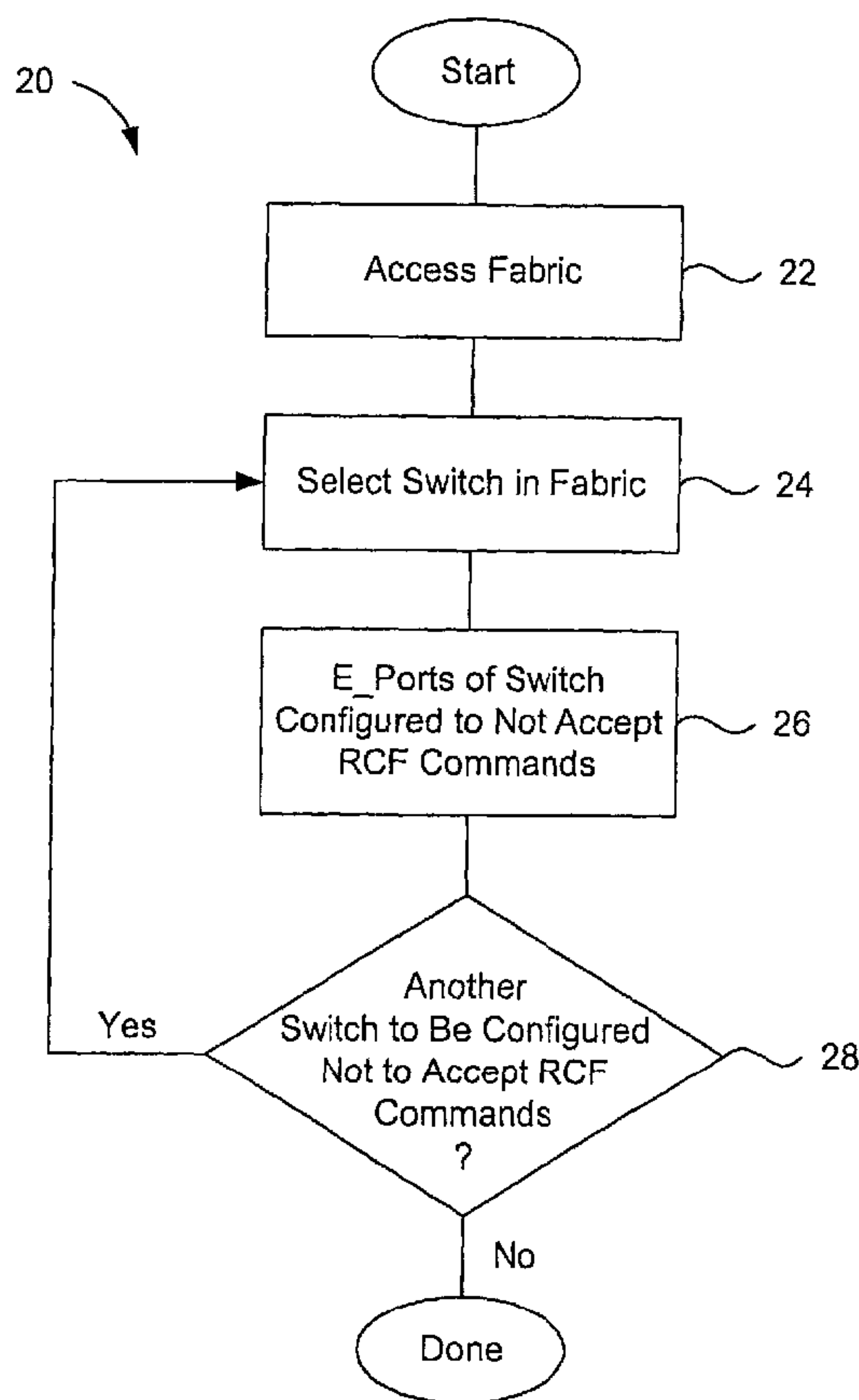




(86) Date de dépôt PCT/PCT Filing Date: 2003/05/22
 (87) Date publication PCT/PCT Publication Date: 2003/12/04
 (45) Date de délivrance/Issue Date: 2011/07/05
 (85) Entrée phase nationale/National Entry: 2004/11/18
 (86) N° demande PCT/PCT Application No.: US 2003/016449
 (87) N° publication PCT/PCT Publication No.: 2003/101144
 (30) Priorité/Priority: 2002/05/24 (US10/155,698)

(51) Cl.Int./Int.Cl. *H04Q 11/00* (2006.01),
H04L 12/24 (2006.01), *H04L 29/06* (2006.01)
 (72) Inventeurs/Inventors:
DESANTI, CLAUDIO, US;
DI BENEDETTO, MARCO, US
 (73) Propriétaire/Owner:
CISCO TECHNOLOGY, INC., US
 (74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : DISPOSITIF ET PROCEDE PERMETTANT D'EVITER LES INTERRUPTIONS DANS DES MATRICES DE CANAUX DE FIBRES OPTIQUES DUES A DES MESSAGES DE RECONFIGURATION DE MATRICE (RCF)
 (54) Title: APPARATUS AND METHOD FOR PREVENTING DISRUPTION OF FIBRE CHANNEL FABRICS CAUSED BY RECONFIGURE FABRIC (RCF) MESSAGES



(57) **Abrégé/Abstract:**

An apparatus and method for preventing the disruption of Fibre Channel Fabrics caused by ReConfigure Fabric (RCF) messages is disclosed. The apparatus includes a storage area network and a plurality of Fibre Channel Switches arranged in a Fabric. Each

(57) **Abrégé(suite)/Abstract(continued):**

of the plurality of Switches includes logic to selectively configure their Ports to either reject or accept RCF messages. When configured to reject RCF messages, the Switch Port that receives an RCF message will generate a reject message along with a reason code explanation "E Port Isolated", and then transition into an Isolated state. When the Switch that generated the RCF message receives the reject message, its Port also transition into the Isolated state. In accordance with the method of the present invention, either a Storage Service Provider or a client can access the Switches of the Fabric through either a command line interpreter or a management application. Once access to the Fabric is established, the logic of the Ports of the Switches can be selectively configured to reject or accept RCF messages as described above.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
4 December 2003 (04.12.2003)

PCT

(10) International Publication Number
WO 2003/101144 A3

(51) International Patent Classification⁷: **H04Q 11/00**,
H04L 29/06, 12/24

[IT/US]; 4141 Olga Drive, San Jose, CA 95117 (US). **DI BENEDETTO, Marco** [IT/US]; 3534 Shafer Drive, Santa Clara, CA 95051 (US).

(21) International Application Number:
PCT/US2003/016449

(74) Agent: **WEAVER, Jeffrey, K.**; Beyer Weaver & Thomas LLP, P.O. Box 778, Berkeley, CA 94704-0778 (US).

(22) International Filing Date: 22 May 2003 (22.05.2003)

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/155,698 24 May 2002 (24.05.2002) US

(71) Applicant (*for all designated States except US*): **ANDI-AMO SYSTEMS** [US/US]; 375 East Tasman Drive, San Jose, CA 95134 (US).

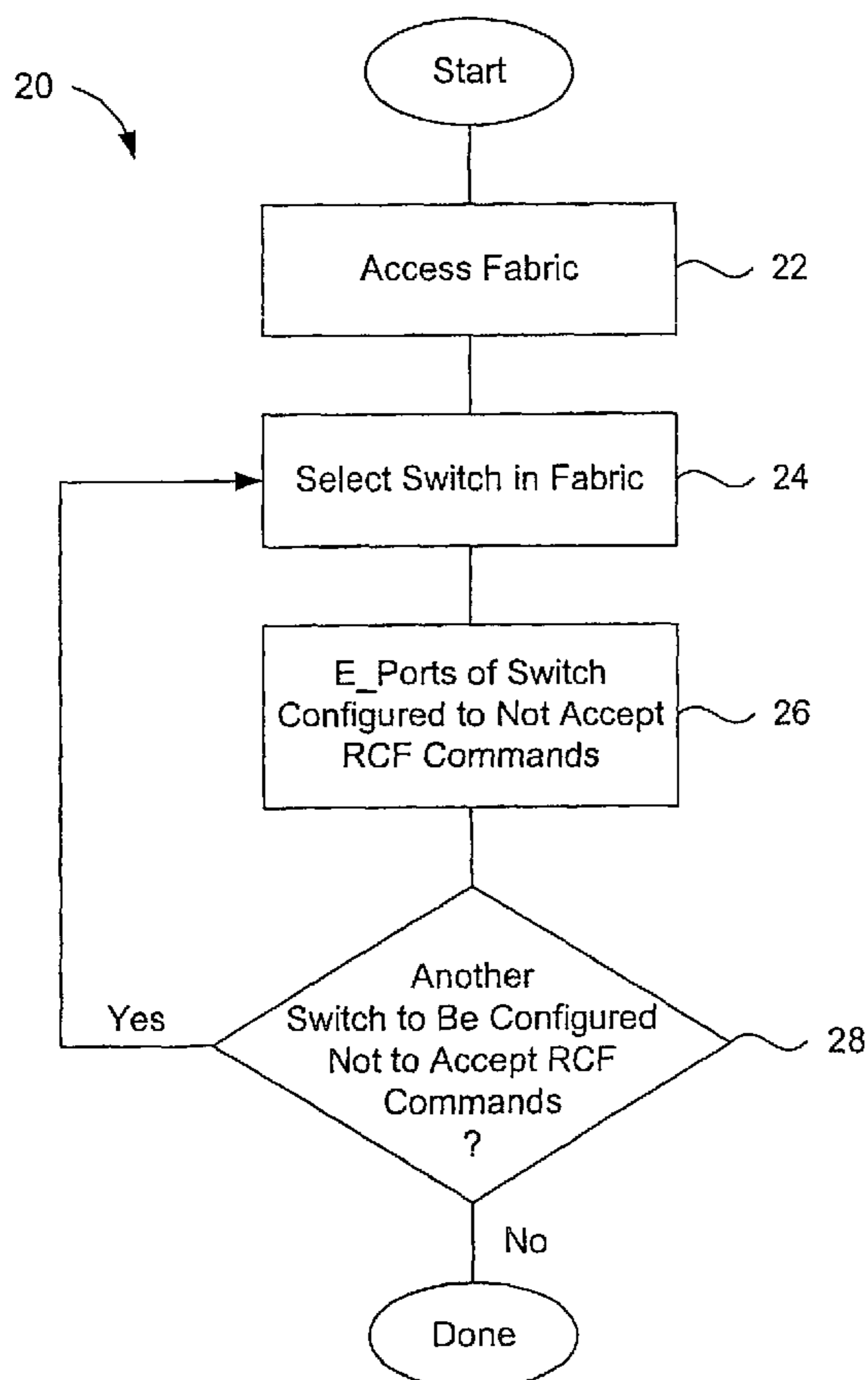
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **DESANTI, Claudio**

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR PREVENTING DISRUPTION OF FIBRE CHANNEL FABRICS CAUSED BY RECONFIGURE FABRIC (RCF) MESSAGES



(57) Abstract: An apparatus and method for preventing the disruption of Fibre Channel Fabrics caused by ReConfigure Fabric (RCF) messages is disclosed. The apparatus includes a storage area network and a plurality of Fibre Channel Switches arranged in a Fabric. Each of the plurality of Switches includes logic to selectively configure their Ports to either reject or accept RCF messages. When configured to reject RCF messages, the Switch Port that receives an RCF message will generate a reject message along with a reason code explanation "E Port Isolated", and then transition into an Isolated state. When the Switch that generated the RCF message receives the reject message, its Port also transition into the Isolated state. In accordance with the method of the present invention, either a Storage Service Provider or a client can access the Switches of the Fabric through either a command line interpreter or a management application. Once access to the Fabric is established, the logic of the Ports of the Switches can be selectively configured to reject or accept RCF messages as described above.

WO 2003/101144 A3

WO 2003/101144 A3



SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:

22 January 2004

PATENT APPLICATION

APPARATUS AND METHOD

FOR

5
PREVENTING DISRUPTION OF FIBRE CHANNEL FABRICS CAUSED BY
RECONFIGURE FABRIC (RCF) MESSAGESBACKGROUND OF THE INVENTION

10 1. Field of the Invention

The present invention relates to storage area networks, and more particularly, to an apparatus and method for preventing the disruption of Fibre Channel Fabrics caused by ReConfigure Fabric (RCF) messages.

2. Background of the Invention

15 With the increasing popularity of Internet commerce and network centric computing, businesses and other organizations are becoming more and more reliant on information. To handle all of this data, storage area networks or SANs have become very popular. A SAN typically includes a number of storage devices, a number of hosts, and a plurality of Switches arranged in a Switching Fabric. The
20 Switches selectively connect the storage devices and the hosts within the SAN.

Most SANs rely on the Fibre Channel protocol for communication within the Fabric. For a detailed explanation of the Fibre Channel protocol and Fibre Channel Switching Fabrics, see the Fibre Channel Framing and Signaling Standard, Rev 1.70, American National Standard of Accredited Standards Committee (NCITS), February
25 8, 2002 and the Fibre Channel Switch Fabric - 2, Rev. 5.4, NCITS, June 26, 2001,

In Fibre Channel, each device (hosts, storage devices and Switches) is identified by an unique eight (8) byte wide Node_Name assigned by the manufacturer. When the Fibre Channel devices are interconnected to form a SAN, the Node_Name
30 (along with other parameters) is used to identify each device. Fibre Channel frames

are used for communication among the devices in the SAN. The Node_Name, however, is not used by the frames. Instead the Fibre Channel Port of each end device (hosts and storage devices) is addressed via a three (3) byte Fibre Channel address (or FC_ID), allocated dynamically to the end devices by the Fabric. Each end device
5 acquires its FC_ID by performing a Fabric Login procedure with the Switching Fabric. In this procedure, the end device and the Fabric exchange their credentials and the operating parameters required for a successful communication across the SAN. Initially the Fabric identifies itself by an unique Fabric_Name and the end device by its unique Node_Name. Thereafter the Fabric assigns the FC_IDs to the end devices.

10 The three byte wide Fibre Channel addresses are hierarchically structured in three fields, each one byte long: Domain_ID, Area_ID, and Port_ID. Each Switch within the Fabric is assigned a Domain_ID. The end devices attached to a particular Switch are assigned the Domain_ID of that Switch. The Switch manages the allocation of the Area_ID and Port_ID fields for each end device to guarantee the
15 uniqueness of the assigned addresses in that Domain. For example, if a Switch is assigned a Domain number five and the Switch subdivides its address space in two areas each having three connected end devices, then a possible Fibre Channel address allocation is: 5:1:1, 5:1:2, 5:1:3, 5:2:1, 5:2:2, and 5:2:3.

When the Switching Fabric initializes, one of the Switches is selected as the
20 Principal Switch. The Principal Switch assigns the Domain_IDs to all the Switches in the Fabric and its Node_Name becomes the Fabric_Name of the Switching Fabric. To select the Principal Switch, all the Switches exchange with each other a message called Exchange Fabric Parameters (EFP). The EFP contains, among other parameters, the Node_Name of the sending Switch. The Switch with the lowest
25 Node_Name is designated as the Principal Switch. All the other Switches are referred to as non-principal Switches. Once the Principal Switch is selected, it sends to its neighbor Switches a Domain Identifier Assigned (DIA) message, which informs the neighbor Switches that it has been assigned a Domain_ID by the Principal Switch. In reply, the neighbor Switches send a Request Domain-Identifier (RDI) message to the
30 Principal Switch. The Principal Switch allocates the Domain Ids and responds by sending each Switch its Domain_ID. Thereafter, the Switches that received a Domain_ID send a DIA to their neighbor Switches, receive an RDI in reply, and

forward the RDI to the Principal Switch, which assigns the Domain_IDs to the requesting Switches. This process continues until all the Switches received a Domain_ID. After having received a Domain_ID, the individual Switches assign the Area_IDs and Port_IDs for each end device in its Domain. The Fabric configuration is considered completed when all the Switches have been assigned a Domain_ID. Consequently the end devices are all assigned their Area_IDs and Port_IDs.

Fibre Channel allows the merging of two separate Switching Fabrics into one. This happens when a connection is established between two Switches each belonging to a different Fabric. When such an event occurs, the Domain_ID of some of the Switches and the FC_ID of their end devices of the merged Fabric may need to be reassigned. For example, if a Fabric A which includes Domain_IDs one, two and three (1, 2 and 3) is to be merged with a second Fabric B which includes Domain_IDs one and two (1 and 2), then the overlapping Domain_IDs (1 and 2) of one of the Fabrics must be reassigned. When two Fabrics are connected, an EFP message is exchanged across the link that connects them to determine if there is any overlap among the Domain_IDs. Depending on the outcome, one of two things may happen.

If there is any overlap of Domain_ID assignments among the Switches, the link that connects the two original Fabrics is isolated. The link is logically disconnected and is not recognized by the devices, although the physical link still remains. A SAN administrator may then request a disruptive reconfiguration of the joined Fabrics to resolve the Domain_ID conflict. In this case a ReConfigure Fabric (RCF) message is flooded across all the Switches of the two original Fabrics. This stops the delivery of all the data traffic, and each Switch revokes its Domain_ID. Thereafter, a Principal Switch is selected, new Domain_IDs are assigned to the Switches, and new FC_IDs are assigned to the end devices in the same way as described above. In this manner, the two Fabrics are merged into one.

If there is no Domain_ID overlap among the Switches, then a non-disruptive Fabric reconfiguration is automatically performed. A Build Fabric (BF) message is flooded across all the Switches of the two original Fabrics. Data frames delivery is not stopped, and each Switch keeps its Domain_ID. Since the two Fabrics each have a Principal Switch, one of the two has to "resign" from its principal status leaving only

one Principal Switch for the merged Fabric. Consequently the Principal Switch selection process described above takes place. Each non-Principal Switch then makes an RDI request to the surviving Principal Switch asking for the same Domain_ID that it had before the BF message. In this way, the two Fabrics are merged without
5 changing any Switch Domain_ID assignments or any FC_IDs assigned to the end devices.

For one of the two original Fabric, however, the Principal Switch is changed. Consequently the Fabric_Name for those Switches needs to be updated. Given that the Fabric_Name is part of the Fabric Login state information that each end device
10 maintains, the Switches of the losing Fabric have to re-initialize their end devices to update their new status. This process causes a disruption of the data traffic in the Fabric with the losing Principal Switch.

From the perspective of SAN availability, both RCF and BF messages are potentially problematic. A BF may lead to a partial disruption of data traffic in
15 situations where two distinct Fabrics are merged. In general, no disruption occurs if the BF protocol is invoked inside a single Fabric. RCFs, however, will always halt the data traffic across the Fabric while the Principal Switch is identified and the Domain_IDs and FC_IDs are reassigned. As a consequence, RCF messages pose serious security concerns because a Switch in a Fabric maybe used to initiate an RCF,
20 disrupting the functionality of the Fabric.

Traditionally this security problem is solved using “physical security”, where all the Switches of a Fabric are contained inside a secure location and only the system administrator or other authorized personal are allowed to access the Fabric. In this manner, a third party such as a user or client cannot access the Switches of the Fabric
25 and trigger an RCF. But whenever the Switches are not confined in a secure location, as in the case for example of a multi-building enterprise campus, or in the case of Storage Service Providers (SSPs), this approach is not satisfactory.

This problem is especially critical for Storage Service Providers, because they provide storage services to different clients across their infrastructure. If multiple
30 clients are connected to the same Fabric using zoning techniques to isolate their traffic, one client could trigger an RCF. As a result, data flow operations for all

clients serviced by the Fabric would be disrupted. This scenario is clearly undesirable from both the Storage Service Provider and the clients perspective.

To address this concern, SSPs typically provide a separate Fabric for each client. Thus if one client wishes to merge or otherwise update its Fabric, the Fabric of other clients will not be effected. This arrangement, however, is less than ideal. Building and maintaining separate Fabrics for each client can be expensive and difficult to manage and support.

An apparatus and method for preventing the disruption of Fibre Channel Fabrics caused by ReConfigure Fabric (RCF) messages is therefore needed.

10

SUMMARY OF THE INVENTION

To achieve the foregoing, and in accordance with the purpose of the present invention, an apparatus and method for preventing the disruption of Fibre Channel Fabrics caused by ReConfigure Fabric (RCF) messages is disclosed. The apparatus includes a storage area network and a plurality of Fibre Channel Switches arranged in a Fabric. Each of the plurality of Switches includes logic to selectively configure their Ports to either reject or accept RCF messages. When configured to reject RCF messages, the Switch Port that receives an RCF message will generate a reject message along with a reason code explanation "E_Port Isolated", and then transition into an Isolated state. When the Switch that generated the RCF message receives the reject message, its Port also transition into the Isolated state. In accordance with the method of the present invention, either a Storage Service Provider or a client can access the Switches of the Fabric through either a command line interpreter or a management application. Once access to the Fabric is established, the logic of the Ports of the Switches can be selectively configured to reject or accept RCF messages as described above.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a Switching Fabric of a storage area network according to the present invention.

30

Figure 2 is a flowchart illustrating how the Switches' Ports of the Fabric are configured to reject RCF messages according to the present invention.

Figure 3 illustrates a logical disconnect between a core Switch and a client Switch according to the present invention.

5

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps have not been described in detail in order not to unnecessarily obscure the present invention.

Referring to Figure 1, a Switching Fabric of a typical storage area network which may be used by a Storage Service Provider is shown. The storage area network (SAN) 10 includes a Switching Fabric 12 that includes a plurality of Fibre Channel Switches SW located at the premises of the SSP and a plurality of clients Switches 14 located in the client premises. Each client includes one or more hosts H that can access a plurality of storage devices D through the SSP's Fabric 12 and its client Switches 14. In one embodiment, a tool to manage the Fabric 12, such as a command line interpreter or a management application 16, is connected to the Fabric 12 through the host 18 inside the SSP premises. In an alternative embodiment, the command line interpreter or management application 16 access the Fabric 12 through one of the hosts H connected to a client Switch 14. The command line interpreter or management application 16 enables a network administrator to access and apply management changes across the Fabric 12.

According to various embodiments of the invention, the hosts H can be any type of host including but not limited to servers or personal computers running on either the Unix, Windows, or any other computing platform, or a combination thereof. Similarly, the storage devices D can be any type of storage device including but not limited to tape back-up systems, emulated tape back-up systems, CD-ROM storage

30

arrays, or one or more disks such as a Redundant Array of Independent Disks (RAID), or a combination thereof. The Switches SW can be any type of Fibre Channel Switch such as those commercially available from Brocade of San Jose, CA or Andiamo Systems, the assignee of the present application. It should also be noted that the
5 Fabric 12 as shown in the figure is merely illustrative of a SAN useful for describing the present invention. In no way should its simplicity be construed as limiting the present invention which may be used in any SAN configuration. The present invention may be used in a SAN with many clients (more than the two shown) or with a SAN with multiple zones for example.

10 The present invention provides a way to configure the Switches SW of the Fabric 12 to selectively reject RCF messages received over their Ports. This technique can be used either when the Fabric 12 is initially configured or when a network administrator would like to implement a change across the Fabric 12 after it is in operation using either the command line interpreter or the management application
15 16. Further, the technique can be implemented by either a Storage Service Provider through a client controlled by the provider, through a third party client connected to the Fabric 12, typically with permission from the Storage Service Provider, or directly by the SSP itself.

Referring to Figure 2, a flow chart 20 illustrating how the Switch Ports of
20 Fabric 12 are configured to reject RCF messages according to the present invention is shown. According to the FC-SW-2 terminology, the term Port is used to indicate a generic Switch Port (potentially connected to a host or a storage device or to another Switch) while the term E_Port is used to indicate only a Switch Port connected to another Switch Port. Initially, the Fabric 12 is accessed by a system administrator
25 through a command line interpreter or a management application 16 (Box 22). Thereafter, the administrator selects a Switch in the Fabric 12 (Box 24). A Switch is generally selected because it may be at risk of receiving an RCF message. The relevant Ports of the selected Switch are configured to not accept RCF messages (Box 26) using a specific configuration command. A configuration command is an
30 administrative instruction that the system administrator issues to the selected Switch using the command line interpreter or management application 16. The configuration command is not a Switch-to-Switch message. It is therefore not defined by FC-SW-2.

Rather, the configuration command is an option of the Switch that, when set, will cause the Switch E_Ports to reject RCF messages. The behavior of the Switch therefore remains in compliance with the FC-SW-2 standard. During operation, when an RCF message is received at any of the so configured E_Ports, the E_Port generates
5 a reject message with a reason code explanation "E_Port is Isolated" and thereafter the E_Port transitions into an Isolated state. In response to the reject message, the E_Port of the Switch that generated the RCF also transitions into an Isolated state. At decision diamond 28, the administrator determines if other Ports of another Switch should be configured to not accept RCF messages. If not, the sequence is complete. If
10 yes, another Switch is selected and the aforementioned sequence is repeated.

Referring to Figure 3, a diagram illustrating the logical disconnect between the E_Ports of a client Switch and a SSP Switch is shown. The diagram shows the E_Port of a Switch 32 of the Fabric 12 belonging to the SSP and the E_Port of a Switch 34 of the client logically disconnected by a break in the connection 36. It should be noted
15 that the disconnect is a logical disconnect and not a physical disconnect, as is described in the Fibre Channel standard FC-SW-2 as the resulting status of when the two E_Ports connected by a link are in the Isolated state. In the manner described above, the Fabric 12 can be configured so that some or all of the Ports of the Switches can be configured to reject RCF messages. This arrangement allows, from a practical
20 point of view, the Fabric 12 to be used by two (or more) clients. The arrangement also prevents any one client from disrupting the Fabric 12 to the detriment of the other client(s) while attempting to perform an action that involves an RCF message. The Fabric will remain in this state and can therefore be accessed by two or more clients until the Ports of the Switches are re-configured to accept RCF messages. Typically
25 the Ports of the Switches can be re-configured to accept RCF messages only by an explicit management action intended to revoke the aforementioned state of the Ports.

The embodiments of the present invention described above are to be considered as illustrative and not restrictive. For example, the present invention does not necessarily have to be used with a SAN. Rather, it can be used by any type of
30 network with Fibre Channel Switches operating as described in the Fibre Channel standard FC-SW-2 to perform the Fabric configuration. The invention is not to be limited to the details given herein, but may be modified within the scope and

equivalents of the appended claims.

CLAIMS

1. A method for preventing disruption of a Fabric of a storage area network, the method comprising:
 - selectively configuring one or more Ports of Fibre Channel Switches, including a first port in a first fibre channel switch of the Fabric of the storage area network to reject ReConfigure Fabric (RCF) messages;
 - determining that the first port has received an RCF message from a second port;
 - transitioning the first port to an isolated state after the first port receives the RCF message;
 - transitioning the second port sending the RCF message to an isolated state after the first port transitions to the isolated state;
 - reconfiguring the first port to accept RCF messages upon receiving a management action to revoke the isolated state of the first port.
2. The method of claim 1, wherein the configuring of the Ports to selectively reject RCF messages is performed by a Storage Service Provider.
3. The method of claim 1, wherein the configuring of the Ports to selectively reject RCF messages is performed by a client.
4. The method of claim 1, further comprising: enabling a plurality of clients to access the Fabric.
5. The method of claim 1, wherein the Ports of the Switches of the Fabric are configured to generate a reject message with a reason code explanation "E_Port Isolated" when RCF messages are received.
6. The method of claim 1, further comprising configuring the Ports of the Switches of the Fabric through a command line interpreter or a management application.
7. The method of claim 6, further comprising using a management action for configuring the Ports of the Switches of the Fabric to reject the RCF messages.

8. The method of any one of claims 1 to 7 , further comprising selectively reconfiguring the Ports of the Switches of the Fabric of the storage area network to accept RCF messages by an explicit management action.
9. The method of any one of claims 1 to 8, wherein the Switches rely on one of the following types of protocols for communication: Fibre Channel, or Fibre Channel over the Internet Protocol (FCIP), or Fibre Channel over any other technology.
10. A method as claimed in claim 1, wherein a plurality of clients are permitted to use the Fabric; the clients having the ability to perform actions that invoke RCF messages.
11. The method of claim 10, further comprising logically isolating an E_Port which received an RCF message from a client Switch.
12. A method as claimed in claim 1, further comprising allowing an administrator to establish a connection to the Fabric; and allowing the administrator to configure selectively one or more Ports of the Fibre Channel Switches of the Fabric to reject RCF messages.
13. The method of claim 12, further comprising establishing the connection to the Fabric through a command line interpreter or a management application.
14. A Switch configured to be included in the Fabric of a storage area network, characterised in that the Switch comprises:
 - a processor; and
 - memory having stored thereon computer-readable instructions, the computer-readable instructions, when executed by the processor, cause the Switch to selectively reject ReConfigure Fabric (RCF) messages, wherein a first port transitions to an isolated state after receiving an RCF message and triggers a second port sending the RCF message to transition to the isolated state, wherein the first port remains in the isolated state until a management action reconfigures the first port to accept RCF messages.
15. The Switch of claim 14, wherein the computer-readable instructions are configured to selectively cause an E_Port of the Switch to reject RCF messages when the logic is selected to reject RCF messages.

16. The Switch of claim 15, wherein the computer-readable instruction are further configured to cause an E_Port to generate a reject message with a reason code explanation "E_Port Isolated" if an RCF message is received.
17. The Switch of claim 14, wherein the computer-readable instructions are adapted to be reconfigured to allow RCF messages to be accepted.
18. An apparatus comprising:
 - a storage area network with a Fibre Channel Fabric; and
 - a plurality of Switches as claimed in any one of claims 14 to 17 arranged in the Fabric.
19. The apparatus of claim 18, further comprising a connection to provide access to the Fabric, the connection providing access from a command line interpreter or a management application.
20. The apparatus of claim 18 or 19, wherein the Fabric relies on one of the following types of protocols for communication: Fibre Channel, or Fibre Channel over the Internet Protocol (FCIP), or Fibre Channel over any other technology.

TOR_LAW\7221886\3

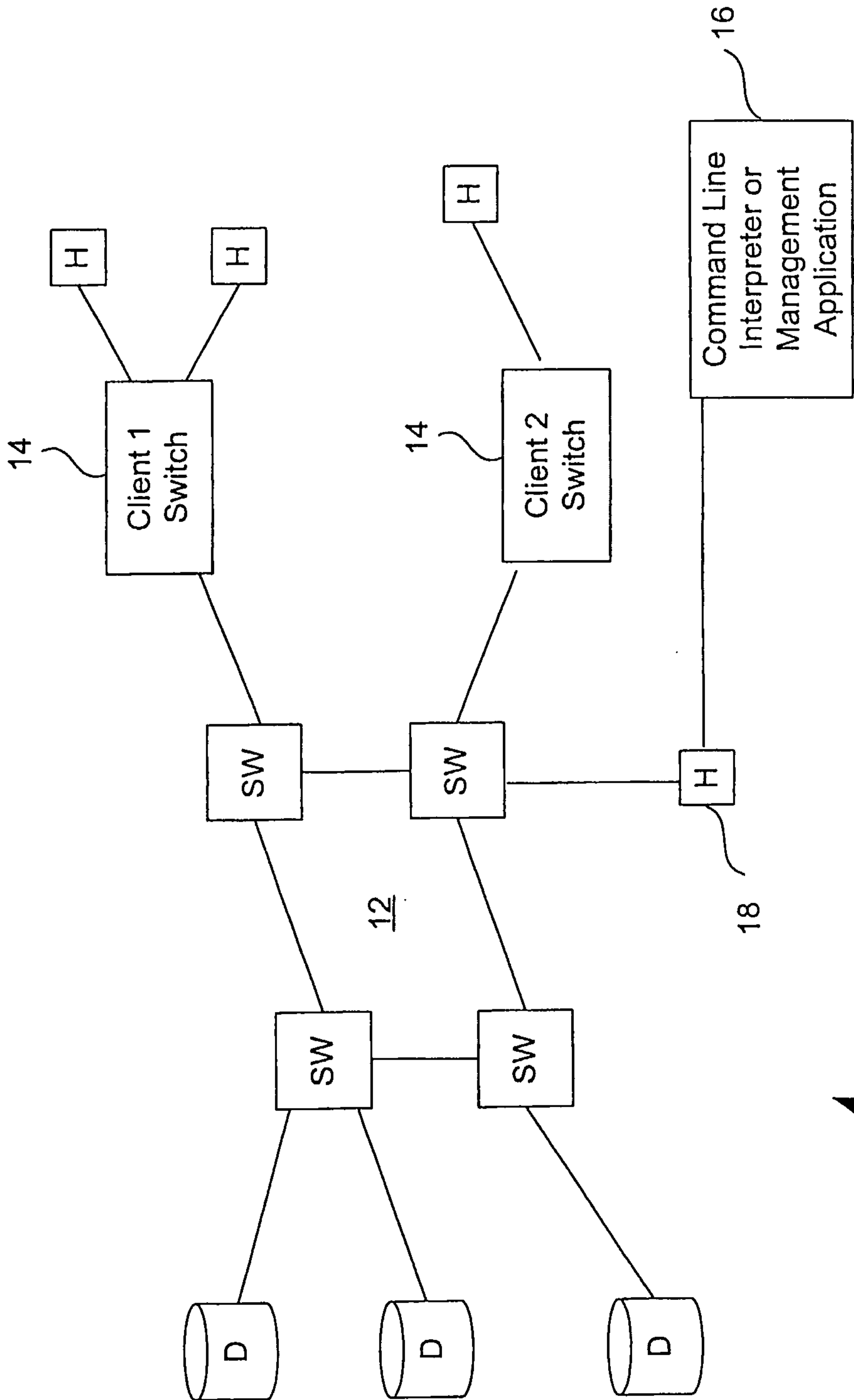


FIG. 1

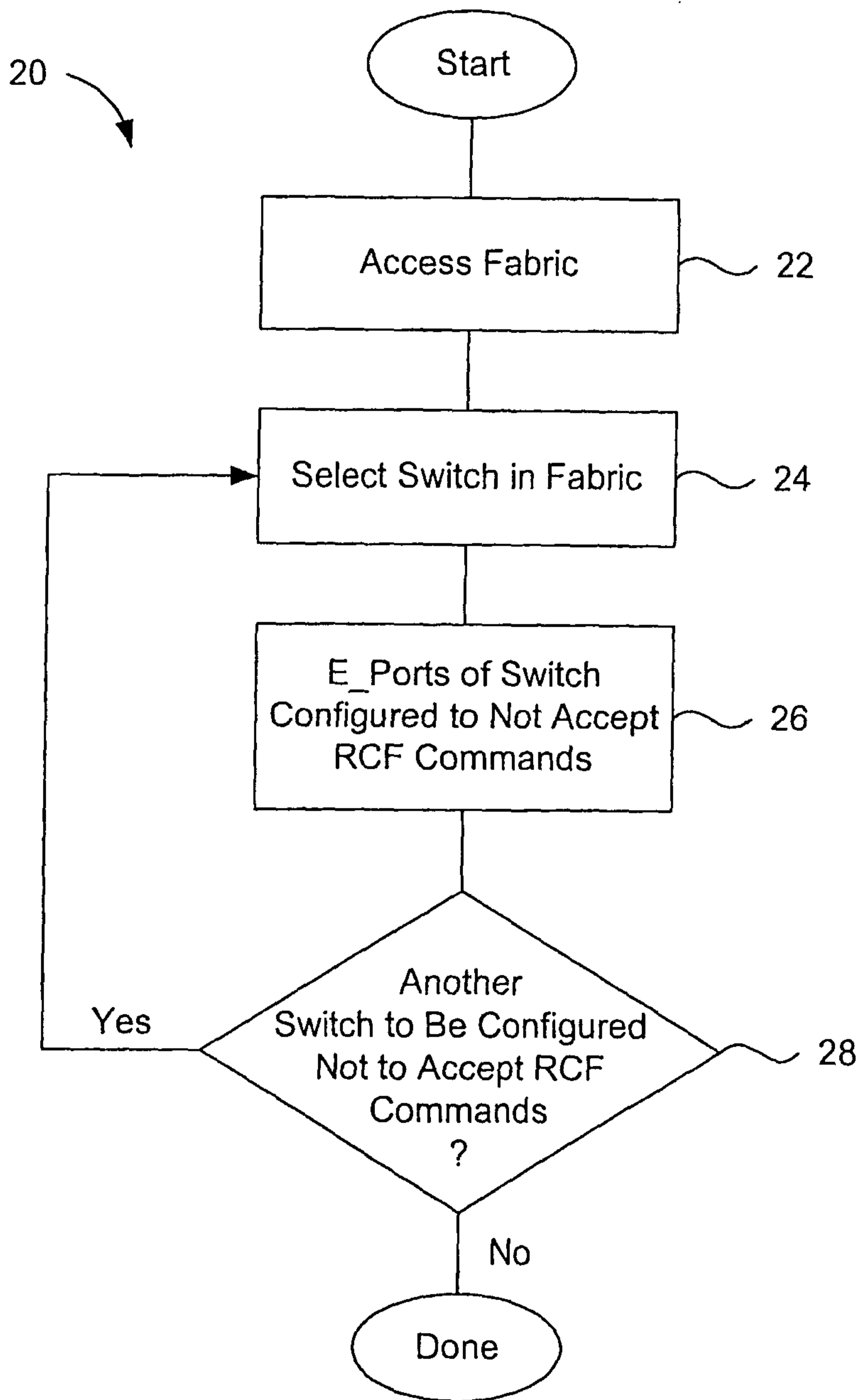


FIG. 2

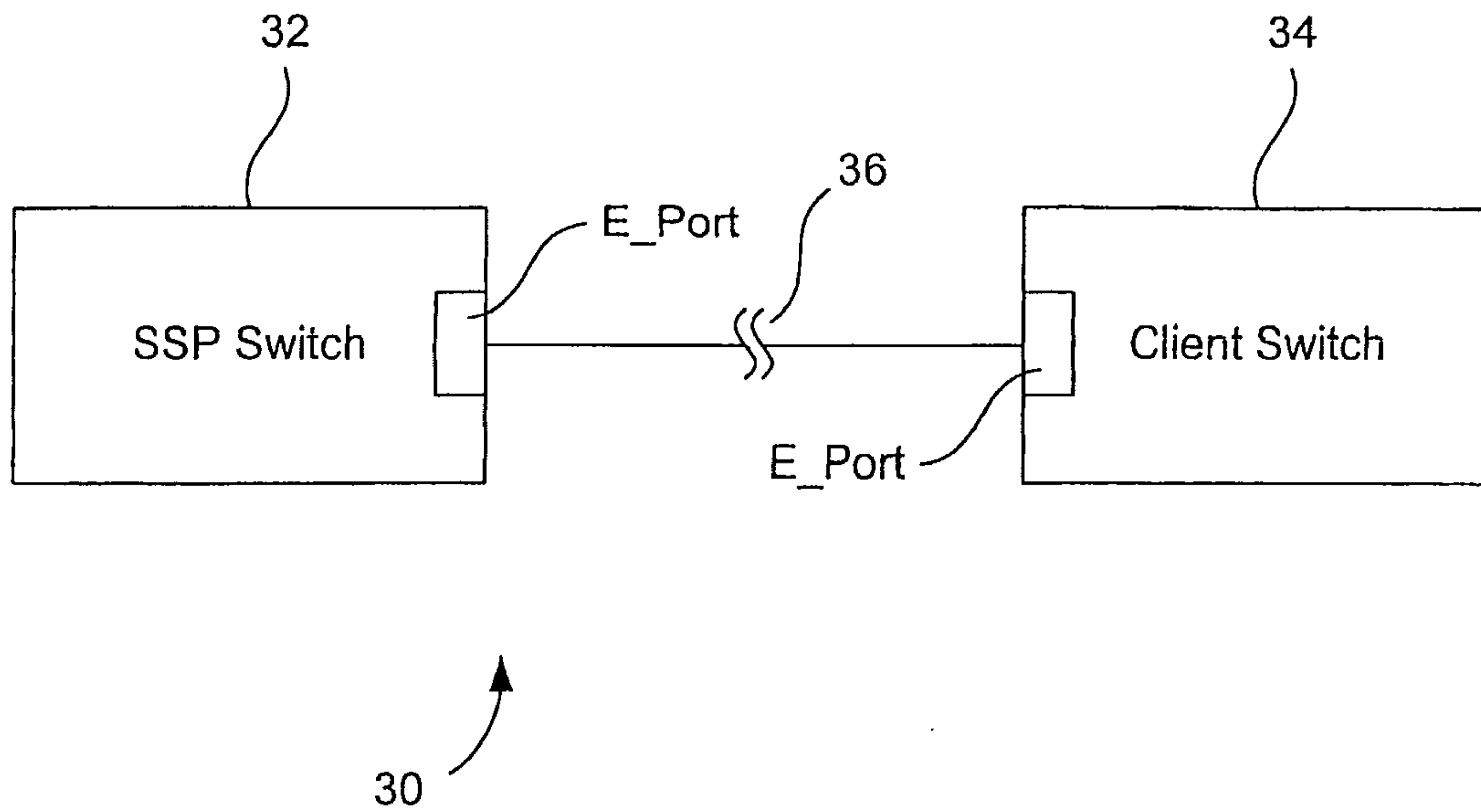


FIG. 3

20

Start

Access Fabric

22

Select Switch in Fabric

24

E_Ports of Switch
Configured to Not Accept
RCF Commands

26

Another
Switch to Be Configured
Not to Accept RCF
Commands
?

28

Yes

No

Done

