

UTILITY PATENT APPLICATION TRANSMITTAL <i>(Only for new nonprovisional applications under 37 CFR 1.53(b))</i>	Attorney Docket No.	160142
	First Named Inventor	Joseph L. Vilella
	Title	Mutually secure optical data network and method
	Express Mail Label No.	Filed via EFS-Web

APPLICATION ELEMENTS <i>See MPEP chapter 600 concerning utility patent application contents.</i>	ADDRESS TO: Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450
--	--

<ol style="list-style-type: none"> 1. ☒ Fee Transmittal Form (PTO/SB/17 or equivalent) 2. ☒ Applicant asserts small entity status. See 37 CFR 1.27 3. ☐ Applicant certifies micro entity status. See 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent. 4. ☒ Specification [Total Pages <u>18</u>] Both the claims and abstract must start on a new page. (See MPEP § 608.01(a) for information on the preferred arrangement) 5. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets <u>6</u>] 6. Inventor's Oath or Declaration [Total Pages _____] (including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e)) <ol style="list-style-type: none"> a. ☐ Newly executed (original or copy) b. ☐ A copy from a prior application (37 CFR 1.63(d)) 7. ☒ Application Data Sheet * See note below. See 37 CFR 1.76 (PTO/AIA/14 or equivalent) 8. CD-ROM or CD-R In duplicate, large table, or Computer Program (Appendix) <div style="margin-left: 20px;"> ☐ Landscape Table on CD </div> 9. Nucleotide and/or Amino Acid Sequence Submission (if applicable, items a. – c. are required) <ol style="list-style-type: none"> a. ☐ Computer Readable Form (CRF) b. ☐ Specification Sequence Listing on: <ol style="list-style-type: none"> i. ☐ CD-ROM or CD-R (2 copies); or ii. ☐ Paper c. ☐ Statements verifying identity of above copies 	ACCOMPANYING APPLICATION PAPERS <ol style="list-style-type: none"> 10. ☐ Assignment Papers (cover sheet & document(s)) Name of Assignee _____ 11. ☐ 37 CFR 3.73(c) Statement ☐ Power of Attorney (when there is an assignee) 12. ☐ English Translation Document (if applicable) 13. ☐ Information Disclosure Statement (PTO/SB/08 or PTO-1449) ☐ Copies of citations attached 14. ☐ Preliminary Amendment 15. ☐ Return Receipt Postcard (MPEP § 503) (Should be specifically itemized) 16. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed) 17. ☐ Nonpublication Request Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent. 18. ☐ Other: _____ _____ _____ _____
---	---

***Note:** (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must** be included in an Application Data Sheet (ADS).
 (2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS

☒ The address associated with Customer Number: <u>24243</u>				OR ☐ Correspondence address below	
Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	
Signature			Date		
/John Buchaca/			2016-11-14		
Name (Print/Type)			Registration No. (Attorney/Agent)		
John D. Buchaca			37289		

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	160042
		Application Number	
Title of Invention	Mutually secure optical data network and method		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor	1					Remove
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Joseph	L.	Vilella			
Residence Information (Select One) • US Residency Non US Residency Active US Military Service						
City	San Diego	State/Province	CA	Country of Residence	US	
Mailing Address of Inventor:						
Address 1	Spada Innovations, Inc.					
Address 2	4660 La Jolla Village Dr., Suite 500					
City	San Diego	State/Province	CA			
Postal Code	92122	Country	US			
Inventor	2					Remove
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	James	R.	Reynante			
Residence Information (Select One) • US Residency Non US Residency Active US Military Service						
City	San Diego	State/Province	CA	Country of Residence	US	
Mailing Address of Inventor:						
Address 1	Spada Innovations, Inc.					
Address 2	4660 La Jolla Village Dr., Suite 500					
City	San Diego	State/Province	CA			
Postal Code	92122	Country	US			
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						
Add						

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	160042
		Application Number	
Title of Invention	Mutually secure optical data network and method		

☐ An Address is being provided for the correspondence information of this application.

Customer Number	24243		
Email Address	john@charmason.com	<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	Mutually secure optical data network and method		
Attorney Docket Number	160042	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	6	Suggested Figure for Publication (if any)	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:
☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	24243		

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	160042
		Application Number	
Title of Invention	Mutually secure optical data network and method		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	14419092	2015-02-02
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14419092	a 371 of international	PCT/US2013/053389	2013-08-02
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
PCT/US2013/053389	Claims benefit of provisional	61678977	2012-08-02
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	160042
		Application Number	
Title of Invention	Mutually secure optical data network and method		

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

☐ NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	160042
		Application Number	
Title of Invention	Mutually secure optical data network and method		

Applicant	1		Remove
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>			
		Clear	
☒ Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor	
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
<div style="border: 1px solid black; height: 15px; width: 100%;"></div>			
Name of the Deceased or Legally Incapacitated Inventor : <div style="border: 1px solid black; width: 400px; height: 15px;"></div>			
If the Applicant is an Organization check here. ☐			

Prefix	Given Name	Middle Name	Family Name	Suffix
<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>
Mailing Address Information For Applicant:				
Address 1	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>			
Address 2	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>			
City	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	State/Province	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	
Country	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Postal Code	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	
Phone Number	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	Fax Number	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>	
Email Address	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>			
Additional Applicant Data may be generated within this form by selecting the Add button.				Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.	
Assignee	1
<p>Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.</p>	
Remove	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	160042
		Application Number	
Title of Invention	Mutually secure optical data network and method		

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country ⁱ		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.					
Signature	/John Buchaca/			Date (YYYY-MM-DD)	2016-11-14
First Name	John	Last Name	Buchaca	Registration Number	37289
Additional Signature may be generated within this form by selecting the Add button.					<input type="button" value="Add"/>

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Mutually secure optical data network and method

Prior Application

This is a continuation-in-part of US Patent Application Serial No. 14419092, filed 2015-02-02, which is a 371 of International Application Serial No. PCT/US2013/053389, filed 2013-08-02, which claims the benefit of U.S. Provisional Patent Application Serial No. 61678977, filed 2012-08-02 all of which are incorporated herein by reference.

Field of the Invention

The instant invention relates to computer networks and more particularly to optical data network traffic routing to multiple users in a local area.

Background

Nowadays a wide variety of entities are moving towards the use of Passive Optical Networks (“PON”) and benefit from the interconnectivity provided by local and wide area networks, and connection to the Internet. Many entities depending on their purpose have many types of devices connected to the network including personal computers, wireless controllers, application servers, printers, scanners, ambient control systems, security cameras and sensors, phone systems, gaming consoles and television sets. The digital signals carried by the PON include converged voice, data and video signal content traffic.

Many individual and business users send and receive digital information which is intended to remain private and can be confidential to the individual users. Such users can be businesses located in the same office building as co-tenants, guests located in a hotel, users located in a commercial, local, state, federal or similar entity, subscribers in a residential entity such as owners or tenants. In the past, reasonable privacy and security can be accomplished by each user connecting directly to a secure service provider carrier using a dedicated headend located in the entity space including a modem, workgroup switches and routing equipment. This equipment typically requires its own cooling equipment. Often the connection throughout the local network and to the carrier is through copper wiring which, due to its electrical resistance, can generate additional heat requiring cooling. All this equipment and cooling capability is often multiplied by the number of individual tenants in a building, leading to high power consumption.

A typical limiting factor using copper wiring for digital connection lines is bandwidth. Thus, a particular business tenant may elect to upgrade its individual local network and its connection to the carrier using high bandwidth equipment. Increasing the bandwidth often requires additional copper wiring, and more air conditioning.

With the development of optical fiber technology, photonic networks which are typically referred to as Passive Optical Networks can deliver significantly higher bandwidth and lower power consumption. This need for increased speed and sustainability by reduced power consumption has promoted the accelerated adoption of PON in most commercial and residential sectors.

The higher available bandwidth has led to network designs where one or more PON interface routers can distribute data streams to a multiplicity of users through an Optical Line Terminal (“OLT”). Further, this can eliminate the need for a dedicated router for each user. Unfortunately however, this creates an increased cyber-security risk for all those users connected to the PON interface routers since the global routing table can be surreptitiously accessed by a nefarious user, or some cyber-entity mimicking a user on the PON.

The instant invention results from efforts to provide an improved passive optical networking system that addresses one or more of the above problems.

Summary

The primary and secondary objects of the invention are to provide an improved optical networking system. These and other objects are achieved by providing an optical network interface router including at least one virtual routing table for each of a plurality of optical network units to which the interface router is connected.

In some embodiments there is provided a multi-user optical data network apparatus comprises: a plurality of network service carrier lines connected to a passive optical network interface router; at least one uplink connecting said interface router to an optical line terminal; said optical line terminal being connected to a number of passive optical network feeds for carrying a common data feed to a plurality of optical network units each supporting at least one of a plurality of private user devices; said interface router being configured to have at least one virtual routing table for each one of said plurality of optical network units; and, wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices.

In some embodiments said common data feed is encrypted.

In some embodiments said interface router is a premise router.

In some embodiments said interface router is further configured to have a global routing table, and wherein a number of destinations listed in said at least one virtual routing table are associated with corresponding destinations listed in said global routing table.

In some embodiments each of said optical network units provides service to a separate number of private users.

In some embodiments said uplink carries data including digitized voice and video data.

In some embodiments there is provided a multi-user optical data network apparatus comprises: a plurality of network service carrier lines connected to a plurality of passive optical network interface routers; a plurality of uplinks connecting said interface routers to an optical line terminal; said optical line terminal being connected to a number of passive optical network feeds for carrying a common data feed to a plurality of optical network units each supporting at least one of a plurality of private user devices; wherein each of said interface routers is configured to have at least one virtual routing table for each one of said plurality of optical network units to which said each of said interface routers is connected; and, wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices.

In some embodiments there is provided a digital data network communication method comprises: accepting a plurality of private data streams into a passive optical network interface router serving a plurality of private users through a plurality of optical network units; aggregating said private data streams into a combined data feed; routing said data feed to at least two of said plurality of optical network units; extracting from said data feed a first one of said private data streams; wherein said routing comprises: providing a global routing table; providing an independently unique virtual routing table for each of said plurality of optical network units; tagging ethernet frames intended for a first one of said plurality of optical network units according to entries in a first one of said virtual routing tables associated with a first one of said optical network units; distributing said tagged ethernet frames according to both of said global routing table and said first one of said virtual routing tables.

In some embodiments said distributing comprises associating destinations listed in said first one of said virtual routing tables with destinations listed in said global routing table.

In some embodiments each of said optical network units provides service to a separate number of private users.

In some embodiments said accepting comprises: interfacing a plurality of service provider data lines through a single headend.

In some embodiments said interfacing comprises: utilizing at least one premise router and a radio frequency video converter; and, feeding an output of said premise router through an optical line terminal.

In some embodiments said interfacing further comprises: feeding an output of said converter through said optical line terminal.

In some embodiments said optically routing comprises: sending said encrypted data feed through an optical splitter.

In some embodiments each of said streams comprises: encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed; and, wherein said extracting comprises: partially decrypting said encrypted data feed.

In some embodiments said encrypted data feed comprises: a plurality of encrypted ethernet frames; wherein a subset of said frames are associated with a first one of said users and a second subset of said frames is associated with a second one of said users.

In some embodiments said extracting comprises: operating an optical network unit at each of said tenants; wherein said operating comprises: decrypting incoming intended data packets from said feed; not decrypting incoming unintended data packets from said feed; and, encrypting outgoing data packets to said feed.

In some embodiments said aggregating comprises using an enterprise aggregating switch.

In some embodiments there is provided a specialized headend encrypting/decrypting aggregation unit feeding an encrypted optical data feed to each user, and providing a specialized encrypting/decrypting optical terminal device at each user for extracting and injecting the end user's data to/from the feed.

In some embodiments there is provided a digital data network communication method comprises: accepting a plurality of private data streams serving a plurality of private users; encrypting each of said streams; aggregating said encrypted streams into a combined encrypted data feed; optically routing said encrypted data feed to at least two of said plurality of private users; extracting from said encrypted data feed a first one of said private data streams; wherein said extracting comprises: partially decrypting said encrypted feed.

In some embodiments there is provided a digital data network communication method comprises: accepting a plurality of private non-encrypted data streams serving a plurality of

private users; aggregating said non-encrypted streams into a combined non-encrypted data feed; optically routing said non-encrypted data feed to at least two of said plurality of private users; extracting from said non-encrypted data feed a first one of said private non-encrypted data streams.

In some embodiments said encrypting each of said streams comprises: encrypting informational data; encrypting telephone data; and, encrypting video data.

In some embodiments said private non-encrypted data streams comprise: non-encrypted informational data; non-encrypted telephone data; and, non-encrypted video data.

In some embodiments said accepting comprises: interfacing a plurality of service provider data lines through a single headend.

In some embodiments said interfacing comprises: utilizing a premise router and a radio frequency video converter; and, feeding an output of said premise router through an optical line terminal.

In some embodiments said interfacing further comprises: feeding an output of said converter through said optical line terminal.

In some embodiments said optically routing comprises: sending said encrypted data feed through an optical splitter.

In some embodiments said optically routing comprises: sending said non-encrypted data feed through an optical splitter.

In some embodiments said encrypted data feed comprises: a plurality of encrypted ethernet frames; wherein a subset of said frames are associated with a first one of said users and a second subset of said frames is associated with a second one of said users.

In some embodiments said non-encrypted data feed comprises: a plurality of non-encrypted ethernet frames; wherein a subset of said frames are associated with a first one of said users and a second subset of said frames is associated with a second one of said users.

In some embodiments said extracting comprises: operating an optical network unit at each of said users; wherein said operating comprises: decrypting incoming intended data packets from said feed; not decrypting incoming unintended data packets from said feed; and, encrypting outgoing data packets to said feed.

In some embodiments said extracting comprises: operating an optical network unit at each of said users; wherein said operating comprises: receiving incoming intended data packets from said feed; not receiving incoming unintended data packets from said feed; and, sending outgoing data packets to said feed.

In some embodiments said aggregating comprises using an enterprise aggregating switch.

In some embodiments there is provided a multi-tenant optical data network comprises: a plurality of network service carrier lines connected to a premise router; at least one uplink connecting said premise router to an optical line terminal; said optical line terminal being connected to a number of feeder passive optical network feeds for carrying a common encrypted data feed to a plurality of optical network units each supporting at least one of a plurality of private tenant devices; and, wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices.

The text of the original claims is incorporated herein by reference as describing features in some embodiments.

Brief Description of the Drawings

Fig. 1 is a functional block diagram of several data service providers supplying multi-tenant building through a single headend according to an exemplary embodiment of the invention.

Fig. 2 is a functional block diagram of main point of entry room for the data network servicing a multi-tenant building according to an exemplary embodiment of the invention.

Fig. 3 is a functional block diagram for a premise router according to an exemplary embodiment of the invention.

Fig. 4 is a functional block diagram of an optical line terminal servicing multiple tenant users with a common data feed according to an exemplary embodiment of the invention.

Fig. 5 is a functional block diagram of an optical line terminal aggregating data and video streams into a common optical data feed according to an exemplary embodiment of the invention.

Fig. 6 is a functional block diagram of an optical network unit interfacing a tenant private network with a common optical data feed according to an exemplary embodiment of the invention.

Description of the Exemplary Embodiments

Referring now to the drawing, there is illustrated in Figs. 1 - 6 the components of a system **1** used to provide a mutually secure, shared Local Area Network ("LAN") implementation which can supply a multi-tenant site such as an office building **100** with

converged voice, data and video signal content traffic at gigabit speeds to a plurality of mutually secure end point users such as building tenants having multiple end user devices such as computers, access points and wireless controllers, application servers and printers, and television sets.

As shown in Figure 1, a single building **100** can have multiple tenants **102, 104, 106** such as individual companies, each potentially having multiple digital network devices. The system offers each tenant the ability to specify and use their own private address space even if the data feed overlaps with neighboring tenant on the same network, and the transmission of converged content traffic over the shared infrastructure while maintaining the separation and security of the individual tenant content traffic.

The system relies upon a collection of standards-based technologies that are designed and implemented to provide a point-to-multipoint networking through a single aggregation switch that is capable of providing thousands of IP voice, data, and video connection ports.

In a basic configuration, the aggregate downstream rate can be 2.5 Gbps, while the upstream rate can be 1.25 Gbps. Each of the connections can be adapted to support high-bandwidth multimedia applications on a single optical fiber over a distance of 20km or more. Telecommunications service traffic that includes Internet, public switched telephone networks, and broadcast/cable television **108, 110, 112** for the building are provided by one or more commercial carriers **114, 116, 118**. The telecommunications services carrier lines **120,122,124** enter the building **100** at a Main Point Of Entry (MPOE) room **126** and terminate into headend equipment **128**. From the headend equipment, the voice, video and data content traffic can distributed to each of the tenants **102, 104, 106** over data feeds carried by fiber optic cabling **130, 132, 134**.

As shown in Figure 2, the secure, shared multi-tenant LAN architecture can include a Passive Optical Network (“PON”) interface router, which for clarity in this embodiment is a single premise router **140**, an aggregation switch referred to as an Optical Line Terminal (OLT) **146**, a plurality of end user terminal devices such as computers, telephones and televisions located within the physically separate tenant **102, 104, 106** spaces, and an optical distribution network that consists of splitters and fiber cabling infrastructure. It shall be understood that a plural number of interface routers such as premise routers can be used.

The headend equipment **128** receives the plurality of telecommunications service carrier lines **120,122,124** from the separate carrier providers **114, 116, 118**. An RF-based video signal can be supplied by one or more of the carriers to the headend equipment via a broadband coaxial

cable **130**. The interface to the carrier lines within the headend equipment is the premise router **140**.

The premise router **140** can be configured with Virtual Routing and Forwarding (VRF) as described in RFC 4381 and RFC 4382, and utilizes Virtual Local Area Network (VLAN) tagging to separate and manage the distribution of the voice, video and data content traffic to each of the users. The VLAN-tagged voice, video, and data content traffic is connected to the Optical Line Terminal (OLT) **146** through an uplink **142** that provides primary communication. Optionally, a secondary uplink **144** may be employed as a backup communication path.

The OLT **146** can be powered by dual 48 VDC power feeds **148, 150** from rectifier modules **152, 154** that are attached to separate AC Mains **156, 158** through an uninterruptible power supply **160**. The OLT has a minimum of eight optical ports, but can have well over fifty such ports. Each port delivers a beam of light that contains the aggregated data for a multiplicity of users. The aggregated data may or may not be encrypted based on the type of PON.

The OLT **146** takes the VLAN-tagged voice, video, and data content traffic **142, 144** and processes each of the ethernet frames by first optionally encrypting them, then converting them into light, and outputting them as a photonic broadcast stream to the appropriate initial passive optical network feeds **162, 164, 166, 168, 170** that connects to an optical distribution patch panel **172**. The optical distribution patch panel **172** is used to provide the ability for cross-connecting the initial feeds **162, 164, 166, 168, 170** to the distribution feeds **174, 176, 178, 180** that traverse the distance to the remotely located tenants **102, 104, 106**. A tenant **106** requiring larger bandwidth can accept multiple distribution feeds **178, 180**.

In the case where a carrier provider **114** supplies an RF-based video signal **130**, the headend equipment **128** receives the RF-based video signal and converts it into light by processing the electrical analog signal and using it to modulate a laser which outputs the equivalent video photonic stream. This new video photonic stream is then combined with an initial feed **162** which results in a modified initial feed **164** that contains a photonic broadcast stream that contains the voice, video and data content traffic that is then fed into the optical distribution patch panel **172**. Of course in some instances the initial feed can contain digitized voice, video and data in which case no bypass of the OLT is necessary.

As shown in Figure 3, the premise router **140** can be the interface to each of the commercial carrier providers **114, 116, 118** through either a packet-switched or a leased-line Wide Area Network (WAN) interface in order to utilize the telecommunications services

provided over carrier lines **120,122,124**. Logical circuits can make connections between the premise router **140** and carrier providers **114, 116, 118**, utilizing a shared-bandwidth connection that may be shared with other carrier customers and could potentially affect quality of service and bandwidth availability. The leased-line connection provides a direct interface access to the carrier and eliminates the possibility of being affected by other carrier customers. The premise router **140** can be configured with a global routing table **412** that accesses the virtual routing table instantiations **420, 422, 424, 426** for each Optical Network Unit (ONU) serving a tenant. This configuration provides for creation of multiple routing tables, one for each ONU, within the single premise router **140**. This capability supports the overlapping of IP addresses for any of the tenants because the routing instances are independent. In this way, data traffic intended for one tenant is automatically isolated from traffic intended for other tenants. Furthermore, queries emanating from one tenant are identified so that one tenant cannot mimic the identity of another. In other words, unique routing for each tenant effectively isolates its traffic from other tenants, vastly improving the networks defense against cyber-attack.

Thus, the premise router processor **410** gets and puts the tenant-specific routing information in the global routing table **412** which in turn reads and updates the appropriate virtual routing tables **420, 422, 424, 426**. The updated virtual routing tables are used to uniquely VLAN-tag the voice, video, and data content traffic that is sent and received through the uplinks **142**, to the OLT **146**. In this way, the overlapping IP address on a single PON infrastructure allows each tenant connected to the infrastructure to transmit and receive information to any of the carriers. Thus all the tenants in a building can simply connect to the PON infrastructure without the need for their own dedicated headend.

A configuration file loaded into the premise router contains the commands to implement the virtual routing tables for each of the ONUs providing service to the tenant users. By way of example, the following pseudo-code implements independent virtual routing tables for two ONUs serving two users, namely "Tenant A" and "Tenant B". Comment lines begin with an exclamation point ("!"):

!-- Begin gateway configuration and programming

!-- Configure gateway identity

!-- Establish express forwarding to optimize network performance and scalability

```
!--- For each tenant (1..n) Do
!--- Instantiate virtual route table for the Tenant
!--- Enable VPN (Virtual Private Network) for the Tenant
!--- Establish routing and forwarding for the virtual routing table
!--- Creates lists of import and export route-target extended communities
!--- End Do

!--- Set IP (Internet Protocol) address, netmask and enable IS-IS routing

!--- For each tenant (1..n) Do
!--- Establish loopback identifier for the Tenant
!--- Enable VRF (Virtual Routing and Forwarding) for the Tenant
!--- Associate the VRF instance with an interface or sub-interface.
!--- Loopbacks use the same IP address because they belong to different
    Tenant VRF's
!--- Broadcast to all hosts on the subnet
!--- End Do

!--- Define and configure the gateway ingress interface
!--- Set bandwidth
!--- Config IP address and netmask
!--- Enable MPLS (MultiProtocol Label Switching)

!--- Enables logging of BGP (Border Gateway Protocol) neighbor resets.
!--- Adds an entry to the BGP or multiprotocol BGP neighbor table
!--- Enables BGP sessions to use a specific operational interface for TCP
    (Transmission Control Protocol) connections

!--- Enter address family configuration mode

!--- Sends the community attribute to a BGP neighbor

!--- For each tenant (1..n) Do
!--- Set the address family for the tenant
!--- End Do

!--- Use longest prefix matching or default route

!--- end gateway configuration and programming
```

The above example shows that the premise router **140** can be programmed to create an independent virtual routing table for each user ONU. Thus, each user is effectively encased within its own separate routing environment, vastly restricting access by cyber attackers to the PON. In this way, the premise router includes a number of destinations listed in virtual routing tables which are associated with corresponding destinations listed in said global routing table.

Figure 4 represents the Passive Optical Network infrastructure which is an optical distribution network used to convey the photonic broadcast stream feeds that contain the encrypted data packets such as VLAN-tagged ethernet frames **300, 302, 304, 306** that are distributed back and forth between the various tenant spaces **102, 104, 106** and the OLT **146**. Essentially, the OLT can broadcast the combined encrypted VLAN-tagged ethernet frames **300, 302, 304, 306** over the distribution feeds **174, 176, 178, 180** to a number of splitters **308, 310, 312, 314**.

Each splitter **308** can replicate the incoming photonic broadcast stream equally over each of its drop lines **320, 322, 324**. The splitter **308** can attach to the simplex, single-mode fiber from the OLT **146** and can passively redistribute the incoming light stream up to 64 times. The splitter is a Planar Lightwave Circuit (PLC) that is constructed using silica glass waveguide circuits and aligned fiber optic pigtails that are all integrated inside of a single package. The attenuation of the light signal through the PLC of the splitter **308** is symmetrical in both directions. The signal loss from a 1x8 PLC splitter is expected to be less than one dB greater than what would be expected from a perfect splitter, approximately 10 dB. A typical 1x32 PLC splitter shall have approximately 17 dB or less.

Each of the outputs from the optical splitter can be an individual simplex, single-mode fiber called a drop line **320, 322, 324**. The drop lines can be routed and fed into the appropriate tenant physical space **102, 104, 106** and terminated into the tenant's dedicated Optical Network Unit (ONU) **330, 332, 334**.

Each ONU **330, 332, 334** is operated so that it utilizes the VLAN-tagging to select those of the incoming ethernet frames assigned to the particular tenant, and then removes the encryption from the selected ethernet frames. Thus, each ONU strips out or extracts only those incoming frames that are intended for the particular tenant. The decrypted ethernet frames **301, 303, 305** are then made available **340, 342, 344** for the tenant's IP/ethernet end-user equipment. Those frames not assigned to the particular tenant are ignored and cannot be decrypted by the particular tenant. In other words, a first subset of the frames can be associated with a first piece of end-user equipment and a second subset of the frames is associated with a second piece of end-user equipment. The first and second pieces of equipment can be common to a single tenant or can be split among separate tenants.

In other words, for example, tenant A **102** gets supplied to its ONU **330** all incoming encrypted frames **300, 302, 304, 306** via its drop line **320** including those frames that are intended for it **300, 306** and those frames that are unintended for it **302, 304**. The ONU strips out

its intended encrypted frames **300**, and **306** and decrypts them to form its intended decrypted frames **301** which it makes available to Tenant A's dedicated, private data line **340**. The ONU also encrypts outgoing frames.

As shown in Figure 5, the OLT **146** that typically resides in the MPOE room **126** can be a key component of the headend equipment **128**. The OLT **146** can perform as the Layer-2 workgroup switching mechanism for voice, video and data content traffic that is sent and received from the individual tenants.

The OLT **146** equipment can be a chassis having multiple slots used to host circuit boards that perform various functions. Operations of the OLT are managed and controlled by a processor **500**. A backplane **502** of the OLT can provide the communication path for all of the control, management, and data signals between the circuit boards installed within the OLT. A network interface **504** provides the interface to/from the primary uplink **142** and backup uplink **144** connections to the premise router **140**. A switching fabric component **506** can be used to encrypts the VLAN-tagged ethernet frames using the appropriate symmetric key for a specific tenant and sends the result to an optical conversion component **508** for transmission to the tenant. The content traffic on the switching fabric component **506** is encrypted for each tenant location before being transmitted over the shared optical distribution network. Encryption of the layer-2 ethernet frames is used to provide the confidentiality of each tenant's signal traffic.

A symmetric-key algorithm can be used for the encryption of the ethernet frame data packets. This particular implementation utilizes a fixed block size of 128-bits and a key size of 128-bits that operate on a 4x4 column-major order matrix of bytes. It performs 10 cycles of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round can consists of:

- a. First, a byte substitution function is performed where each byte in the state matrix is replaced using an 8-bit substitution.
- b. Next, each of the rows of the state are shifted by a certain number of steps. The first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Row n is shifted left circular by n-1 bytes.
- c. Finally, the columns of the state are mixed by combining the four bytes in each column. The four bytes of each column of the state are combined using linear transformation. Encryption is used to specifically prevent man-in-the-middle attacks. Additionally, the PON configuration also supports IEEE 802.1x authentication in order to provide provide port based

Network Access Control to limit network access, with features like IP//MAC address limiting to secure the network from unauthorized/malicious users.

The optical conversion component **508** of the OLT **146** can convert the electrical signals of the encrypted VLAN-tagged ethernet frames and output them over the initial feeds **162**, **166**, **168**, **170** as modulated optical signals.

In the case where a carrier provider **114** supplies an RF-based video signal **130** to the headend equipment **128**, the signal is connected to a laser transmitter **520** where the input broadband signal is used to modulate a laser. The modulated output of the laser is a low-level photonic light stream. The photonic light stream is sent to an erbium-doped fiber amplifier **522**, where the signal is increased to approximately 30 dBmV. The resulting amplified video signal is then overlayed on an initial feed **162** through the use of a wave division multiplexor combiner **524**. The output from the wave division multiplexor combiner **524** is a feed line **164** that contains encrypted VLAN-tagged ethernet frames and a laser-modulated, RF-based video signal.

As shown in Figure 6, each tenant can have one or more of an ONU **330** that accepts drop line **320** connections. The ONU **330** terminates optical fibers from a splitter **308** and sends/receives decrypted ethernet frames **340** to the tenant's IP/ethernet equipment, and RF video signals **656** to the tenant's television. The ONU has a processor **600** which controls and manages all activity of the ONU by directly communicating all of the control and management signals **602**, **604**, **606** to/from its internal components **610**, **612**, **640**. The ONU receives the photonic light stream transmitted over the drop line **320**. The optical converter **610** examines the encrypted photonic light stream that enters the component. If the VLAN-tagged ethernet frame has been encrypted with the same symmetric key, it indicates that the VLAN-tagged frame belongs to the tenant of that ONU. After the optical converter **610** performs the decryption, the VLAN-tagged ethernet frame is sent to the network interface **612** of the ONU via the direct communication path **608**. The network interface **612** demultiplexes the electrical signal to divide out baseband telephony/data signals from broadband video channels. The network interface sends/receives the VLAN-tagged ethernet frames to the appropriate physical connection interface **622**, **632**, **652**. The ONU can supply a basic 802.3 ethernet interface **622**, or an 802.3 ethernet interface that include power-over-ethernet (PoE) capability **632**, or an RF-based video F-Type interface **652** to transmit the RF-based video signal **656**. The PoE port injector **640** implements the Power-Over-Ethernet and Power-Over-Ethernet Plus based upon the IEEE 802.3af-2003 and IEEE 802.3at-2009 standards respectively.

In this way, the above described system empowers a multi-tenant building **100** with an environment to securely host individual tenant data traffic with overall network flexibility. This ability of the system allows it to leverage the high bandwidth and energy efficiency of passive optical network equipment for the entire building. Because optical bandwidth is comparatively unlimited, existing systems often do not utilize this capacity. Thus, the high bandwidth capability of optical fiber can be leveraged to route all traffic optically and uniformly throughout the building on an aggregated feed. Each tenant can extract its share of the traffic from the feed. In this way, a single headend having reduced air conditioning requirements can be located at the building's main point of entry, and no additional air conditioning is needed at the individual tenant spaces for what would have been headend-type network equipment.

While the preferred embodiment of the invention has been described, modifications can be made and other embodiments may be devised without departing from the spirit of the invention and the scope of the appended claims.

What is claimed is:

CLAIMS

1. A multi-user optical data network apparatus comprises:
 - a plurality of network service carrier lines connected to a passive optical network interface router;
 - at least one uplink connecting said interface router to an optical line terminal;
 - said optical line terminal being connected to a number of passive optical network feeds for carrying a common data feed to a plurality of optical network units each supporting at least one of a plurality of private user devices;
 - said interface router being configured to have at least one virtual routing table for each one of said plurality of optical network units; and,
 - wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices.
2. The apparatus of Claim 1, wherein said common data feed is encrypted.
3. The apparatus of Claim 1, wherein said interface router is a premise router.
4. The apparatus of Claim 1, wherein said interface router is further configured to have a global routing table, and wherein a number of destinations listed in said at least one virtual routing table are associated with corresponding destinations listed in said global routing table.
5. The apparatus of Claim 1, wherein each of said optical network units provides service to a separate number of private users.
6. The apparatus of Claim 1, wherein said uplink carries data including digitized voice and video data.
7. A multi-user optical data network apparatus comprises:
 - a plurality of network service carrier lines connected to a plurality of passive optical network interface routers;
 - a plurality of uplinks connecting said interface routers to an optical line terminal;

said optical line terminal being connected to a number of passive optical network feeds for carrying a common data feed to a plurality of optical network units each supporting at least one of a plurality of private user devices;

wherein each of said interface routers is configured to have at least one virtual routing table for each one of said plurality of optical network units to which said each of said interface routers is connected; and,

wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices.

8. A digital data network communication method comprises:

accepting a plurality of private data streams into a passive optical network interface router serving a plurality of private users through a plurality of optical network units;

aggregating said private data streams into a combined data feed;

routing said data feed to at least two of said plurality of optical network units;

extracting from said data feed a first one of said private data streams;

wherein said routing comprises:

providing a global routing table;

providing an independently unique virtual routing table for each of said plurality of optical network units;

tagging ethernet frames intended for a first one of said plurality of optical network units according to entries in a first one of said virtual routing tables associated with a first one of said optical network units;

distributing said tagged ethernet frames according to both of said global routing table and said first one of said virtual routing tables.

9. The method of Claim 8, wherein said distributing comprises associating destinations listed in said first one of said virtual routing tables with destinations listed in said global routing table.

10. The method of Claim 8, wherein each of said optical network units provides service to a separate number of private users.

11. The method of Claim 8, wherein said accepting comprises:

interfacing a plurality of service provider data lines through a single headend.

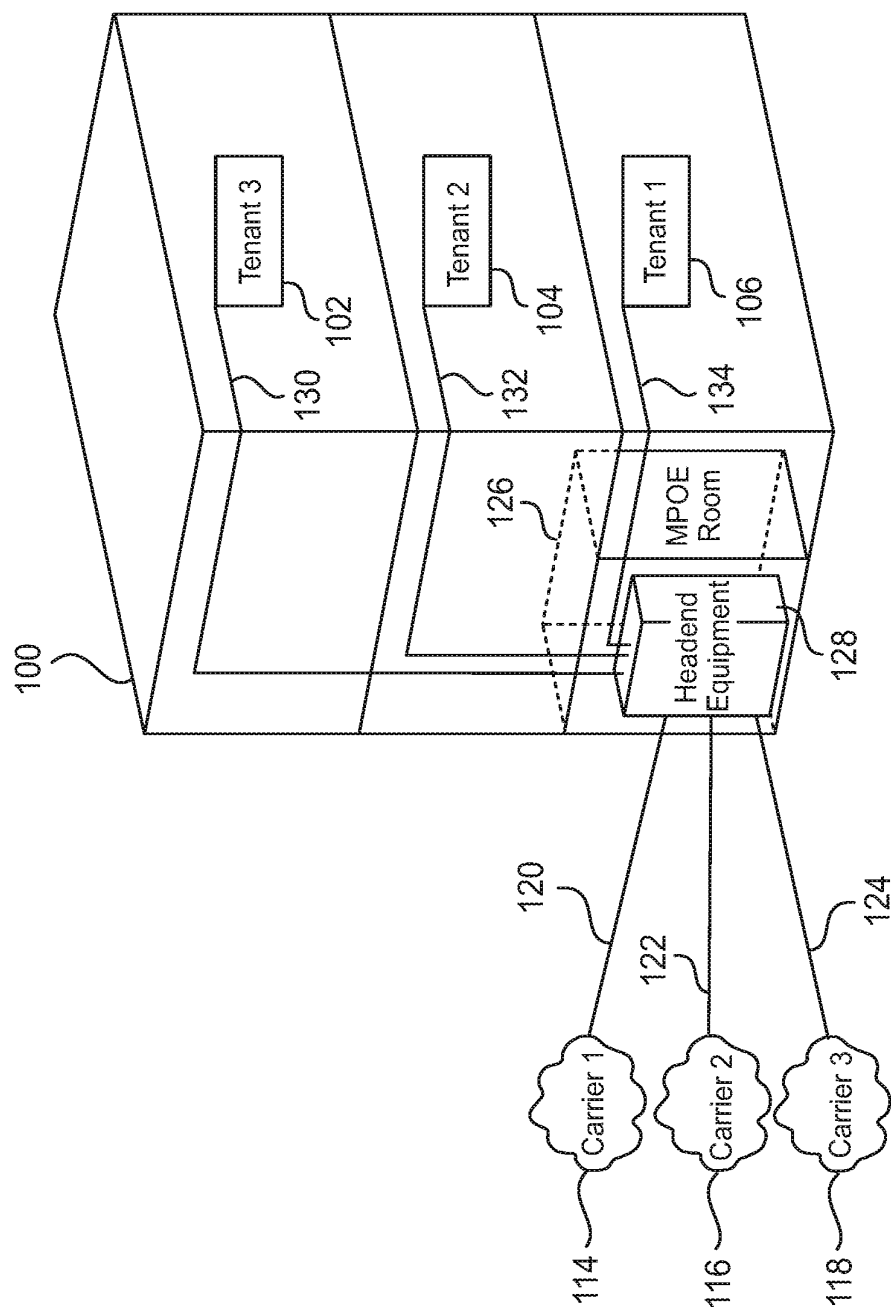
12. The method of Claim 11, wherein said interfacing comprises:
 - utilizing at least one premise router and a radio frequency video converter; and,
 - feeding an output of said premise router through an optical line terminal.
13. The method of Claim 12, wherein said interfacing further comprises:
 - feeding an output of said converter through said optical line terminal.
14. The method of Claim 11, wherein said optically routing comprises:
 - sending said encrypted data feed through an optical splitter.
15. The method of Claim 8, wherein each of said streams comprises:
 - encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed; and,
 - wherein said extracting comprises:
 - partially decrypting said encrypted data feed.
16. The method of Claim 15, wherein said encrypted data feed comprises:
 - a plurality of encrypted ethernet frames;
 - wherein a subset of said frames are associated with a first one of said users and a second subset of said frames is associated with a second one of said users.
17. The method of Claim 8, wherein said extracting comprises:
 - operating an optical network unit at each of said tenants;
 - wherein said operating comprises:
 - decrypting incoming intended data packets from said feed;
 - not decrypting incoming unintended data packets from said feed; and,
 - encrypting outgoing data packets to said feed.
18. The method of Claim 8, wherein said aggregating comprises using an enterprise aggregating switch.

Mutually secure optical data network and method

ABSTRACT

A digital optical data network system for improving information security in both encrypted and non-encrypted Passive Optical Networks (“PON”) by protecting one or more interface devices to allow safe data traffic between multiple carriers, service providers and multiple end users such as tenants in a building, employees of a business entity, or subscribers in a residential community.

160142



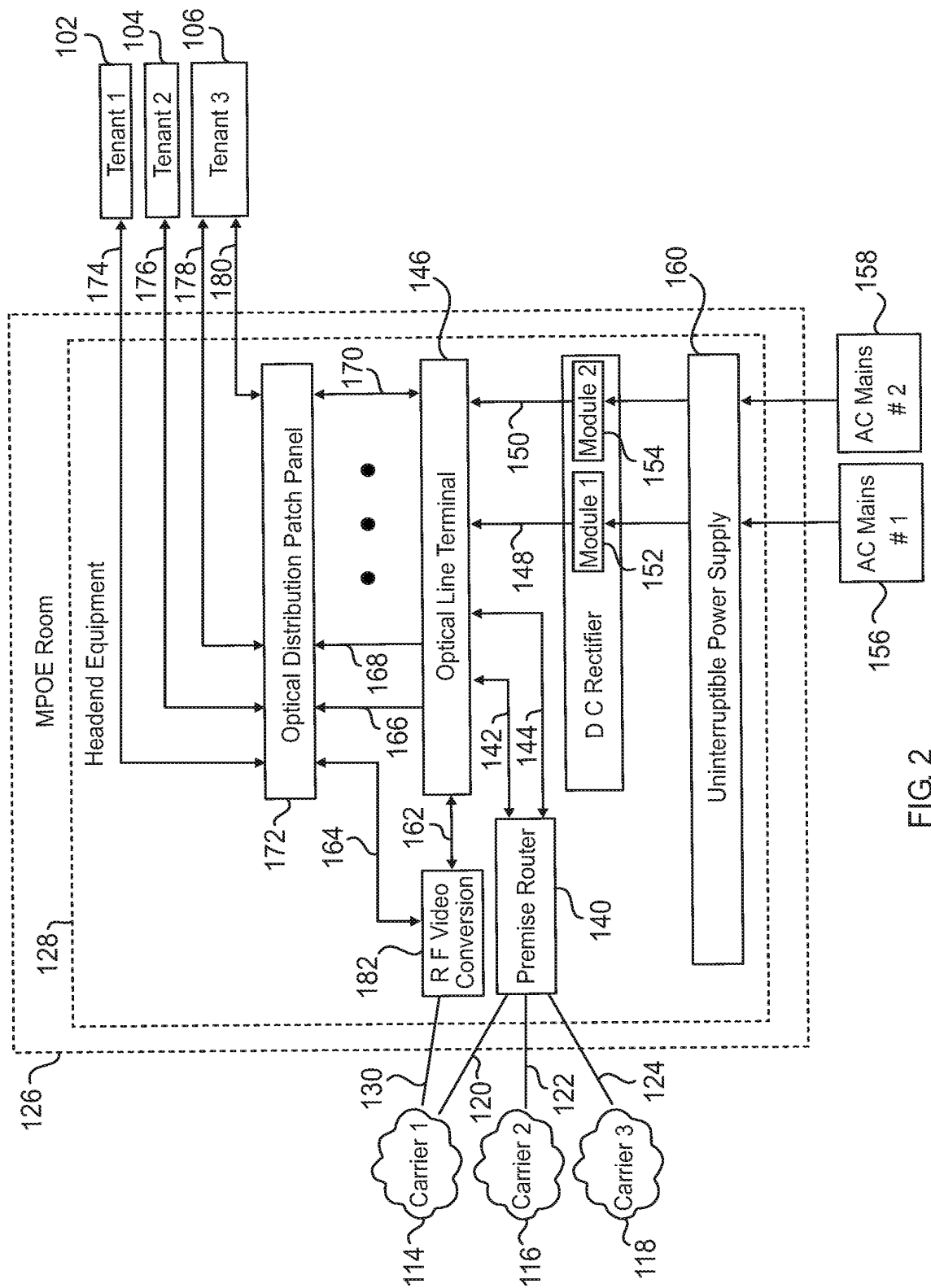


FIG. 2

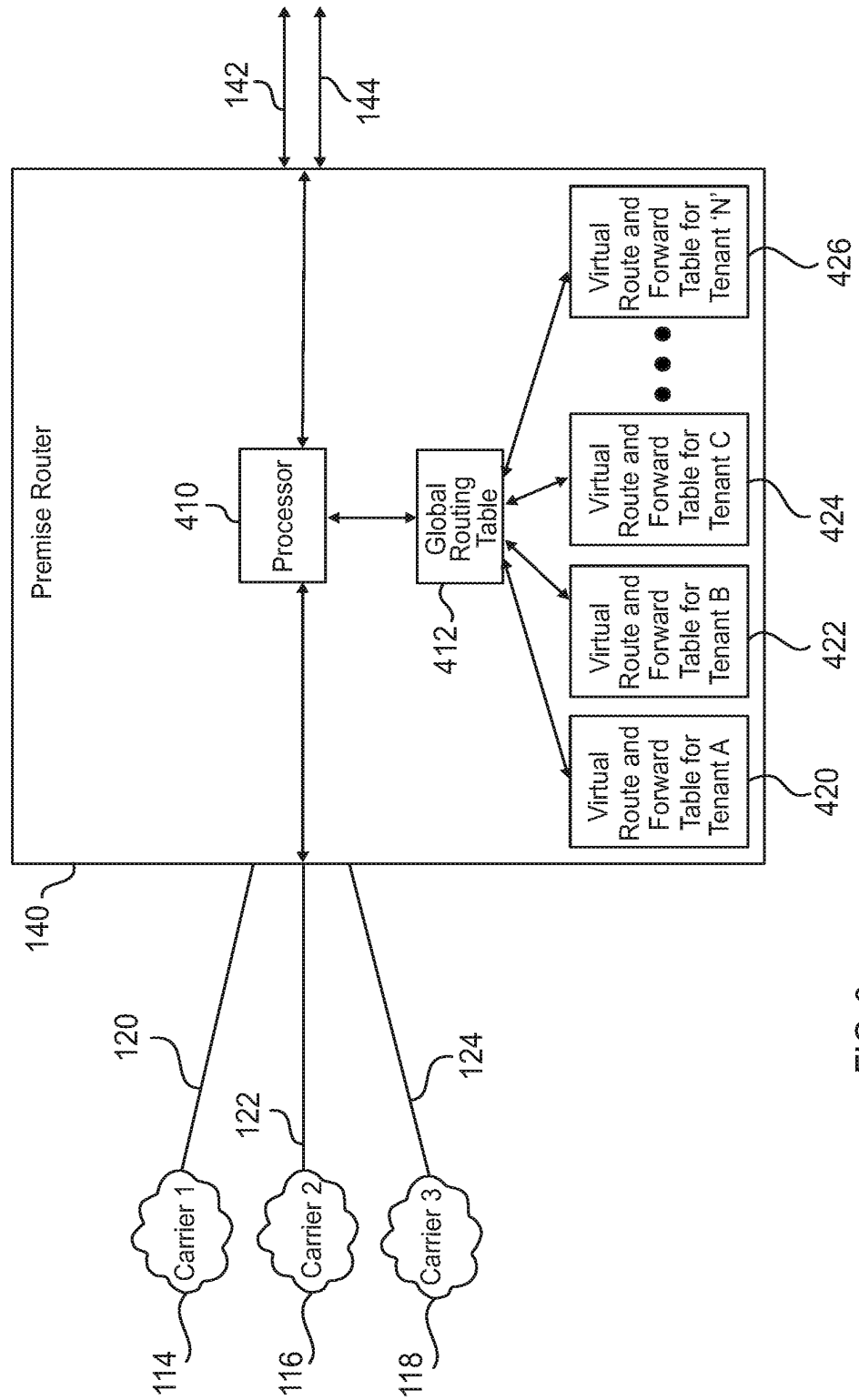


FIG. 3

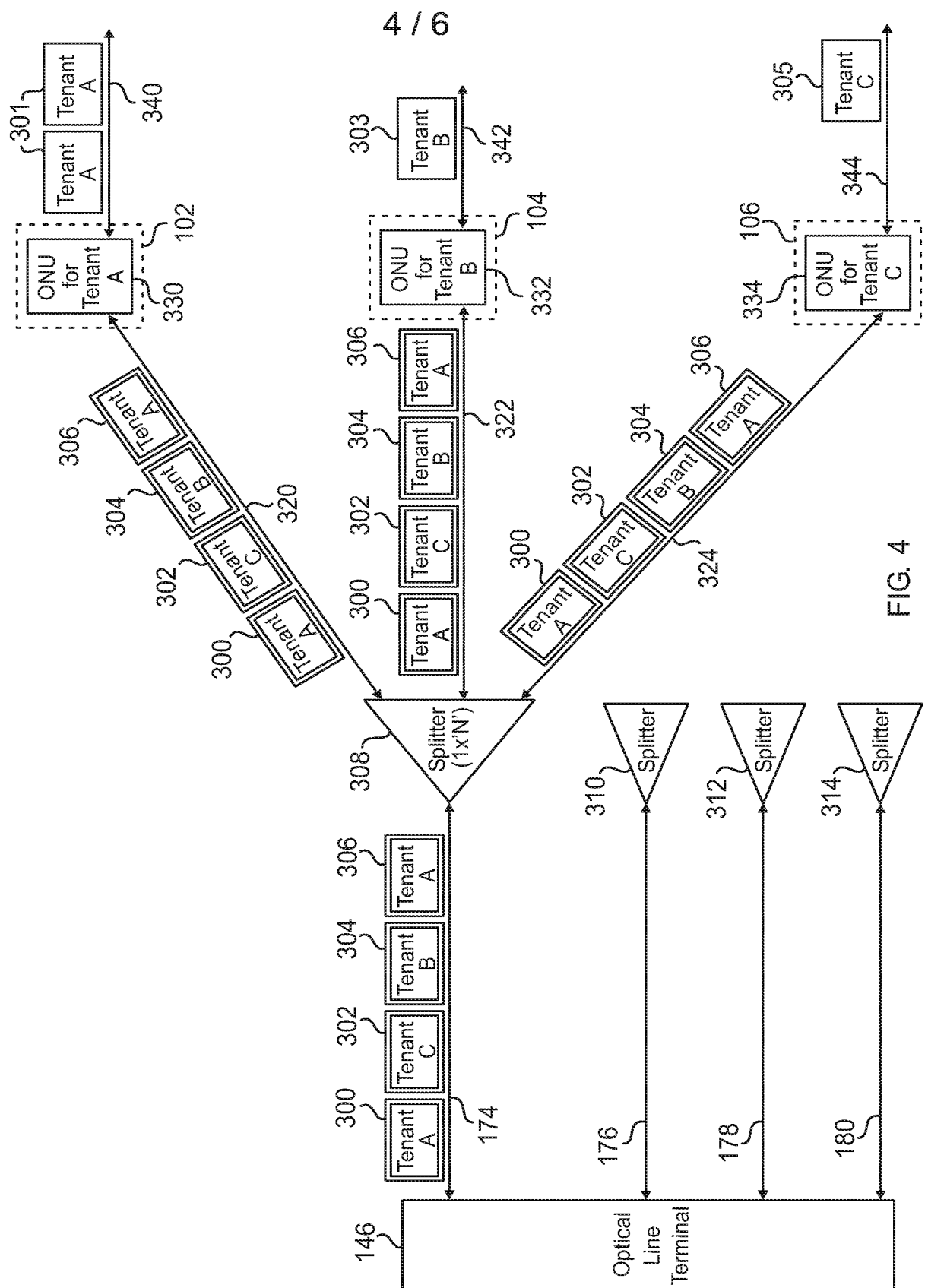


FIG. 4

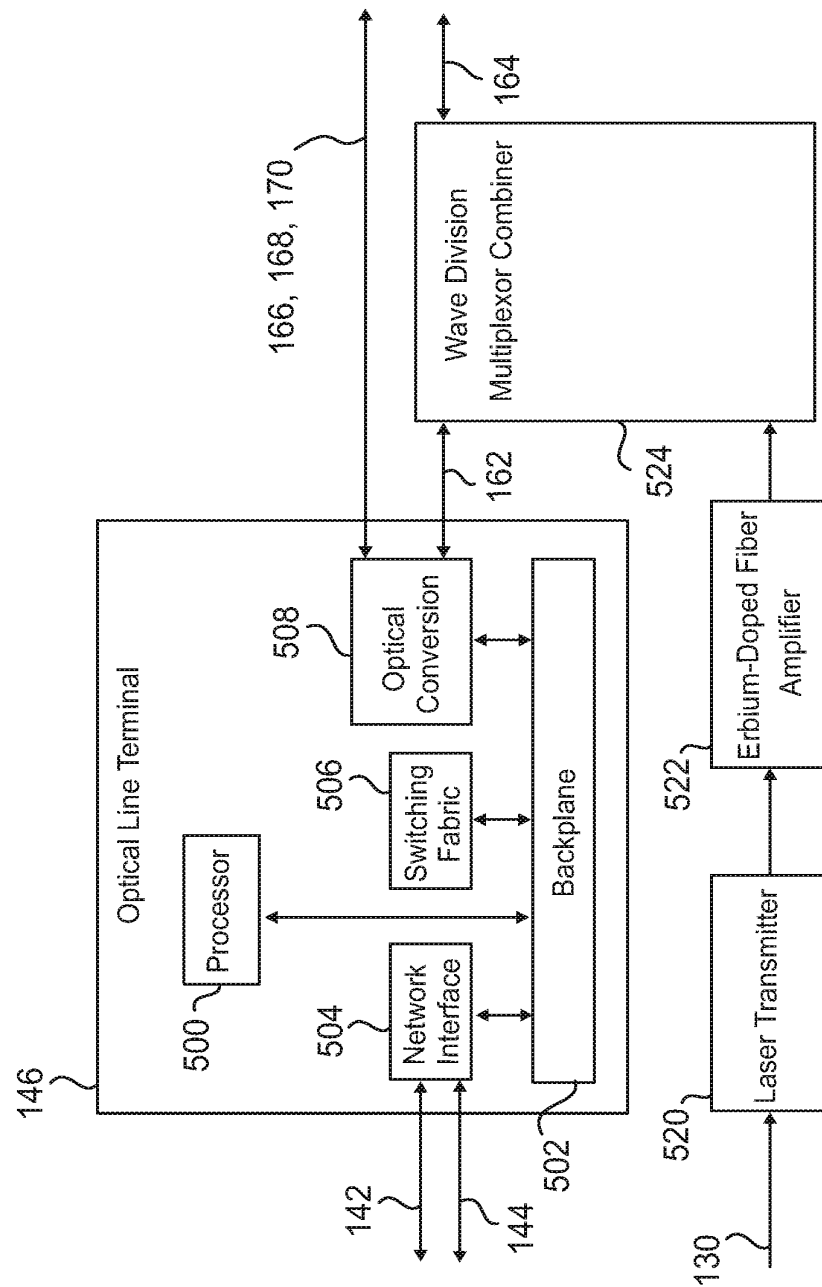


FIG. 5

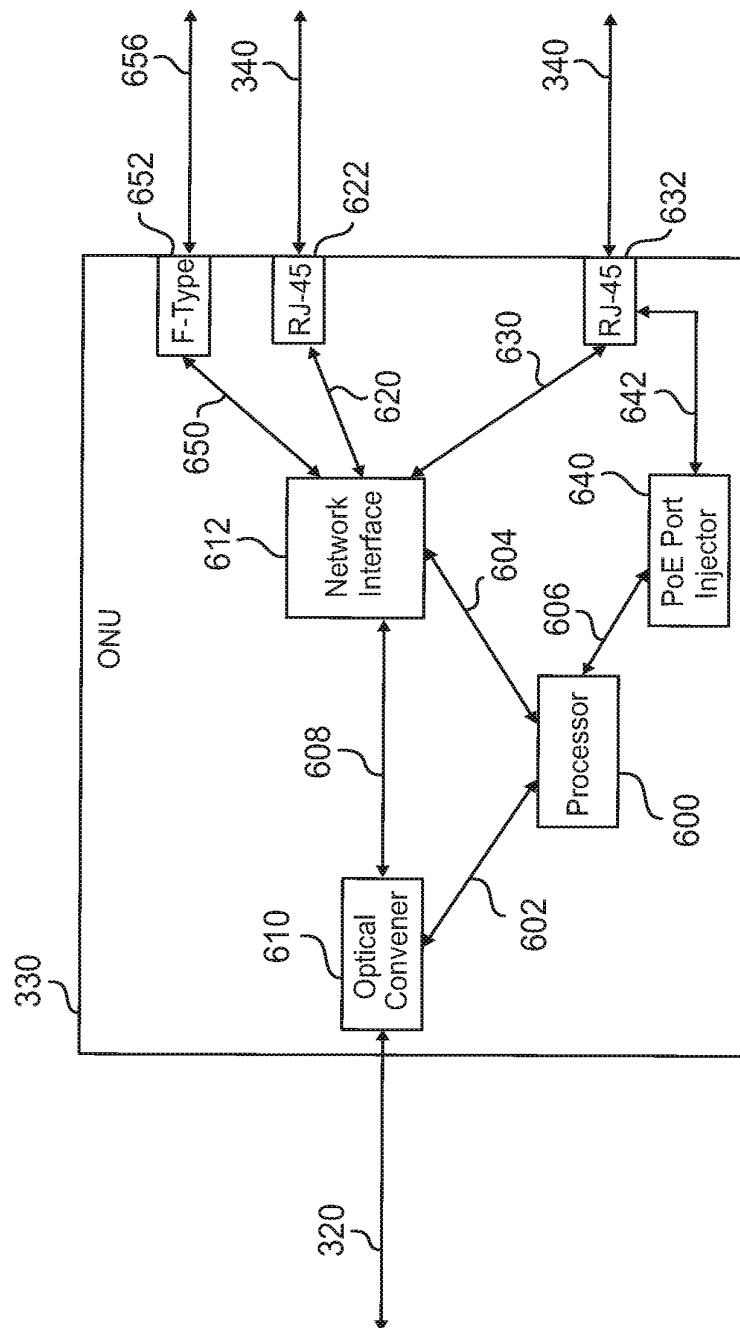


FIG. 6

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		Mutually secure optical data network and method		
First Named Inventor/Applicant Name:		Joseph L. Vilella		
Filer:		John David Buchaca		
Attorney Docket Number:		160142		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	70	70
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				70

Electronic Acknowledgement Receipt	
EFS ID:	27508607
Application Number:	15351315
International Application Number:	
Confirmation Number:	2023
Title of Invention:	Mutually secure optical data network and method
First Named Inventor/Applicant Name:	Joseph L. Vilella
Customer Number:	24243
Filer:	John David Buchaca
Filer Authorized By:	
Attorney Docket Number:	160142
Receipt Date:	14-NOV-2016
Filing Date:	
Time Stamp:	20:21:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 70
RAM confirmation Number	111516INTEFSW20235300
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	2016-11-14_160142_Transmittal.pdf	107555	no	1
			f6768beecd7712b360e544c1d33affa6cb0e741		
Warnings:					
Information:					
2	Application Data Sheet	2016-11-14_160142_ADS.pdf	1894881	no	7
			c18887be35df829d6d6c68b16c65d11d9faec914		
Warnings:					
Information:					
3		2016-11-14_160142_DescriptionClaimsAbstract.pdf	447936	yes	18
			84a58708f2e5b686f01fd9f735efaed8822fec914		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	14	
	Claims		15	17	
	Abstract		18	18	
Warnings:					
Information:					
4	Drawings-only black and white line drawings	2016-11-14_160142_Drawing.pdf	213293	no	6
			5b1ceb0bb54f4dfa0e717d101fe3a5a28bec590b		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	29922	no	2
			413a5e950a0555fa2095af206ba9a75f8938e91e		

Warnings:	
Information:	
Total Files Size (in bytes):	2693587
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
15/351,315	11/14/2016	2636	70	160042	18	3

CONFIRMATION NO. 2023

FILING RECEIPT



24243
CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108

Date Mailed: 11/25/2016

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Joseph L. Vilella, San Diego, CA;
James R. Reynante, San Diego, CA;

Applicant(s)

Joseph L. Vilella, San Diego, CA;
James R. Reynante, San Diego, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CIP of 14/419,092 02/02/2015
which is a 371 of PCT/US2013/053389 08/02/2013
which claims benefit of 61/678,977 08/02/2012

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/23/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/351,315**

Projected Publication Date: 03/02/2017

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Mutually secure optical data network and method

Preliminary Class

398

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

page 2 of 3

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 15/351,315			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A			
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A			
TOTAL CLAIMS (37 CFR 1.16(i))	18	minus 20 = *	x 40 =	0.00	OR				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	x 210 =	0.00					
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00					
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00					
			TOTAL	730		TOTAL			
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	x	=
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	x	=
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/351,315	11/14/2016	Joseph L. Vilella	160042

24243
CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108

**CONFIRMATION NO. 2023
FORMALITIES LETTER**



Date Mailed: 11/25/2016

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
The surcharge is due for any one of:
 - late submission of the basic filing fee, search fee, or examination fee,
 - late submission of inventor's oath or declaration,
 - filing an application that does not contain at least one claim on filing, or
 - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- \$ **70** surcharge.
- \$ **300** search fee.
- \$ **360** examination fee.
- \$(**0**) previous unapplied payment amount.
- \$ **730** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's

page 1 of 2

oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
Joseph L. Vilella
James R. Reynante

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice".
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/fhadera/

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date
15351315	2016-11-14

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☒ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

24243

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☒ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

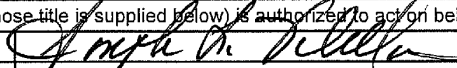
I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

--

- ☒ Inventor or Joint Inventor (title not required below)
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
- ☐ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature  Date (Optional) 01/10/17

Name Joseph L. Viella

Title Inventor/Owner

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal				
Application Number:		15351315		
Filing Date:		14-Nov-2016		
Title of Invention:		Mutually secure optical data network and method		
First Named Inventor/Applicant Name:		Joseph L. Vilella		
Filer:		John David Buchaca		
Attorney Docket Number:		160142		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY SEARCH FEE	2111	1	300	300
UTILITY EXAMINATION FEE	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	70	70
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				730

Electronic Acknowledgement Receipt	
EFS ID:	28150996
Application Number:	15351315
International Application Number:	
Confirmation Number:	2023
Title of Invention:	Mutually secure optical data network and method
First Named Inventor/Applicant Name:	Joseph L. Vilella
Customer Number:	24243
Filer:	John David Buchaca
Filer Authorized By:	
Attorney Docket Number:	160142
Receipt Date:	24-JAN-2017
Filing Date:	14-NOV-2016
Time Stamp:	14:49:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 730
RAM confirmation Number	012517INTEFSW14510400
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	2017-01-24_160142_Transmittal.pdf	96517	no	1
			6f2bb504e77f109830058a6254810fcc954dadcl		
Warnings:					
Information:					
2	Oath or Declaration filed	2017-01-24_160142_DeclarationVilella.pdf	99437	no	1
			c3ff9dc1865775b81333c1dd92bde42176074ece		
Warnings:					
Information:					
3	Oath or Declaration filed	2017-01-24_160142_DeclarationReynante.pdf	99169	no	1
			5f83e4828a5ed5ebfd0baed81e967f1998671a34		
Warnings:					
Information:					
4	Power of Attorney	2017-01-24_160142_POA.pdf	120411	no	1
			a36e64e8e14afa18d12ed816188c50791dd2d2c1		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	35323	no	2
			f46fd6e926709adf0adb234b14f1d2533b97e952		
Warnings:					
Information:					
Total Files Size (in bytes):			450857		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: TRAN.LET

Document Description: Transmittal Letter

PTO/SB/21 (07-09)

Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	15351315
	Filing Date	2016-11-14
	First Named Inventor	Joseph L. Vilella
	Art Unit	2636
	Examiner Name	unassigned
	Attorney Docket Number	160142
Total Number of Pages in This Submission		6

ENCLOSURES (Check all that apply)		
☒ Fee Transmittal Form	☐ Drawing(s)	☐ After Allowance Communication to TC
☒ Fee Attached	☐ Licensing-related Papers	☐ Appeal Communication to Board of Appeals and Interferences
☐ Amendment/Reply	☐ Petition	☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
☐ After Final	☐ Petition to Convert to a Provisional Application	☐ Proprietary Information
☐ Affidavits/declaration(s)	☒ Power of Attorney, Revocation Change of Correspondence Address	☐ Status Letter
☐ Extension of Time Request	☐ Terminal Disclaimer	☒ Other Enclosure(s) (please identify below):
☐ Express Abandonment Request	☐ Request for Refund	2 Inventor Declarations
☐ Information Disclosure Statement	☐ CD, Number of CD(s) _____	
	☐ Landscape Table on CD	
☐ Certified Copy of Priority Document(s)	Remarks	
☐ Reply to Missing Parts/Incomplete Application	2 Inventor Declarations - 2 sheets	
☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53	Power of Attorney - 1 sheet	
	EFS-Web-generated Fee Sheet - 2 sheets	
	This Transmittal - 1 sheet	

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	Charmasson, Buchaca & Leach, LLP		
Signature	/John Buchaca/		
Printed name	John D. Buchaca		
Date	2017-01-24	Reg. No.	37289

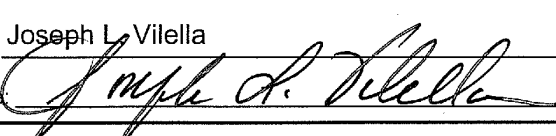
CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:			
Signature	/John Buchaca/		
Typed or printed name	John D. Buchaca	Date	2017-01-24

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Mutually secure optical data network and method
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: ☐ The attached application, or ☒ United States application or PCT international application number <u>15351315</u> filed on <u>2016-11-14</u></p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Joseph L. Vilella</u> Date (Optional): <u>01/10/17</u></p> <p>Signature: </p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of
Invention

Mutually secure optical data network and method

As the below named inventor, I hereby declare that:

This declaration
is directed to:

☐

The attached application, or

☒

United States application or PCT international application number 15351315

filed on 2016-11-14

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: James R. Reynante

Date (Optional): 01/10/2017

Signature: James R. Reynante

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/351,315	11/14/2016	Joseph L. Vilella	160142

24243
CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108

**CONFIRMATION NO. 2023
PUBLICATION NOTICE**



Title:Mutually secure optical data network and method

Publication No.US-2017-0063542-A1

Publication Date:03/02/2017

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
15/351,315	11/14/2016	2431	800	160142	18	3

CONFIRMATION NO. 2023

UPDATED FILING RECEIPT



0000000091280591

24243
CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108

Date Mailed: 05/11/2017

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Joseph L. Vilella, San Diego, CA;
James R. Reynante, San Diego, CA;

Applicant(s)

Joseph L. Vilella, San Diego, CA;
James R. Reynante, San Diego, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CIP of 14/419,092 02/02/2015 ABN
which is a 371 of PCT/US2013/053389 08/02/2013
which claims benefit of 61/678,977 08/02/2012

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/23/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/351,315**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Mutually secure optical data network and method

Preliminary Class

380

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

page 2 of 3

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 15/351,315			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A			
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A			
TOTAL CLAIMS (37 CFR 1.16(ii))	18	minus 20 = *	x 40 =	0.00	OR				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	x 210 =	0.00					
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00					
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00					
			TOTAL	730		TOTAL			
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(ii))	*	Minus	**	=	x	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	x	=
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(ii))	*	Minus	**	=	x	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	x	=
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
						TOTAL ADD'L FEE		TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/351,315	11/14/2016	Joseph L. Vilella	160142

24243
CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108

**CONFIRMATION NO. 2023
IMPROPER CPOA LETTER**



Date Mailed: 05/11/2017

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the power of attorney filed 01/24/2017. The power of attorney in this application is not accepted for the reason(s) listed below:

- The signature(s) of James R. Reynante, co-inventor(s) in this application, has/have been omitted. The power of attorney will be entered upon receipt of confirmation signed by said co-inventor(s).

/agizaw/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/351,315	11/14/2016	Joseph L. Vilella	160142	2023
24243 7590 07/10/2018 CHARMASSON, BUCHACA & LEACH, LLP 2635 Camino Del Rio South Suite 102 SAN DIEGO, CALIFORNIA 92108 UNITED STATES OF AMERICA			EXAMINER FAROOQUI, QUAZI	
			ART UNIT 2491	PAPER NUMBER
			NOTIFICATION DATE 07/10/2018	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

john@charmason.com

Detailed Action

The present application is being examined under the pre-AIA first to invent provisions. This office action is response to the application 15/351,315 filed on 11/14/2016. Claims 1-18 are pending in this communication.

Priority

This application claims priority from US provisional application 61/678,977 08/02/2012. Priority date has been accepted.

Drawings

The examiner contends that the drawing(s) submitted on 11/14/2016 are acceptable for examination proceedings.

Objection

In claim 17 line 2, the method lacks antecedent basis -“an optical network unit”. Clear antecedent is requested from the independent claim 8.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the

subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-14 & 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Farmer; James O. et al. (hereinafter **FARMER**), Pat. No.: US 7,583,897 B2 in view of Bettinger et al. (hereinafter **BETTINGER**), Pat. No.: US 7,509,144 B2.

Regarding Claim 1, FARMER teaches a multi-user optical data network apparatus comprises:

a plurality of network service carrier lines connected to a passive optical network interface router (**Fig.3 element 355 and col.10 lines 42-45, the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol for communicating with one or more laser transceiver nodes 120 (fig.2).** Here, optical router is interfacing with internet router and multiple optical interfaces. Optical router device is passive or cross-connect optical links);

at least one uplink connecting said interface router to an optical line terminal (**Fig.3 element 350 & col.10 lines 41-43, the data service hub 110 can further comprise a logic interface 350 that is connected to a laser transceiver node routing device 355.** Here, optical routing device (355) is connected to multiple uplink interfaces such as internet router 340, telephone switch 345);

said optical line terminal being connected to a number of passive optical network feeds for carrying a common data feed to a plurality of optical network units each supporting at least one of a plurality of private user devices (**Fig.3 elements 365 /170 & col.11 lines 1-11, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360. From the bi-directional splitter 360, respective optical receivers 370 can convert the upstream optical signals into the electrical domain. The upstream electrical signals generated by respective optical receivers 370 are then fed into the laser transceiver node routing device 355. As noted above, each optical receiver 370 can comprise one or more photoreceptors or photodiodes that convert optical signals into electrical signals.** Here, 365/170 are different networks or subscribers using uplinks optical routing device, internet router and other sources of carrier links);

FARMER, however, does not teach

said interface router being configured to have at least one virtual routing table for each one of said plurality of optical network units; and,

wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices.

In analogous teaching BETTINGER teaches

said interface router being configured to have at least one virtual routing table for each one of said plurality of optical network units (**Fig.8, Fig.9A & col.10 lines 42-44, each single terminal 802 includes a satellite modem 902, a remote and a remote virtual router tag table 908.** Here, each device 802 has virtual tables to communicate with uplink virtual router 904); and,

wherein each of said optical network units is adapted to extract data packets intended for a supported one of said devices (**Fig.9A, Fig.9B & col.10 lines 47-51, the remote virtual router 904 and remote virtual router tag table 908 work with the upstream virtual router 910 and upstream virtual router tag table 914 (described below) in conjunction with the shared network equipment, to provide a virtual router capability.** Here, upstream virtual router 910 is getting data from individual virtual router 904).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network.

All references are inventions in analogous area but each invention teaches specific claimed limitation specifically and other references mutually cure each other's deficiencies. When all claimed techniques are combined they teach claimed invention.

To provide a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, in view of the teachings of BETTINGER, since the techniques were known in the prior art and one skilled in the art could have combined the

technique (*eMPEP sec 2141 sub-section C (III) items (C) - use of known technique to improve similar devices (methods, or products) in the same way, & (D) - applying a known technique to a known device (method, or product) ready for improvement to yield predictable results*), the elements as claimed by a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network to achieve obvious predictable result.

The combination would have yielded nothing more than predictable results to one of ordinary skill at the time of the invention, i.e., one skilled in the art would have recognized that the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network used in: BETTINGER would allow the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER to function as invention claimed.

This enhancement provides a secured technique of a network router connecting to passive optical carrier lines, distributes to multiple optical subscriber ports, have virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeps individual subscriber's data separate from other subscribers private and secured by avoiding use of individual router for each subscriber provided by the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic,

keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of BETTINGER with FARMER's the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. Furthermore, this enhancement facilitates service providers and subscribers using common optical router equipment with virtual routing tables shared between multiple independently administered networks by managing each subscriber's data private separate and saves installation, maintenance and operation cost by avoiding providing individual router to each subscriber. The common optical router equipment is reconfigurable and expandable and provides changed communication capacity and functions when additional elements are added or reconfigured.

In view of Supreme Court Decision in KSR International Co. v. Teleflex Inc., 550 U.S. -, 82 USPQ2d 11385 (2007), the Supreme Court stated that the Federal Circuit erred when it applied the well-known teaching-suggestion-motivation (TSM) test in an overly rigid and formalistic way. According to the Supreme Court, the TSM test is one of a number of valid rationales that could be used to determine obviousness. It is NOT the only rationale that may be relied upon to support a conclusion of obviousness.

Regarding Claim 3, FARMER & BETTINGER teaches all the features of claim 1, FARMER further teaches

said interface router is a premise router (**Fig.3 element 355**, optical routing device is a premise router providing secured services to multiple subscribers or tenants 365 170).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. FARMER further teaches - optical routing device is a premise router providing secured services to multiple subscribers or tenants.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - optical routing device is a premise router providing secured services to multiple subscribers or tenants.

Regarding Claim 4, FARMER & BETTINGER teaches all the features of claim 1,
BETTINGER further teaches

said interface router is further configured to have a global routing table (**Fig.9A, Fig.9B, col.10 & lines 49-51, upstream virtual router tag table 914 (described below) in conjunction with the shared network equipment, to provide a virtual router capability.** Here, router tag table 914 is global routing table), and wherein a number of destinations listed in said at least one virtual routing table are associated with corresponding destinations listed in said global routing table (**Fig.9A, Fig.9B, col.10 and lines 47-49, the remote virtual router 904 and remote virtual router tag table 908 work with the upstream (virtual router 910 and upstream virtual router tag table 914.** Here, multiple virtual router provides individual separate and private network to upstream global router).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. BETTINGER further teaches - multiple virtual router provides individual separate and private network to upstream global router.

Thus given the teaching of BETTINGER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual

routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add BETTINGER's further teaching technique - multiple virtual router provides individual separate and private network to upstream global router.

Regarding Claim 5, FARMER & BETTINGER teaches all the features of claim 1, FARMER further teaches

each of said optical network units provides service to a separate number of private users **(Fig.3 elements 365 /170 & col.11 lines 1-11, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360. From the bi-directional splitter 360, respective optical receivers 370 can convert the upstream optical signals into the electrical domain. The upstream electrical signals generated by respective optical receivers 370 are then fed into the laser transceiver node routing device 355. As noted above, each optical receiver 370 can comprise one or more photoreceptors or photodiodes that convert optical signals into electrical signals. Here, 365/170 are different private subscribers or tenants are using uplinks optical routing device, internet router and other sources of carrier links).**

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent

BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. FARMER further teaches - different private subscribers or tenants are using uplinks optical routing device, internet router and other sources of carrier links.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - different private subscribers or tenants are using uplinks optical routing device, internet router and other sources of carrier links.

Regarding Claim 6, FARMER & BETTINGER teaches all the features of claim 1,
FARMER further teaches

said uplink carries data including digitized voice and video data ([0002] lines 1-7, the invention relates to video, voice, and data communications. More particularly, the invention relates to a fiber-to-the-home (FTTH) system that is capable of supporting upstream radio-frequency (RF) return signals formatted according to a cable modem

protocol that originate from a subscriber and are sent upstream to a data service provider.

Here, optical network handles digital triple play or voice, video & data).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. FARMER further teaches - optical network handles digital triple play or voice, video & data.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - optical network handles digital triple play or voice, video & data.

Regarding claim 7, claim 7 is claim to an apparatus using the apparatus of claim 1.

Therefore, claim 7 is rejected for the reasons set forth for claim 1.

Regarding Claim 8, FARMER teaches a digital data network communication method comprises:

accepting a plurality of private data streams into a passive optical network interface router serving a plurality of private users through a plurality of optical network units (**Fig.3 element 355 and col.10 lines 42-45, the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol for communicating with one or more laser transceiver nodes 120 (fig.2).** Here, optical router is interfacing with internet router and multiple optical interfaces. Optical router device is passive or cross-connect optical links);

aggregating said private data streams into a combined data feed (**Fig.3 is showing that individual data from different stream of 170 (drawing shows 3 times for example) are feeding in single optical router device 355 which aggregates data from individuals to single upstream interface 350 with routing device 355);**

routing said data feed to at least two of said plurality of optical network units (**Fig.3 is also showing that optical routing device 355 is connecting to two upstream units 340 and 345);**

extracting from said data feed a first one of said private data streams (**Fig.3 elements 170 (3 instances for example) is feeding data into upstream or upstream routing device is extracting or taking inputs from individual units shows by 170, 360, 370);**

FARMER, however does not teach wherein said routing comprises:

providing a global routing table;

providing an independently unique virtual routing table for each of said plurality of optical network units;

tagging ethernet frames intended for a first one of said plurality of optical network units according to entries in a first one of said virtual routing tables associated with a first one of said optical network units;

distributing said tagged ethernet frames according to both of said global routing table and said first one of said virtual routing tables.

In another analogous patent BBB teaches wherein said routing comprises:

providing a global routing table (**Fig.9A, Fig.9B, col.10 & lines 49-51, upstream virtual router tag table 914 (described below) in conjunction with the shared network equipment, to provide a virtual router capability.** Here, router tag table 914 is global routing table);

providing an independently unique virtual routing table for each of said plurality of optical network units (**Fig.9A, Fig.9B, col.10 and lines 47-49, the remote virtual router 904 and remote virtual router tag table 908 work with the upstream (virtual router 910 and upstream virtual router tag table 914.** Here, multiple virtual router provides individual separate and private network);

tagging ethernet frames intended for a first one of said plurality of optical network units according to entries in a first one of said virtual routing tables associated with a first one of said optical network units (**Fig.8, col.10 & lines 23-27, multidrop communication link 808 may include, for example, an RS-422 data link or an Ethernet data link. Further, a plurality of user computers 806 may communicate**

with network A via a single terminal 802 using a wireless communication link 810.

Here, ethernet links are used for downstream data);

distributing said tagged ethernet frames according to both of said global routing table and said first one of said virtual routing tables (**As described above in Fig.9A, Fig.9B & col.10**, Ethernet frames are fed into individual optical device and ultimately connected to uplink global optical router).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network.

All references are inventions in analogous area but each invention teaches specific claimed limitation specifically and other references mutually cure each other's deficiencies. When all claimed techniques are combined they teach claimed invention.

To provide a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, in view of the teachings of BETTINGER, since the techniques were known in the prior art and one skilled in the art could have combined the

technique (*eMPEP sec 2141 sub-section C (III) items (C) - use of known technique to improve similar devices (methods, or products) in the same way, & (D) - applying a known technique to a known device (method, or product) ready for improvement to yield predictable results*), the elements as claimed by a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network to achieve obvious predictable result.

The combination would have yielded nothing more than predictable results to one of ordinary skill at the time of the invention, i.e., one skilled in the art would have recognized that the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network used in BETTINGER would allow the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER to function as invention claimed.

This enhancement provides a secured technique of a network router connecting to passive optical carrier lines, distributes to multiple optical subscriber ports, have virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeps individual subscriber's data separate from other subscribers private and secured by avoiding use of individual router for each subscriber provided by the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic,

keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of BETTINGER FARMER's the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. Furthermore, this enhancement facilitates service providers and subscribers using common optical router equipment with virtual routing tables shared between multiple independently administered networks by managing each subscriber's data private separate and saves installation, maintenance and operation cost by avoiding providing individual router to each subscriber. The common optical router equipment is reconfigurable and expandable and provides changed communication capacity and functions when additional elements are added or reconfigured.

In view of Supreme Court Decision in KSR International Co. v. Teleflex Inc., 550 U.S. -, 82 USPQ2d 11385 (2007), the Supreme Court stated that the Federal Circuit erred when it applied the well-known teaching-suggestion-motivation (TSM) test in an overly rigid and formalistic way. According to the Supreme Court, the TSM test is one of a number of valid rationales that could be used to determine obviousness. It is NOT the only rationale that may be relied upon to support a conclusion of obviousness.

Regarding Claim 9, FARMER & BETTINGER teaches all the features of claim 1, BETTINGER further teaches

said distributing comprises associating destinations listed in said first one of said virtual routing tables with destinations listed (**Fig.9A, Fig.9B, col.10 and lines 47-49, the remote**

virtual router 904 and remote virtual router tag table 908 work with the upstream (virtual router 910 and upstream virtual router tag table 914. Here, multiple virtual router provides individual separate and private network to upstream global router) in said global routing table (Fig.9A, Fig.9B, col.10 & lines 49-51, upstream virtual router tag table 914 (described below) in conjunction with the shared network equipment, to provide a virtual router capability. Here, router tag table 914 is global routing table).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. BETTINGER further teaches - multiple virtual router provides individual separate and private network to upstream global router.

Thus given the teaching of BETTINGER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER &

BETTINGER to add BETTINGER's further teaching technique - multiple virtual router provides individual separate and private network to upstream global router.

Regarding claim 10, claim 10 is a dependent claim of claim 8, claim 10 is claim to method using the apparatus of claim 5. Therefore, claim 10 is rejected for the reasons set forth for claim 5.

Regarding Claim 11, FARMER & BETTINGER teaches all the features of claim 8, FARMER further teaches

interfacing a plurality of service provider data lines through a single headend (**Fig.3 elements 340, 345, 350 & col.10 lines 25-36**, the data service hub 110 can further comprise a telephone switch 345 that supports telephony service to the subscribers of the optical network system 100. However, other telephony service such as Internet Protocol telephony can be supported by the data service hub 110. If only Internet Protocol telephony is supported by the data service hub 110, then it is apparent to one of ordinary skill in the art that the telephone switch 345 could be eliminated in favor of lower cost VoIP equipment. For example, in another exemplary embodiment (not shown), the telephone switch 345 could be substituted with other telephone interface devices such as a soft switch and gateway. Here, multiple service providers are connected to the optical routing device).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent

BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. FARMER further teaches - multiple service providers are connected to the optical routing device.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - multiple service providers are connected to the optical routing device.

Regarding Claim 12, FARMER & BETTINGER teaches all the features of claims 11 & 8, FARMER further teaches wherein said interfacing comprises:

utilizing at least one premise router and a radio frequency video converter; and, feeding an output of said premise router through an optical line terminal **(col.10 lines 9-16, to support data services or to support incidental services related to the downstream video services, a data-to-RF converter 307 that transforms RF return packets back into their original RF analog electrical format can be coupled to an Internet Router 340. Further details of RF**

converter 307 will be discussed below with respect to FIG. 8. The RF analog electrical signals generated by the data-to-RF converter 307 are demodulated by an RF receiver 309.

Here, radio frequency converter is used for data conversion to appropriate form for uplink and downlink).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. FARMER further teaches - radio frequency converter is used for data conversion to appropriate form for uplink and downlink.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - radio frequency converter is used for data conversion to appropriate form for uplink and downlink.

Regarding claim 13, claim 13 is a dependent claim of claims 12, 11 & 8 claim 13 is claim to method using the method of claim 12. Therefore, claim 13 is rejected for the reasons set forth for claim 12.

Regarding Claim 14, FARMER & BETTINGER teaches all the features of claims 11 & 8, FARMER further teaches wherein said optically routing comprises:

sending said encrypted data feed through an optical splitter (col.10 lines 58-67, the laser transceiver node routing device 355 can supply downstream data signals to respective optical transmitters 325. The data signals converted by the optical transmitters 325 can then be propagated to a bi-directional splitter 360. The optical signals sent from the optical transmitter 325 into the bidirectional splitter 360 can then be propagated towards a bi-directional data input/ output port 365 that is connected to a second optical waveguide 170 that supports bi-directional optical data signals between the data service hub 110 and a respective laser transceiver node 120. Here, passive optical splitter devices are used for optical connectivity, which is converted later in uplink).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber

traffic to uplink data carrier network. FARMER further teaches - passive optical splitter devices are used for optical connectivity, which is converted later in uplink.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - passive optical splitter devices are used for optical connectivity, which is converted later in uplink.

Regarding Claim 18, FARMER & BETTINGER teaches all the features of claim 8, FARMER further teaches wherein said aggregating comprises using an enterprise aggregating switch (**Fig.3 elements 340, 345, 355 are enterprise switches and routers for aggregating data streams**). Here, Fig.3 is showing that individual data from different stream of 170 (drawing shows 3 times for example) are feeding in single optical router device 355 which aggregates data from individuals to single upstream interface 350 with routing device 355. Data is getting aggregated for uplink and reverse for delivery in downlink).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing

traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. FARMER further teaches - data is getting aggregated for uplink and reverse for delivery in downlink.

Thus given the teaching of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add FARMER's further teaching technique - data is getting aggregated for uplink and reverse for delivery in downlink.

Claims 2, 16 & 17 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Farmer; James O. et al. (hereinafter **FARMER**), Pat. No.: US 7,583,897 B2 in view of Bettinger et al. (hereinafter **BETTINGER**), Pat. No.: US 7,509,144 B2 and DiCrescenzo et al. (hereinafter **DICRESCENZO**), Pub. No.: US 2010/0232608 A1.

Regarding Claim 2, FARMER & BETTINGER teaches all the features of claim 1, they, however fails to teach

said common data feed is encrypted.

In another patent publication DICRESCENZO teaches

said common data feed is encrypted ([0030] lines 14-16, steps 3 and 4 consist of the **aggregation of the n encrypted pseudo-data streams into a single encrypted signal s(t).**

Here, individual data stream is encrypted and is aggregated in to a single data stream. Common data feed is interpreted as claimed aggregated data feed).

All references are inventions in analogous area but each invention teaches specific claimed limitation specifically and other references mutually cure each other's deficiencies.

When all claimed techniques are combined they teach claimed invention.

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. DICRESCENZO teaches - individual data stream is encrypted and is aggregated in to a single data stream.

Thus given the teaching of DICRESCENZO, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink

ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add DICRESCENZO's further teaching technique - individual data stream is encrypted and is aggregated in to a single data stream.

Regarding Claim 16, FARMER & BETTINGER teaches all the features of claims 15 & 8, DICRESCENZO further teaches wherein each of said streams comprises:

encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed (**Fig.1 element 102 & [0018] lines 1-3, FIG. 1 is a block diagram of digital encryption 100 with an encryption algorithm 102, taking as input a data stream 104 and a key stream 106.** Here, digital data is encrypted for processing securely); and,

wherein said extracting comprises:

partially decrypting said encrypted data feed (**[0018] lines 3-8, returning a ciphertext stream that may be eavesdropped by the adversary, and a decryption algorithm 108, taking as input the ciphertext stream returned by the encryption algorithm and a key stream 110, and returning a data stream 112 that would be equal to the data stream 104 input to the encryption algorithm 102.** Here, digital data is decrypted for secure delivery).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing

traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. DICRESCENZO further teaches - digital data is encrypted for processing securely, and digital data is decrypted for secure delivery.

Thus given the teaching of DICRESCENZO, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add DICRESCENZO's further teaching technique - digital data is encrypted for processing securely, and digital data is decrypted for secure delivery.

Regarding Claim 17, FARMER & BETTINGER teaches all the features of claim 8, FARMER further teaches extracting comprises:

operating an optical network unit at each of said tenants **(Fig.3 elements 365 /170 & col.11 lines 1-11, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360. From the bi-directional splitter 360,**

respective optical receivers 370 can convert the upstream optical signals into the electrical domain. The upstream electrical signals generated by respective optical receivers 370 are then fed into the laser transceiver node routing device 355. As noted above, each optical receiver 370 can comprise one or more photoreceptors or photodiodes that convert optical signals into electrical signals. Here, 365/170 are different networks or subscribers using uplinks optical routing device, internet router and other sources of carrier links);

DICRESCENZO further teaches wherein said operating comprises:

decrypting incoming intended data packets from said feed ([0018] lines 3-8, returning a ciphertext stream that may be eavesdropped by the adversary, and a decryption algorithm 108, taking as input the ciphertext stream returned by the encryption algorithm and a key stream 110, and returning a data stream 112 that would be equal to the data stream 104 input to the encryption algorithm 102. Here, digital data is decrypted for secure delivery);

not decrypting incoming unintended data packets from said feed; and, encrypting outgoing data packets to said feed (Fig.1 element 102 & [0018] lines 1-3, FIG. 1 is a block diagram of digital encryption 100 with an encryption algorithm 102, taking as input a data stream 104 and a key stream 106. Here, digital data is encrypted for processing securely).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber

traffic to uplink data carrier network. DICRESCENZO further teaches - digital data is encrypted for processing securely, and digital data is decrypted for secure delivery.

Thus given the teaching of DICRESCENZO, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add DICRESCENZO's further teaching technique - digital data is encrypted for processing securely, and digital data is decrypted for secure delivery.

Claim 15 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Farmer; James O. et al. (hereinafter **FARMER**), Pat. No.: US 7,583,897 B2 in view of Bettinger et al. (hereinafter **BETTINGER**), Pat. No.: US 7,509,144 B2 and DiCrescenzo et al. (hereinafter **DICRESCENZO**), Pub. No.: US 2010/0232608 A1, and further in view of Kanter et al. (hereinafter **KANTER**), PAT. No.: US 8,315,387 B2.

Regarding Claim 15, FARMER & BETTINGER teaches all the features of claims 8, they, however do not disclose wherein each of said streams comprises:

encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed.

wherein said extracting comprises:

partially decrypting said encrypted data feed.

In another patent publication DICRESCENZO discloses wherein each of said streams comprises:

encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed (**Fig.1 element 102 & [0018] lines 1-3, FIG. 1 is a block diagram of digital encryption 100 with an encryption algorithm 102, taking as input a data stream 104 and a key stream 106.** Here, digital data is encrypted for processing securely); and,

In another patent KANTER discloses wherein said extracting comprises:

partially decrypting said encrypted data feed (**col.15 lines 59-63, a hierarchy of keys can be used such that the data at the access point can be partially decrypted into a standard encrypted format which allows for digital processing such as error correction and descrambling. Acknowledgement packets can then be sent as in a standard system.** Here, a technique of partial decryption is used for input encrypted data).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent BETTINGER teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network. DICRESCENZO teaches that digital data is encrypted for processing securely. KANTER teaches a technique of partial decryption is used for input

encrypted data.

All references are inventions in analogous area but each invention teaches specific claimed limitation specifically and other references mutually cure each other's deficiencies. When all claimed techniques are combined they teach claimed invention.

Thus given the teaching of DICRESCENZO & KANTER, it would have been obvious to one of ordinary skill at the time of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & BETTINGER to add DICRESCENZO's teaching technique - digital data is encrypted for processing securely, AND FARMER's teaching technique - of partial decryption is used for input encrypted data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to QUAZI FAROOQUI whose telephone number is (571) 270-1034. The examiner can normally be reached on M-F 8:30AM-5:00PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok B. Patel can be reached on 571-272-3972. The fax phone number for Examiner Farooqui assigned is 571-270-2034.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/QUAZI FAROOQUI/

Examiner, Art Unit 2491

/ASHOKKUMAR B PATEL/

Supervisory Patent Examiner, Art Unit 2491

<i>Notice of References Cited</i>	Application/Control No. 15/351,315		Applicant(s)/Patent Under Reexamination Vilella et al.	
	Examiner QUAZI FAROOQUI		Art Unit 2491	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20060269285-A1	11-2006	Farmer; James O.	H04J3/0664	398/72
*	B	US-20100232608-A1	09-2010	DiCrescenzo; Giovanni	H04K1/006	380/287
*	C	US-7509144-B2	03-2009	Bettinger; David D.	G06Q30/04	370/316
*	D	US-8315387-B2	11-2012	Kanter; Gregory S.	H04L9/0852	380/256
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001)

Notice of References Cited

Part of Paper No. 20180628

<i>Search Notes</i> 	Application/Control No. 15/351,315	Applicant(s)/Patent Under Reexamination Vilella et al.
	Examiner QUAZI FAROOQUI	Art Unit 2491

CPC - Searched*		
Symbol	Date	Examiner
H04L9/00 H04L9/32-3297 H04L63/04-0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12	07/02/2018	/QF/
H04L9/06,08 H04Q11/00, H04B10/27	07/02/2018	/QF/
H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00	07/02/2018	/QF/

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
380	26,28-30, 44-47,255-286	07/02/2018	/QF/
713	150-154,160-168,189-193	07/02/2018	
726	1-33	07/02/2018	

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor and assignee search in PALM	06/30/2018	/QF/
Inventor and assignee search in EAST all database	07/02/2018	
Classification search in EAST	07/02/2018	
text search in EAST	07/02/2018	
updated EAST search with class and text	07/02/2018	

/QUAZI FAROOQUI/ Examiner, Art Unit 2491	
---	--

<i>Search Notes</i> 	Application/Control No. 15/351,315	Applicant(s)/Patent Under Reexamination Vilella et al.
	Examiner QUAZI FAROOQUI	Art Unit 2491

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/QUAZI FAROOQUI/ Examiner, Art Unit 2491	
---	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	574634	(H04L9/00 H04L9/32-3297 H04L63/04-0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/07/02 15:11
L2	598937	(H04L9/00 H04L9/32-3297 H04L63/04-0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC. (H04L9/06,08 H04Q11/00, H04B10/27).CPC. (H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/07/02 15:13
L3	660848	(H04L9/00 H04L9/32-3297 H04L63/04-0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC. (H04L9/06,08 H04Q11/00, H04B10/27).CPC. (H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00).cpc. (380/26,28-30,44-47,255-286 713/150-154,160-168,189-193 726/1-33).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/07/02 15:15
L4	2	(Optical adj2 data adj2 network) and ((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/07/02 15:16
L5	0	L4 and L3	USPAT	OR	OFF	2018/07/02 15:16
L6	392	(Optical adj2 data adj2 network) and (virtual many multiple plural\$3)	USPAT	OR	OFF	2018/07/02 15:17
L7	60	L6 and L3	USPAT	OR	OFF	2018/07/02 15:17
L8	47	L7 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2018/07/02 15:20
L9	41	L7 AND ((@ad @pd) < "20120801")	USPAT	OR	OFF	2018/07/02 15:21
L10	10	(Optical adj2 data adj2 network) and (virtual same (many multiple plural\$3) same rout\$5)	USPAT	OR	OFF	2018/07/02 15:23

L11	3	8 and 10	USPAT	OR	OFF	2018/07/02 15:23
L12	6	L10 AND ((@ad @pd) < "20120801")	USPAT	OR	OFF	2018/07/02 15:24
S1	24961	(aggregat\$3 near5 encrypt\$3) optical near5 data near5 stream	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:03
S2	2	(aggregat\$3 near5 encrypt\$3) SAME (optical near5 data near5 stream)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:04
S3	333	(radio adj frequency) same (video near5 converter)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:06
S4	5	(radio adj frequency) same (video near5 converter) same router	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:07
S5	51	(radio adj frequency) same (video near5 converter) same (router switch)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:07
S6	3	S5 and (optical adj splitter)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:09
S7	3	"6751302".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:50
S8	0	"SPADA INNOVATIONS, INC.".as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:13

S9	0	"SPADA INNOVATIONS, INC." .asn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:13
S10	133	"SPADA" .asn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:13
S11	2	S10 and optical and encrypt\$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:14
S12	34	((VILELLA near2 JOSEPH) OR (REYNANTE near4 JAMES)).inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:16
S13	2	S12 and encrypt\$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:16
S14	520	"3" AND H04L9/0852.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:24
S15	52	"S3" AND H04L9/0852.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:24
S16	37	"S3" AND 380/256.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:25
S17	0	"20170063542" .pn.	USPAT	OR	ON	2018/06/29 11:31
S18	3	"20170063542" .pn.	US-PGPUB; USPAT; USOCR;	OR	ON	2018/06/29 11:39

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S19	403	(Optical adj2 data adj2 network)	USPAT	OR	OFF	2018/06/29 13:33
S20	0	(Optical adj2 data adj2 network) same3 (virtual near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:35
S21	0	(Optical adj2 data adj2 network) and (virtual near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:36
S22	2	(Optical adj2 data adj2 network) and ((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:36
S23	3346	((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:39
S24	448	(virtual many multiple plural\$3) adj2 rout\$3 adj2 table	USPAT	OR	OFF	2018/06/29 13:39
S25	21	S24 and (optical adj5 network)	USPAT	OR	OFF	2018/06/29 13:40
S26	24	S24 and (optical adj5 (network router switch))	USPAT	OR	OFF	2018/06/29 13:42
S27	24	S26 AND (@ad @pd @prad @rlad @ptad < "20120801")	USPAT	OR	OFF	2018/06/29 13:42
S28	24	S26 AND (@ad @pd < "20120801")	USPAT	OR	OFF	2018/06/29 13:43
S29	1203	398/70-72.ccls. (H04B10/00).cpc.	USPAT	OR	OFF	2018/06/29 16:39
S30	403	(Optical adj2 data adj2 network)	USPAT	OR	OFF	2018/06/29 16:40
S31	13	S30 and S29	USPAT	OR	OFF	2018/06/29 16:40
S32	122	S29 and virtual	USPAT	OR	OFF	2018/06/29 16:40
S33	64	"pluris".asn.	USPAT	OR	OFF	2018/06/30 14:45
S34	41	"sycamore networks".asn.	USPAT	OR	OFF	2018/06/30 14:46
S35	3	"sycamore networks".asn. and frequency and splitter	USPAT	OR	OFF	2018/06/30 14:46
S36	54148	"pluris"" .asn.and" frequency and splitter	USPAT	OR	OFF	2018/06/30 14:47
S37	54148	"pluris"" .asn.and" frequency and splitter	USPAT	OR	OFF	2018/06/30 14:47
S38	0	S33 and frequency and splitter	USPAT	OR	OFF	2018/06/30 14:47
S39	17	S33 and aggrega\$4	USPAT	OR	OFF	2018/06/30 14:48
S40	19	S33 and optical	USPAT	OR	OFF	2018/06/30 14:48
S41	8	S33 and optical and router	USPAT	OR	OFF	2018/06/30 14:49
S42	3	S33 and (optical same2 router)	USPAT	OR	OFF	2018/06/30 14:49
S43	30913	(aggregat\$3 near5 encrypt\$3) optical	US-PGPUB;	OR	ON	2018/06/30

EAST Search History

		near5 data near5 stream	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:00
S44	1285	S43 and (encrypt\$4 same2 decrypt\$4)	USPAT	OR	OFF	2018/06/30 15:00
S45	1198	S43 and (encrypt\$4 with decrypt\$4)	USPAT	OR	OFF	2018/06/30 15:01
S46	45	S43 and (encrypt\$4 with decrypt\$4) and splitter	USPAT	OR	OFF	2018/06/30 15:01

7/ 2/ 2018 3:25:13 PM

C:\Users\qfarooqui\Documents\EAST\Workspaces\15351315-VILELLA (CIP of ABAN
14419092).wsp

Bibliographic Data

Application No: 15/351,315

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged: /QUAZI FAROOQUI/

Examiner's Signature

Initials

Title:

Mutually secure optical data network and method

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/14/2016	380	2491	160142
RULE			

APPLICANTS

INVENTORS

Joseph L. Vilella San Diego, CA, UNITED STATES

James R. Reynante San Diego, CA, UNITED STATES

CONTINUING DATA

This application is a CIP of 14419092 02/02/2015

14419092 is a 371 of PCT/US2013/053389 08/02/2013

PCT/US2013/053389 has PRO of 61678977 08/02/2012

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

11/23/2016

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

CHARMASSON, BUCHACA & LEACH, LLP

2635 Camino Del Rio South

Suite 102

SAN DIEGO, CA 92108

UNITED STATES

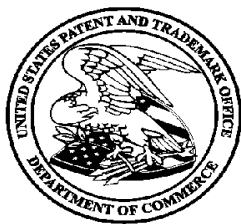
FILING FEE RECEIVED

\$70

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108



**Courtesy Reminder for
Application Serial No: 15/351,315**

Attorney Docket No: 160142
Customer Number: 24243
Date of Electronic Notification: 07/10/2018

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
john@charmason.com

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>. If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/351,315	Filing Date 11/14/2016	☐ To be Mailed
---	--	---------------------------	---------------------------------------

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

(Column 1)		(Column 2)			RATE (\$)	FEE (\$)
FOR	NUMBER FILED	NUMBER EXTRA				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*			X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*			X \$ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			

APPLICATION AS AMENDED – PART II

(Column 1)		(Column 2)	(Column 3)			RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	09/28/2018	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total (37 CFR 1.16(i))	* 9	Minus	** 20	= 0	X \$50 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X \$230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE						0	

(Column 1)		(Column 2)	(Column 3)			RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE							

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
HALLEY MASSEY

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal				
Application Number:		15351315		
Filing Date:		14-Nov-2016		
Title of Invention:		Mutually secure optical data network and method		
First Named Inventor/Applicant Name:		Joseph L. Vilella		
Filer:		John David Buchaca		
Attorney Docket Number:		160142		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 2 months with \$0 paid	2252	1	300	300
Miscellaneous:				
Total in USD (\$)				300

Electronic Acknowledgement Receipt	
EFS ID:	34525734
Application Number:	15351315
International Application Number:	
Confirmation Number:	2023
Title of Invention:	Mutually secure optical data network and method
First Named Inventor/Applicant Name:	Joseph L. Vilella
Customer Number:	24243
Filer:	John David Buchaca
Filer Authorized By:	
Attorney Docket Number:	160142
Receipt Date:	07-DEC-2018
Filing Date:	14-NOV-2016
Time Stamp:	18:54:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 300
RAM confirmation Number	121018INTEFSW18561100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	2018-12-07_160142_Transmittal.pdf	145332	no	1
			40213bef00e21a336374dd0ee140810a285f66ff		
Warnings:					
Information:					
2	Extension of Time	2018-12-07_160142_Extension.pdf	126711	no	1
			910a34e381429320997de65387170fc090a6c2a		
Warnings:					
Information:					
3	Amendment/Req. Reconsideration-After Non-Final Reject	2018-12-07_160142_Amendment.pdf	262256	no	7
			a2cbbb4c70526cef1c02ede53838c40643a68f9		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	29904	no	2
			b599a9ee37634a4730c44a3dfde277db0dc72daa		
Warnings:					
Information:					
Total Files Size (in bytes):			564203		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>	Application Number	15351315	
	Filing Date	2016-11-14	
	First Named Inventor	Joseph L. Vilella	
	Art Unit	2491	
	Examiner Name	Farooqui, Quazi	
Total Number of Pages in This Submission	11	Attorney Docket Number	160142

ENCLOSURES (Check all that apply)		
☒ Fee Transmittal Form ☒ Fee Attached ☒ Amendment/Reply ☐ After Final ☐ Affidavits/declaration(s) ☒ Extension of Time Request ☐ Express Abandonment Request ☐ Information Disclosure Statement ☐ Certified Copy of Priority Document(s) ☐ Reply to Missing Parts/ Incomplete Application ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☐ Power of Attorney, Revocation ☐ Change of Correspondence Address ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____ ☐ Landscape Table on CD	☐ After Allowance Communication to TC ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☐ Other Enclosure(s) (please identify below):
Remarks Amendment - 7 sheets Extension of Time - 1 sheet EFS-Web-generated Fee Sheet - 2 sheets This Transmittal - 1 sheet		
SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm Name	Charmasson, Buchaca & Leach, LLP	
Signature	/John Buchaca/	
Printed name	John D. Buchaca	
Date	2018-12-07	Reg. No. 37289

CERTIFICATE OF TRANSMISSION/MAILING	
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:	
Signature	/John Buchaca/
Typed or printed name	John D. Buchaca
Date	2018-12-07

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 160142
Application Number 15351315	Filed 2016-11-14	
For Mutually secure multi-tenant optical data network and method		
Art Unit 2491	Examiner Farooqui, Quazi	

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ _____
☒ Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ <u>300</u>
☐ Three months (37 CFR 1.17(a)(3))	\$1,400	\$700	\$350	\$ _____
☐ Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100	\$550	\$ _____
☐ Five months (37 CFR 1.17(a)(5))	\$3,000	\$1,500	\$750	\$ _____

☒ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☐ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to
Deposit Account Number _____.

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☒ attorney or agent of record. Registration number 37289

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____

/John Buchaca/ 2018-12-07

Signature Date

John D. Buchaca 619-294-2922

Typed or printed name Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

WASHINGTON, D.C.

In re application of:	)	
	)	Examiner: Farooqui, Quazi
Joseph L. Vilella, et al.	)	
	)	
Serial No: 15351315	)	Art Unit: 2491
	)	
Filed: 2016-11-14	)	
	)	
For: Mutually secure optical data	)	
network and method	)	
	)	

AMENDMENT

Mail Stop Amendment
Commissioner for Patents
Via EFS-Web

Please amend the application as indicated below.

In the Claims

Please amend the claims as indicated below:

1 1. (Currently Amended) A multi-user digital optical data network apparatus comprises:
2 a plurality of network service digital carrier lines connected to a passive optical
3 network interface router;
4 at least one uplink connecting said interface router to an optical line terminal;
5 said optical line terminal being connected to a number of passive optical network
6 feeds for carrying a common digital data feed to a plurality of optical network units each
7 supporting at least one of a plurality of private user devices;
8 said interface router being configured to have at least one unique virtual routing
9 table for each one of said plurality of optical network units; and,
10 wherein each of said optical network units is adapted to extract digital data
11 packets intended for a supported one of said devices.

1 2. (Currently Amended) The apparatus of Claim 1, wherein said common digital data
2 feed is encrypted.

1 3. (Original) The apparatus of Claim 1, wherein said interface router is a premise router.

1 4. (Currently Amended) The apparatus of Claim 1, wherein said interface router is
2 further configured to have a global routing table, and wherein a number of destinations
3 listed in said at least one unique virtual routing table are associated with corresponding
4 destinations listed in said global routing table.

1 5. (Original) The apparatus of Claim 1, wherein each of said optical network units
2 provides service to a separate number of private users.

1 6. (Currently Amended) The apparatus of Claim 1, wherein said uplink carries digital
2 data including digitized voice and video data.

1 7. (Currently Amended) A multi-user optical data network apparatus comprises:
2 a plurality of network service digital carrier lines connected to a plurality of
3 passive optical network interface routers;
4 a plurality of uplinks connecting said interface routers to an optical line terminal;
5 said optical line terminal being connected to a number of passive optical network
6 feeds for carrying a common digital data feed to a plurality of optical network units each
7 supporting at least one of a plurality of private user devices;
8 wherein each of said interface routers is configured to have at least one unique
9 virtual routing table for each one of said plurality of optical network units to which said
10 each of said interface routers is connected; and,
11 wherein each of said optical network units is adapted to extract digital data
12 packets intended for a supported one of said devices.

1 8. (Currently Amended) A digital data network communication method comprises:
2 accepting a plurality of private digital data streams into a passive optical network
3 interface router serving a plurality of private users through a plurality of optical network
4 units;
5 aggregating said private digital data streams into a combined digital data feed;
6 routing said digital data feed to at least two of said plurality of optical network
7 units;
8 extracting from said digital data feed a first one of said private digital data
9 streams;
10 wherein said routing comprises:
11 providing a ~~global routing table~~ at least one premise router;
12 ~~providing~~ configuring said at least one premise router to have an
13 independently unique virtual routing table for each of said plurality of optical network
14 units;
15 tagging ethernet frames intended for a first one of said plurality of optical
16 network units according to entries in a first one of said independently unique virtual
17 routing tables associated with a first one of said optical network units;

18 distributing said tagged ethernet frames ~~according to both of said global~~
19 ~~routing table and said first one of said virtual routing tables~~ to said first one of said
20 plurality of optical network units.

1 9. (Currently Amended) The method of Claim 8, ~~wherein said distributing comprises~~
2 ~~associating destinations listed in said first one of said virtual routing tables with~~
3 ~~destinations listed in said global routing table~~ wherein said configuring comprises:
4 _____ establishing a global routing table on said at least one premise router for
5 accessing virtual routing table instantiations for each of said plurality of optical network
6 units.

1 10. (Original) The method of Claim 8, wherein each of said optical network units
2 provides service to a separate number of private users.

1 11. (Currently Amended) The method of Claim 8, wherein said accepting comprises:
2 interfacing a plurality of service provider digital data lines through a single
3 headend.

1 12. (Currently Amended) The method of Claim 11, wherein said interfacing comprises:
2 utilizing ~~at least one premise router and~~ a radio frequency video converter; and,
3 feeding an output of said at least one premise router through an optical line
4 terminal.

1 13. (Original) The method of Claim 12, wherein said interfacing further comprises:
2 feeding an output of said converter through said optical line terminal.

1 14. (Currently Amended) The method of Claim 11, wherein said ~~[[optically]]~~ routing
2 comprises:
3 sending said encrypted data feed through an optical splitter.

1 15. (Currently Amended) The method of Claim 8, wherein each of said private digital
2 data streams comprises:
3 encrypted informational data, encrypted telephone data, and, encrypted video data
4 to form an encrypted data feed; and,
5 wherein said extracting comprises:
6 partially decrypting said encrypted data feed.

1 16. (Original) The method of Claim 15, wherein said encrypted data feed comprises:
2 a plurality of encrypted ethernet frames;
3 wherein a subset of said frames are associated with a first one of said users and a
4 second subset of said frames is associated with a second one of said users.

1 17. (Currently Amended) The method of Claim 8, wherein said extracting comprises:
2 operating ~~an optical network unit~~ at least one of said optical network units at each
3 of said tenants;
4 wherein said operating comprises:
5 decrypting incoming intended data packets from said encrypted data feed;
6 not decrypting incoming unintended data packets from said encrypted data
7 feed; and,
8 encrypting outgoing data packets to said encrypted data feed.

1 18. (Original) The method of Claim 8, wherein said aggregating comprises using an
2 enterprise aggregating switch.

REMARKS

Claims 1-18 remain pending after this amendment. Claims 1, 7, and 8 are independent. The independent claims have been amended to more specifically require the digital nature of the claimed network, and to require that the global routing table within the interface router be configured to have a *unique* virtual routing table for each particular, individual optical network unit being serviced by the interface router. This language is supported by originally filed application, specifically, for example at Claim 8, Fig. 3, and the specification page 9, lines 5-19. Care has been taken to avoid the introduction of any new matter.

Claim 17 has been amended to improve clarity and to correct the antecedency issue identified by the examiner.

The examiner has rejected the independent claims for obviousness in light of Farmer et al., U.S. Pat. No. 7583897 (Farmer) in view of Bettinger et al., U.S. Pat. No. 7509144 (Bettinger). However, the combination of these references does not result in the claims as amended.

Specifically, neither Farmer nor Bettinger appear to disclose or suggest providing an interface router, such as a premise router, which has been configured to have a plurality of virtual routing tables, *within* the interface router, where each of these tables is *unique* for each optical network unit being serviced by that interface router.

The examiner relies on Bettinger to disclose such virtual routing tables. However, in Bettinger, the single Remote Virtual Router Tag Table (908 in Bettinger Fig. 9A) is not configured on what would be the interface router serving a plurality of terminals, but rather on an individual remote terminal (800 in Bettinger Fig. 9A). This is because Bettinger addresses a large scale communications system that feeds identical data to a large number of satellite users that are intended to have the same access to all that data. In the context of individual users on a network, the claimed invention, on the other hand, does not provide the same access to the supplied data between different users. Instead, that access is restricted by one of the uniquely populated individual virtual routing tables dedicated to that particular user which is located within the router servicing all users. Thus the combination of Farmer and Bettinger does not result in the invention as claimed. And therefore, the claims are non-obvious.

It should be pointed out as well, that there would be no motivation to adapt the Bettinger system to have the multiple virtual routing tables of the claimed invention since doing so would add unnecessary complexity and tend to slow down network throughput.

In light of this amendment, early allowance of the pending claims is earnestly solicited.

Applicant reserves the right to further pursue the original claims and any other broad claims supported by the original disclosure in one or more continuing applications.

Respectfully submitted,

2018-12-07



John D. Buchaca
Registration No. 37, 289
2635 Camino Del Rio South, Suite 102
San Diego, California 92108
Telephone: (619) 294-2922
Fax No. (619) 294-8674

160142

I hereby certify that this correspondence is being transmitted electronically via the United States Patent and Trademark Office EFS-Web system to: Mail Stop Amendment, Commissioner for Patents, on 2018-12-07, by John D. Buchaca, Reg. No. 37,289.

Signature: _____



Date: _____

2018-12-07



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/351,315	11/14/2016	Joseph L. Vilella	160142	2023
24243 7590 03/04/2019 CHARMASSON, BUCHACA & LEACH, LLP 2635 Camino Del Rio South Suite 102 SAN DIEGO, CA 92108			EXAMINER FAROOQUI, QUAZI	
			ART UNIT	PAPER NUMBER
			2491	
			NOTIFICATION DATE	DELIVERY MODE
			03/04/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

john@charmason.com

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

Response to Amendment

This office action is response to the amendment filed on 12/07/2018 to the application 15/351,315 filed on 11/14/2016. Claims 1-15 are pending in this communication. Applicant's arguments filed on 12/07/2018 have been fully considered but they are moot in view of the new ground(s) of rejection necessitated by the amendments. Thus, Dumitriu; Dan Mihai et al. (US 9,900,224 B2) has been used to address the newly added issues. Accordingly, this action has been made final.

Response to Arguments

Applicant's arguments filed 12/07/2018 have been fully considered.

Applicant's Argument:

Neither Farmer nor Bettinger appear to disclose or suggest providing an interface router, such as a premise router, which has been configured to have a plurality of virtual routing tables, *within* the interface router, where each of these tables is *unique* for each optical network unit being serviced by that interface router.

Examiner's response:

These arguments have been respectfully considered and the following rejection addresses them. FARMER discloses a routing device can combine a conventional router and interface with internet router with multiple digital carrier lines (**Fig.3 element 355 - 'Laser transceiver Node**

Routing Device and col.10 lines 42-45, the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol).

Applicant's Argument:

In the context of individual users on a network, the claimed invention, on the other hand, does not provide the same access to the supplied data between different users. Instead, that access is restricted by one of the uniquely populated individual virtual routing tables dedicated to that particular user which is located within the router servicing all users.

Examiner's response:

Dumitriu; Dan Mihai et al. (US 9900224 B2) discloses for each customer site a unique routing table is maintained which is separate from other customer site data (**Fig. 8 element 201 – ‘Internet connected Router’, elements 203, 204, 205 - ‘edge connector’ (edge router) & col. 28 & lines 13-17, a global routing table is maintained for each virtual L3 router. The global routing table may be stored on in a distributed state in the shared database. Alternatively, the global routing table may be stored on a selected edge connector).**

Applicant's Argument:

Applicant argues that other independent claims & dependent claims are allowable at least for reasons including some of those discussed above in connection with claim 1.

Examiner's response:

These arguments have been respectfully considered but they are not persuasive as the previously presented as well as amended limitations are taught or suggested by cited references. Other independent claims & dependent claims are rejected for the same reasons mentioned in independent claim as answered above.

Claims 1, 3-14 & 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Farmer; James O. et al. (hereinafter **FARMER**), Pat. No.: US 7,583,897 B2 in view of Dumitriu; Dan Mihai et al. (hereinafter **DUMITRIU**), Pat. No.: US 9,900,224 B2 (Provisional application No. 61/514,990).

Regarding Claim 1, FARMER teaches a multi-user digital optical data network apparatus comprises:

a plurality of network service digital carrier lines (**Fig. 3 element 340 – ‘Internet Router’ & element 345 ‘Telephone Switch’**). Here, internet router can receive multiple carrier lines) connected to a passive optical network interface router (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’** and col.10 lines 42-45, the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol. Here, a routing device which can combine a conventional router and interfacing with internet router with multiple digital carrier lines);

at least one uplink connecting said interface router to an optical line terminal (**Fig. 2 elements 120 – ‘Laser Transceiver Node’** and col. 10 lines 43-46, the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol for communicating with one or more laser transceiver nodes 120. Here, Interface Router (355) connected to multiple claimed ‘optical line terminals’ or Laser Transceiver Nodes 120);

said optical line terminal being connected to a number of passive optical network feeds for carrying a common digital data feed to a plurality of optical network units (**Fig. 3 elements 365 – ‘optical input output port device’ & col. 11 lines 1-4, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data**

input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360. Here, element 365 is claimed ‘Optical Network Unit’) each supporting at least one of a plurality of private user devices (**col. 11 lines 4-6, from the bi-directional splitter 360, respective optical receivers 370 can convert the upstream optical signals into the electrical domain.** Here, converted electrical signals of data are fed into user devices);

... said interface router (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’ and col.10 lines 42-45.** Here, optical router, which can combine a conventional router, is interfacing with internet router with multiple digital carrier lines) ... (have virtual routing table for each end customer or subscriber. NOTE: ‘Interface Router’ prior art reference is not repeated); and,

... said optical network units (**Fig. 3 elements 365 – ‘optical input output port device’ & col. 11 lines 1-4.** Here, element 365 is claimed ‘Optical Network Unit’. NOTE: ‘Optical Network Unit’ prior art reference is not repeated) ...

FARMER, however, does not teach

... (said interface router) being configured to have at least one unique virtual routing table for each one of said plurality of optical network units; and,

wherein each of ... (said optical network units) is adapted to extract digital data packets intended for a supported one of said devices.

In analogous teaching DUMITRIU teaches

... (said interface router) being configured to have at least one unique virtual routing table for each one of said plurality of ... (optical network units) (**Fig. 8 element 201 –‘Internet connected Router’, elements 203, 204, 205 - ‘edge connector’ (edge router) & col. 28 & lines 13-17, a global routing table is maintained for each virtual L3 router. The global routing**

table may be stored on in a distributed state in the shared database. Alternatively, the global routing table may be stored on a selected edge connector. Here, for each customer site a unique routing table is maintained which is separate from other customer site data. Host 210, 221, 222 are examples of unique customer sites.); and,

wherein each of ... (said optical network units) is adapted to extract digital data packets intended for a supported one of said devices (**Fig. 8 element 201 –‘Internet connected Router’, elements 203, 204, 205 - ‘edge connector’ (edge router) & col. 27** . Here, packets received from Internet router 201 is routed to individual customer / site ‘edge connector’ devices 203-205 for end user VM 211-214 by look up of virtual routing tables for destination interfaces).

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In patent DUMITRIU teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber’s data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network.

All references are inventions in analogous area but each invention teaches specific claimed limitation specifically and other references mutually cure each other’s deficiencies. When all claimed techniques are combined they teach claimed invention.

To provide a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER, it would have been obvious to one of

ordinary skill at the time of the invention, in view of the teachings of DUMITRIU, since the techniques were known in the prior art and one skilled in the art could have combined the technique (*eMPEP sec 2141 sub-section C (III) items (C) - use of known technique to improve similar devices (methods, or products) in the same way, & (D) - applying a known technique to a known device (method, or product) ready for improvement to yield predictable results*), the elements as claimed by a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network to achieve obvious predictable result.

The combination would have yielded nothing more than predictable results to one of ordinary skill at the time of the invention, i.e., one skilled in the art would have recognized that the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network used in: DUMITRIU would allow the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER to function as invention claimed.

This enhancement provides a secured technique of a network router connecting to passive optical carrier lines, distributes to multiple optical subscriber ports, have virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeps individual subscriber's data separate from other subscribers private and secured by avoiding use

of individual router for each subscriber provided by the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of DUMITRIU with FARMER's the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. Furthermore, this enhancement facilitates service providers and subscribers using common optical router equipment with virtual routing tables shared between multiple independently administered networks by managing each subscriber's data private separate and saves installation, maintenance and operation cost by avoiding providing individual router to each subscriber. The common optical router equipment is reconfigurable and expandable and provides changed communication capacity and functions when additional elements are added or reconfigured.

In view of Supreme Court Decision in KSR International Co. v. Teleflex Inc., 550 U.S. -, 82 USPQ2d 11385 (2007), the Supreme Court stated that the Federal Circuit erred when it applied the well-known teaching-suggestion-motivation (TSM) test in an overly rigid and formalistic way. According to the Supreme Court, the TSM test is one of a number of valid rationales that could be used to determine obviousness. It is NOT the only rationale that may be relied upon to support a conclusion of obviousness.

Regarding Claim 3, FARMER & DUMITRIU disclose all the features of claim 1 and FARMER further discloses

said interface router is a premise router (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’ and col.10 lines 42-45. the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol.** Here, optical router is the claimed premise router, which can combine a conventional router and interface with internet router with multiple digital carrier lines).

Thus given the additional teaching of DUMITRIU, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber’s data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER’s further teaching technique where optical router is the claimed premise router, which can combine a conventional router, is interfacing with internet router with multiple digital carrier lines.

Regarding Claim 4, FARMER & DUMITRIU disclose all the features of claim 1 and DUMITRIU further discloses

said interface router is further configured to have a global routing table, and wherein a number of destinations listed in said at least one unique virtual routing table are associated with corresponding destinations (**col. 27 lines 40-47, assume a packet was received at edge connector 203 on a physical network interface card (NIC) from the internet 151 via the**

internet connected router 201 and that the packet is destined for virtual machine 211.

Recall that the packet is the first packet of a flow, so there is no flow rule corresponding to the packet in the flow table. Because there is no corresponding flow entry in the flow table, the decision engine is invoked. Here, data is routed after route and interface lookup by control plane of router) listed in said global routing table (**Fig. 8 element 201 – ‘Internet connected Router’, elements 203, 204, 205 - ‘edge connector’ (edge router) & col. 28 lines 13-17, a global routing table is maintained for each virtual L3 router. The global routing table may be stored on in a distributed state in the shared database. Alternatively, the global routing table may be stored on a selected edge connector.** Here, for each customer site a unique routing table is maintained which is separate from other customer site data. Host 210, 221, 222 are examples of unique customer sites).

Thus given the additional teaching of DUMITRIU, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber’s data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add DUMITRIU’s further teaching technique where data is routed after route and interface lookup by control plane of router’s global routing table.

Regarding Claim 5, FARMER & DUMITRIU disclose all the features of claim 1 and FARMER further discloses

each of said optical network units (**Fig. 3 elements 365**) provides service to a separate number of private users (**col. 11 lines 4-6, from the bi-directional splitter 360, respective optical receivers 370 can convert the upstream optical signals into the electrical domain.** Here, converted electrical signals of data are fed into user devices).

Thus given the additional teaching of DUMITRIU, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER's further teaching technique where converted electrical signals of data are fed into user devices.

Regarding Claim 6, FARMER & DUMITRIU disclose all the features of claim 1 and FARMER further discloses

said uplink carries digital data including digitized voice and video data (**[0002] lines 1-7, the invention relates to video, voice, and data communications. More particularly, the invention relates to a fiber-to-the-home (FTTH) system that is capable of supporting upstream radio-frequency (RF) return signals formatted according to a cable modem**

protocol that originate from a subscriber and are sent upstream to a data service provider.

Here, optical network handles digital triple play or voice, video & data).

Thus given the additional teaching of FARMER, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER's further teaching technique where optical network handles digital triple play or voice, video & data.

Regarding claim 7, claim 7 is claim to an apparatus using the apparatus of claim 1.

Therefore, claim 7 is rejected for the reasons set forth for claim 1.

Regarding Claim 8, FARMER teaches a digital data network communication method comprises:

accepting a plurality of private digital data streams (**Fig. 3 element 340 – ‘Internet Router’ & element 345 ‘Telephone Switch’**). Here, internet router can receive multiple carrier lines) into a passive optical network interface router (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’** and col.10 lines 42-45, the laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol. Here, optical router,

which can combine a conventional router, is interfacing with internet router with multiple digital carrier lines) serving a plurality of private users through a plurality of optical network units (**Fig. 3 elements 365 – ‘optical input output port device’ & col. 11 lines 1-4, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360.** Here, element 365 is claimed ‘Optical Network Unit’);

aggregating said private digital data streams into a combined digital data feed (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’ and col.10 lines 42-4,.** Here, interface router is combining or aggregating carrier feeds for all customers);

routing said digital data feed to at least two of said plurality of optical network units (**Fig. 3 elements 365 – ‘optical input output port device’ & col. 11 lines 1-4, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360.** Here, element 365 is claimed ‘Optical Network Unit’);

extracting from said digital data feed a first one of said private digital data streams (**Fig. 2 elements 120 ‘Laser Transceiver Nodes’ & col. 14, lines 10-13, optical signals can be coupled from each respective diplexer 420 to a combined signal input/output port 445 that is connected to a respective distribution optical waveguide 150.** Here, multiple element 455 devices distributes data to individual customers);

...

providing at least one premise router (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’ and col.10 lines 42-45.** Here, a routing device can combine a conventional router and interfacing with internet router with multiple digital carrier lines) ... (have virtual

routing table for each end customer or subscriber. NOTE: 'Interface Router' prior art reference is not repeated);

... optical network units (**Fig. 3 elements 365 – 'optical input output port device' & col. 11 lines 1-4.** Here, element 365 is claimed 'Optical Network Unit'. NOTE: 'Optical Network Unit' prior art reference is not repeated).

FARMER does not disclose wherein said routing comprises:

...

configuring said at least one ... (premise router) to have an independently unique virtual routing table for each of said plurality of ... (optical network units);

tagging Ethernet frames intended for a first one of said plurality of ... (optical network units) according to entries in a first one of said independently unique virtual routing tables associated with a first one of said optical network units;

In a teaching DUMITRIU teaches

configuring said at least one ... (premise router) to have an independently unique virtual routing table for each of said plurality of ... (optical network units) (**Fig. 8 element 201 – 'Internet connected Router', elements 203, 204, 205 - 'edge connector' (edge router) & col. 28 & lines 13-17, a global routing table is maintained for each virtual L3 router. The global routing table may be stored on in a distributed state in the shared database. Alternatively, the global routing table may be stored on a selected edge connector.** Here, for each customer site a unique routing table is maintained which is separate from other customer site data. Host 210, 221, 222 are examples of unique customer sites);

tagging Ethernet frames (**col. 10 lines 41-49, the data service hub 110 can further comprise a logic interface 350 that is connected to a laser transceiver node routing device**

355. The laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol for communicating with one or more laser transceiver nodes 120. This interface protocol can comprise one of gigabit or faster Ethernet, Internet Protocol (IP) or SONET protocols intended for a first one of said plurality of ... (optical network units) according to entries in a first one of said independently unique virtual routing tables associated with a first one of (said optical network units) (**Fig. 8 element 201 –‘Internet connected Router’, elements 203, 204, 205 - ‘edge connector’ (edge router) & col. 27.** Here, packets received from Internet router 201 is routed to individual customer / site ‘edge connector’ devices 203-205 for end user VM 211-214 by look up of virtual routing tables for destination interfaces);

distributing said tagged Ethernet frames to said first one of ... (said plurality of optical network units) (**col. 16 line 64 to col. 17 line 1, the data interface 555 can comprise an interface to a Voice over Internet Protocol (VoIP) telephone or Ethernet telephone. The data interface 555 can comprise one of Ethernet (10BaseT, 100BaseT, Gigabit) interface).**

In summary, FARMER teaches a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. In an analogous patent DUMITRIU teaches a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber’s data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network.

All references are inventions in analogous area but each invention teaches specific

claimed limitation specifically and other references mutually cure each other's deficiencies.

When all claimed techniques are combined they teach claimed invention.

To provide a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber of FARMER, it would have been obvious to one of ordinary skill at the time of the invention, in view of the teachings of DUMITRIU, since the techniques were known in the prior art and one skilled in the art could have combined the technique (*eMPEP sec 2141 sub-section C (III) items (C) - use of known technique to improve similar devices (methods, or products) in the same way, & (D) - applying a known technique to a known device (method, or product) ready for improvement to yield predictable results*), the elements as claimed by a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network to achieve obvious predictable result.

The combination would have yielded nothing more than predictable results to one of ordinary skill at the time of the invention, i.e., one skilled in the art would have recognized that the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network used in DUMITRIU would allow the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing

traffic by avoiding use of individual router for each subscriber of FARMER to function as invention claimed.

This enhancement provides a secured technique of a network router connecting to passive optical carrier lines, distributes to multiple optical subscriber ports, have virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeps individual subscriber's data separate from other subscribers private and secured by avoiding use of individual router for each subscriber provided by the technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of DUMITRIU FARMER's the technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber. Furthermore, this enhancement facilitates service providers and subscribers using common optical router equipment with virtual routing tables shared between multiple independently administered networks by managing each subscriber's data private separate and saves installation, maintenance and operation cost by avoiding providing individual router to each subscriber. The common optical router equipment is reconfigurable and expandable and provides changed communication capacity and functions when additional elements are added or reconfigured.

In view of Supreme Court Decision in KSR International Co. v. Teleflex Inc., 550 U.S. -, 82 USPQ2d 11385 (2007), the Supreme Court stated that the Federal Circuit erred when it applied the well-known teaching-suggestion-motivation (TSM) test in an overly rigid and

formalistic way. According to the Supreme Court, the TSM test is one of a number of valid rationales that could be used to determine obviousness. It is NOT the only rationale that may be relied upon to support a conclusion of obviousness.

Regarding Claim 9, FARMER & DUMITRIU disclose all the features of claim 1 and DUMITRIU further discloses

said configuring comprises: establishing a global routing table on said at least one ... (premise router) for accessing virtual routing table instantiations for each of said plurality of ... (optical network units) (**Fig. 8 element 201 – ‘Internet connected Router’, elements 203, 204, 205 - ‘edge connector’ (edge router) & col. 28 & lines 13-17, a global routing table is maintained for each virtual L3 router. The global routing table may be stored on in a distributed state in the shared database. Alternatively, the global routing table may be stored on a selected edge connector.** Here, for each customer site a unique routing table is maintained which is separate from other customer site data. Host 210, 221, 222 are examples of unique customer sites).

FARMER further discloses

... premise router (**Fig.3 element 355 - ‘Laser transceiver Node Routing Device’ and col.10 lines 42-45.** Here, a routing device can combine a conventional router and interfacing with internet router with multiple digital carrier lines) ...

... optical network units (**Fig. 3 elements 365 – ‘optical input output port device’ & col. 11 lines 1-4.** Here, element 365 is claimed ‘Optical Network Unit’) ...

Thus given the additional teaching of DUMITRIU, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an

optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add DUMITRIU's further teaching technique where for each customer site a unique routing table is maintained which is separate from other customer site data.

Regarding claim 10, claim 10 is a dependent claim of claim 8, claim 10 is claim to method using the apparatus of claim 5. Therefore, claim 10 is rejected for the reasons set forth for claim 5.

Regarding Claim 11, FARMER & DUMITRIU disclose all the features of claim 1 and FARMER further discloses

wherein said accepting comprises: interfacing a plurality of service provider digital data lines through a single headend (**Fig. 3 element 350 & col. 10 lines 41-43, the data service hub 110 can further comprise a logic interface 350 that is connected to a laser transceiver node routing device 355.** Here, a single headend device 350 receives all carrier lines and feed into interface router 355).

Thus given the additional teaching of FARMER, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an

optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER's further teaching technique where a single headend device receives all carrier lines and feed into interface router.

Regarding Claim 12, FARMER & DUMITRIU disclose all the features of claim 1 and FARMER further discloses

said interfacing comprises: utilizing radio frequency video converter; and, feeding an output of said at least one premise router through an optical line terminal (**col.10 lines 9-16, to support data services or to support incidental services related to the downstream video services, a data-to-RF converter 307 that transforms RF return packets back into their original RF analog electrical format can be coupled to an Internet Router 340. Further details of RF converter 307 will be discussed below with respect to FIG. 8. The RF analog electrical signals generated by the data-to-RF converter 307 are demodulated by an RF receiver 309.** Here, radio frequency converter is used for data conversion to appropriate form for uplink and downlink.

Thus given the additional teaching of FARMER, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical

subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER's further teaching technique where radio frequency converter is used for data conversion to appropriate form for uplink and downlink.

Regarding claim 13, claim 13 is a dependent claim of claims 12, 11 & 8 claim 13 is claim to method using the method of claim 12. Therefore, claim 13 is rejected for the reasons set forth for claim 12.

Regarding Claim 14, FARMER & DUMITRIU disclose all the features of claims 11 & 8 and FARMER further discloses

said routing comprises: sending said encrypted data feed through an optical splitter (col.10 lines 58-60, the laser transceiver node routing device 355 can supply downstream data signals to respective optical transmitters 325. The data signals converted by the optical transmitters 325 can then be propagated to a bi-directional splitter 360. Here, passive optical splitter devices are used for optical connectivity).

Thus given the additional teaching of FARMER, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical

subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER's further teaching technique where passive optical splitter devices are used for optical connectivity.

Regarding Claim 18 FARMER & DUMITRIU disclose all the features of claim 8 and FARMER further discloses

said aggregating comprises using an enterprise aggregating switch (**Fig.3 element 355 - 'Laser transceiver Node Routing Device' and col.10 lines 42-4,,** where interface router is a aggregation switch/ OSI Layer 3 router and is combining or aggregating carrier feeds for all customers).

Thus given the additional teaching of FARMER, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add FARMER's further teaching technique

where interface router is a aggregation switch/ OSI Layer 3 router and is combining or aggregating carrier feeds for all customers.

Claims 2 & 15-17 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Farmer; James O. et al. (hereinafter **FARMER**), Pat. No.: US 7,583,897 B2 in view of Dumitriu; Dan Mihai et al. (hereinafter **DUMITRIU**), Pat. No.: US 9,900,224 B2 (Provisional application No. 61/514,990) and further in view of Ueno; Takafumi et al. (hereinafter **UENO**), Pat. No.: US 6,460,095 B1.

Regarding Claim 2, FARMER & DUMITRIU disclose all the features of claim 1.

FARMER & DUMITRIU do not disclose

common digital data feed is encrypted.

In reference UENO discloses

common digital data feed is encrypted (**col. 18 lines 59-61, if the encrypted continuously input data whose transfer was enabled by the first encryption circuit 50 is video data or voice data, etc.**).

Thus given the additional teaching of UENO, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data

separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add UENO's further teaching technique where individual data streams are encrypted.

Regarding Claim 15, FARMER & DUMITRIU disclose all the features of claim 1 and FARMER & DUMITRIU do not disclose

each of said private digital data streams comprises: encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed; and, wherein said extracting comprises: partially decrypting said encrypted data feed.

In reference UENO discloses

each of said private digital data streams comprises: encrypted informational data, encrypted telephone data, and, encrypted video data to form an encrypted data feed (**col. 18 lines 59-61, if the encrypted continuously input data whose transfer was enabled by the first encryption circuit 50 is video data or voice data, etc.**); and,

wherein said extracting comprises: partially decrypting said encrypted data feed (**col. 18 lines 63-65, the data cannot be decoded to the original video data or voice data unless the data is decrypted**).

Thus given the additional teaching of UENO, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to

different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add UENO's further teaching technique where individual digital data streams are encrypted and decrypted for consumption.

Regarding Claim 16, FARMER & DUMITRIU disclose all the features of claims 15 & 8 and DUMITRIU further discloses said encrypted data feed comprises:

a plurality of encrypted Ethernet frames; wherein a subset of said frames are associated with a first one of said users and a second subset of said frames is associated with a second one of said users (**col. 10 lines 41-49, the data service hub 110 can further comprise a logic interface 350 that is connected to a laser transceiver node routing device 355. The laser transceiver node routing device 355 can comprise a conventional router that supports an interface protocol for communicating with one or more laser transceiver nodes 120. This interface protocol can comprise one of gigabit or faster Ethernet, Internet Protocol (IP) or SONET protocols.** Here, an IP packet is composed of many Ethernet frames. Each customer site's data feed is unique and composed of respective Ethernet frames in IP data).

Thus given the additional teaching of DUMITRIU, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscribe, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data

separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add DUMITRIU's further teaching technique where an IP packet is composed of many Ethernet frames. Each customer site's data feed is unique and composed of respective Ethernet frames in IP data.

Regarding Claim 17, FARMER & DUMITRIU disclose all the features of claim 8.

FARMER further discloses

at least one of said optical network units at each of said tenants (**Fig. 3 elements 365 – ‘optical input output port device’ & col. 11 lines 1-4, upstream optical signals received from a respective laser transceiver node 120 can be fed into the bi-directional data input/output port 365 where the optical signals are then forwarded to the bi-directional splitter 360.**

Here, element 365 is claimed ‘Optical Network Unit’ for each customer);

UENO further discloses wherein said extracting comprises:

wherein said operating comprises: decrypting incoming intended data packets from said encrypted data feed; not decrypting incoming unintended data packets from said encrypted data feed (**col. 18 lines 63-65, the data cannot be decoded to the original video data or voice data unless the data is decrypted.** Here, only permitted data is delivered after decryption); and

encrypting outgoing data packets to said encrypted data feed (**col. 18 lines 59-61, if the encrypted continuously input data whose transfer was enabled by the first encryption circuit 50 is video data or voice data, etc.).**

Thus given the additional teaching of UENO, it would have been obvious to one of ordinary skill before the effective filing date of the invention, to modify a technique of an optical network router connecting to uplink optical carrier lines, distributes to multiple optical

subscriber downlink ports for individual subscriber connected to different ports, the optical router maps incoming and outgoing traffic by avoiding use of individual router for each subscriber, and a technique of having virtual routing tables for individual subscriber connected to different ports to map incoming and outgoing traffic, keeping individual subscriber's data separate from other subscriber private, secured, and managing all subscriber traffic to uplink data carrier network of FARMER & DUMITRIU to add UENO's further teaching technique where encrypting outbound data and only permitted data is delivered after decryption.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **QUAZI FAROOQUI** whose telephone number is (571) 270-1034. The examiner can normally be reached on M-F 8:30AM-5:00PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok B. Patel can be

reached on 571-272-3972. The fax phone number for the organization where this application or proceeding is assigned is 571-270-2034.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/QUAZI FAROOQUI/

Examiner, Art Unit 2491

/ASHOKKUMAR B PATEL/

Supervisory Patent Examiner, Art Unit 2491

<i>Notice of References Cited</i>	Application/Control No. 15/351,315		Applicant(s)/Patent Under Reexamination Vilella et al.	
	Examiner QUAZI FAROOQUI		Art Unit 2491	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20060269285-A1	11-2006	Farmer; James O.	H04J3/0664	398/72
*	B	US-9900224-B2	02-2018	Dumitriu; Dan Mihai	H04L12/4625	1/1
*	C	US-6460095-B1	10-2002	Ueno; Takafumi	G06F5/06	710/12
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001)

Notice of References Cited

Part of Paper No. 20190131

<i>Search Notes</i> 	Application/Control No. 15/351,315	Applicant(s)/Patent Under Reexamination Vilella et al.
	Examiner QUAZI FAROOQUI	Art Unit 2491

CPC - Searched*		
Symbol	Date	Examiner
H04L9/00 H04L9/32-3297 H04L63/04-0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12	07/02/2018	QF
H04L9/06,08 H04Q11/00, H04B10/27	07/02/2018	QF
H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00	07/02/2018	QF

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
380	26,28-30, 44-47,255-286	07/02/2018	QF
713	150-154,160-168,189-193	07/02/2018	
726	1-33	07/02/2018	

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/QUAZI FAROOQUI/ Examiner, Art Unit 2491	
---	--

<i>Search Notes</i> 	Application/Control No. 15/351,315	Applicant(s)/Patent Under Reexamination Vilella et al.
	Examiner QUAZI FAROOQUI	Art Unit 2491

Search Notes		
Search Notes	Date	Examiner
Inventor and assignee search in PALM	06/30/2018	QF
Inventor and assignee search in EAST all database	07/02/2018	QF
Classification search in EAST	07/02/2018	QF
text search in EAST	07/02/2018	QF
updated EAST search with class and text	07/02/2018	QF
updated EAST search with inventor and assignee	01/31/2019	QF
updated EAST search with class and text	01/31/2019	QF
updated EAST search with text	02/01/2019	QF

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/QUAZI FAROOQUI/ Examiner, Art Unit 2491	
---	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	24961	(aggregat\$3 near5 encrypt\$3) optical near5 data near5 stream	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:03
S2	2	(aggregat\$3 near5 encrypt\$3) SAME (optical near5 data near5 stream)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:04
S3	333	(radio adj frequency) same (video near5 converter)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:06
S4	5	(radio adj frequency) same (video near5 converter) same router	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:07
S5	51	(radio adj frequency) same (video near5 converter) same (router switch)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:07
S6	3	S5 and (optical adj splitter)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:09
S7	3	"6751302".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/11 14:50
S8	0	"SPADA INNOVATIONS, INC.".as.	US-PGPUB;	OR	ON	2016/02/16

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			11:13
S9	0	"SPADA INNOVATIONS, INC." .asn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:13
S10	133	"SPADA" .asn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:13
S11	2	S10 and optical and encrypt\$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:14
S12	34	((VILELLA near2 JOSEPH) OR (REYNANTE near4 JAMES)).inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:16
S13	2	S12 and encrypt\$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:16
S14	520	"3" AND H04L9/0852.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:24
S15	52	"S3" AND H04L9/0852.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/02/16 11:24
S16	37	"S3" AND 380/256.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2016/02/16 11:25

			IBM_TDB			
S17	0	"20170063542".pn.	USPAT	OR	ON	2018/06/29 11:31
S18	3	"20170063542".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/06/29 11:39
S19	403	(Optical adj2 data adj2 network)	USPAT	OR	OFF	2018/06/29 13:33
S20	0	(Optical adj2 data adj2 network) same3 (virtual near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:35
S21	0	(Optical adj2 data adj2 network) and (virtual near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:36
S22	2	(Optical adj2 data adj2 network) and ((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:36
S23	3346	((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/06/29 13:39
S24	448	(virtual many multiple plural\$3) adj2 rout\$3 adj2 table	USPAT	OR	OFF	2018/06/29 13:39
S25	21	S24 and (optical adj5 network)	USPAT	OR	OFF	2018/06/29 13:40
S26	24	S24 and (optical adj5 (network router switch))	USPAT	OR	OFF	2018/06/29 13:42
S27	24	S26 AND (@ad @pd @prad @rlad @ptad < "20120801")	USPAT	OR	OFF	2018/06/29 13:42
S28	24	S26 AND (@ad @pd < "20120801")	USPAT	OR	OFF	2018/06/29 13:43
S29	1203	398/70-72.ccls. (H04B10/00).cpc.	USPAT	OR	OFF	2018/06/29 16:39
S30	403	(Optical adj2 data adj2 network)	USPAT	OR	OFF	2018/06/29 16:40
S31	13	S30 and S29	USPAT	OR	OFF	2018/06/29 16:40
S32	122	S29 and virtual	USPAT	OR	OFF	2018/06/29 16:40
S33	64	"pluris".asn.	USPAT	OR	OFF	2018/06/30 14:45
S34	41	"sycamore networks".asn.	USPAT	OR	OFF	2018/06/30 14:46
S35	3	"sycamore networks".asn. and frequency and splitter	USPAT	OR	OFF	2018/06/30 14:46
S36	54148	"pluris".asn.and" frequency and splitter	USPAT	OR	OFF	2018/06/30 14:47
S37	54148	"pluris".asn.and" frequency and splitter	USPAT	OR	OFF	2018/06/30 14:47
S38	0	S33 and frequency and splitter	USPAT	OR	OFF	2018/06/30 14:47
S39	17	S33 and aggrega\$4	USPAT	OR	OFF	2018/06/30 14:48
S40	19	S33 and optical	USPAT	OR	OFF	2018/06/30 14:48

S41	8	S33 and optical and router	USPAT	OR	OFF	2018/06/30 14:49
S42	3	S33 and (optical same2 router)	USPAT	OR	OFF	2018/06/30 14:49
S43	30913	(aggregat\$3 near5 encrypt\$3) optical near5 data near5 stream	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/06/30 15:00
S44	1285	S43 and (encrypt\$4 same2 decrypt\$4)	USPAT	OR	OFF	2018/06/30 15:00
S45	1198	S43 and (encrypt\$4 with decrypt\$4)	USPAT	OR	OFF	2018/06/30 15:01
S46	45	S43 and (encrypt\$4 with decrypt\$4) and splitter	USPAT	OR	OFF	2018/06/30 15:01
S47	574634	(H04L9/00 H04L9/32-3297 H04L63/04- 0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/07/02 15:11
S48	598937	(H04L9/00 H04L9/32-3297 H04L63/04- 0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC. (H04L9/06,08 H04Q11/00, H04B10/27).CPC. (H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/07/02 15:13
S49	660848	(H04L9/00 H04L9/32-3297 H04L63/04- 0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F15/16-18 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC. (H04L9/06,08 H04Q11/00, H04B10/27).CPC. (H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00).cpc. (380/26,28-30,44-47,255-286 713/150- 154,160-168,189-193 726/1-33).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/07/02 15:15
S50	2	(Optical adj2 data adj2 network) and ((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/07/02 15:16
S51	0	S50 and S49	USPAT	OR	OFF	2018/07/02 15:16
S52	392	(Optical adj2 data adj2 network) and (virtual many multiple plural\$3)	USPAT	OR	OFF	2018/07/02 15:17
S53	60	S52 and S49	USPAT	OR	OFF	2018/07/02 15:17

S54	47	S53 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2018/07/02 15:20
S55	41	S53 AND ((@ad @pd) < "20120801")	USPAT	OR	OFF	2018/07/02 15:21
S56	10	(Optical adj2 data adj2 network) and (virtual same (many multiple plural\$3) same rout\$5)	USPAT	OR	OFF	2018/07/02 15:23
S57	3	S54 and S56	USPAT	OR	OFF	2018/07/02 15:23
S58	6	S56 AND ((@ad @pd) < "20120801")	USPAT	OR	OFF	2018/07/02 15:24
S59	2	(Optical adj2 data adj2 network) and ((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2018/07/02 18:28
S60	1	(optical adj data adj network) near5 (traffic adj rout\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 15:20
S61	3	(optical adj data adj network) with (traffic near3 rout\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 15:21
S62	35	((VILELLA near2 JOSEPH) OR (REYNANTE near4 JAMES)).inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/01/31 15:22
S63	0	"SPADA INNOVATIONS, INC.".asn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/01/31 15:22
S64	698408	(H04L9/00 H04L9/32-3297 H04L63/04-0492 H04L63/08-0892 H04L63/10 H04L63/1408 H04L63/1416 H04L67/12 G06F21/00 G06F21/30-46 G06F21/60-645 G06F21/554 G06F2221/033 G06F9/00 H04N7/167 H04W12/00-12).CPC. (H04L9/06,08 H04Q11/00, H04B10/27).CPC.(H04L9/0852 or H04Q11/0003 or H04B10/27 or H04L9/065 or H04Q11/0062 or H04Q2011/0079 or H04Q2011/0073 or H04B10/00).cpc. (380/26,28-30,44-47,255-286 713/150-154,160-168,189-193 726/1-33).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 15:23
S65	1	S61 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2019/01/31 15:25
S66	2	S61 and S64	US-PGPUB; USPAT;	OR	OFF	2019/01/31 15:27

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S67	7	(global adj rout\$3 adj table) same (virtual adj rout\$3 adj table) same router	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 15:37
S68	3	S67 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2019/01/31 15:37
S69	240	(Optical NEAR5 network) and ((virtual many multiple plural\$3) near5 rout\$3 near5 table)	USPAT	OR	OFF	2019/01/31 16:28
S70	26	S64 AND S69	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 16:28
S71	22	S70 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2019/01/31 16:29
S72	22	S64 AND S71	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 16:29
S73	115	(Optical NEAR5 network) and ((virtual) near5 rout\$3 near5 table)	USPAT	OR	OFF	2019/01/31 17:56
S74	0	(Optical NEAR5 network) same ((virtual) near5 rout\$3 near5 table)	USPAT	OR	OFF	2019/01/31 17:56
S75	115	(Optical NEAR5 network) and ((virtual) near5 rout\$3 near5 table)	USPAT	OR	OFF	2019/01/31 17:57
S76	95	S75 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2019/01/31 17:57
S77	15	S64 and S76	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 17:57
S78	10467	Optical and (virtual near5 rout\$3)	USPAT	OR	OFF	2019/01/31 18:06
S79	301	Optical same (virtual near5 rout\$3)	USPAT	OR	OFF	2019/01/31 18:06
S80	67	S64 and S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 18:07

S81	9	Optical same (virtual near5 rout\$3 near5 table)	USPAT	OR	OFF	2019/01/31 18:08
S82	8	S81 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2019/01/31 18:08
S83	0	S64 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 18:09
S84	2	optical with (virtual near3 routing near3 table)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/01/31 18:56
S85	98678	(encrypt\$3 near5 data) same3 (decrypt\$3 near5 data)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/01 16:10
S86	23	(encrypt\$3 near5 data near3 voice near3 video) same3 (decrypt\$3 near5 data near3 voice near3 video)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/01 16:12
S87	4	S86 AND ((@ad @pd @prad @rlad @ptad) < "20120801")	USPAT	OR	OFF	2019/02/01 16:13

2/ 1/ 2019 6:33:21 PM

C:\Users\qfarooqui\Documents\EAST\Workspaces\15351315-VILELLA (CIP of ABAN 14419092).wsp

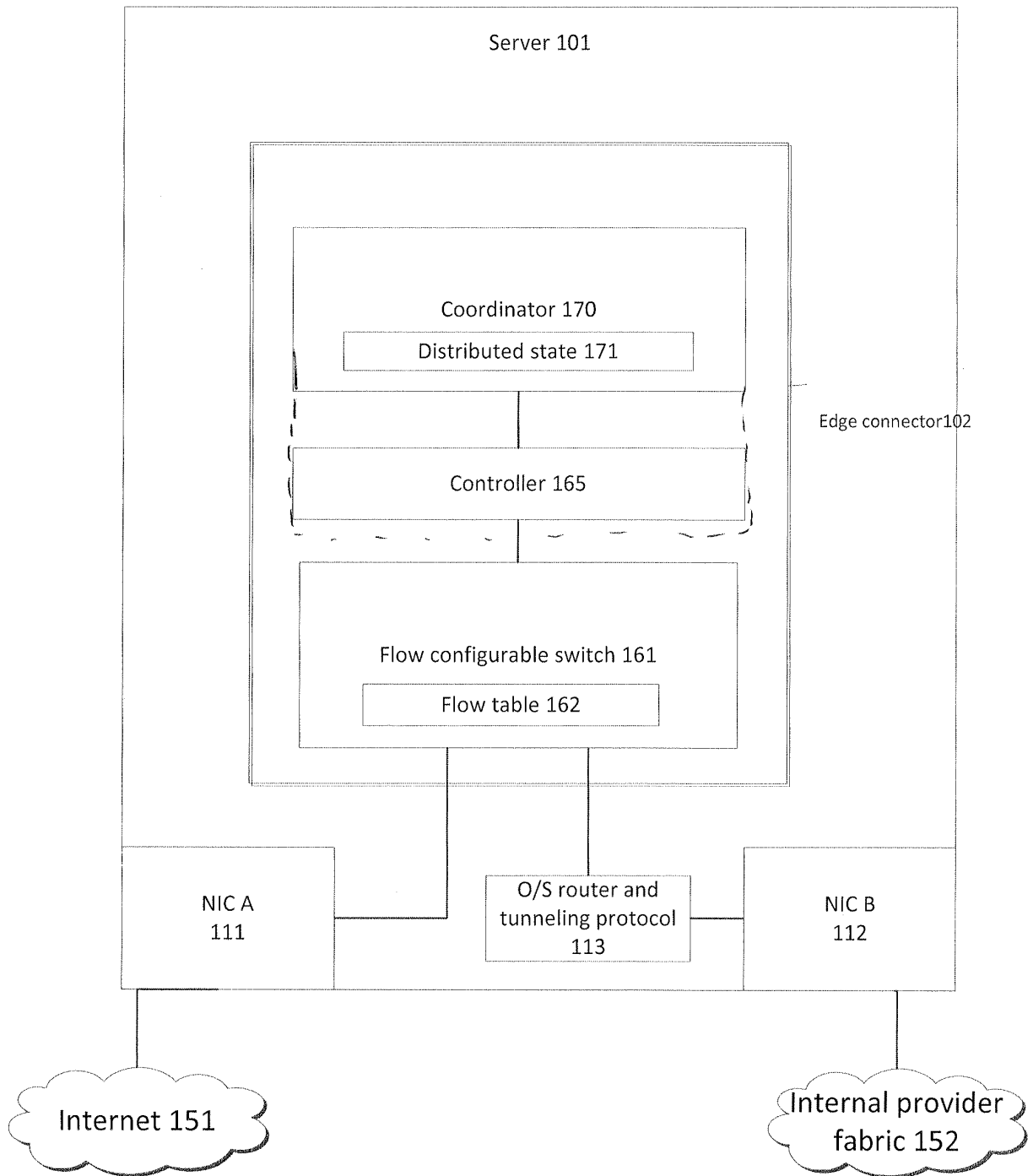


FIG. 1

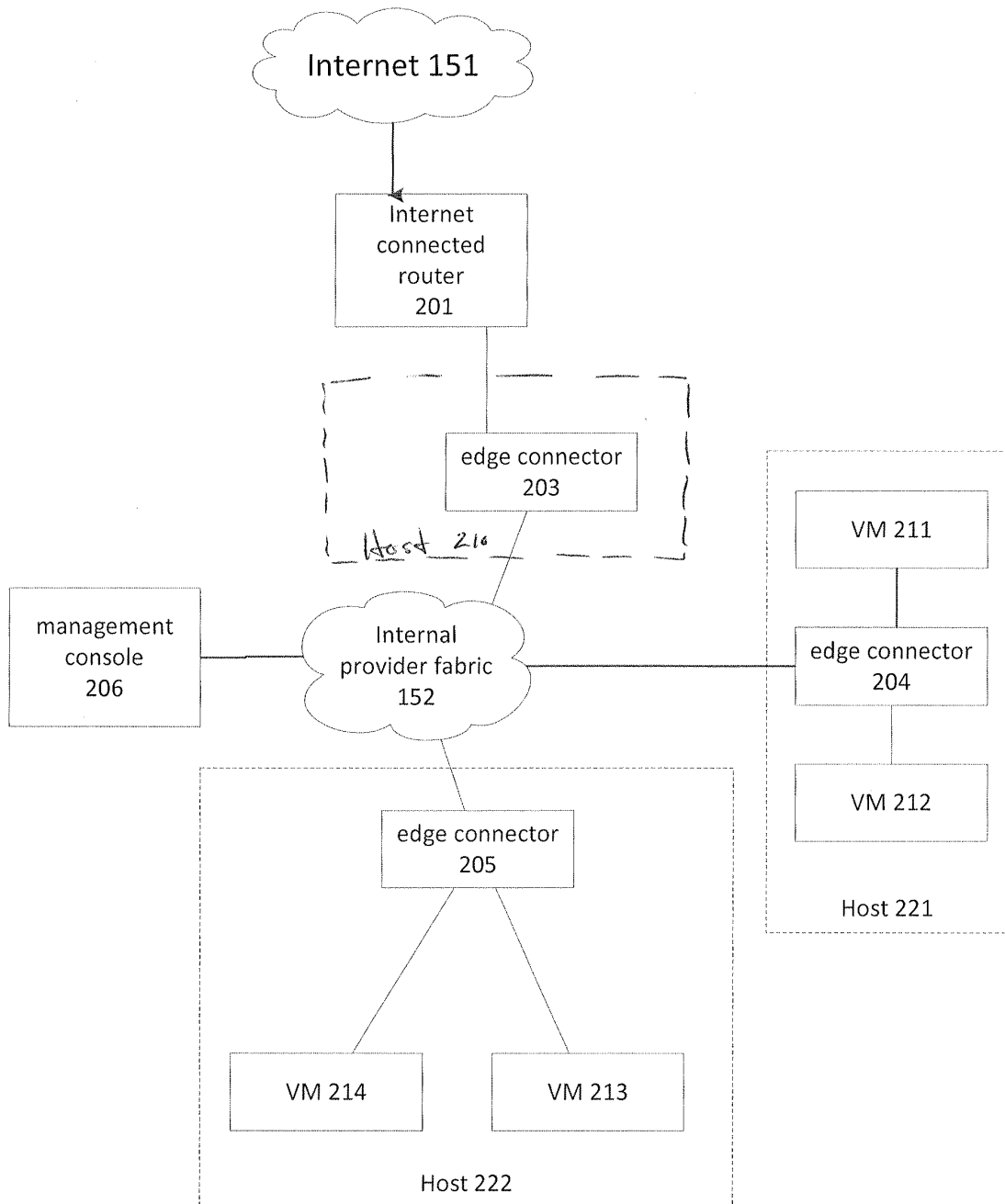


Fig 2

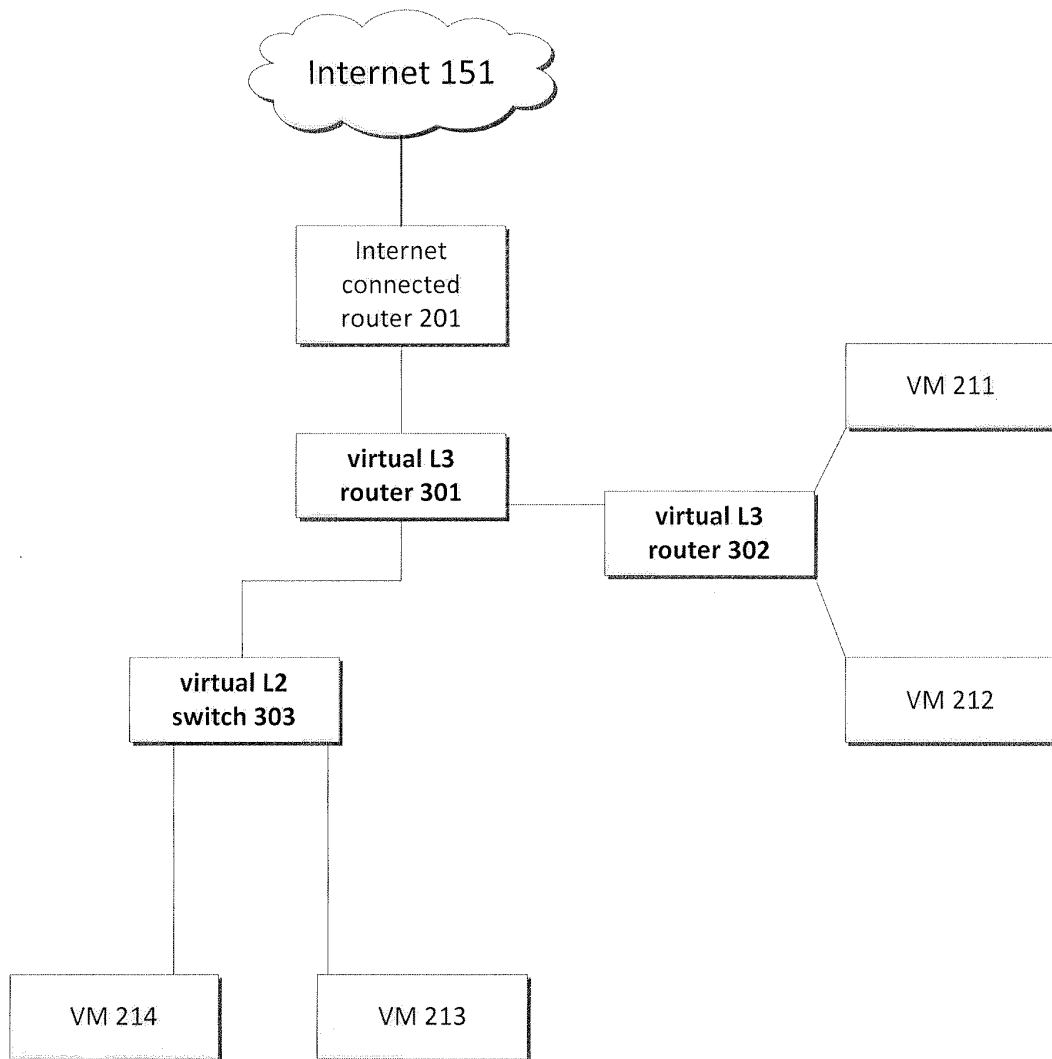


Fig 3

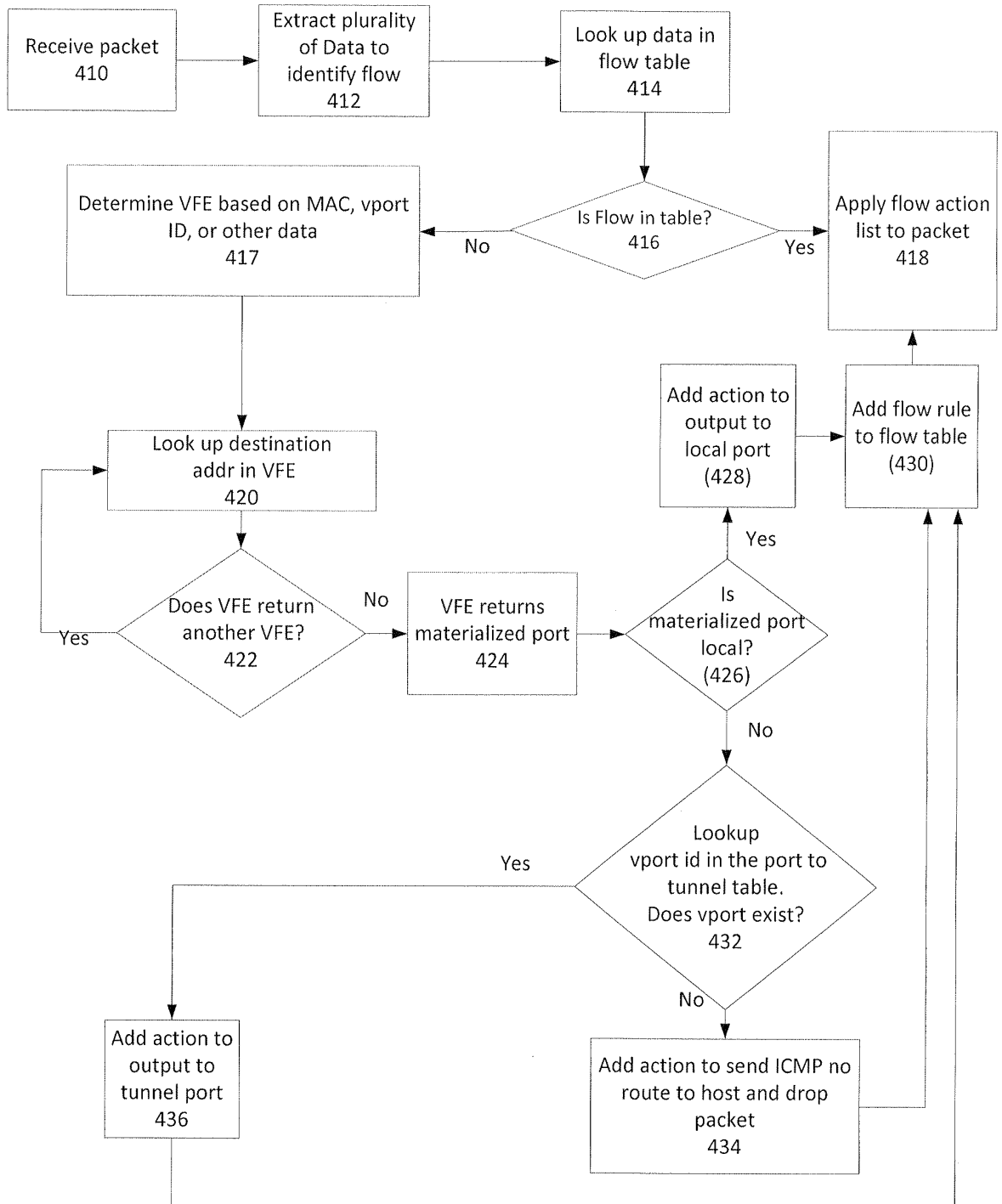


Fig 4

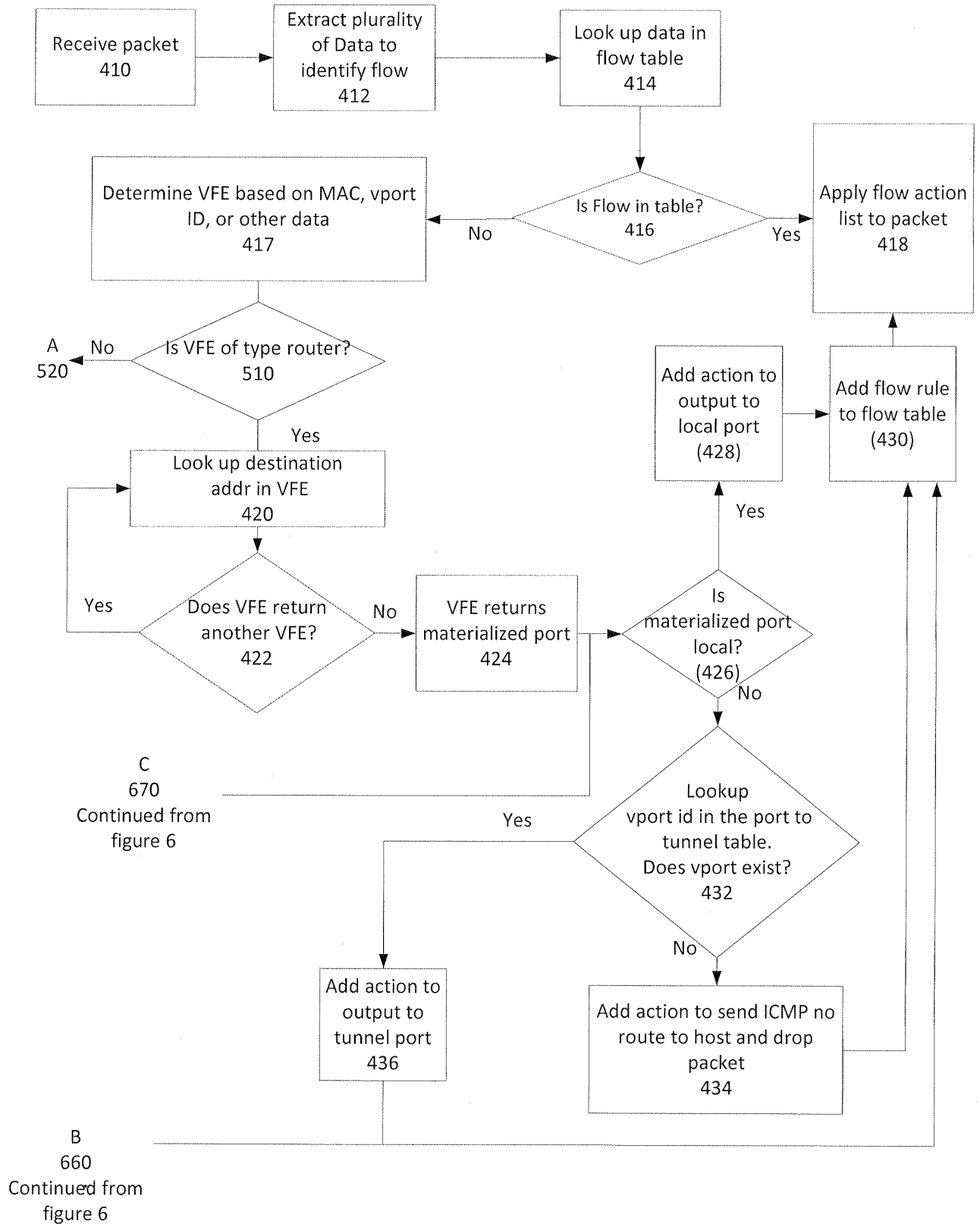


Fig 5

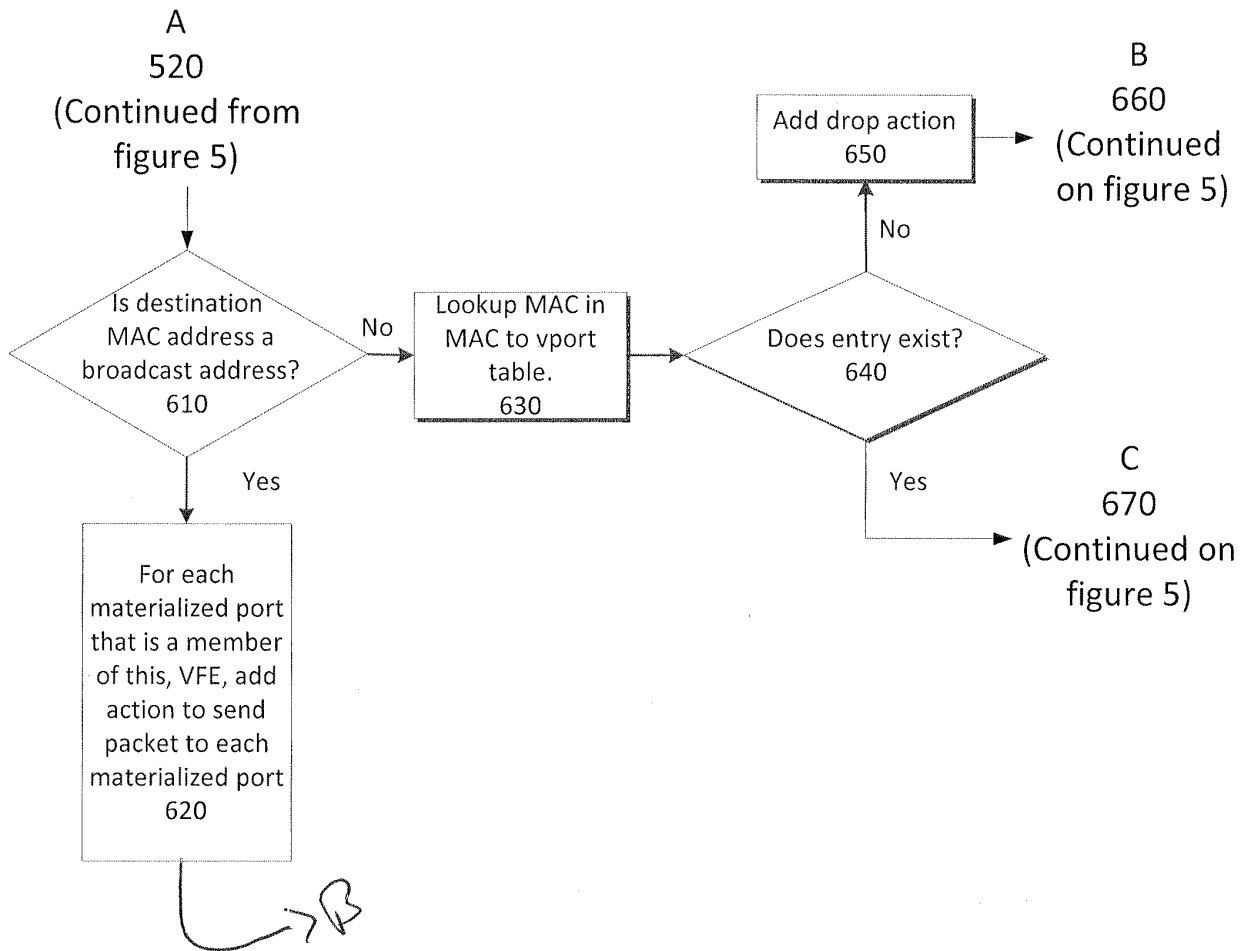


Fig 6

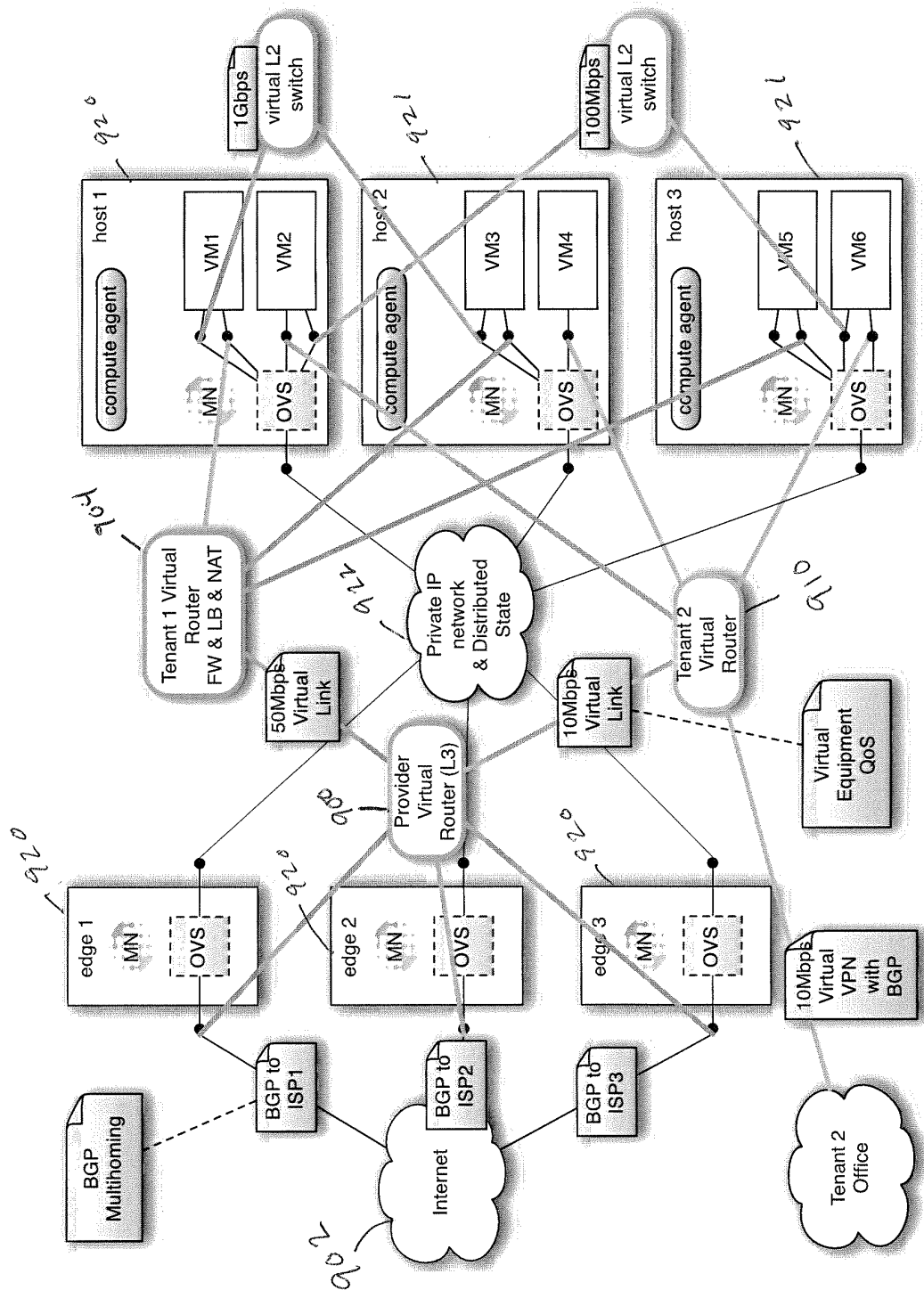


Fig. 8

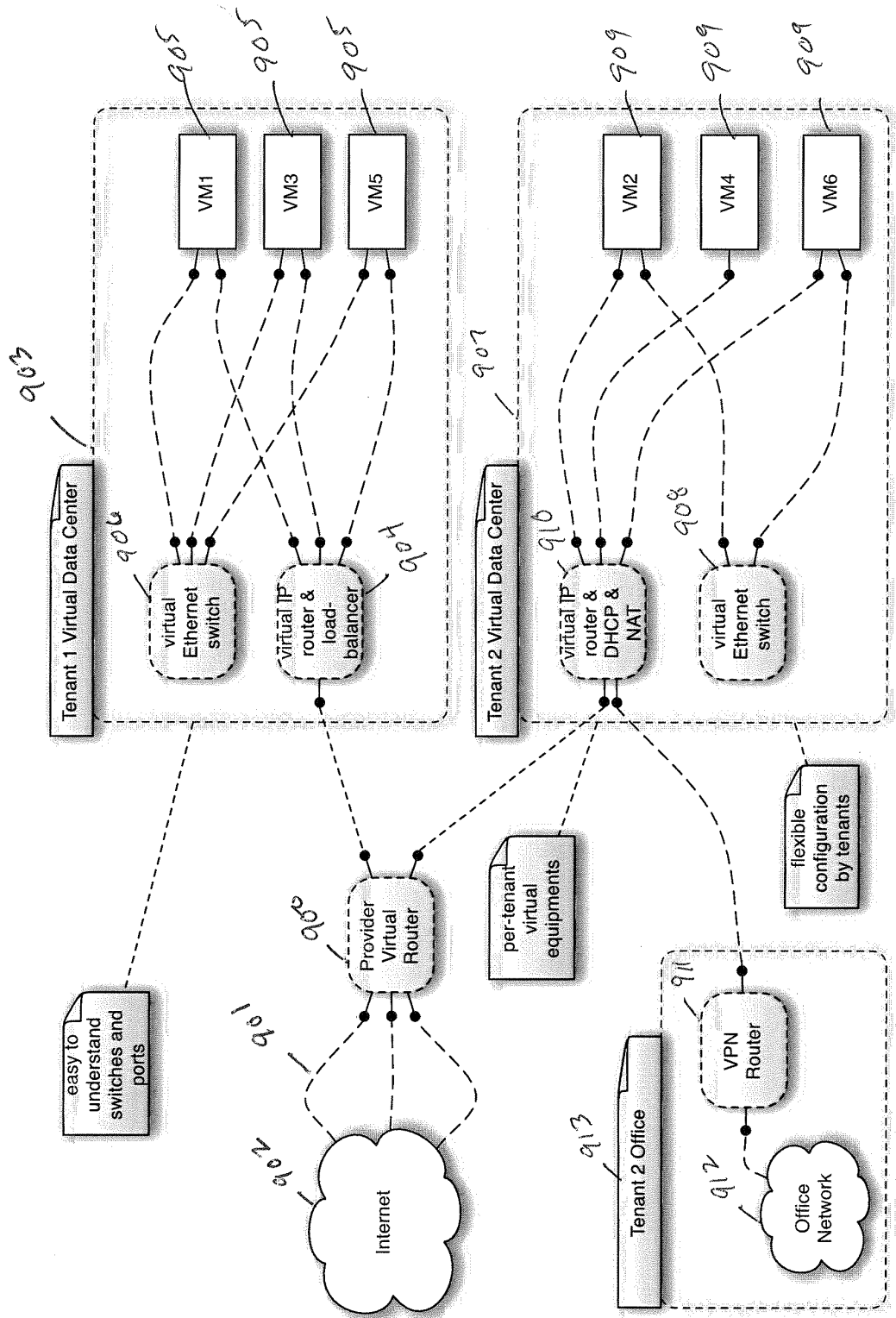


Fig. 7

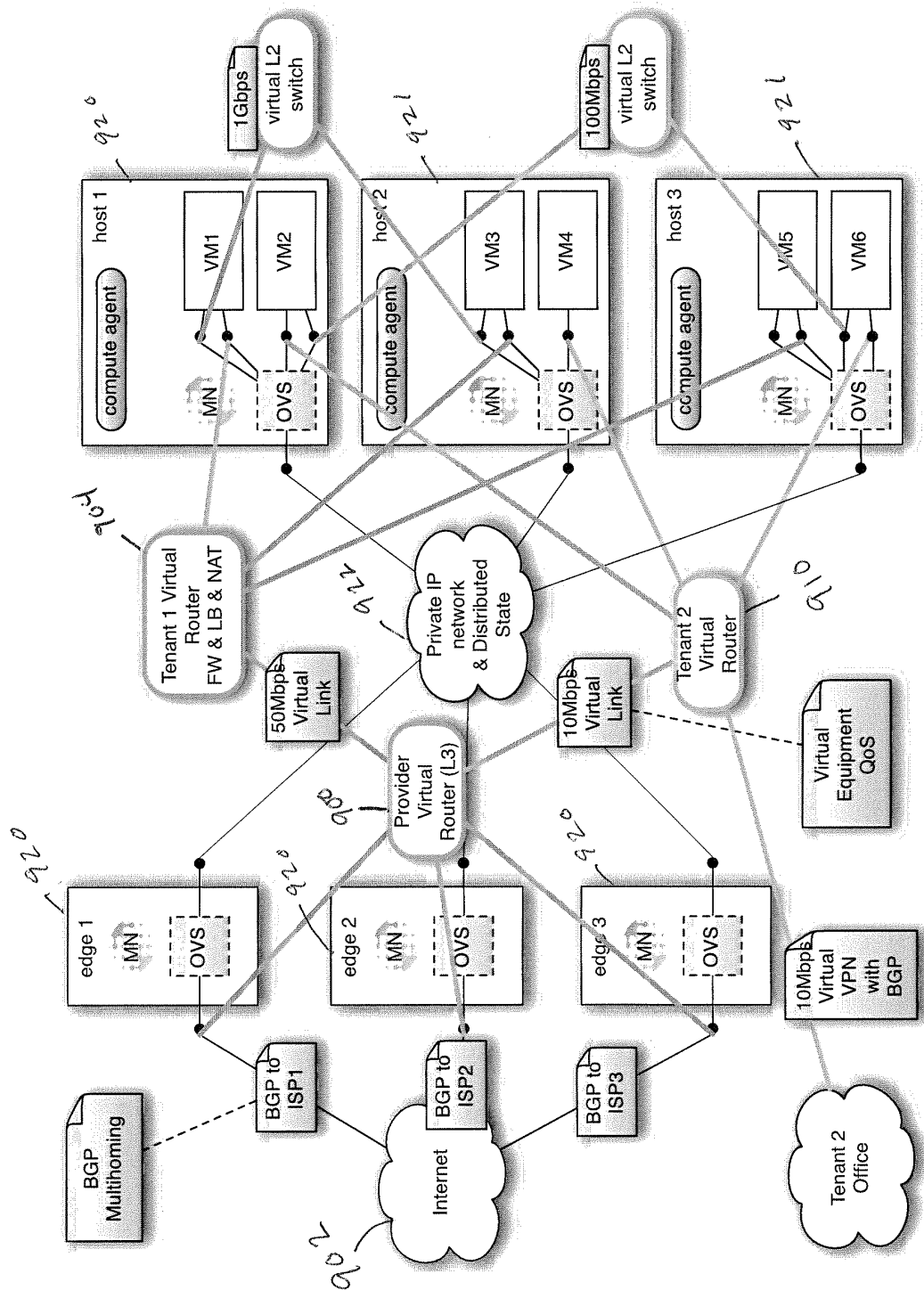


Fig. 8

What is claimed is:

1. A method for routing a packet from a first edge connector to a second edge connector, the method comprising:

accessing a virtual routing table and determining a next hop for a packet received at a first edge connector, and, if the next hop is a logical port, continuing to access one or more virtual routing tables and determining a next hop until the next hop is determined to be a materialized port; and

sending the packet over a network fabric to a second edge connector.

2. The method of claim 1 further comprising the step of:

applying a pre-routing transformation to the packet for at least one of the next hops prior to sending the packet over a network fabric to a second edge connector.

3. The method of claim 1 further comprising the step of:

applying a post-routing transformation to the packet for at least one of the next hops prior to sending the packet over a network fabric to a second edge connector.

4. The method of claim 1 where the next hop is determined based on at least one of the source address and the destination address.

5. The method of claim 1 wherein the virtual routing table is stored in a distributed state shared by at least the first edge connector and the second edge connector.

6. The method of claim 1 wherein the network fabric comprises an IP network connecting at least the first edge connector and the second edge connector.

7. A method of stateful connection tracking for deleting a flow entry, the method comprising:

receiving a FIN packet with a sequence number at an edge node with a flow configurable switch, the flow configurable switch having a flow rule corresponding to the packet;

checking that the packet matches the flow rule at the flow configurable switch;

marking the flow for deletion in a distributed shared state;

and forwarding the packet.

8. The method of claim 7 in which the flow entry corresponds to the inbound flow of a TCP connection.

9. The method of claim 7 further comprising:

deleting the flow when an ACK packet is sent corresponding to the FIN packet.

10. The method of claim 9 further comprising:

identifying a corresponding flow in the opposite direction of the flow marked for deletion in the distributed shared state; and

deleting the corresponding flow when the ACK packet is sent.

11. A method for performing network address translation, the method comprising:

receiving a first packet at an ingress edge connector and creating a first flow corresponding to the first packet;

performing destination network address translation on the destination address of the packet and inserting the first flow containing the network address translation into a distributed state;

receiving a second packet at an egress edge connector in response to the first packet;

constructing a second flow corresponding to the second packet and identifying the first flow in the distributed state from a reverse map of the second flow;

using the destination network address translation of first flow to translate a source address of the second packet based on the first flow.

12. The method of claim 11 further comprising:

waiting until the first flow is stored in the distributed state before forwarding the first packet, such that the first flow is stored in the distributed state the second packet is received at the egress.

13. The method of claim 11 where the first flow and the second flow correspond to a TCP connection.

14. The method of claim 13 where performing destination network address translation on the destination address of the packet further comprises applying a load balancing algorithm.

15. The method of claim 14 where the load balancing algorithm is randomized.
16. A method of routing a packet from a first node to a second node, the method comprising:
receiving a packet at a first node of a underlying network;
accessing a virtual routing table to determine a next hop for the packet in a virtual network topology, where the next hop is either a logical port or a materialized port, and continuing to access subsequent virtual routing tables in series until the next hop is determined to be a materialized port on a second node of the network; and
sending the packet over the underlying network to the materialized port at the second node.
17. The method of claim 16, where the step of accessing a virtual routing table to determine a next hop for the packet comprises:
executing a lookup in each virtual routing table, where the lookup table contains the next hop data for the packet.
18. The method of claim 16, where the first node of the network is configured to access an external network, and where the second node of the network is configured to host a virtual machine.
19. The method of claim 16 further comprising:
applying a pre-routing modification to the packet for at least one hop in the virtual network topology.
20. The method of claim 16 further comprising:
applying a post-routing modification to the packet for at least one hop in the virtual network topology.
21. The method of claim 16, where the next top for a packet is determined from at least one of a source address and a destination address.

22. The method of claim 16, further comprising:
storing at least one virtual routing table in a distributed state on a plurality of nodes in the network.
23. The method of claim 16, where sending the packet over the underlying network comprises:
accessing an Ethernet network to transfer the packet from the first node to the second node.
24. The method of claim 16, where the underlying network comprises a private IP network.
25. The method of claim 16, where the underlying network comprises a public IP network.
26. A method of routing packets comprising the steps of:
receiving a packet of a flow at a first node;
accessing a flow table and determining that the packet does not match an existing flow rule;
communicating the packet to a controller;
accessing a virtual network topology stored in a distributed state accessible by a plurality of nodes;
creating a flow rule for the packet;
communicating the flow rule to the flow table; and
storing the flow rule in the distributed state on the underlying network.
27. The method of claim 26, where the step of creating a flow rule for the packet comprises:
identifying an existing flow rule for the flow created by a different controller in the underlying network; and
receiving the existing flow from the distributed state at the controller.
28. The method of claim 26, where the step of creating a flow rule for the data packet comprises:
determining a routing sequence for the packet in the network based on a virtual network topology established by a network tenant.

29. The method of claim 26, where the step of storing the flow rule in the distributed state on the network comprises:

communicating the flow rule to a selected node of the network, where the selected node stores the distributed state comprising flow rules from each node of the underlying network.

30. The method of claim 26, where the step of storing the flow rule in a distributed state on the network comprises:

communicating the flow rule to an edge node of the underlying network.

31. A method of stateful connection tracking for deleting a flow entry, the method comprising:

receiving a FIN packet with a sequence number at an edge node with a flow configurable switch;

identifying a flow rule corresponding to the packet in the flow configurable switch;

identifying the flow rule for deletion and communicating the identified flow rule to a distributed state; and

communicating the packet based upon the corresponding flow rule.

32. The method of claim 31, where the flow rule corresponds an inbound flow of a TCP connection.

33. The method of claim 31, where the flow rule corresponds to an output flow of a TCP connection.

34. The method of claim 31, further comprising:

deleting the identified flow rule upon receiving an ACK packet corresponding to the FIN packet.

35. The method of claim 31, further comprising:

identifying an opposite direction flow rule stored in the distributed state that corresponds to the identified flow rule; and

identifying the opposite direction flow rule for deletion.

36. The method of claim 35, further comprising:

deleting the identified flow rule and the opposite direction flow rule upon receiving an ACK packet corresponding to the FIN packet.

37. A method of performing destination network address translation comprising:

receiving a first packet at a first node, the first packet having a destination address;

creating a first flow rule corresponding to the first packet, the first flow rule comprising a routing rule and a destination network address translation rule,

applying the destination network address translation rule on the destination address of the first packet;

storing the first flow rule in a distributed state;

receiving a second packet at a second node in response to the first packet, the second packet having a source address;

creating a second flow rule corresponding to the second packet; and

accessing the first flow rule from the distributed state and applying the destination network address translation to the source address of the second packet.

38. The method of claim 37 further comprising:

waiting until the first flow rule is stored in the distributed state before forwarding the first packet such that the second packet is not received until the first flow rule is stored in the distributed state.

39. The method of claim 37, where the first packet and second packet correspond to a TCP connection.

40. The method of claim 39 where the step of applying the destination network address translation rule further comprises:

applying a load balancing algorithm to balance loads on the network resources.

41. The method of claim 40, where the load balancing algorithm is randomized.

42. A cloud computing system comprising:
- a plurality of edge nodes configured to access an external network and a plurality of host nodes configured to host virtual machines;
 - an underlying network interconnecting the plurality of edge nodes and the plurality of host nodes adapted to transport data packets throughout the underlying network;
 - a distributed state system in communication with each of the edge nodes and each of the host nodes of the network, the distributed state system storing a virtual network topology;
- where the virtual network topology comprises:
- a provider virtual router identifying a plurality of materialized ports corresponding to the plurality of edge nodes, and
 - a plurality of tenant virtual routers in communication with the provider virtual routers, the tenant virtual routers being configured to expose at least one public IP address, and where the plurality of tenant virtual routers are configured to provide access to the external network through each of the plurality of edge nodes.
43. The cloud computing system of claim 42, where the external network is the Internet.
44. The cloud computing system of claim 42, where the underlying network is a private IP network interconnecting the plurality of edge nodes, the plurality of host nodes, and the distributed state system.
45. The cloud computing system of claim 42, where the virtual machines are tenant virtual machines.
46. The cloud computing system of claim 42, where the virtual network topology has a plurality of virtual routers for at least one tenant, each tenant virtual router configured to access a subset of the tenant virtual machines associated with a given tenant.

METHOD AND APPARATUS FOR COMPUTING

BACKGROUND AND SUMMARY

[01] The present disclosure relates to networking, and more particularly to the design and use of virtual routers and flow based routing.

[02] The advent of cloud-based computing has created new demands for service providers. Service providers would like to provide each customer with a virtual network, with the ability to add hosts and change topology decoupled from the physical network. Virtualization of the network allows service providers to create customer-configurable network topologies which can be changed by altering virtual routers without any change in hardware. Virtual routers also allow segregation of customers' data for security and use-based pricing. Dedicated hardware can provide some of these features but can be expensive.

[03] There remains a need in the art for a tool that allows a virtual network to be overlaid over an existing network and allows that virtual network's topology to change.

[04] Presently disclosed are a system and method that facilitate packet routing using a virtual network overlaid on a physical network. In various embodiments, the present disclosure provides for the flexible interconnection of network elements at multiple layers of the OSI model, including, L2 (Layer-2, i.e. Link Layer), L3 (Layer-3, i.e. Network Layer) and L4 (Layer-4, i.e. Transport Layer). Network elements may be interconnected with virtual L2 switches and L3 routers. The virtual L2 networks' packets may be transported over the existing L3 network using GRE tunneling, without requiring any changes to the L3 network. The Internet Protocol (IP) packets routed by the virtual L3 router may be transported over the existing L3 network, without requiring any changes to the existing L3 network.

[05] In an embodiment, the virtual L2 switches and virtual L3 routers appear to the elements they connect as physical L2 switches and physical L3 routers, although they may not be implemented using physical L2 and L3 network elements. There can be an arbitrary number of virtual network elements (switches or routers), each virtually connected to an arbitrary number of network elements. In one configuration, each virtual L2 switch is connected to one virtual L3 router, which can be connected to an arbitrary number of other L3 routers.

[06] The system's virtual L2 switches and virtual L3 routers can connect a large number of network elements, regardless of geographical separation. The system can connect elements that are

either physical or virtual, connecting, for example, virtual machines emulated on server computers to physical routers that are connected to the internet.

[07] A method and system for creating and managing virtual networks comprising a plurality of virtual routers and switches is provided. The method and system may also provide for L3/L4 firewall services, source and/or destination network address translation services, and load balancing as described in more detail below. Presently disclosed is a method of routing a packet from a first node to a second node that comprises receiving a packet at a first node of an underlying network; accessing a virtual routing table to determine a next hop for the packet in a virtual network topology, where the next hop is either a logical port or a materialized port, and continuing to access subsequent virtual routing tables in series until the next hop is determined to be a materialized port on a second node of the network; and sending the packet over the underlying network to the materialized port of the second node. The step of accessing a virtual routing table to determine a next hop for the packet may also include executing a lookup in each virtual routing table, where the lookup table contains the next hop data for the packet. In one embodiment, the first node of the network is configured to access an external network, and the second node of the network is configured to host a virtual machine. The method may also include applying a pre-routing modification and/or post-routing modification to the packet for at least one hop in the virtual network. In one embodiment, the next hop for a packet is determined from the source address and/or destination address. In addition, the pre-routing and post-routing processes may utilize the source address, source port, destination address and/or destination port to determine the desired modification or translation of the packet. The method may also comprise storing at least one virtual routing table in a distributed state on a plurality of nodes in the underlying network. In various embodiments, the underlying network may include an Ethernet network, a private IP network, a public IP network, or other networks capable of providing connectivity between the nodes.

[08] Also disclosed is a method of routing packets comprising the steps of receiving a packet of a flow at a first node; accessing a flow table and determining that the packet does not match an existing flow rule; communicating the packet to a controller; accessing a virtual network topology stored in a distributed state accessible by a plurality of nodes; creating a flow rule for the packet; communicating the flow rule to the flow table; and storing the flow rule in the distributed state on the underlying network. The method may also include identifying an existing flow rule for the flow created by a different controller in the underlying network; and receiving the existing flow from the distributed state at the controller. The step of creating a flow rule may further comprise determining

a routing sequence for the packet in the network based on a virtual topology established by a network tenant. In an embodiment, the step of storing the flow rule in a distributed state on the network comprises communicating the flow rule to a selected node of the underlying network, where the selected node stores the distributed state comprising flow rules from each node of the underlying network. In another embodiment, the step of storing the flow rule in a distributed state on the underlying network comprises communicating the flow rule to an edge node of the underlying network.

[09] Also disclosed is a method of stateful connection tracking for deleting a flow entry comprising the steps of receiving a FIN packet with a sequence number at an edge node with a flow configurable switch; identifying a flow rule corresponding to the packet in the flow configurable switch; identifying the flow rule for deletion and communicating the identified flow rule to a distributed state; and communicating the packet based upon the corresponding flow rule.

[10] In embodiments, the flow rule may correspond an inbound flow or an outbound flow of a TCP connection. The method may further include deleting the identified flow rule upon receiving an ACK packet corresponding to the FIN packet. In an embodiment, the method also comprises identifying an opposite direction flow rule stored in the distributed state that corresponds to the identified flow rule; identifying the opposite direction flow rule for deletion; and deleting the identified flow rule and the opposite direction flow rule upon receiving an ACK packet corresponding to the FIN packet.

[11] In another embodiment, a method of performing destination network address translation comprises the steps of receiving a first packet at a first node, the first packet having a destination address; creating a first flow rule corresponding to the first packet, the first flow rule comprising a routing rule and a destination network address translation rule; applying the destination network address translation rule on the destination address of the first packet; storing the first flow rule in a distributed state; receiving a second packet at a second node in response to the first packet, the second packet having a source address; creating a second flow rule corresponding to the second packet; and accessing the first flow rule from the distributed state and applying the destination network address translation to the source address of the second packet. The method may also comprise waiting until the first flow rule is stored in the distributed state before forwarding the first packet such that the second packet is not received until the first flow rule is stored in the distributed state. In one embodiment, the first packet and second packet correspond to a TCP connection. In

another embodiment, the method further comprises, applying a load balancing algorithm to balance loads on the underlying network resources.

BRIEF DESCRIPTION OF THE DRAWINGS

- [12] FIG. 1 illustrates an example of a server computer used by the system to route packets to and from a general network such as the internet to a service provider's IP fabric.
- [13] FIG. 2 illustrates an example physical network
- [14] FIG. 3 illustrates an example virtual network that could be overlaid on the physical network of FIG. 2.
- [15] FIG. 4 illustrates a process running on an edge connector to route packets in a virtual topology comprised of virtual routers.
- [16] FIG. 5 illustrates a process running on an edge connector to switch and route packets in a virtual topology comprised of virtual routers and virtual switches
- [17] FIG. 6 is a continuation of the process of FIG. 5.
- [18] FIG. 7 illustrates an embodiment of a virtual network.
- [19] FIG. 8 illustrates the virtual network of FIG. 7 overlaid on a physical network.

DETAILED DESCRIPTION

- [20] Referring generally to FIGS. 1 through 8, systems and methods to facilitate packet routing using a virtual network overlaid on an underlying network are presently disclosed. In various embodiments, the underlying network is a physical network, however, in other embodiments, the underlying network may be a virtual or logical network. For clarity, the underlying network may be described in terms of a physical network, however, one or more virtual networks may be layered upon another, each providing the underlying network for the next overlaid virtual network.
- [21] A system of the present disclosure may include a network interconnecting a plurality of nodes. The nodes of the network may correspond to physical components such as servers, routers, or other computing devices in communication with the network. Each device may support one or more nodes. In another embodiment, the nodes may represent logical or virtual devices. The network may be a private network maintained by a service provider, where the service provider sells, leases, or otherwise provides network capabilities to a plurality of tenants. The network may have one or more nodes, such as edge nodes, that provide connectivity to a public network. In one

example, the network includes a plurality of Internet facing nodes providing multiple input/output communication pathways between the Internet and the network. The Internet facing nodes may be Internet connected routers. In another example, the network includes a plurality of nodes configured to host tenant virtual machines. The nodes hosting tenant virtual machines may be host servers or other devices with the necessary resources to operate one or more tenant virtual machines. In some implementations, a node may host multiple virtual machines from a single tenant. In another embodiment, a node may host multiple virtual machines owned by different tenants. In yet another embodiment, a node may operate both to host a tenant virtual machine and to provide Internet connectivity to the network.

[22] A method is disclosed for routing a packet from a first node to a second node. The method comprises the steps of receiving a packet at a first node of a network; accessing a virtual routing table to determine a next hop for the packet, where the next hop is either a logical port or a materialized port, and continuing to access subsequent virtual routing tables in series until the next hop is determined to be a materialized port on a second node of the network; and sending the packet over the underlying network to the materialized port of the second node. The network may be an Ethernet network, a private or public IP network, or other network providing connectivity between the plurality of nodes.

[23] In one embodiment, each node of the network contains an edge connector. Each edge connector contains an instance of a flow configurable switch and a coordinator, both running on the same physical host or node. In one embodiment, a flow configurable switch may comprise software such as Open VSwitch. The coordinator of the edge connector may implement one or more virtual L2 switches and virtual L3 routers. An edge connector may have physical interfaces, virtual interfaces, or both. Virtual interfaces are interfaces such as, for example, tap interfaces or kernel level virtual interfaces. Physical interfaces are, for example, a physical network interface card (NIC).

[24] A flow configurable switch is a software component that applies an action list to all packets that match a flow rule. Associated with an action list is a flow match that specifies what packets match the flow. The flow match may be based on one or more portions of the packet data, including for example, the source and destination ports, source and destination addresses, MAC address. The flow match may also be based on combinations of packet data or subsets of packet data, such as a portion of the source or destination addresses. A flow rule may comprise at least a flow match and an action list, and may be referred to as a “flow.” Two flows (one inbound, one outbound) form a connection. Generally, two flows, an inbound flow and an outbound flow, form a

connection for communications between a client outside the network and a tenant's virtual machine or other provided service within the network. Each flow represented by one or more flow rules may be stored in a distributed state. In one embodiment, each flow rule is stored in a distributed state maintained on a node of the network accessible by all other nodes requiring access to the distributed state. The flow rules may be indexed by their flow match, or by other criteria associated with the flow rules.

[25] In one embodiment, the coordinator of the edge connector may maintain a flow table that caches the routing decisions made for the first packet in one direction of a connection. The flow table is maintained inside the flow configurable switch. The network may have multiple possible access points to the external network, and connections need not use the same virtual route inbound as outbound. Allowing for different inbound and outbound routes may improve the fault tolerance of the system in the event of interruptions in certain portions of the network. Allowing for different inbound and outbound routes may also allow for improved utilization of network resources by balancing loads between different paths in the network.

[26] The network may also contain forwarding elements that route and switch packets between the nodes of the network. The forwarding elements may be either L2 switches, L3 routers, or combinations of L2 switches and L3 routers. The forwarding elements may be either physical or virtual, and the network may include combinations of physical and virtual forwarding elements. A physical forwarding element is a hard component, while a virtual forwarding element may be implemented in software. In one embodiment, a virtual forwarding element is implemented using tables. For example, tables in the coordinators of the edge connectors may be used to route and switch packets according to a virtual topology established for the network.

[27] In the network, virtual routers may be connected to other virtual routers to construct a network topology that may be illustrated by a virtual network graph. Each virtual router may have a plurality of virtual ports, where each virtual port is either a logical port or a materialized port. Logical ports are ports that connect two virtual routers. Each logical port of a virtual router will therefore be connected to another logical port of another virtual router. The logical ports may be implemented in the coordinators of edge connectors. For example, each virtual router may include a virtual routing table, and the logical ports may be identified by performing a lookup in the virtual routing table to determine the next hop for a packet being routed by the virtual routing table. Each lookup can lead to a logical port and another virtual router table or a materialized port, allowing the coordinator to traverse a virtual topology of virtual routers. A materialized port is a port where

packets enter or leave the virtual network. In one embodiment, a materialized port may correspond to a port in a flow configurable switch. In some embodiments, a materialized port may correspond to the location of a node providing Internet connectivity. In another embodiment, a materialized port may correspond to the location of a virtual machine operating within the network. For both logical and materialized ports, the virtual port's static configuration in the shared configuration tree explicitly contains the port's type (logical or materialized) and, in the case of logical ports, the universally unique identifier ("port_uuid") of the other end of the virtual link. Additionally, the virtual routers may have their own IP addresses. Additionally, each virtual router may support protocols such as border gateway protocol ("BGP") and/or internal gateway protocol ("IGP").

[28] In another embodiment, the edge connectors may have tunnel ports that are not ports of the virtual routers. A tunnel port is a port that connects one edge connector to another edge connector across the network. For example, the flow configurable switch of one edge connector may be connected to the flow configurable switch of another edge connector by a tunnel port. In one embodiment, a packet may arrive at one edge connector destined for a virtual machine at another edge connector. When a packet is destined for a materialized port on another edge connector, it is sent to that edge connector via a tunnel. The edge connector may maintain a table that maps materialized ports to edge connectors and a table that maps edge connectors to tunnels. Thus an edge connector may determine through which tunnel to send a packet based on a (non-local) materialized port. In another embodiment, the mapping of materialized ports to edge connectors and of edge connectors to tunnels may be maintained on a separate node, and the edge connectors may communicate with the separate node to determine the appropriate tunnel for a packet.

[29] In one embodiment, the edge connectors on each node have access to a distributed state. The distributed state is maintained and shared by the edge connectors. The distributed state may contain, for example, the configuration tree and other data regarding the virtual and/or physical network topology. In one embodiment, a distributed state may be implemented using Zookeeper and memcache. In another embodiment, part of the distributed state is a configuration tree, but other structures such as hash tables and n-ary trees are contemplated. The configuration tree and other shared data may be accessed by the edge connectors as needed, such as by the coordinators.

[30] The term "client" is used herein to indicate an external network client, such as a web browser, that is trying to reach a server hosted within the system, for example, to access the services of a virtual machine. The term "tenant" is used to indicate a customer of the service provider. A tenant may have one or more virtual machines or other services operating on physical machines

within the system, and may want to dynamically establish load balancing or network address translation (“NAT”) rules between these virtual machines and the clients.

[31] Referring now to FIG. 1, a server 101 is illustrated with two network interface cards, NIC A 111 and NIC B 112. Each computer or physical machine in the system may have the same architecture, for purposes of illustration some nodes may be designated as edge nodes facing internet clients, and providing internet connectivity to the network. Other nodes may be designated as host nodes configured to host tenant virtual machines or other services within the network. For purposes of illustration the edge nodes and host nodes may be shown with symmetric architectures, however, in various embodiments, a variety of architectures may be used for the various nodes in the system. Although illustrated in terms of internet facing edge nodes and virtual machine hosting nodes, the system may also contain intermediate nodes including, data storage devices and support servers desired to facilitate operation of the network. As shown in FIG. 1, NIC A 111 has a connection to the internet 151 and NIC B 112 has a connection to the internal provider fabric 152. The internal provider fabric 152 may be a private IP network, or other network provides IP connectivity between the nodes.

[32] The system includes a software component implementing many of the features of the virtual network overlaid on the physical network. To illustrate the operation of the software components, the actions following receipt of a packet are described.

[33] In one embodiment, a SYN packet is received to establish a TCP connection. The SYN packet is received from the Internet 151 on NIC A 111. Packets are received by the edge connector at the flow configurable switch 161 for switching. The flow configurable switch 161 attempts to identify a flow rule by matching data associated with the packet to the flow rules stored in the flow table 162. The matched data may include, for example, source and destination ports, network addresses, MAC addresses, or other data associated with the packet. The SYN packet is typically the first packet in a flow and therefore the flow configurable switch 161 does not find an entry corresponding to the first packet in the flow table 162. Upon not finding a corresponding entry in the flow table, the flow configurable switch 161 makes a function call to the controller and communicates the packet to the controller 165. The packet may arrive on a port of the flow configurable switch, and the flow configurable switch may communicate the incoming port ID to the controller with the packet. The controller 165 interfaces between the coordinator 170 and the flow configurable switch 161. Although the function of the flow programmable switch, controller, and coordinator are described separately for clarity, it will be apparent that the software components

may be integrated as desired. The controller 170, in one embodiment, is the layer that communicates to the flow configurable switch 161 via the OpenFlow protocol and translates the incoming port ID of the flow configurable switch into a virtual port ID (“vport”) for the coordinator. Alternatively, this mapping may be based on MAC address, or 802.1x credentials instead of incoming port ID. The rest of the packet’s routing is dependent upon its L3 information. The controller 165 passes the packet and vport to the coordinator 170, which has the logic to route the packet. In one embodiment, only the first packet of a connection will cause a call to the controller 165, and then on to the coordinator 170, because, once the flow is created in the flow table 162, there is no need for further calls to the controller 165 from the flow configurable switch. After the first packet, the flow configurable switch has all the information needed to switch subsequent packets from the same flow.

[34] To create a flow rule associated with a new flow, the coordinator builds an action list indicating how to process and forward the packet and inserts it as a flow rule in the flow table. Subsequent packets that match the criteria for that flow have the action list applied, which may include routing the packet to a given port. The coordinator’s operation is discussed in more detail below. If the packet were meant for another edge connector running on another server, it would be routed to the other edge connector via a tunnel port. Tunnel ports connect edge connectors and are used to forward packets between edge connectors but are not virtual ports in the virtual router. Instead, when a packet is meant for a virtual port on another edge connector, it is sent to that edge connector through a tunnel. The tunnel protocol is, in one embodiment GRE+IP. This tunneling protocol allows one flow configurable switch 161 on a server 101 to communicate via the internal provider fabric 152 with another flow configurable switch (not pictured) on another server (not pictured). FIG. 2 illustrates the actual physical interconnection of a plurality of edge connectors 203, 204, 205 connected by the provider’s internal L3 network fabric 202. FIG. 3 illustrates the virtual topology that is overlaid on this network. The tunneling protocol allows the fabric to route the packets between flow configurable switches without modification to the hardware in the provider fabric 152. Because the actual packets travel over IP (L3) as opposed to Ethernet (L2), the network is scalable and may be not limited by distance limitations. The end points of tunnels are ports in the flow configurable switches of the edge connectors, but tunnel ports are treated differently than materialized ports. The IP portion of the tunnel packet header allows the packet to get to the correct host, and then the GRE portion of the header serves to get the packet to the right

tunnel port. Yet another key in the header serves to identify the destination materialized port, so that the receiving edge connector can route the packet to the correct local port.

[35] Referring now to FIG. 2, a network comprising three edge connectors 203, 204, and 205 is illustrated, where each edge connector resides on a host. Continuing with the example from above, assume a packet was received at edge connector 203 on a physical network interface card (NIC) from the internet 151 via the internet connected router 201 and that the packet is destined for virtual machine 211. Recall that the packet is the first packet of a flow, so there is no flow rule corresponding to the packet in the flow table. Because there is no corresponding flow entry in the flow table, flow configurable switch 161 calls the controller 165 which in turn calls the coordinator 170. The controller 165 determines a virtual port (vport) based on the port that the packet was received on by the flow configurable switch, and possibly by the MAC address, and 802.1x credentials. The controller includes the vport in the call to the coordinator with the packet. The vport in this instance is a materialized port corresponding to a NIC and a port in the flow configurable switch. The coordinator uses the vport to determine which virtual router or virtual switch the materialized port is connected to. As discussed above, a virtual router may be implemented by a table accessible to the coordinator and maintained in a distributed state shared by the coordinators. Once the coordinator determines what virtual router is connected to the materialized port, the coordinator selects a matching route by identifying the destination IP address in the corresponding virtual router table. In one embodiment, the coordinator may select one route from several routes using a load balancing algorithm.

[36] In another embodiment, when the coordinator accesses a virtual router table to look up an IP address, pre-routing and post-routing processes may be applied. The pre-routing process may alter the packet, including the source and destination IP addresses and source and destination ports, to perform network address translation ("NAT"). After applying a pre-routing process, the coordinator performs a routing method selected for the flow. The routing method may comprise extracting the source and destination IP addresses, looking up the IP addresses in a virtual routing table corresponding to a virtual router, selecting a destination (if more than one route is found), and forwarding the packet to the port corresponding to the route entry. The forwarding of the packet depends on whether the next hop of the matching route is a logical virtual port or a materialized port. A pair of logical ports connects two virtual routers. Since virtual routers may be implemented as tables in the coordinator, routing between two virtual routers comprises a lookup in successive virtual router tables. In one embodiment, all edge connectors maintain one global routing table for

each virtual L3 router. The global routing table may be stored on in a distributed state on a designed node of the network. Alternatively, the global routing table may be stored on a selected edge connector. In another embodiment, the global routing table is maintained on each edge connector and the edge connectors cooperate to maintain and update the global routing table on each other edge connector in the network.

[37] Referring now to FIG. 3, a virtual topology is illustrated that may be overlaid on an underlying network, such as the physical network of FIG. 2. In one example, a packet may arrive on a materialized port that associated with virtual L3 router 301 and its destination IP address is the IP address of VM 211. The coordinator may use the vport that the packet arrived on to determine what virtual router the vport is connected to, in this case virtual L3 router 301. In one embodiment, the virtual L3 router 301 may be a provider router, created and administered by the service provider operating the network. The coordinator may then utilize the IP address associated with the packet to determine an output port for the packet. The output port may be a materialized port, such as a port associated with a virtual machine, or a logical virtual port connected to a logical port of another virtual router or virtual switch. If the output port is a local materialized port, then a flow is established in the flow configurable switch and the packet is routed to the local materialized port. If the materialized port is not local, the packet is routed out a tunnel port according to a vport to host table and a host to tunnel port table. If the port is a logical port of another router or switch, then the same lookup process is repeated until a materialized port is identified. To continue with FIG. 3, the lookup in the table of virtual router 301 may return a logical virtual port corresponding to virtual router 302. After the lookup is performed, post-routing processes may be applied to the packet as desired. When the lookup returns a logical virtual port corresponding to another virtual router, in this instance virtual L3 router 302, the coordinator may repeat the same process for virtual router 302. Virtual router 302 may be, for example, a virtual router created by a tenant to route traffic between the tenant's virtual machines, virtual machines 211 and 212. The tenant's virtual machines may be on the same host, or may be located on different hosts within the network. A tenant may lease network resources from the service provider to operate any number of virtual machines or other services within the capacity of the network subject to rules established by the service provider. The coordinator performs any pre-routing associated with virtual L3 router 302, looks up the IP address in the virtual routing table to determine a next hop, and then performs any post-routing. In this case, the next hop is virtual machine 211, which is hosted on a different edge connector than edge connector 203. The virtual router table for virtual router 302 provides a vport corresponding

to VM 211 as configured by the tenant or the service provider. In one embodiment, the service provider may move tenant virtual machines between different nodes in the network to manage equipment utilization or to maintain operations during maintenance or repair of physical components in the network. The coordinator then looks up the physical location of the egress vport in a port location dictionary maintained in the distributed state. In one implementation, the port location dictionary is maintained in distributed state using ZooKeeper. The flow configurable switches on different edge nodes may be connected by generic routing encapsulation (“GRE”) tunnels so that the coordinator may determine the OpenFlow port number corresponding to the tunnel to that edge connector 204. Because all packets forwarded by OpenFlow switches are L2 packets, there is space in the L2 packets for MAC addresses. Because tunnel ports are between two flow configurable switches, however, MAC addresses may not be necessary for certain applications. More specifically, in certain embodiments, there is no need to forward the actual MAC addresses because the egress edge connector can construct the MAC address based on its own local information, using ARP to determine the next hop MAC. Instead, the vport of the destination (in this case VM 211) is encoded into the space for the MAC address. The packet is then wrapped in GRE+IP with the IP address of the edge node as the destination. The packet is now ready to be routed via the L3 network. Referring to FIG. 1, an action list containing any pre- and post- routing and the routing destination may be installed in the flow table 162 to match all future packets of this flow and the packet may be sent out via the tunneling protocol and through the operating system router 113 and then to NIC B 112. The packet is, after it exits NIC B 112, routed over the internal provider fabric 152 as any other IP packet would be, with the destination IP address of edge connector 204.

[38] When the packet is received by edge connector 204, it is received on a GRE tunnel corresponding to a tunnel port of the flow configurable switch. Because the packet is received on a tunnel port, the edge connector treats this packet differently than a packet coming in on a materialized port. The packet is again the first packet received on this flow and the edge connector 204 will invoke the controller and coordinator. In one embodiment, the coordinator interprets the source and destination MAC fields of the internal L2 packet as encoding the destination vport id. The coordinator uses the vport id to determine a MAC address and the OpenFlow port number of virtual machine 211. In some instances, the coordinator may have to initiate an ARP request to determine the MAC address of VM 211. Alternatively, the MAC address may be cached in an ARP table. An ARP table (IP to MAC) is maintained per materialized port of a virtual router. After the

coordinator has determined the vport of VM 211, the coordinator may install a flow in the flow table to route future packets of this flow. The packet may then be routed to the port of the flow configurable switch corresponding to VM 211. Although VM 211 is a local virtual machine running on host 221, which also hosts edge connector 205, the coordinator may still use the destination IP address to find the destination MAC address. In this manner, the system abstracts whether the VM is local or a standard port to another router or switch further proving the flexibility of the system.

[39] Once the flows have been established, subsequent inbound packets on the same connection will match the flows in the flow tables of edge connectors 203 and 204 and will be modified and forwarded by the flow configurable switches on those machines without a lookup in the coordinators of those respective machines. This process establishes the inbound flow of a connection through the system to the desired destination.

[40] When VM 211 responds on the same connection, the first packet it sends will trigger the system to establish a corresponding flow in the opposition direction. When a new flow is established, the coordinator accesses the distributed state to determine if a flow was previously established in the opposite direction. This distributed state facilitates implementation of other processes, such as NAT and also enables the system to cleanup terminated connections as described further below.

[41] Referring now to FIG. 4, a high level overview of a process running on an edge connector performing an embodiment of method described above is illustrated. In an embodiment, an edge connector runs on a physical machine with at least one CPU that receives packets from an external network, such as the Internet, where the packets are addressed to an IP address associated with a tenant of the system. The tenant IP addresses may be assigned to tenant virtual machines running on one or more hosts within the system. In one embodiment, the IP address associated with a tenant virtual machine may remain constant even though the tenant or service provider relocates the virtual machine to a different host within the system. In an embodiment, the system allows multiple tenants to share one service provider's uplink, by allowing multiple IP addresses on one uplink to be routed to different edge connectors and different tenant virtual machines. When the edge connector receives a packet at step 410, it extracts a plurality of data at step 412, including but not limited to, source and destination addresses and source and destination ports. After extracting the data, the edge connector looks up the plurality of data in a flow table (step 414) and determines if the flow has already been established (step 416). An example of a flow would be one direction of a TCP connection, with an inbound and outbound flow combining to form a single TCP connection. If

the flow already exists, the flow action list is applied to the packet and the packet is forwarded to the port of the flow configurable switch indicated by the flow action list in step 418.

[42] If the flow does not exist, this is the first packet in the flow received by the node, and the edge connector must determine in step 417 what virtual port the packet arrived on, based on, for example, MAC address, source and destination addresses, or source and destination ports. Once the edge connector determines the virtual port ID, the edge connector can determine what virtual forwarding element that port is connected to. In the embodiment of FIG. 4, the virtual forwarding element is a virtual router, but other virtual forwarding elements, such as virtual switches, may be utilized as necessary in the system as discussed below. Once the edge connector determines the VFE, the edge connector performs another lookup in step 420. The lookup is performed by looking up the destination IP address in a series of virtual forwarding elements. The virtual forwarding elements may comprise any combination of virtual routers and virtual switches including virtual routing tables to determine the appropriate path for the packet being forwarded. In the embodiment shown, in step 420, the controller determines the destination of the packet in a first virtual forwarding element. The first virtual forwarding element may be a virtual router, in which case the destination returned may be either a materialized port or a logical port. As noted above, a logical port is paired to another logical port of a second virtual router, and the second virtual router has another routing table. If a logical port is returned, the controller looks up the destination address in the routing table of the second virtual router in step 420 and continues until a materialized port is returned. In one embodiment, each tenant may have a single virtual router configured to route all packets handled by that tenant. In other embodiments, some tenants may have a plurality of virtual routers, virtual switches or other virtual forwarding elements defining the tenant's portion of the virtual network topology. The controller also builds a series of actions to be performed on the packet from each virtual routing table. Each routing step may also have pre-routing or post-routing processes that are added to the action list and incorporated into the flow rule to be applied to the packets matching the flow.

[43] Once a materialized port has been returned (step 424), the edge connector determines if the materialized port is local (step 426). If the port is local, an action is added to the action list (step 430) to route the packet to the local materialized port. In various embodiments, the local materialized port may be a network interface card in or virtual machine. The flow rule is then added to the flow table (step 430) and applied to the packet (step 418). If the materialized port is not local, then the materialized port is on a different edge connector. In one embodiment, edge connectors

may be connected by tunnel ports, such as GRE_IP tunnel ports. In step 432, the edge connector accesses a virtual port to tunnel table to attempt to map the materialized port to a tunnel port. If there is no corresponding entry in the virtual port to tunnel table mapping, an action to drop the packet and send an ICMP packet is added to the action list (step 434), the flow rule is added to the flow table (step 430), and the flow rule is applied to the packet (step 418).

[44] If the materialized port is in the materialized port to tunnel table, then an action to output the packet to that tunnel is added to the action list (step 436), the flow added to the flow table (step 430), and the action list applied to the packet (step 418).

[45] In one embodiment, the controller installs the action list and flow rule in the flow configurable switch datapath, and the flow configurable switch applies the action list to any subsequent packets that match the flow rule, as shown in step 416. As described above, part of the action list includes which port of the flow configurable switch the packet is to be sent on. The edge connector looks up the port in a port to host IP table, and sends the packet to the IP address. It then stores the action list in a flow table. All subsequent packets that have a matching plurality of data will have the same set of actions applied to them, resulting in them being routed to the same IP address.

[46] During the process of identifying the destination address in the virtual routers, the flow may be unrouteable, black holed, or match a reject route, at which point the packet is dropped, or ICMP packets are returned. In this embodiment, a flow may be created to drop all packets that match the flow's rule. In this manner, the system may be configured to handle unrouteable packets or selectively screen undesired data according to rules established by the service provider or tenant.

[47] In yet another embodiment, an edge connector hosting tenant VMs may have multiple IP addresses and multiple NICs connected to the internal fabric network. In such a case, the internet facing edge connectors can select one of multiple paths to the VM hosting edge connector. Further, a VM hosting edge connector with multiple IP addresses may have a unique ID to identify the edge connector, and the coordinator routing flows may select one of the IP addresses of the VM hosting edge connector, for example using a load balancing algorithm or randomly.

[48] Another embodiment of the system may use identifiers for the edge nodes other than IP addresses. For instance, the network fabric may be circuit based, such as multiprotocol label switching ("MPLS") or another custom OpenFlow controller with dedicated circuits between edge connectors. In this embodiment, the circuits may replace the GRE tunnels between flow configurable switches on edge nodes.

[49] In another embodiment, the system provides for pre-routing and post-routing stages before and after the routing stage. Pre-routing and post-routing may be utilized to implement network address translation (NAT), load balancing, or other L3/L4 features. In one embodiment, the pre-routing stage may change the flow's destination (as, for example, in network address translation) and the outbound routing may change the flow's source (again, as an example, network address translation). To coordinate the mappings performed by the forward and reverse flows composing a single connection, such as in a TCP connection, connection translations may be stored in the distributed state with a large timeout. These translations may also be cleaned up proactively when connection tracking detects a cleanly closed connection.

[50] In one embodiment of the present system, NAT is implemented using pre-routing and post-routing transformations. On flow setup, the NAT pre-routing stage determines if there a flow was previously established in the opposite direction (inbound vs. outbound) in the distributed state and, if so, the previously created map is reversed for the new flow. Because the flow rules are stored in the distributed state system accessible by all nodes, upon creation of a new flow on a different node, it is possible to determine whether an opposite direction flow was previously created. If the opposite direction flow is not in the distributed state, the coordinator creates a new translation and stores its translation map in the distributed state associated with the new flow. For the inbound flow, or alternatively the first flow established, the address translation may be applied to the destination address before the routing step and the routing step may route based on the translated IP address. On the outbound flow, or alternatively the second flow in the connection, NAT may be performed after the routing, to translate the source address to be the external, non-private IP address. The translation information may be stored in the distributed state associated with the flow rule prior to forwarding the initial packet of the flow such that the translation information is accessible when the initial packet of the reverse flow is received at the corresponding edge connector.

[51] In another embodiment, destination network address translation (DNAT) may be used to translate from a publicly available IP address to a private network address to expose services hosted on a private network to the general internet. In some embodiments, a demilitarized zone (DMZ) may be provided between the general internet and the private network. In a DNAT process, the destination address may be translated during a pre-routing stage for the incoming flow, and in the corresponding outgoing flow, the source address may be translated during a post-routing stage. In one implementation, the destination address may be one of several possible servers, and the

destination server may be selected by a load-balancing algorithm, such as a random algorithm or a round-robin algorithm.

[52] In source network address translation (SNAT) multiple clients on the private LAN may share the same public IP address. A source address associated with outbound connections, such as connections from tenant virtual machines to an external network, may be translated to the same IP address in the outbound flow. In the corresponding inbound flow, a packet destination IP address may be translated to the corresponding private IP address based on, for example, port number and source IP address.

[53] In another embodiment, the system may be configured to provide ARP spoofing for private local area networks. The system may permit single network hosts such as a virtual machine guest to be connected to a virtual router port without consuming gateway/broadcast addresses by impersonating other single hosts when the host ARPs for them. In a traditional Ethernet-based design, this would consume at least a /30 address range, including the guest's address, the gateway address, and the broadcast address, plus one unused address.

[54] As one method of reducing the number of IP addresses consumed, each port of the router may be configured with a MAC address and network prefix (nw_prefix) and a flag indicating if there is a single host connected to the port. The gateway address used may be the first address in the nw_prefix range. If the single-host flag is unset, the router may handle traffic to and from the port according to its standard operating rules. If the single-host flag is set, the address portion of the nw_prefix specifies the address of that port's single network host. The router's downstream ports may be configured such that they comprise non-overlapping nw_prefixes with the single-host flag unset and ports with the single-host flag set, which may share identical address ranges specified by their nw_prefixes. In many embodiments, the address ranges used by the single-host and non-single-host ports will not overlap.

[55] If an IP packet is sent between ports with the single-host flag set, the router may forward the IP packet without checking or decrementing the time to live ("TTL"), emulating an L2 switch. If an ARP request is received from a port with the single-host flag set for the address associated with another single-host port, the router responds to the ARP, impersonating the target. The result is that a single-host wanting to send traffic to a host outside what it considers its local segment will ARP for the gateway address, and the normal behavior of the router will return its port's MAC and the host will then send its IP packets. A single-host wanting to send traffic to a host it considers part of its local segment will ARP for that host directly. The router will respond to that ARP if it

has a single-host port for that address, in which case the host will then send its IP packets. Behavior of hosts not on a single-host-flagged ports may be unchanged.

[56] In another embodiment of the system, stateful connection tracking may be used to track the life cycle of connections, such that data associated with those connections may be cleaned up upon certain events, such as termination of the connection. The data to be cleaned up may include various connection state data, including data stored in the distributed state, such as stateful NAT and LB mappings, when the connection is cleanly shutdown. If a connection is not shutdown cleanly, for example if one side or the other crashes or is disconnected, then the connection state may be expired after a large configurable timeout. Connections may be TCP connections, and are composed of two flows, a forward flow, and a return flow. In the case of TCP, the system may simulate the TCP connection state machine in order to determine the connection state.

[57] In yet another embodiment, the system provides for the return flow of a connection to be handled by a different controller or a different node than the forward flow of the connection. A connection of this type may be referred to a split flow, characterized by the forward and reverse flow being handled by different controllers. In one embodiment, the system supports split flows by having the controller seeing the forward and reverse flows communicate the closing of their respective sides. For example, the controller handling the FIN of the forward flow may notify the controller handling the return flow to install an action matching the FIN's ACK, or vice versa. The controllers may cooperate such that the controller identify when both sides of a connection have been closed and the controllers are able to clean up the data associated with the closed connection. This communication among the controllers may occur through the shared state in the distributed state system. Additionally, the distributed state system may identify certain conditions, such as the closing of both sides of a connection, and may communicate notifications to the controllers handling each of the flows of the communication.

[58] In another embodiment, when an edge node or edge connector handles the setup of a flow, either forward or reverse, which is part of a connection that should be tracked (based on whether it is a TCP connection, and whether stateful tracking is needed, e.g. if the connection is being NATed), the edge connector will add an action which checks for the TCP FIN bit and outputs the FIN packet to the controller. Upon receiving a FIN packet, the controller handling the reverse flow may install an action checking for the ACK of the FIN. When the ACK of the FIN is seen by the system, the connection is considered half-open, such that no data but only ACKs are expected. If

data is received by a half-open connection, the system may generate an error indicating an unexpected condition was experienced by the system.

[59] When a controller receives a new flow, it will install a rule which checks for the TCP FIN and RST flags. If the controller receives an RST packet, it modifies the flow rule for the connection to have a short timeout, as the connection is going to be terminated once the peer receives the RST packet. If the controller receives a FIN packet, it inserts into the action list of the return flow an action matching the acknowledged sequence number being the FIN packet's sequence number. If the controller gets a packet acknowledging a FIN, it marks that side of the connection as closed. If both sides are closed, it modifies the flow rule for the connection to have a short timeout. In some instances, the FIN's ACK may be dropped, in which case the closing side will retransmit the FIN packet with the same sequence number. When the flow rules expire, the system identifies that the connection is closed and may cleanup additional state data such as NAT tracking.

[60] In another embodiment of the system and method presently disclosed, a virtual switch is provided as an additional virtual forwarding element. The system may transmit L2 packets between the edge connectors' ports that are part of each virtual L2 switch. In this manner the system may simulate the operation of a physical L2 switch transmitting packets between NICs connected to the physical switch. The system may also transmit packet L3 packets as described above using virtual routers. When setting up a flow, the incoming vport UUID is identified from the mapping of an ingress port or MAC address. Based on this vport UUID, the virtual device to which the vport belongs is determined. Based on the type of virtual device (switch or router), the packet is either routed (as described above) or is switched. That is, if the packet is an L3 packet, it is handled in accordance with the virtual router process described above. Alternatively, the packet is an L2 packet and is processed by a virtual switch, as illustrated in FIGS. 5 and 6. The process illustrated in FIGS. 5 and 6 is substantially similar to the process illustrated in FIG. 4. After the VFE has been determined in step 417, the edge connector determines if the VFE is a virtual router or a virtual switch. If the VFE is a virtual router, processing continues as described with respect to FIG. 4. If the VFE is a virtual switch, processing continues at point A (520), connected to point A (520) in FIG. 6. As illustrated in FIG. 6, if the VFE is a virtual switch, then the edge connector determines if the destination MAC address is a broadcast address or a unicast MAC address (step 610). If the MAC address is a broadcast address, then the packet is sent to each port connected to the virtual switch (step 620). On a per packet basis, this step may be identical to the process of FIG. 4 starting

with step 426. For each material port that is a member of the VFE, the packet is either sent to the local vport or the tunnel port corresponding to that materialized port.

[61] If the packet is not a broadcast packet (e.g. a unicast packet), then the destination MAC is determined, for example, by looking up the destination MAC in a MAC to vport table (step 630). If there is not a corresponding entry (tested in step 640), then a drop action is added to the action list (step 650). Processing then continues at point B on FIG. 5, where the rule is added to the flow table (430) and the action applied to the packet (418).

[62] If there is a corresponding vport in the MAC to vport table of step 640, then processing continues at point C on FIG. 5, processing continues at step 426, as previously described.

[63] Referring now to FIGS. 7 and 8, another embodiment of the system and method presently disclosed is illustrated. As shown in FIG. 7, a virtual network topology includes a provider virtual router 900 having multiple connections 901 to an external network, such as the general Internet 902. In this configuration the virtual network is provided with multiple communication paths to the external network allowing for flexibility and redundancy in the system. The provider virtual router 900 may have a plurality of materialized ports corresponding to a plurality of edge nodes, where an edge node is a physical component providing access to the external network. In one embodiment, an edge node may be an Internet facing router or server. The virtual network topology may also comprise a plurality of tenant virtual routers. In one configuration, each tenant virtual router may be associated with a tenant virtual data center. As shown in FIG. 7, a first tenant virtual data center 903 may include a first tenant virtual router 904 in communication with a plurality of first tenant virtual machines 905. The first tenant virtual machines 905 may also communicate with a tenant virtual switch 906, which may be a virtual Ethernet switch as illustrated. The first tenant virtual machines 905 may reside on one, or more than one servers or host nodes in the network.

[64] As also shown in FIG. 7, the virtual network topology may have a second tenant virtual data center 907, including a second tenant virtual router 910 in communication with the provider virtual router 900 and a plurality of second tenant virtual machines 909. The plurality of second tenant virtual machines 909 may also communicate with a second tenant virtual switch 908, which may be a virtual Ethernet switch as illustrated.

[65] The virtual routers may also perform additional functions such as load balancing, DHCP, and/or network address translation as desired by each tenant. Although only one virtual router is illustrated for each tenant, in other embodiments, a tenant may employ a plurality of virtual routers creating a tenant specific virtual network topology. A tenant specific virtual network topology may

provide for organization of tenant virtual machines in desired arrangements or provide for isolation between virtual machines controlled by the same tenant, such as where a tenant is utilizing the network to host multiple discrete functions or business processes.

[66] In another embodiment, a tenant virtual router may provide secure access to a remote tenant office or other location. As illustrated second tenant virtual router 910 provides for a connection to second tenant VPN router 911 and second tenant office network 912 at second tenant office 913. In this manner, each tenant may define the configuration of its virtual data center. A service provide utilizing the presently disclosed system and method may therefore provide many tenant customizable solutions on a physical network.

[67] Referring now to FIG. 8, the virtual network topology illustrated in FIG. 7 is shown overlaid on a physical network. The physical network may comprise plurality of edge nodes 920 configured to access an external network, such as the Internet 902. The physical network may also include a plurality of host nodes 921 configured to host virtual machines. The network 922 may interconnect the plurality of edge nodes 920 and the plurality of host nodes 921 and be adapted to transport data packets throughout the system. In one embodiment, the network may be a private IP network. The edge nodes 920 and the host nodes 921 may have symmetric architectures. In one embodiment, the edge nodes 920 and host nodes 921 are general purpose servers configured to operate in a cloud computing system. In another embodiment, the edge nodes 920 are dedicated Internet facing routers. In yet another embodiment, a server or other computing device may function both as an edge node and a host node in the same network. The system also includes a distributed state system in communication with each of the edge nodes and each of the host nodes through the network. The distributed state system may store data associated with the virtual network topology. The system may include a software component operating on each of the nodes and implementing the virtual network topology including the provider virtual router and each of the tenant virtual routers. As new routes are configured, the software component operating on each of the nodes may communication with the distributed state system such that the distributed state maintains a comprehensive mapping of the virtual network topology and flow rules for the system. In other examples, the distributed state system may be subdivided such that multiple distributed states are maintained for selected portions of the virtual network.

[68] As illustrated in FIG. 8, the virtual network topology is overlaid on the physical network. The provider virtual router may have a materialized port associated with each of the edge nodes 920. The materialized ports of the provider virtual router 900 may map to one or more access points for

internet service providers and provide multiple connections between the system and an external network, such as the Internet. The provider virtual router 900 may also have logical ports defining virtual links to logical ports of tenant virtual routers. As illustrated, the throughput of each virtual link in the system may be selected. For example, the service provider may provide a 50Mbps virtual link to the first tenant virtual router 904, but provide a 10Mbps virtual link to the second tenant virtual router 910. As the virtual links are configurable, if the second tenant wishes to purchase a greater throughput for its virtual data center, the service provide may modify the available throughput without modifying hardware.

[69] In the embodiment illustrated, each host node 920 is hosting one virtual machine associated with the first tenant and one virtual machine associated with the second tenant. Using the virtual network topology, the service provider may reallocate tenant virtual machines among available host nodes without reconfiguration the physical network hardware. The virtual network topology stored in the distributed state system allows the system to be dynamically reconfigured.

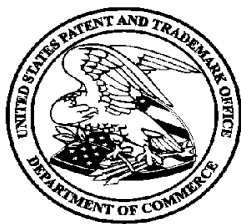
[70] In another embodiment, each of the plurality of tenant virtual routers may be configured to expose at least one public IP address and may be configured to access an external network through one or more of the plurality of edge nodes. By enabling each tenant virtual data center to access the external network through a plurality of edge nodes, the failure of a single edge nodes is less likely to interrupt availability of the tenant's services operating in the network.

[71] While certain embodiments have been described, it must be understood that various changes may be made and equivalents may be substituted without departing from the sprit or scope. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the disclosure without departing from its spirit or scope.

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

CHARMASSON, BUCHACA & LEACH, LLP
2635 Camino Del Rio South
Suite 102
SAN DIEGO, CA 92108



**Courtesy Reminder for
Application Serial No: 15/351,315**

Attorney Docket No: 160142
Customer Number: 24243
Date of Electronic Notification: 03/04/2019

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
john@charmason.com

To view your correspondence online or update your email addresses, please visit us anytime at <https://ppair-my.uspto.gov/pair/PrivatePair>.
If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/351,315	11/14/2016	Joseph L. Vilella	160142	2023
24243	7590	10/16/2019		
CHARMASSON, BUCHACA & LEACH, LLP			EXAMINER	
2635 Camino Del Rio South			FAROOQUI, QUAZI	
Suite 102				
SAN DIEGO, CA 92108			ART UNIT	PAPER NUMBER
			2491	
			NOTIFICATION DATE	DELIVERY MODE
			10/16/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

john@charmason.com

<i>Notice of Abandonment</i>	Application No.	Applicant(s)
	15/351,315	Vilella et al.
	Examiner	Art Unit
	QUAZI FAROOQUI	2491

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

This application is abandoned in view of:

1. ☒ Applicant's failure to timely file a proper reply to the Office letter mailed on 04 March 2019.
 - (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
 - (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 to the final rejection. (A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) if this is utility or plant application, a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. Note that RCEs are not permitted in design applications.)
 - (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
 - (d) ☒ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
 - (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
 - (b) ☐ The submitted fee of \$ _____ is insufficient. A balance of \$ _____ is due.
The issue fee required by 37CFR 1.18 is \$ _____. The publication fee, if required by 37 CFR 1.18(d), is \$ _____.
 - (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
 - (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
 - (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record or other party authorized under 37 CFR 1.33 (b). See 37 CFR 1.138(b).

5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34) upon the filing of a continuing application.

6. ☐ The decision by the Board of Patent Appeals and Interference rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☒ The reason(s) below:

No response has been received for the final office action of 03/04/2019.

/QUAZI FAROOQUI/ Examiner, Art Unit 2491	/ASHOKKUMAR B PATEL/ Supervisory Patent Examiner, Art Unit 2491
---	--

Petitions to revive under 37 CFR 1.137, or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.