end device is sent to a disaster recovery end device for querying; the disaster recovery end device loads the fingerprint to query whether the fingerprint of the differentiated data of the primary end device exists in the disaster recovery end device, and sends a fingerprint existing in the disaster recovery end device to the primary end device; if the fingerprint exists in the disaster recovery end device, it is considered that the differentiated data exists in the disaster recovery end device; or if the fingerprint does not exist in the disaster recovery end device, it is considered that the differentiated data does not exist in the disaster recovery end device, and the primary end device needs to send the differentiated data to the disaster recovery end device.

[0004] However, a problem existing in the prior art is that a fingerprint query operation is extremely complex, and network interaction is increased because of a fingerprint query process, and consequently much network bandwidth is occupied.

SUMMARY

[0005] Embodiments of the present invention provide a de-duplication-based remote replication method and an apparatus, so as to overcome a prior-art problem that a fingerprint query operation is extremely complex, and obtaining, by the primary end device, a second snapshot of the primary end device; determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot; and when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, sending the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device.

[0006] According to a first aspect, an embodiment of the present invention provides a de-duplication-based remote replication method applied to a remote replication system, where the system includes a primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the method includes:

obtaining, by the primary end device, a second snapshot of the primary end device; determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot; and when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, sending the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device.

With reference to the first aspect, in a second possible implementation manner of the first aspect, the determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot includes:

obtaining, by the primary end device, a first transaction number of the first snapshot and a second transaction number of a fingerprint of each data block in the added data blocks; and determining whether the second transaction number is greater than the first transaction number, where when a second transaction number of the fingerprint of the first data block is greater than the first transaction number, the fingerprint of the first data block is different from the fingerprints of the data blocks in the first snapshot, and fingerprints of data blocks excluding the first data block in the added data blocks are the same as the fingerprints of the data blocks in the first snapshot.

With reference to the first aspect, in a second possible implementation manner of the first aspect, the determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot includes:

obtaining, by the primary end device, a differentiated record, where the differentiated record is used to record the added data blocks; and the processing module is specifically configured to:
determine whether the fingerprints of the added data blocks that are recorded in the differentiat-
ed record are the same as the fingerprints of the data blocks in the first snapshot.

[0009] With reference to any one of the first aspect, or the first or the second possible implementation manner of the first aspect, in a third possible implementation manner of the first aspect, the method further includes:

when the fingerprint of the first data block in the added data blocks is the same as the fingerprints of the data blocks in the first snapshot, skipping replicating the first data block to the disaster recovery end device.

[0010] According to a second aspect, an embodiment of the present invention provides a de-duplication-based remote replication method applied to a remote replication system, where the system includes a primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the method includes:

obtaining, by the primary end device, a second snapshot of the primary end device;

obtaining, by the primary end device, a differentiated record, where the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot;

obtaining, by the primary end device, fingerprints of the added data blocks;

sending, by the primary end device, the fingerprints of the added data blocks to the disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device;

receiving, by the primary end device, duplicate check information that is sent by the disaster recovery end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot;

obtaining, by the primary end device, fingerprints of the added data blocks by using a hardware accelerator card.

[0012] According to a third aspect, an embodiment of the present invention provides a primary end device, including:

a storage module, configured to store a first snapshot, where the first snapshot is also stored in a disaster recovery end device;

an obtaining module, configured to obtain a second snapshot of the primary end device;

a processing module, configured to determine whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot; and

a sending module, configured to: when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, send the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device.

[0013] With reference to the third aspect, in a first possible implementation manner of the third aspect, the processing module is specifically configured to:

obtain a first transaction number of the first snapshot and a second transaction number of a fingerprint of each data block in the added data blocks; and
determine whether the second transaction number is greater than the first transaction number, where when a second transaction number of the fingerprint of the first data block is greater than the first transaction number, the fingerprint of the first data block is different from the fingerprints of the data blocks in the first snapshot, and fingerprints of data blocks excluding the first data block in the added data blocks are the same as the fingerprints of the data blocks in the first snapshot.

[0014] With reference to the third aspect, in a second possible implementation manner of the third aspect, the obtaining module is specifically configured to:

obtain a differentiated record, where the differentiated record is used to record the added data blocks; and

the processing module is specifically configured to:

determine whether the fingerprints of the added data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot.

[0015] With reference to any one of the third aspect, or the first or the second possible implementation manner of the third aspect, in a second possible implementation manner of the first aspect, the processing module is further configured to:
According to a fourth aspect, an embodiment of the present invention provides a primary end device, including:

- a storage module, configured to store a first snapshot, where the first snapshot is also stored in a disaster recovery end device;
- an obtaining module, configured to obtain a second snapshot of the primary end device, where the obtaining module is further configured to obtain a differentiated record, where the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot; and
- the obtaining module is further configured to obtain fingerprints of the added data blocks;
- a sending module, configured to send the fingerprints of the added data blocks to the disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device; and
- a receiving module, configured to receive duplicate check information that is sent by the disaster recovery end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot, where the sending module is further configured to send, according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device.

According to the de-duplication-based remote replication according to a method embodiment of the present invention, a primary end device includes a processor and a memory, where the processor and the memory communicate with each other by using a bus, and the processor executes a computer instruction in the memory to perform any method in the first aspect.

According to a fifth aspect, an embodiment of the present invention provides a primary end device applied to a remote replication system, where the system includes the primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the primary end device includes a processor and a memory, where the processor and the memory communicate with each other by using a bus, and the processor executes a computer instruction in the memory to perform any method in the first aspect.

FIG. 1 is a flowchart of Embodiment 1 of a de-duplication-based remote replication method according to the present invention;
FIG. 2 is a schematic diagram of remote data replication according to a method embodiment of the present invention;
FIG. 3 is a flowchart of Embodiment 2 of a de-duplication-based remote replication method according to the present invention;
FIG. 4 is a flowchart of Embodiment 3 of a de-
duplication-based remote replication method according to the present invention;
FIG. 5 is a flowchart 2 of Embodiment 3 of a deduplication-based remote replication method according to the present invention;
FIG. 6 is a schematic structural diagram of Embodiment 1 of a primary end device according to the present invention;
FIG. 7 is a schematic structural diagram of Embodiment 2 of a primary end device according to the present invention; and
FIG. 8 is a schematic structural diagram of Embodiment 3 of a primary end device according to the present invention.

DESCRIPTION OF EMBODIMENTS

[0022] To make the objectives, technical solutions, and advantages of the embodiments of the present invention clearer, the following clearly describes the technical solutions in the embodiments of the present invention with reference to the accompanying drawings in the embodiments of the present invention. Apparently, the described embodiments are a part rather than all of the embodiments of the present invention. All other embodiments obtained by persons of ordinary skill in the art based on the embodiments of the present invention without creative efforts shall fall within the protection scope of the present invention.

[0023] FIG. 1 is a flowchart of Embodiment 1 of a deduplication-based remote replication method according to the present invention. FIG. 2 is a schematic diagram of remote data replication according to a method embodiment of the present invention. The method in this embodiment may be applied to a remote replication system. The system includes a primary end device and a disaster recovery end device, and this embodiment may be performed by the primary end device. As shown in FIG. 1, in the method in this embodiment, both the primary end device and the disaster recovery end device store a first snapshot, and the method includes:

Step 101: The primary end device obtains a second snapshot of the primary end device.
Step 102: The primary end device determines whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot.
Step 103: When a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, send the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device. Specifically, the primary end device first needs to create a second snapshot of to-be-replicated data, and then obtains a first snapshot of replicated data. Both the primary end device and the disaster recovery end device store the first snapshot, and the replicated data is last-replicated data. Further, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot needs to be determined. The first snapshot and the second snapshot herein may have multiple fingerprints each. If a fingerprint of a data block in the data blocks added in the second snapshot compared with the first snapshot is different from the fingerprints of the data blocks in the first snapshot, the data block is marked as a first data block, and the first data block, the fingerprint of the first data block, and metadata of the added data blocks are sent to the disaster recovery end device. The metadata includes fingerprint indexes of the data blocks, that is, description information such as locations in the data blocks, storage locations of the data blocks, sizes of the data blocks, and identifiers of the data blocks.

[0024] As shown in FIG. 2, the first snapshot has been replicated to the disaster recovery end device. If a fingerprint of a data block added in the second snapshot, that is, a fingerprint 4 in the second snapshot, is different from the fingerprints of the data blocks in the first snapshot, a data block 4 corresponding to the fingerprint 4, metadata 23 and the fingerprint 4 of the data block 4, metadata 21 of a data block 2 corresponding to a fingerprint 2 in the second snapshot, and metadata 22 of a data block 3 corresponding to a fingerprint 3 in the second snapshot, that is, data in a dashed-line box in FIG. 2, are sent to the disaster recovery end device. After receiving the data, the disaster recovery end device writes the data, and creates a snapshot after replication is completed.

[0025] Optionally, the method in this embodiment further includes:

when the fingerprint of the first data block in the added data blocks is the same as the fingerprints of the data blocks in the first snapshot, skipping replicating the first data block to the disaster recovery end device.

[0026] Specifically, if the fingerprints of all the data blocks added in the second snapshot are the same as the fingerprints of the data blocks in the first snapshot, the first data block is not replicated to the disaster recovery end device.

[0027] In this embodiment, a primary end device obtains a second snapshot of the primary end device; the primary end device determines whether fingerprints of data blocks added in the second snapshot compared with a first snapshot are the same as fingerprints of data blocks in the first snapshot; and when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, the first data block, the fingerprint of the first data block,
and metadata of the added data blocks are sent to a disaster recovery end device, where both the primary end device and the disaster recovery end device store the first snapshot. This implements de-duplication-based remote replication, and during replication, no fingerprint needs to be sent to the disaster recovery end device for querying. Therefore, fingerprint query operations and network interaction are reduced, that is, occupied network bandwidth is reduced. This improves performance of disaster recovery backup of remote replication, and resolves a prior-art problem that a fingerprint query operation is extremely complex, and network interaction is increased because of a fingerprint query process, and consequently much network bandwidth is occupied.

[0028] FIG. 3 is a flowchart of Embodiment 2 of a de-duplication-based remote replication method according to the present invention. As shown in FIG. 3, in the method in this embodiment, the determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot includes:

obtaining, by the primary end device, a first transaction number of the first snapshot and a second transaction number of a fingerprint of each data block in the added data blocks; and

determining whether the second transaction number is greater than the first transaction number, where when a second transaction number of the fingerprint of the first data block is greater than the first transaction number, the fingerprint of the first data block is different from the fingerprints of the data blocks in the first snapshot, and fingerprints of data blocks excluding the first data block in the added data blocks are the same as the fingerprints of the data blocks in the first snapshot.

[0029] Optionally, the determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot includes:

obtaining, by the primary end device, a differentiated record, where the differentiated record is used to record the added data blocks; and

determining, by the primary end device, whether the fingerprints of the added data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot.

[0030] Specifically, during initial replication, the primary end device needs to create a snapshot, and replicate data of the snapshot of the primary end device to the disaster recovery end device. After the replication is completed, the disaster recovery end device also creates a snapshot. After the replication is completed, snapshot data of the disaster recovery end device is the same as snapshot data of the primary end device, and data replicated each time later is differentiated data between a currently replicated snapshot and a last-replicated snapshot.

[0031] Therefore, if currently replicated data already exists in the last-replicated snapshot, the currently replicated data certainly exists in the disaster recovery end device.

[0032] After de-duplication is enabled on the primary end device and the disaster recovery end device, if a fingerprint of to-be-replicated data exists in the last-replicated snapshot, the fingerprint of the data certainly exists in the disaster recovery end device.

[0033] As shown in FIG. 2 and FIG. 3, the second snapshot of the to-be-replicated data first needs to be created, and then the first snapshot of the replicated data is obtained, where the replicated data is the last-replicated data. The differentiated record between the second snapshot and the first snapshot is obtained, and the differentiated record is used to record the added data blocks. As shown in FIG. 2, the differentiated record is the metadata 21, the metadata 22, and the metadata 23. The fingerprints of the data blocks that are recorded in the differentiated record are obtained, and the fingerprints are the fingerprint 2, the fingerprint 3, and the fingerprint 4. Whether the fingerprints of the data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot is determined, that is, whether the fingerprint 2, the fingerprint 3, and the fingerprint 4 are the same as the fingerprints of the data blocks in the first snapshot is determined. In this embodiment, whether the fingerprints of the data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot may be determined in a transaction number manner, and a specific process is as follows:

The first transaction number of the first snapshot and the second transaction number of the fingerprint of each data block in the added data blocks are obtained; the first snapshot is corresponding to a first transaction number, and a fingerprint of each data block in the first snapshot is also corresponding to a transaction number, and the transaction number corresponding to the fingerprint may be equal to the first transaction number; and the fingerprint of each data block in the data blocks added in the second snapshot is corresponding to a second transaction number. It is assumed that the first transaction number corresponding to the first snapshot is 1, transaction numbers corresponding to a fingerprint 1, a fingerprint 2, and a fingerprint 3 that are in the first snapshot are also 1; and that a second transaction number corresponding to the fingerprint 2 in the second snapshot is 1, a second transaction number corresponding to the fingerprint 3 in the second snapshot is 1, and a second transaction number cor-
responding to the fingerprint 4 in the second snapshot is 2. In this case, the second transaction numbers of the fingerprint 2 and the fingerprint 3 that are in the second snapshot are equal to the first transaction number of the first snapshot, and therefore the fingerprint 2 and the fingerprint 3 that are in the second snapshot are the same as the fingerprint 2 and the fingerprint 3 that are in the first snapshot, and the data block 2 and the data block 3 respectively corresponding to the fingerprint 2 and the fingerprint 3 that are in the second snapshot do not need to be transmitted to the disaster recovery end device. The second transaction number of the fingerprint 4 in the second snapshot is greater than the first transaction number corresponding to the first snapshot, and therefore the fingerprint 4 in the second snapshot is different from all the fingerprints in the first snapshot. Therefore, a first data block corresponding to the fingerprint 4, the metadata 23 of the first data block, and the fingerprint 4 need to be transmitted to the disaster recovery end device, and the metadata 21 and the metadata 22 respectively corresponding to the data block 2 and the data block 3 also need to be transmitted to the disaster recovery end device.

[0034] A transaction (Transaction) is a program execution unit (unit) that accesses data and that may update the data. A transaction is usually generated in execution of a user program written in a high-level programming language (such as SQL, C++, or Java), and is defined by using a statement (or a function call) in a form of a begin transaction and an end transaction. The transaction includes all operations executed between the begin transaction (begin transaction) and the end transaction (end transaction). Each transaction is corresponding to a number, that is, a transaction number. A transaction has four attributes: atomicity, consistency, isolation, and durability.

[0035] FIG. 4 is a flowchart 1 of Embodiment 3 of a de-duplication-based remote replication method according to the present invention, and FIG. 5 is a flowchart 2 of Embodiment 3 of the de-duplication-based remote replication method according to the present invention. The method in this embodiment is applied to a remote replication system. The system includes a primary end device and a disaster recovery end device, and an execution body may be the primary end device. As shown in FIG. 4 and FIG. 5, in the method in this embodiment, both the primary end device and the disaster recovery end device store a first snapshot, and the method includes:

Step 401: The primary end device obtains a second snapshot of the primary end device.
Step 402: The primary end device obtains a differentiated record, where the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot.
Step 403: The primary end device obtains fingerprints of the added data blocks.
Step 404: The primary end device sends the fingerprints of the added data blocks to the disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device.
Step 405: The primary end device receives duplicate check information that is sent by the disaster recovery end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot.
Step 406: The primary end device sends, according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device.

[0036] Specifically, the primary end device first needs to create a second snapshot of to-be-replicated data, and then obtains a first snapshot of replicated data. Both the primary end device and the disaster recovery end device store the first snapshot, and the replicated data is last-replicated data. A differentiated record between the second snapshot and the first snapshot is obtained, where the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot. As shown in FIG. 2, the differentiated record is metadata 21, metadata 22, and metadata 23. Fingerprints of the data blocks that are recorded in the differentiated record are obtained, and the fingerprints are a fingerprint 2, a fingerprint 3, and a fingerprint 4. The fingerprints are sent to the disaster recovery end device, and the disaster recovery end device performs duplicate check on the fingerprints that are sent by the primary end device. If the fingerprints exist in the disaster recovery end device, it is considered that these data blocks that are recorded in the differentiated record exist in the disaster recovery end device; or if the fingerprints do not exist in the disaster recovery end device, these data blocks that are recorded in the differentiated record do not exist in the disaster recovery end device, and the primary end device needs to send the data blocks that are recorded in the differentiated record to the disaster recovery end device. The disaster recovery end device sends duplicate check information to the primary end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot, that is, a fingerprint 4. After receiving the duplicate check information, the primary end device sends the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device. That is, a data block 4 corresponding to the fingerprint 4 is sent to the disaster recovery end device, and the sent data further includes the metadata 23 of the data block 4, the fingerprint 4, and
the metadata 21 and the metadata 22 that are corresponding to other fingerprints. After receiving the data, the disaster recovery end device writes the data, and creates a snapshot after replication is completed.

[0037] Optionally, the obtaining, by the primary end device, fingerprints of the added data blocks includes:

obtaining, by the primary end device, the fingerprints of the added data blocks by using a hardware accelerator card.

[0038] Specifically, in a main memory of the primary end device, because a main service imposes a requirement on a central processing unit CPU delay, there is a strong possibility that the main service does not have a de-duplication function, or the de-duplication function is manually/automatically disabled. Therefore, in the solution of this embodiment, de-duplication-based remote replication may be implemented by a method of calculating a fingerprint at a primary end using a hardware accelerator card.

[0039] In this embodiment, a primary end device obtains a second snapshot of the primary end device; the primary end device obtains a differentiated record, where the differentiated record is used to record data blocks added in the second snapshot compared with a first snapshot; the primary end device obtains fingerprints of the added data blocks; the primary end device sends the fingerprints of the added data blocks to a disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device; the primary end device receives duplicate check information that is sent by the disaster recovery end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot; and the primary end device sends, according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device. This implements de-duplication-based remote replication when a primary end does not have a de-duplication function. The primary end calculates a fingerprint by using a hardware accelerator card, sends the fingerprint to the disaster recovery end device for duplicate check, and sends a newly-added data block to the disaster recovery end device according to a fingerprint of the newly-added data block indicated by the duplicate check information. This improves performance of disaster recovery backup of remote replication.

[0040] FIG. 6 is a schematic structural diagram of Embodiment 1 of a primary end device according to the present invention. As shown in FIG. 6, the primary end device in this embodiment includes an obtaining module 601, a processing module 602, a sending module 603, and a storage module 604.

[0041] The storage module 604 is configured to store a first snapshot, where the first snapshot is also stored in a disaster recovery end device.

[0042] The obtaining module 601 is configured to obtain a second snapshot of the primary end device.

[0043] The processing module 602 is configured to determine whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot.

[0044] The sending module 603 is configured to: when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, send the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device.

[0045] Optionally, the processing module 602 is specifically configured to:

obtain a first transaction number of the first snapshot and a second transaction number of a fingerprint of each data block in the added data blocks; and determine whether the second transaction number is greater than the first transaction number, where when a second transaction number of the fingerprint of the first data block is greater than the first transaction number, the fingerprint of the first data block is different from the fingerprints of the data blocks in the first snapshot, and fingerprints of data blocks excluding the first data block in the added data blocks are the same as the fingerprints of the data blocks in the first snapshot.

[0046] Optionally, the obtaining module 601 is specifically configured to:

obtain a differentiated record, where the differentiated record is used to record the added data blocks.

[0047] The processing module 602 is specifically configured to:

determine whether the fingerprints of the added data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot.

[0048] Optionally, the processing module 602 is further configured to:

when the fingerprint of the first data block in the added data blocks is the same as the fingerprints of the data blocks in the first snapshot, skip replicating the first data block to the disaster recovery end device.

[0049] The primary end device in this embodiment may be configured to execute the technical solution of the method embodiment shown in FIG. 1. Implementation principles and technical effects thereof are similar, and
FIG. 7 is a schematic structural diagram of Embodiment 2 of a primary end device according to the present invention. As shown in FIG. 7, the primary end device in this embodiment includes an obtaining module 701, a sending module 702, a receiving module 703, and a storage module 704.

[0051] The storage module 704 is configured to store a first snapshot, where the first snapshot is also stored in a disaster recovery end device. The obtaining module 701 is configured to obtain a second snapshot of the primary end device.

[0052] The obtaining module 701 is further configured to obtain a differentiated record, where the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot. The obtaining module 701 is further configured to obtain fingerprints of the added data blocks.

[0053] The sending module 702 is configured to send the fingerprints of the added data blocks to the disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device.

[0054] The receiving module 703 is configured to receive duplicate check information that is sent by the disaster recovery end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot.

[0055] The sending module 702 is further configured to send, according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device.

[0056] Optionally, the obtaining module 701 is specifically configured to:

obtain the fingerprints of the added data blocks by using a hardware accelerator card.

[0057] The primary end device in this embodiment may be configured to execute the technical solution of the method embodiment shown in FIG. 4. Implementation principles and technical effects thereof are similar, and details are not described herein.

[0058] FIG. 8 is a schematic structural diagram of Embodiment 3 of a primary end device according to the present invention. As shown in FIG. 8, the primary end device in this embodiment is applied to a remote replication system. The system includes the primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot. The primary end device includes a processor 801 and a memory 802, where the processor 801 and the memory 802 communicate with each other by using a bus 803, and the processor 801 executes a computer instruction in the memory 802 to perform any method in the method embodiment shown in FIG. 1.

[0059] In Embodiment 4 of a primary end device according to the present invention, the primary end device in this embodiment may use the schematic structural diagram shown in FIG. 8, and is applied to a remote replication system. The system includes the primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot. The primary end device includes a processor and a memory, where the processor and the memory communicate with each other by using a bus, and the processor executes a computer instruction in the memory to perform the method in the method embodiment shown in FIG. 4.

[0060] In several embodiments provided in the present application, it should be understood that the disclosed device and method may be implemented in other manners. For example, the described device embodiment is merely an example. For example, the unit or module division is merely logical division and may be other division in actual implementation. For example, a plurality of units or modules may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections may be implemented through some interfaces. The indirect couplings or communication connections between the devices or modules may be implemented in electronic, mechanical, or other forms.

[0061] The modules described as separate parts may or may not be physically separate, and parts displayed as modules may or may not be physical modules, may be located in one position, or may be distributed on a plurality of network units. Some or all the modules may be selected according to actual needs to achieve the objectives of the solutions of the embodiments.

[0062] Persons of ordinary skill in the art may understand that all or some of the steps of the method embodiments may be implemented by a program instructing relevant hardware. The program may be stored in a computer-readable storage medium. When the program runs, the steps of the method embodiments are performed. The foregoing storage medium includes: any medium that can store program code, such as a ROM, a RAM, a magnetic disk, or an optical disc.

[0063] Finally, it should be noted that the foregoing embodiments are merely intended for describing the technical solutions of the present invention, but not for limiting the present invention. Although the present invention is described in detail with reference to the foregoing embodiments, persons of ordinary skill in the art should understand that they may still make modifications to the technical solutions described in the foregoing embodiments or make equivalent replacements to some or all technical features thereof, without departing from the scope of the technical solutions of the embodiments of the present invention.
Claims

1. A de-duplication-based remote replication method applied to a remote replication system, wherein the system comprises a primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the method comprises:

   obtaining, by the primary end device, a second snapshot of the primary end device;
   determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot; and
   when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, sending the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device.

2. The method according to claim 1, wherein the determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot comprises:

   obtaining, by the primary end device, a first transaction number of the first snapshot and a second transaction number of each fingerprint of the added data blocks; and
   determining whether the second transaction number is greater than the first transaction number, wherein when a second transaction number of the fingerprint of the first data block is greater than the first transaction number, the fingerprint of the first data block and fingerprints of data blocks excluding the first data block in the added data blocks are the same as the fingerprints of the data blocks in the first snapshot.

3. The method according to claim 1, wherein the determining, by the primary end device, whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot comprises:

   obtaining, by the primary end device, a differentiated record, wherein the differentiated record is used to record the added data blocks; and
   determining, by the primary end device, whether the fingerprints of the added data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot.

4. The method according to any one of claims 1 to 3, further comprising:

   when the fingerprint of the first data block in the added data blocks is the same as the fingerprints of the data blocks in the first snapshot, skipping replicating the first data block to the disaster recovery end device.

5. A de-duplication-based remote replication method applied to a remote replication system, wherein the system comprises a primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the method comprises:

   Obtaining, by the primary end device, a second snapshot of the primary end device;
   Obtaining, by the primary end device, a differentiated record, wherein the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot;
   Obtaining, by the primary end device, fingerprints of the added data blocks;
   Sending, by the primary end device, the fingerprints of the added data blocks to the disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device;
   Receiving, by the primary end device, duplicate check information that is sent by the disaster recovery end device, wherein the duplicate check information comprises a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot; and
   Sending, by the primary end device according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device.

6. The method according to claim 5, wherein the obtaining, by the primary end device, fingerprints of the added data blocks comprises:

   obtaining, by the primary end device, the fingerprints of the added data blocks by using a hardware accelerator card.

7. A primary end device, comprising:
a storage module, configured to store a first snapshot, wherein the first snapshot is also stored in a disaster recovery end device;
an obtaining module, configured to obtain a second snapshot of the primary end device;
a processing module, configured to determine whether fingerprints of data blocks added in the second snapshot compared with the first snapshot are the same as fingerprints of data blocks in the first snapshot; and
a sending module, configured to: when a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, send the first data block, the fingerprint of the first data block, and metadata of the added data blocks to the disaster recovery end device.

8. The primary end device according to claim 7, wherein the processing module is specifically configured to:

obtain a first transaction number of the first snapshot and a second transaction number of a fingerprint of each data block in the added data blocks; and
determine whether the second transaction number is greater than the first transaction number, wherein when a second transaction number of the fingerprint of the first data block is greater than the first transaction number, the fingerprint of the first data block is different from the fingerprints of the data blocks in the first snapshot, and fingerprints of data blocks excluding the first data block in the added data blocks are the same as the fingerprints of the data blocks in the first snapshot.

9. The primary end device according to claim 7, wherein the obtaining module is specifically configured to:

obtain a differentiated record, wherein the differentiated record is used to record the added data blocks; and
the processing module is specifically configured to:

determine whether the fingerprints of the added data blocks that are recorded in the differentiated record are the same as the fingerprints of the data blocks in the first snapshot.

10. The primary end device according to any one of claims 7 to 9, wherein the processing module is further configured to:

when the fingerprint of the first data block in the added data blocks is the same as the fingerprints of the data blocks in the first snapshot, skip replicating the first data block to the disaster recovery end device.

11. A primary end device, comprising:

a storage module, configured to store a first snapshot, wherein the first snapshot is also stored in a disaster recovery end device;
an obtaining module, configured to obtain a second snapshot of the primary end device, wherein the obtaining module is further configured to obtain a differentiated record, wherein the differentiated record is used to record data blocks added in the second snapshot compared with the first snapshot; and
the obtaining module is further configured to obtain fingerprints of the added data blocks;
the sending module, configured to send the fingerprints of the added data blocks to the disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device; and
a receiving module, configured to receive duplicate check information that is sent by the disaster recovery end device, wherein the duplicate check information comprises a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot, wherein the sending module is further configured to send, according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device.

12. The primary end device according to claim 11, wherein the obtaining module is specifically configured to:

obtain the fingerprints of the added data blocks by using a hardware accelerator card.

13. A primary end device applied to a remote replication system, wherein the system comprises the primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the primary end device comprises a processor and a memory, wherein the processor and the memory communicate with each other by using a bus, and the processor executes a computer instruction in the memory to perform the method described in any one of claims 1 to 4.
14. A primary end device applied to a remote replication system, wherein the system comprises the primary end device and a disaster recovery end device, and both the primary end device and the disaster recovery end device store a first snapshot; and the primary end device comprises a processor and a memory, wherein the processor and the memory communicate with each other by using a bus, and the processor executes a computer instruction in the memory to perform the method described in claim 5 or 6.
A primary end device obtains a second snapshot of the primary end device

The primary end device determines whether fingerprints of data blocks added in the second snapshot compared with a first snapshot are the same as fingerprints of data blocks in the first snapshot

When a fingerprint of a first data block in the added data blocks is different from the fingerprints of the data blocks in the first snapshot, send the first data block, the fingerprint of the first data block, and metadata of the added data blocks to a disaster recovery end device

FIG. 1
FIG. 2
Primary end device

Obtain a first snapshot and a second snapshot

Obtain a differentiated record between the first snapshot and the second snapshot

Obtain a fingerprint in the differentiated record and a second transaction number corresponding to the fingerprint

Obtain a first transaction number of the first snapshot

If the second transaction number is less than or equal to the first transaction number, current differentiated data certainly exists in a disaster recovery end device

Read the differentiated data

Send a first data block, a fingerprint and metadata of the first data block, and metadata of data blocks excluding the first data block in newly-added data blocks to the disaster recovery end device

Replication is completed

Write the data

Create a snapshot

FIG. 3
A primary end device obtains a second snapshot of the primary end device

The primary end device obtains a differentiated record, where the differentiated record is used to record data blocks added in the second snapshot compared with a first snapshot

The primary end device obtains fingerprints of the added data blocks

The primary end device sends the fingerprints of the added data blocks to a disaster recovery end device, so that the disaster recovery end device determines whether the fingerprints of the added data blocks already exist in the disaster recovery end device

The primary end device receives duplicate check information that is sent by the disaster recovery end device, where the duplicate check information includes a fingerprint that is of a first data block in the added data blocks and that is different from fingerprints of data blocks in the first snapshot

The primary end device sends, according to the duplicate check information, the first data block indicated by the duplicate check information and metadata of the added data blocks to the disaster recovery end device

FIG. 4
Obtain a second snapshot and a first snapshot
Obtain a differentiated record between the second snapshot and the first snapshot
Obtain a fingerprint of a data block recorded in the differentiated record
Send the fingerprint
Return duplicate check information
Send a first data block, a fingerprint and metadata of the first data block, and metadata of newly-added data blocks excluding the first data block to a disaster recovery end device
Write the data
Create a snapshot
Replication is completed

FIG. 5

FIG. 6
### INTERNATIONAL SEARCH REPORT

#### A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/30 (2006.01) i
According to International Patent Classification (IPC) or to both national classification and IPC

#### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPDOC, CNKI, GOOGLE: disaster tolerance, fingerprint, back w up, synchroniz+, snapshot, mirror, edition, increments+, diff+

#### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PX</td>
<td>CN 104484480 A (HUAWEI TECHNOLOGIES CO., LTD.), 01 April 2015 (01.04.2015), claims 1-14</td>
<td>1-14</td>
</tr>
<tr>
<td>X</td>
<td>CN 102624871 A (HANGZHOU JIETANG INFORMATION TECHNOLOGY CO., LTD.), 01 August 2012 (01.08.2012), description, paragraphs [0001] and [0005]-[0010]</td>
<td>1, 3-7, 9-14</td>
</tr>
<tr>
<td>A</td>
<td>CN 103870362 A (HUAWEI TECHNOLOGIES CO., LTD.), 18 June 2014 (18.06.2014), the whole document</td>
<td>1-14</td>
</tr>
<tr>
<td>A</td>
<td>CN 102510340 A (INSURP ELECTRONIC INFORMATION INDUSTRY CO., LTD.), 20 June 2012 (20.06.2012), the whole document</td>
<td>1-14</td>
</tr>
<tr>
<td>A</td>
<td>US 2013212074 A1 (NEC CORPORATION), 15 August 2013 (15.08.2013), the whole document</td>
<td>1-14</td>
</tr>
</tbody>
</table>

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
  *“A” document defining the general state of the art which is not considered to be of particular relevance
  *“E” earlier application or patent but published on or after the international filing date
  *“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  *“O” document referring to an oral disclosure, use, exhibition or other means
  *“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

- **Date of the actual completion of the international search:** 07 December 2015 (07.12.2015)
- **Date of mailing of the international search report:** 31 December 2015 (31.12.2015)

Name and mailing address of the ISA/OCN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62010451

Authorized officer: HU, Lili
Telephone No.: (86-10) 010-82245948

Form PCT/ISA/210 (second sheet) (July 2009)
<table>
<thead>
<tr>
<th>Patent Documents referred in the Report</th>
<th>Publication Date</th>
<th>Patent Family</th>
<th>Publication Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN 104484480 A</td>
<td>01 April 2015</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CN 102624871 A</td>
<td>01 August 2012</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CN 103870362 A</td>
<td>18 June 2014</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CN 102510340 A</td>
<td>20 June 2012</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2013514558 A</td>
<td>25 April 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 103098035 A</td>
<td>08 May 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2012029258 A1</td>
<td>08 March 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2809224 A1</td>
<td>08 March 2012</td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (patent family annex) (July 2009)