US008356334B2

(12) **United States Patent**
Yik et al.

(10) **Patent No.: US 8,356,334 B2**
(45) **Date of Patent: Jan. 15, 2013**

(54) **DATA NETWORK NODE HAVING ENHANCED SECURITY FEATURES**

(75) Inventors: **James Ching-Shau Yik**, Mission Viejo, CA (US); **Eric Lin**, Hacienda Heights, CA (US)

(73) Assignee: **Conexant Systems, Inc.**, Newport Beach, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 3275 days.

(21) Appl. No.: **09/866,259**

(22) Filed: **May 25, 2001**

(65) **Prior Publication Data**

US 2003/0208571 A1 Nov. 6, 2003

(51) **Int. Cl.**
G06F 7/04 (2006.01)

(52) **U.S. Cl.** **726/3**; 726/2; 380/247; 380/248; 380/249; 380/250; 709/225

(58) **Field of Classification Search** 709/208, 709/225; 713/162; 726/2, 3; 380/247, 248, 380/249, 250
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,893,340	A *	1/1990	Lubarsky et al.	709/208
5,996,021	A *	11/1999	Civanlar et al.	709/238
6,069,889	A *	5/2000	Feldman et al.	370/351
6,870,844	B2 *	3/2005	Tuck et al.	370/390
7,065,644	B2 *	6/2006	Daniell et al.	713/166
2002/0147916	A1 *	10/2002	Strongin et al.	713/193
2002/0156888	A1 *	10/2002	Lee et al.	709/224
2003/0014665	A1 *	1/2003	Anderson et al.	713/201

OTHER PUBLICATIONS

Badger, M.R. and Murphy, S.L. Digitial Signature Protection of the OSPF Routing Protocol, 1996 IEEE, pp. 93-102.*

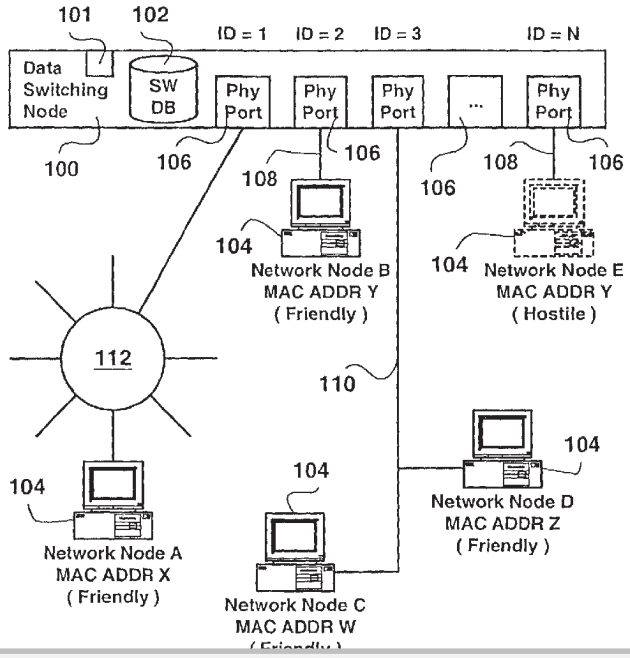
* cited by examiner

Primary Examiner — Edan Orgad
Assistant Examiner — Roderick Tolentino
(74) *Attorney, Agent, or Firm* — Jackson Walker L.L.P.; Christopher J. Rourk

(57) **ABSTRACT**

An apparatus and methods for securely forwarding data packets at a data switching node in a data transport network is provided. The data switching node maintains a switching database of switching entries. Each switching entry has a modification protection feature preventing its modification when activated. Dynamic topology discovery of data network nodes can be disabled via topology discovery control flags associated with individual physical communications ports of the data switching node. Unknown destination flood data traffic is not replicated to physical communications ports having topology discovery disabled or specifying the suppression of replication of such unknown destination data traffic thereto. The advantages are derived from a data switching node being enabled to operate concurrently in friendly and hostile environments while detecting, preventing and reporting incidences of hostile MAC ADDR attacks.

20 Claims, 3 Drawing Sheets



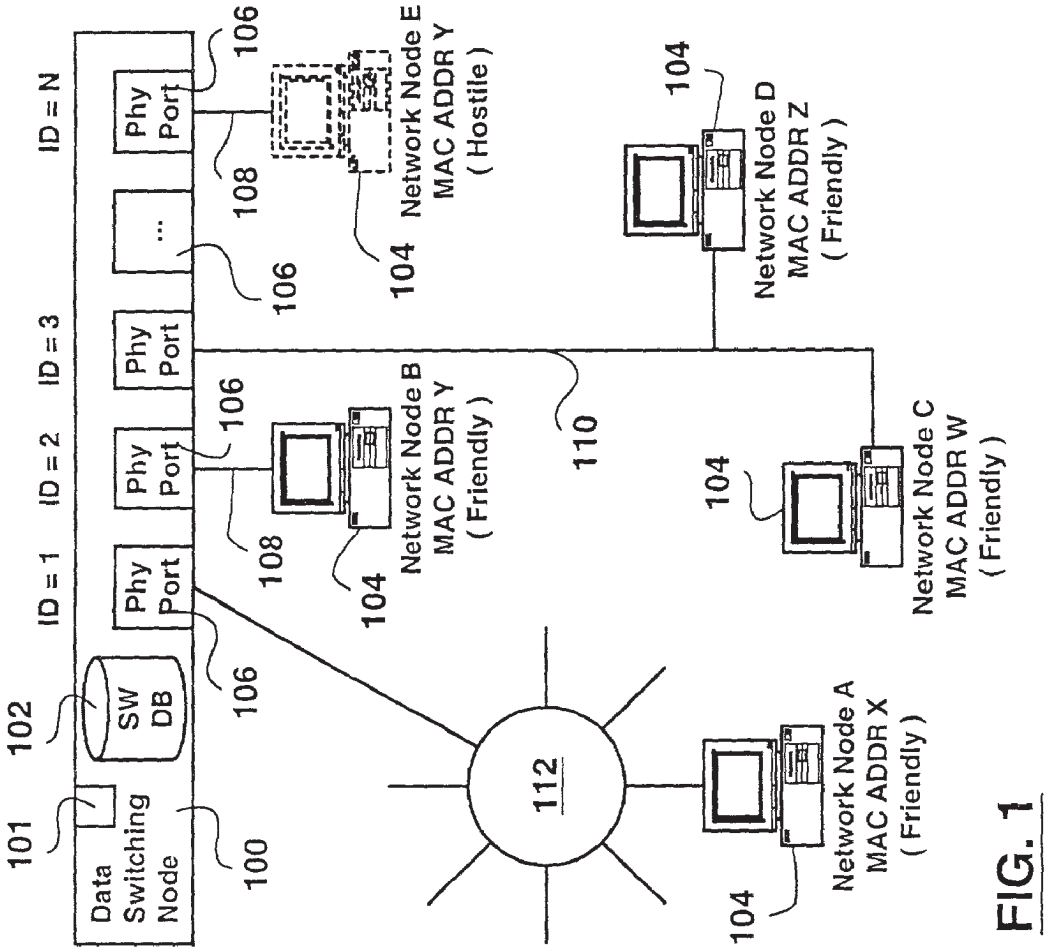


FIG. 1

Global Controls	
Topology Discovery	Enable
Unknown Destination Flood Suppresion	Disable

400

FIG. 4A

Global Controls	
MAC ADDR Attack Protection	Enable

410

FIG. 4B

Entry #	Routing Entry Protection Status	Source MAC Address	Physical Port ID
0	unProtected	X	1
1	Protected	Y	2
2	unProtected	W	3
3	Protected	Z	3
...	...	...	...

202 202 202 202

200

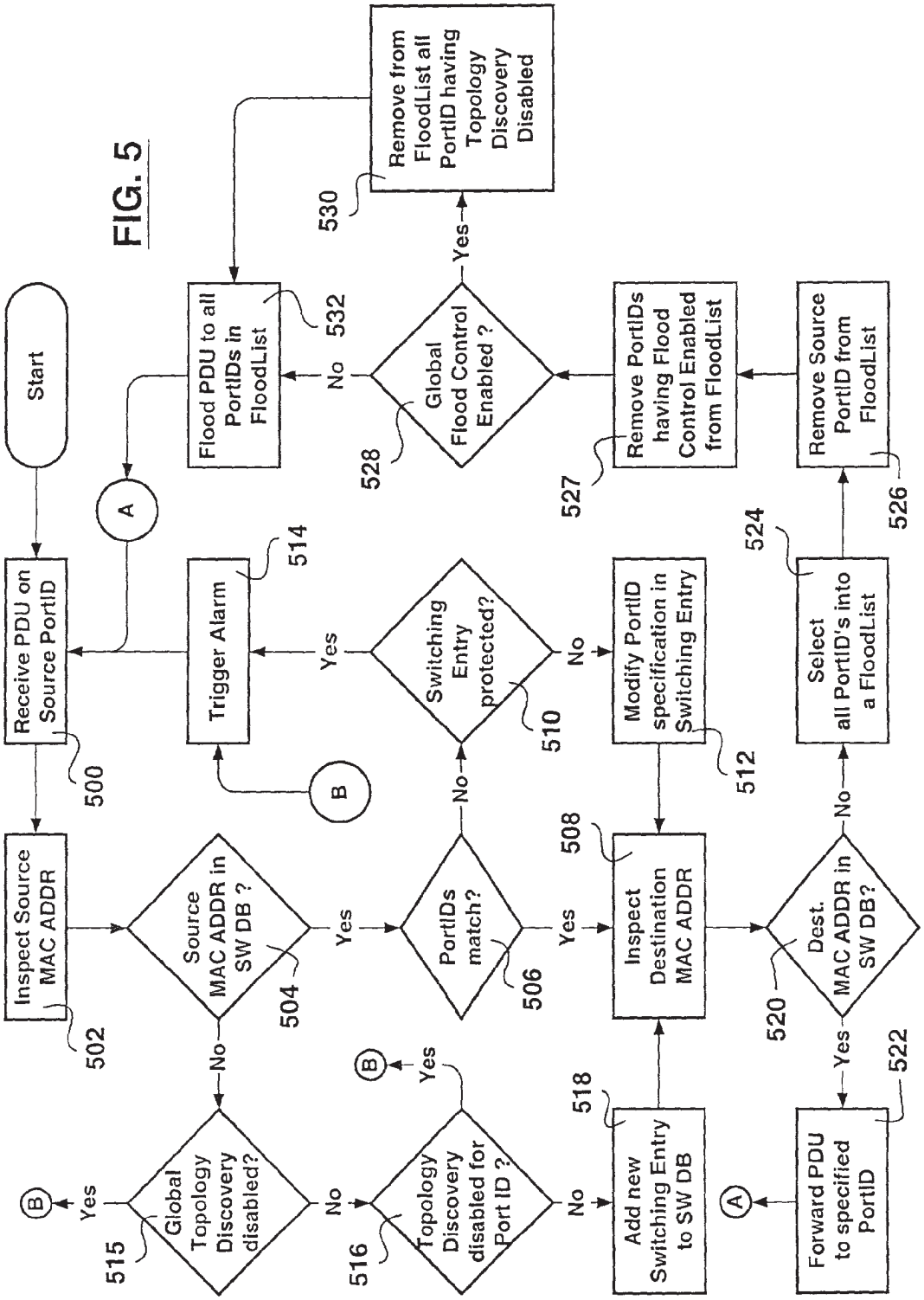
FIG. 2

Physical Port ID	Topology Discovery	Unknown Destination Flood Suppression
1	Enabled	Enabled
2	Enabled	Disabled
3	Disabled	Enabled
...	...	...
N	...	...

300

FIG. 3

FIG. 5



DATA NETWORK NODE HAVING ENHANCED SECURITY FEATURES

FIELD OF THE INVENTION

The invention relates to data switching in a data transport network and in particular to methods and apparatus providing enhanced networking security.

BACKGROUND OF THE INVENTION

In conveying data over data transport networks, data switching nodes are used to direct the flow of data traffic over interconnecting data links. Each data link is connected to a data switching node via a physical communications port having a port identifier.

The data to be conveyed is typically divided into Payload Data Units (PDUs) such as data packets, frames, cells, etc. Each PDU includes routing information and a payload. The routing information is typically held in a PDU header. For example the routing information includes Media Access Control ADDResses (MAC ADDRs). MAC ADDRs are unique and are associated with data network interfacing equipment associated with data network nodes. An example network interfacing equipment is a Network Interface Card (NIC). Therefore a MAC ADDR is said to represent a data network node identifier. MAC ADDR instances in the routing information are associated with what are known as Source and Destination Addresses.

Data switching nodes make use of the MAC ADDR information for dynamic topology discovery of connected data network nodes and to forward data traffic to particular destination MAC ADDRs. Such a data switching node maintains a switching database and is said to perform "Layer 2 switching". Layer 2 refers to the Open Systems Interconnection (OSI) protocol stack, which specification is well known in the art of data switching and transport, and is included herein by reference.

An exemplary implementation of a switching database is a table having switching database entries, each entry specifying an association between a MAC ADDR and Port IDentifier (PortID). Any received PDU specifying a MAC ADDRs held in the switching database is switched to the PortID specified in the corresponding database entry.

Without the switching database the data switching node behaves like a hub which broadcasts each PDU over all physical communications ports associated therewith except for the physical communications port on which the PDU was received. This broadcast operation is also known as "flooding". Having the switching database reduces the incidence of flooding to instances in which received PDUs bear unknown destination MAC ADDRs not present in the switching database.

In constructing a switching database, process also known as topology discovery, a controller associated with the data switching node extracts the source MAC ADDRs of PDUs received on each physical communications port. If the MAC ADDR:PortID pair is not found in the switching database, the controller creates an entry in the switching database storing the new MAC ADDR:PortID association. This ability to construct the switching database also provides a dynamic discovery of data network nodes recently added to data network segments connected to the data switching node. Dynamically discovering data network nodes and constructing a switching

interaction and absolute knowledge of connected data network nodes in the data transport network.

The plug-and-play operation is often extended to enabling the data switching node to keep track of movement of data network nodes as they connect to different segments of the data transport network associated with the data switching node. The association between the MAC ADDR and PortID is changed in the switching database when a PDU having a MAC ADDR specified in an entry is received from a different physical communications port having a different PortID than the PortID specified therein. In such a case, the new PortID is simply written over the previous PortID specification stored in the entry.

While the plug-and-play functionality reduces human involvement in the discovery of data network nodes in the associated data transport network in the construction and, the reconfiguration of the switching database as data network nodes move in the associated data network, the plug-and-play functionality exposes data network nodes to hostile MAC ADDR attacks. An exposure to a hostile environment exists when the data switching node bridges connectivity between two data transport networks, but is not limited thereto.

For example, in a hostile environment, a hostile data network node may try to spy on the traffic destined to a specific MAC ADDR by taking advantage of the automatic switching database reconfiguration feature of the data switching node.

According to an exemplary scenario, the hostile data network node sends towards the data switching node a data packet having a source MAC ADDR corresponding to the MAC ADDR of the data network node to be attacked. The data switching node registers a data network node move and modifies the switching database entry corresponding to the MAC ADDR by overwriting the PortID specification with the PortID corresponding to the physical communications port with which the hostile data network node is associated. Thereafter, all PDUs destined to the MAC ADDR of the attacked data network node are forwarded by the data switching node to the hostile data network node. The MAC ADDR attack can be as extensive as the hostile data network node taking over the functionality of the attacked data network node. The incident fully complies with the intended operation of currently deployed data switching equipment and would otherwise go undetected.

Therefore, there is a need to enable data switching nodes to operate concurrently in friendly and hostile environments while detecting, preventing and reporting incidences of hostile MAC ADDR attacks.

SUMMARY OF THE INVENTION

In accordance with an aspect of the invention, a secure data switching node is provided. The data switching node maintains a switching database having switching database entries. Each database entry is provided with a corresponding entry protection flag. Each entry protection flag is used to selectively disable the editing of the corresponding database entry and enable the data switching node to operate securely concurrently in friendly and hostile data networking environments.

In accordance with another aspect of the invention, a secure data switching node is provided. The data switching node forwards data traffic between a plurality of physical communications ports and particularly between data network nodes connected to data network segments reachable via physical communications ports. Each physical communications port

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.