

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

INVALIDITY CLAIM CHART

Invalidity of U.S. Patent No. 9,560,177 in view of Rijhsinghani

U.S. Patent Application Publication No. 6,526,052B1 (“Rijhsinghani”) was filed on December 23, 1998, and was issued on February 25, 2003. Rijhsinghani therefore qualifies as prior art to the '177 patent under, at least, (pre-AIA) 35 U.S.C. § 102(a) and/or (b). Rijhsinghani anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) the Asserted Claims of the '177 patent, at least as Dell understands Cloud Byte’s application of the Asserted Claims in an effort to show infringement.

To the extent Cloud Byte argues that any element below is not disclosed by Rijhsinghani, a person of ordinary skill in the art would have found it obvious to combine the teachings of Rijhsinghani with the background knowledge of a person of ordinary skill in the art and/or the additional references, and exemplary teachings, set forth in Dell’s Invalidity Contentions and accompanying charts and/or in Appendix C.

The chart below provides representative examples of where each element of each claim is found within Rijhsinghani. Citations are meant to be exemplary, not exhaustive, and Dell reserves the right to identify and discuss additional portions of the reference in support of its contentions and/or to rebut arguments made by Cloud Byte. Citations to figures, drawings, tables, and the like include reference to any accompanying or related text. All internal cross references are meant to incorporate the cross-referenced material as if fully set forth therein. Where Cloud Byte states that Rijhsinghani “discloses” a limitation, that disclosure may be express, implicit, and/or inherent.

It is Dell’s position that Cloud Byte’s Infringement Contentions have not established that any accused product or service infringes any valid claim. Thus, Dell’s statements below should not be treated as an admission, implication, or suggestion that Dell agrees with Cloud Byte regarding either the scope, construction, or interpretation of any of the Asserted Claims or the infringement theories advanced by Cloud Byte in its Infringement Contentions, including whether any Asserted Claim satisfies 35 U.S.C. §§ 101 or 112. Nothing in this chart is intended to suggest that Dell agrees with Cloud Byte’s application of any claim element, suggest a proposed construction at this stage of the case, or suggest that construction is needed, as the parties are not required to exchange terms for construction or propose claim constructions until a later date.

Cloud Byte has yet to identify any limitation of the Asserted Claims that it contends is not anticipated and/or rendered obvious by Rijhsinghani. Dell therefore expressly reserves the right to respond to any such contention, including by identifying additional obviousness combinations, if Cloud Byte makes any such contention. This chart is subject to all reservations, objections, and disclaimers in Dell’s Invalidity Contentions and any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
[1.pre] 1. A switch apparatus, comprising:	Dell takes no position in these Invalidity Contentions on whether the entirety of the preamble of this claim is a limitation. To the extent it is a limitation, Rijhsinghani discloses, expressly and/or inherently a switch apparatus. <i>See, e.g.:</i> Rijhsinghani at Fig. 1:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

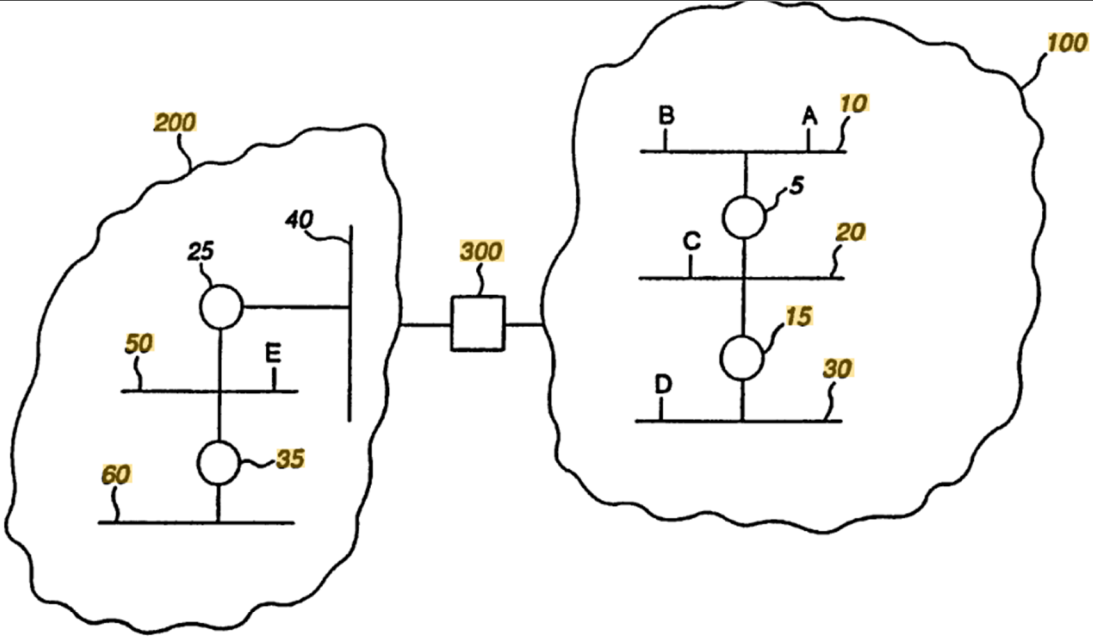
Asserted Claims	Rijhsinghani
	 FIG. 1 Rijhsinghani at 1:20-30: FIG. 1 depicts an exemplary interconnected bridged LAN system. The numerals 10, 20, 30, etc., are used to identify individual LANs Bridges between LANs are designated by the numerals 5, 15, 25 and 35. A router between bridged LAN 100 and bridged LAN 200 is identified with the reference

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	numeral 300. In the bridged LAN system depicted, a user A is able to communicate with a user B without leaving the LAN 10. If user A desires to communicate with user C in LAN 20 or user D in LAN 30, the communication is transmitted via bridges 5 and 15. Rijhsinghani at Fig. 2:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

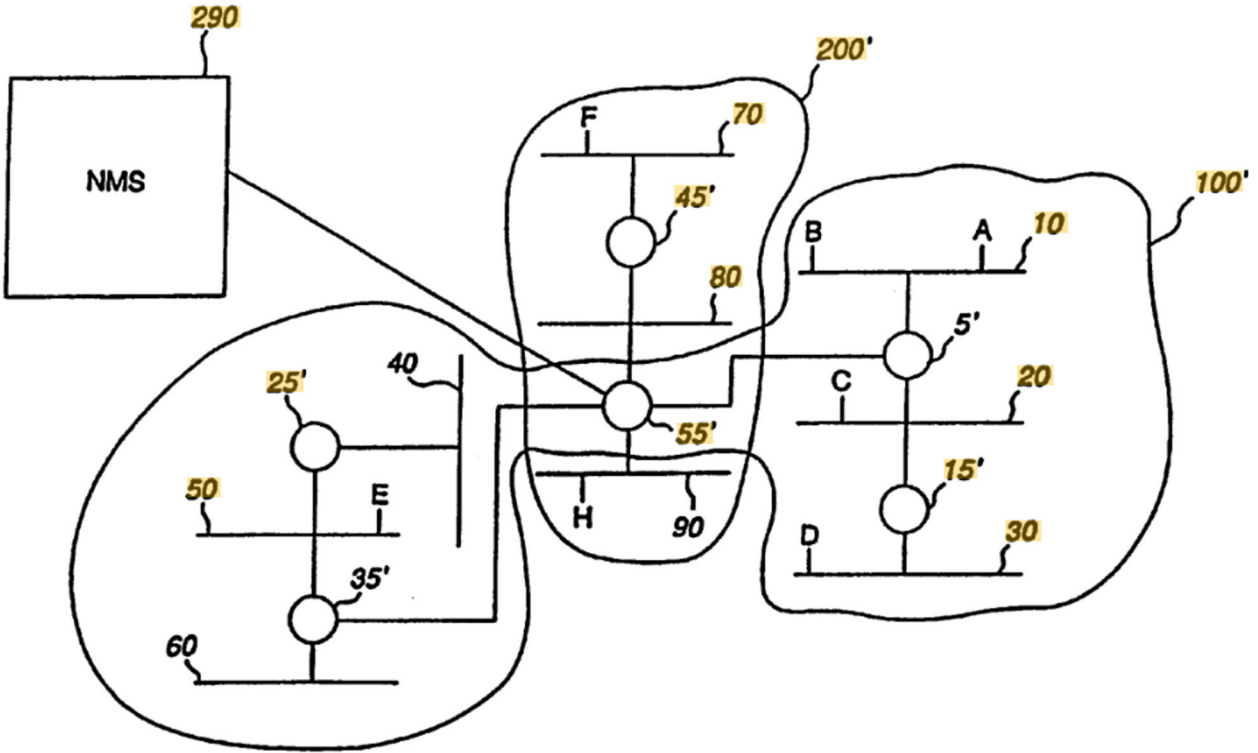
Asserted Claims	Rijhsinghani
	 FIG. 2 Rijhsinghani at 7:25: FIG. 2 depicts a known VLAN configuration;

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

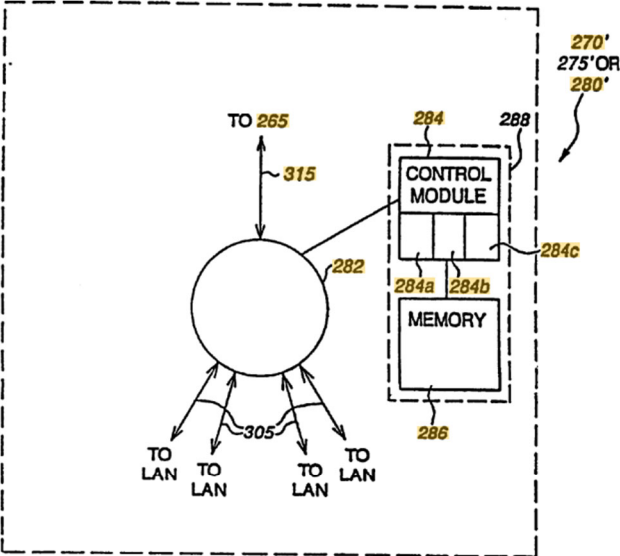
Asserted Claims	Rijhsinghani
	Rijhsinghani at Fig. 8:  FIG. 8

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 7:35-38: FIG. 8 depicts a switch which can be utilized in the VLAN system depicted in FIG. 7 in accordance with the present invention; Rijhsinghani at 2:8-2:56: For example, as shown in FIG. 2, individual LANs 10, 20, 30, 40, 50, 60, 70, 80, 90 (10-90) are interconnected by layer 2 switches 5', 15', 25', 35', 45', (5'-55'). A network management station (NMS) 290 controls the interconnection of the individual LANs such that LANs can be easily bridged to other LANs on a long term or short term basis without the need to rewire the network. As depicted in FIG. 2, the NMS 290 has configured two VLANs by instructing, e.g., programming, and thereby configuring the switches 5'-55' such that LANs 10-60 are bridged together by switches 5', 15', 55', 35' to form VLAN 100' and LANs 70-90 are bridged together by switches 45' and 55' to form VLAN 200'. This is possible because, unlike the bridges 5-35 of FIG. 1, which include only two ports, and accordingly are able to only transfer information from one LAN to another LAN, the switches 5'-55' are multi-ported and programmable by the NMS 290 such that the network can be configured and reconfigured in any desired manner by simply changing the switch instructions. As shown in FIG. 2, the switch 55' has been instructed to transmit communications from user A of LAN 10 to user E of LAN 50, since both users are configured within VLAN 100'. User A, however, is not allowed to communicate with users H or F since these users are not configured within the VLAN 100' user group. This does not, however, prohibit users F and H, both of whom are members of VLAN 200', from communicating with one another via switches 45' and 55'. If it becomes desirable to change the network configuration, this is easily accomplished by issuing commands from NMS 290 to the applicable switches 5'-55'. For example, if desired, user H could be easily added to VLAN 100' by simply reconfiguring VLAN 100' from the NMS 290. The NMS 290 issues an instruction to switch 55', instructing switch 55' to allow communications to flow between

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	users A-D and E and user H via switch 55', i.e., to include LAN 90 in VLAN 100' and remove it from VLAN 200'. Because the switches 5'-55' are layer 2 switches, a bridge formed by the switch is transparent to the users within the VLAN. Hence, the transmission delays normally associated with routers, such as the router 300 of FIG. 1, are avoided. The flexibility of the VLAN lies in its' ability to have its' network configuration controlled through software on the NMS 290. More particularly, in accordance with its' programmed instructions, the NMS 290 generates and transmits signals to instruct the switches 5'-55' to form the desired VLAN configurations. Rijhsinghani at 6:25-7:15: Accordingly, the present invention provides rules of precedence for directing communications within different types of VLANs, in order to provide for predictable and desirable network behavior when there are areas of the network in which there is overlap in VLAN configurations, and to allow conflict resolutions by switches in the VLAN system. Advantageously, switches are provided that route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, based upon predefined rules of precedence. Advantageously, switches route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, in a secure manner. Physical security is ensured by giving a higher precedence to port-based VLAN classifications than to other types of VLAN classifications. In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-ported reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g. a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (I) the port and protocol-based virtual networks precedence over the port-based virtual networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks. Typically, the communication will include at least a source address and a protocol identifier, which the switch control detects, along with the port at which the communication is received, to identify the VLAN. After the VLAN has been identified, the switch control adds a VLAN tag representing the identified VLAN to form a VLAN communication. The switch control then directs the VLAN communication to the second communication port for transmission over the identified virtual local area network. In accordance with other aspects of the invention, a virtual communications system can be implemented using multiple switches of the type described above. A network manager, interconnected to the multiple switches, is capable of configuring virtual local area networks of differing types a described above. Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305.
[1.a] a storage storing a table, the table including	Rijhsinghani discloses, expressly and/or inherently, a storage storing a table, the table including rules and actions corresponding to the rules.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
rules and actions corresponding to the rules; and	<i>See, e.g.:</i> Rijhsinghani at 1:20-30: FIG. 1 depicts an exemplary interconnected bridged LAN system. The numerals 10, 20, 30, etc., are used to identify individual LANs. Bridges between LANs are designated by the numerals 5, 15, 25 and 35. A router between bridged LAN 100 and bridged LAN 200 is identified with the reference numeral 300. In the bridged LAN system depicted, a user A is able to communicate with a user B without leaving the LAN 10. If user A desires to communicate with user C in LAN 20 or user D in LAN 30, the communication is transmitted via bridges 5 and 15. Rijhsinghani at 2:8-2:56: For example, as shown in FIG. 2, individual LANs 10, 20, 30, 40, 50, 60, 70, 80, 90 (10-90) are interconnected by layer 2 switches 5', 15', 25', 35', 45', (5'-55'). A network management station (NMS) 290 controls the interconnection of the individual LANs such that LANs can be easily bridged to other LANs on a long term or short term basis without the need to rewire the network. As depicted in FIG. 2, the NMS 290 has configured two VLANs by instructing, e.g., programming, and thereby configuring the switches 5'-55' such that LANs 10-60 are bridged together by switches 5', 15', 55', 35' to form VLAN 100' and LANs 70-90 are bridged together by switches 45' and 55' to form VLAN 200'. This is possible because, unlike the bridges 5-35 of FIG. 1, which include only two ports, and accordingly are able to only transfer information from one LAN to another LAN, the switches 5'-55' are multi-ported and programmable by the NMS 290 such that the network can be configured and reconfigured in any desired manner by simply changing the switch instructions. As shown in FIG. 2, the switch 55' has been instructed to transmit communications from user A of LAN 10 to user E of LAN 50, since both users are configured within VLAN 100'. User A, however, is not allowed to communicate with users H or F since these users are not configured within the

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	VLAN 100' user group. This does not, however, prohibit users F and H, both of whom are members of VLAN 200', from communicating with one another via switches 45' and 55'. If it becomes desirable to change the network configuration, this is easily accomplished by issuing commands from NMS 290 to the applicable switches 5'-55'. For example, if desired, user H could be easily added to VLAN 100' by simply reconfiguring VLAN 100' from the NMS 290. The NMS 290 issues an instruction to switch 55', instructing switch 55' to allow communications to flow between users A-D and E and user H via switch 55', i.e., to include LAN 90 in VLAN 100' and remove it from VLAN 200'. Because the switches 5'-55' are layer 2 switches, a bridge formed by the switch is transparent to the users within the VLAN. Hence, the transmission delays normally associated with routers, such as the router 300 of FIG. 1, are avoided. The flexibility of the VLAN lies in its' ability to have its' network configuration controlled through software on the NMS 290. More particularly, in accordance with its' programmed instructions, the NMS 290 generates and transmits signals to instruct the switches 5'-55' to form the desired VLAN configurations. Rijhsinghani at 6:25-7:15: Accordingly, the present invention provides rules of precedence for directing communications within different types of VLANs, in order to provide for predictable and desirable network behavior when there are areas of the network in which there is overlap in VLAN configurations, and to allow conflict resolutions by switches in the VLAN system. Advantageously, switches are provided that route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, based upon predefined rules of precedence. Advantageously, switches route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, in a secure manner. Physical security is ensured by giving a higher precedence to port-based VLAN classifications than to other types of VLAN classifications. In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-portable reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g. a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (I) the port and protocol-based virtual networks precedence over the port-based virtual networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks. Typically, the communication will include at least a source address and a protocol identifier, which the switch control detects, along with the port at which the communication is received, to identify the VLAN. After the VLAN has been identified, the switch control adds a VLAN tag representing the identified VLAN to form a VLAN Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 11:11-40:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	For example, referring to FIG. 9, the following steps would be performed at switch 275' when a system user at address U on LAN 240 transmits a communication packet with a protocol identifier for P1 addressed to a system user at address L on LAN 220, and the system is programmed to identify packets with a protocol identifier for protocol P1 with protocol-based VLAN 1000. First, switch 275' receives the packet at an access port 305. Second, detector 284 b of the control module 288 of switch 275' detects the receive port, the source address U of the packet, and the protocol identifier for P1 of the packet. Third, the control module 288 of switch 275', in accordance with the programmed instructions stored on the memory 286, determines five VLAN matches. Specifically, the control module determines that the packet may be appropriately associated with port-based VLAN 800 because the receive port at which LAN 240 is connected is a member of VLAN 800, the packet may be appropriately associated with address-based VLAN 900 because the source address U is a member of VLAN 900, the packet may be appropriately associated with protocol-based VLAN 1000 because the protocol identifier of the packet is for P1, the packet may be appropriately associated with port and protocol-based VLAN 1100 because the receive port at which LAN 240 is connected is a member of VLAN 1100 when the protocol identifier of the packet is for P1, and the packet may be appropriately associated with address and protocol-based VLAN 1200 because the source address U is a member of VLAN 1200 when the protocol identifier of the packet is for P1.
[1.b] a controller comprising:	Rijhsinghani discloses, expressly and/or inherently, a controller. <i>See, e.g.:</i> Rijhsinghani at Fig. 8:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

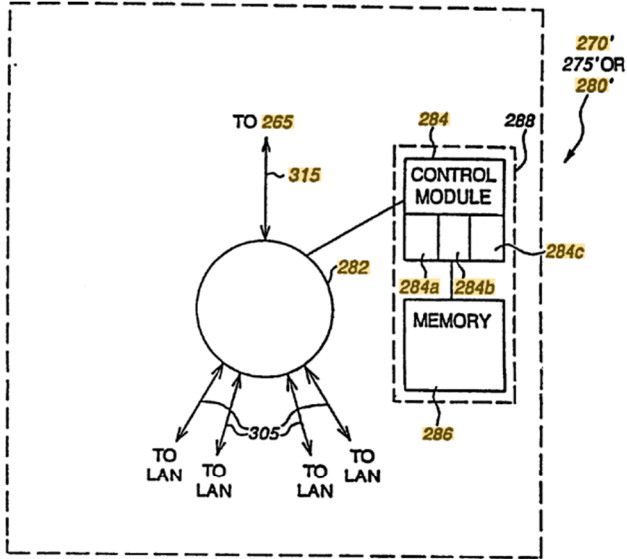
Asserted Claims	Rijhsinghani
	 FIG. 8 Rijhsinghani at 7:35-38:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 depicts a switch which can be utilized in the VLAN system depicted in FIG. 7 in accordance with the present invention; Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 8:41-9:22: The detector 284 b of a switch detects all communications over the backbone LAN 265, which the control module 284 handles in the following manner. If a detected communication is deliverable to a network addressee on any of the LANs connected to an access port of the applicable switch, the controller 284 a of the applicable switch controls the switching device 282 to transmit the communication from the trunk port 315 to the applicable access port 305. More specifically, if the detected communication is properly addressed to the addressee and forwarded from an authorized member of the system, the controller 284 a of the applicable switch controls the switching device 282 to transmit the message to the applicable LAN. An authorized member is a member of the VLAN that includes the addressee. In the case where the addressee is a member of the default group, however, an authorized member is any other member of the system because the member is not a member of any VLAN. The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. If the detected communication has been received via an access port 305 of the switch and is properly addressed and deliverable to a network addressee on any of the other LANs connected to the switch, the controller 284 a of the switch controls the switching device 282 to transmit the message from the input access port 305 to the applicable output access port 305. In such a case, where the sender and addressee are each members of a LAN connected to the same switch, there is no need to add a VLAN header to the communication before directing it to output port 305. However, if such a communication is to be multicast transmitted to one or more LANs within the applicable VLAN that are directly connected to other switches by access ports, the communication output from the trunk port 315 of the applicable switch will, of course, be tagged by the tagger before transmission via the trunk 265 as discussed above. Rijhsinghani at 10:55-63: In step 1320, the control module 288, in accordance with the programmed instructions stored in the memory 286, determines one or more VLAN matches, i.e. determines one or more VLANs with which the communication may be appropriately associated. Depending on the instruction, this determination may be based upon the receive port and protocol considered jointly, the receive port, the source address and protocol considered jointly, the address, and the protocol.
[1.c] a memory storing instructions; and	Rijhsinghani discloses, expressly and/or inherently, a memory storing instructions. <i>See, e.g.:</i> Rijhsinghani at Fig. 8:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 Rijhsinghani at 7:35-38:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 depicts a switch which can be utilized in the VLAN system depicted in FIG. 7 in accordance with the present invention; Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 9:30-45: The NMS 290' is capable of configuring VLANs of differing types. More particularly, the NMS 290' can configure or define VLANs which are port-based, address-based, protocol-based, port and protocol-based, and address and protocol-based. The NMS 290' instructs the switches 270'-280' as to the configurations of the different types of VLANs. Each of the switches 270'-280' is programmed to consider the applicable characteristics of each communication received, via an access port, in order to determine the appropriate VLAN tag to add to the communication before transmission via the trunk port 315 to the high speed LAN backbone or trunk 265. These instructions may be stored in the memory 286 of the switch, as depicted in FIG. 8, and utilized by the switch control module 284 in determining which tag to add to a communication received at an access port 305. Rijhsinghani at 10:55-63: In step 1320, the control module 288, in accordance with the programmed instructions stored in the memory 286, determines one or more VLAN matches, i.e. determines one or more VLANs with which the communication may be appropriately associated. Depending on the instruction, this

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	determination may be based upon the receive port and protocol considered jointly, the receive port, the source address and protocol considered jointly, the address, and the protocol. Rijhsinghani at 11:11-40: For example, referring to FIG. 9, the following steps would be performed at switch 275' when a system user at address U on LAN 240 transmits a communication packet with a protocol identifier for P1 addressed to a system user at address L on LAN 220, and the system is programmed to identify packets with a protocol identifier for protocol P1 with protocol-based VLAN 1000. First, switch 275' receives the packet at an access port 305. Second, detector 284 b of the control module 288 of switch 275' detects the receive port, the source address U of the packet, and the protocol identifier for P1 of the packet. Third, the control module 288 of switch 275', in accordance with the programmed instructions stored on the memory 286, determines five VLAN matches. Specifically, the control module determines that the packet may be appropriately associated with port-based VLAN 800 because the receive port at which LAN 240 is connected is a member of VLAN 800, the packet may be appropriately associated with address-based VLAN 900 because the source address U is a member of VLAN 900, the packet may be appropriately associated with protocol-based VLAN 1000 because the protocol identifier of the packet is for P1, the packet may be appropriately associated with port and protocol-based VLAN 1100 because the receive port at which LAN 240 is connected is a member of VLAN 1100 when the protocol identifier of the packet is for P1, and the packet may be appropriately associated with address and protocol-based VLAN 1200 because the source address U is a member of VLAN 1200 when the protocol identifier of the packet is for P1.
[1.d] a processor configured to execute the instructions to:	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute instructions. <i>See, e.g.:</i> Rijhsinghani at Fig. 8:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 Rijhsinghani at 7:35-38:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 depicts a switch which can be utilized in the VLAN system depicted in FIG. 7 in accordance with the present invention; Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 8:41-9:22: The detector 284 b of a switch detects all communications over the backbone LAN 265, which the control module 284 handles in the following manner. If a detected communication is deliverable to a network addressee on any of the LANs connected to an access port of the applicable switch, the controller 284 a of the applicable switch controls the switching device 282 to transmit the communication from the trunk port 315 to the applicable access port 305. More specifically, if the detected communication is properly addressed to the addressee and forwarded from an authorized member of the system, the controller 284 a of the applicable switch controls the switching device 282 to transmit the message to the applicable LAN. An authorized member is a member of the VLAN that includes the addressee. In the case where the addressee is a member of the default group, however, an authorized member is any other member of the system because the member is not a member of any VLAN. The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. If the detected communication has been received via an access port 305 of the switch and is properly addressed and deliverable to a network addressee on any of the other LANs connected to the switch, the controller 284 a of the switch controls the switching device 282 to transmit the message from the input access port 305 to the applicable output access port 305. In such a case, where the sender and addressee are each members of a LAN connected to the same switch, there is no need to add a VLAN header to the communication before directing it to output port 305. However, if such a communication is to be multicast transmitted to one or more LANs within the applicable VLAN that are directly connected to other switches by access ports, the communication output from the trunk port 315 of the applicable switch will, of course, be tagged by the tagger before transmission via the trunk 265 as discussed above. Rijhsinghani at 9:30-45: The NMS 290' is capable of configuring VLANs of differing types. More particularly, the NMS 290' can configure or define VLANs which are port-based, address-based, protocol-based, port and protocol-based, and address and protocol-based. The NMS 290' instructs the switches 270'-280' as to the configurations of the different types of VLANs. Each of the switches 270'-280' is programmed to consider the applicable characteristics of each communication received, via an access port, in order to determine the appropriate VLAN tag to add to the communication before transmission via the trunk port 315 to the high speed LAN backbone or trunk 265. These instructions may be stored in the memory 286 of the switch, as depicted in FIG. 8, and utilized by the switch control module 284 in determining which tag to add to a communication received at an access port 305. Rijhsinghani at 10:55-63: In step 1320, the control module 288, in accordance with the programmed instructions stored in the memory 286, determines one or more VLAN matches, i.e. determines one or more VLANs with

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	which the communication may be appropriately associated. Depending on the instruction, this determination may be based upon the receive port and protocol considered jointly, the receive port, the source address and protocol considered jointly, the address, and the protocol. Rijhsinghani at 11:11-40: For example, referring to FIG. 9, the following steps would be performed at switch 275' when a system user at address U on LAN 240 transmits a communication packet with a protocol identifier for P1 addressed to a system user at address L on LAN 220, and the system is programmed to identify packets with a protocol identifier for protocol P1 with protocol-based VLAN 1000. First, switch 275' receives the packet at an access port 305. Second, detector 284 b of the control module 288 of switch 275' detects the receive port, the source address U of the packet, and the protocol identifier for P1 of the packet. Third, the control module 288 of switch 275', in accordance with the programmed instructions stored on the memory 286, determines five VLAN matches. Specifically, the control module determines that the packet may be appropriately associated with port-based VLAN 800 because the receive port at which LAN 240 is connected is a member of VLAN 800, the packet may be appropriately associated with address-based VLAN 900 because the source address U is a member of VLAN 900, the packet may be appropriately associated with protocol-based VLAN 1000 because the protocol identifier of the packet is for P1, the packet may be appropriately associated with port and protocol-based VLAN 1100 because the receive port at which LAN 240 is connected is a member of VLAN 1100 when the protocol identifier of the packet is for P1, and the packet may be appropriately associated with address and protocol-based VLAN 1200 because the source address U is a member of VLAN 1200 when the protocol identifier of the packet is for P1.
[1.e] receive the rules and the actions from a control apparatus;	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute instructions to receive the rules and the actions from a control apparatus. <i>See, e.g.:</i> Rijhsinghani at Fig. 2:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

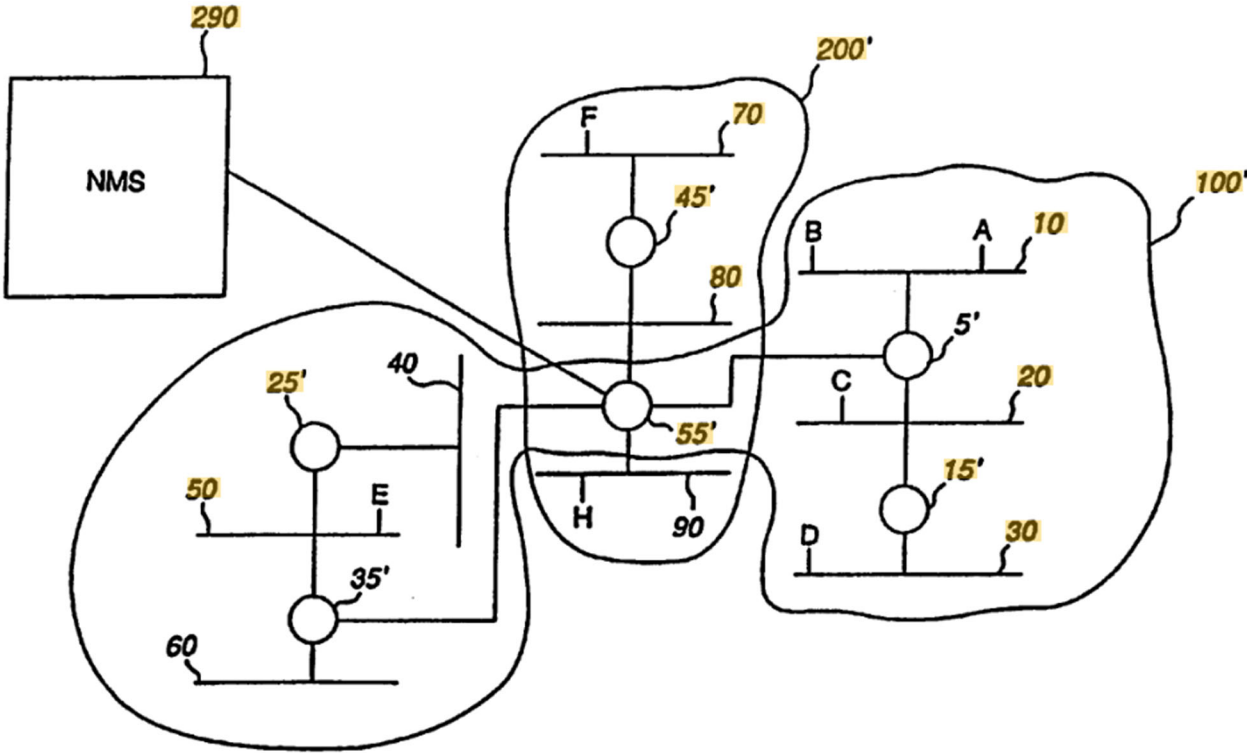
Asserted Claims	Rijhsinghani
	 FIG. 2 Rijhsinghani at 7:25: FIG. 2 depicts a known VLAN configuration;

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

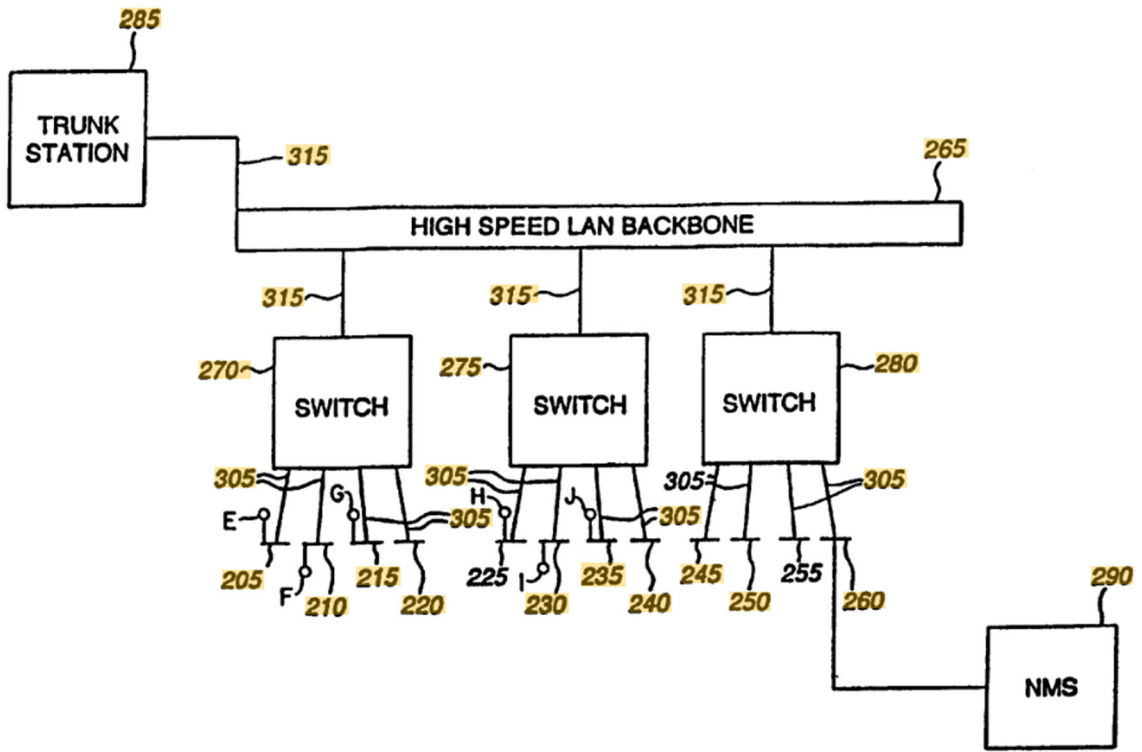
Asserted Claims	Rijhsinghani
	Rijhsinghani at Fig. 5:  FIG. 5

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

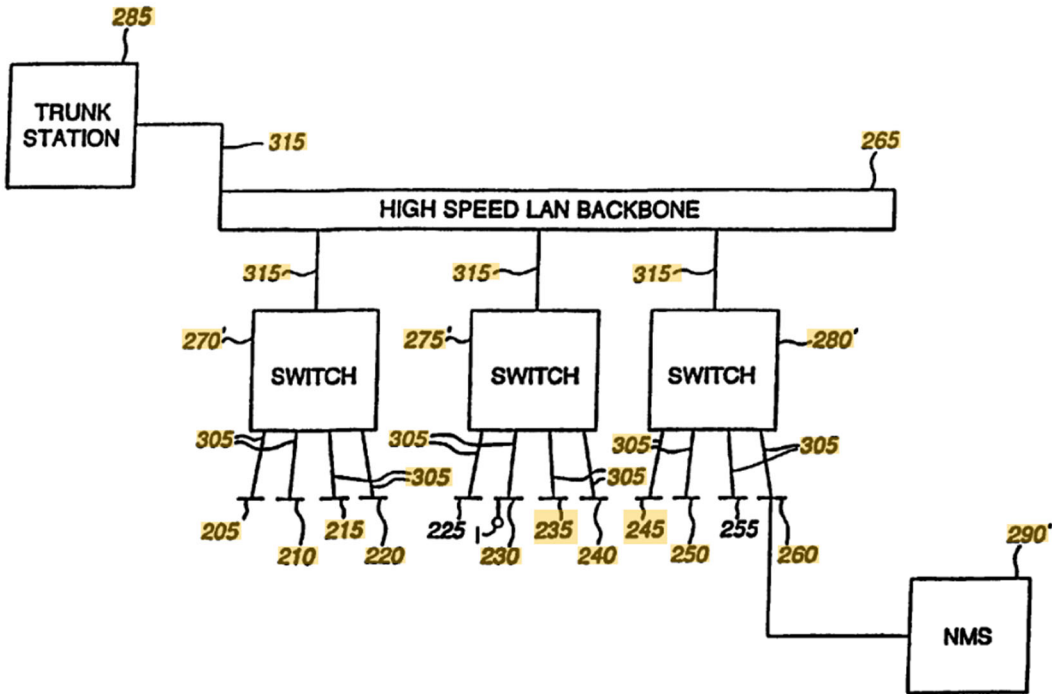
Asserted Claims	Rijhsinghani
	Rijhsinghani at 7:29-30: FIG. 5 depicts a schematic diagram of a conventional VLAN system; Rijhsinghani at Fig. 7:  FIG. 7 Rijhsinghani at 7:33-34

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 7 depicts a VLAN system in accordance with the present invention; Rijhsinghani at 2:8-26: For example, as shown in FIG. 2, individual LANs 10, 20, 30, 40, 50, 60, 70, 80, 90 (10-90) are interconnected by layer 2 switches 5', 15', 25', 35', 45', (5'-55'). A network management station (NMS) 290 controls the interconnection of the individual LANs such that LANs can be easily bridged to other LANs on a long term or short term basis without the need to rewire the network. As depicted in FIG. 2, the NMS 290 has configured two VLANs by instructing, e.g., programming, and thereby configuring the switches 5'-55' such that LANs 10-60 are bridged together by switches 5', 15', 55', 35' to form VLAN 100' and LANs 70-90 are bridged together by switches 45' and 55' to form VLAN 200'. This is possible because, unlike the bridges 5-35 of FIG. 1, which include only two ports, and accordingly are able to only transfer information from one LAN to another LAN, the switches 5'-55' are multi-ported and programmable by the NMS 290 such that the network can be configured and reconfigured in any desired manner by simply changing the switch instructions. Rijhsinghani at 2:36-56: If it becomes desirable to change the network configuration, this is easily accomplished by issuing commands from NMS 290 to the applicable switches 5'-55'. For example, if desired, user H could be easily added to VLAN 100' by simply reconfiguring VLAN 100' from the NMS 290. The NMS 290 issues an instruction to switch 55', instructing switch 55' to allow communications to flow between users A-D and E and user H via switch 55', i.e., to include LAN 90 in VLAN 100' and remove it from VLAN 200'. Because the switches 5'-55' are layer 2 switches, a bridge formed by the switch is transparent to the users within the VLAN. Hence, the transmission delays normally associated with routers, such as the router 300 of FIG. 1, are avoided. The flexibility of the VLAN lies in its' ability to have its' network configuration controlled through software on the NMS 290. More particularly, in accordance with its'

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	programmed instructions, the NMS 290 generates and transmits signals to instruct the switches 5'-55' to form the desired VLAN configurations. Rijhsinghani at 2:62-3:22: FIG. 5 is a schematic of a conventional VLAN system. The VLAN system includes LANs 205-260 which are connected by switches 270-280 to a high-speed LAN backbone or trunk 265. An NMS 290 is interconnected to the switches 270-280 via LAN 260. The NMS 290 is interconnected via LAN 260 as an example and could be interconnected to switches 270-280 via any of the LANs 205-260. A trunk station 285 is connected to the high-speed LAN backbone 265 via a trunk port 315. The LANs 205-215, and 230-235 have designated members F-J. LANs connect to each of the switches 270-280 by a plurality of access ports 305. For example, switch 270 is connected via access ports 305 to LANs 205-220. Each switch is capable of interconnecting a LAN connected via an access port 305 with another LAN connected via an access port 305. For example, switch 270 can be instructed by the NMS 290 to interconnect LAN 205 to LAN 215 by configuring a VLAN including LANs 205 and 215, thereby enabling communications between members F and H. Each switch is also capable of interconnecting a LAN connected by an access port 305 with a LAN connected to another switch by an access port 305 via high-speed LAN backbone 265. For example, Switches 270 and 275 can be instructed by the NMS 290 to interconnect LANs 205 and 230 by configuring a VLAN including LANs 205 and 230, thereby enabling communications between member E of LAN 205 and member I of LAN 230. Rijhsinghani at 3:34-44: For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received. For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V,

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 7:49-8:5: FIG. 7 depicts a virtual communications system or network in accordance with the present invention. The network includes multiple Local Area Networks (LANs) 205-260 interconnected by multiple multi-ported reconfigurable switches 270', 275' and 280' all of which are connected by a high speed backbone LAN 265, often referred to as the trunk. Each LAN, other than the backbone LAN 265 is connected to one of the switches 270', 275' or 280' by an access port 305, while the backbone LAN 265 is connected to each switch by a trunk port 315. A network management station (NMS) 290', which may be a workstation having network management software loaded thereon, manages the network by configuring the network via the switches 270', 275' and 280' to form one or more virtual local area networks (VLANs). A trunk station 285 is connected to the backbone LAN 265 via a trunk port 315. The trunk stations 285 may, for example, be a network server or other network resource to which some or all of the members of the LANs 205-260 may require high speed access from time to time or on a continuous basis as is known in the art. Each of the switches 270', 275' and 280' is capable of linking, via the backbone LAN 265, members of each of the LANs 205-260 to members of the one or more other LANs within the VLANs configured by the NMS 290'. Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 8:34-40: For the network depicted in FIG. 8, communications from NMS 290' are detected differently. The detectors 284 b of switches 270' and 275' detect communications from NMS 290' via the backbone LAN 265 at a trunk port 315, while the detector 284 b of switch 280' detects communications from the NMS 290' at the access port 305 connected to LAN 260. Rijhsinghani at 8:41-9:22: The detector 284 b of a switch detects all communications over the backbone LAN 265, which the control module 284 handles in the following manner. If a detected communication is deliverable to a network addressee on any of the LANs connected to an access port of the applicable switch, the controller 284 a of the applicable switch controls the switching device 282 to transmit the communication from the trunk port 315 to the applicable access port 305. More specifically, if the detected communication is properly addressed to the addressee and forwarded from an authorized member of the system, the controller 284 a of the applicable switch controls the switching device 282 to transmit the message to the applicable LAN. An authorized member is a member of the VLAN that includes the addressee. In the case where the addressee is a member of the default group, however, an authorized member is any other member of the system because the member is not a member of any VLAN. The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. If the detected communication has been received via an access port 305 of the switch and is properly addressed and deliverable to a network addressee on any of the other LANs connected to the switch, the controller 284 a of the switch controls the switching device 282 to transmit the message from the input access port 305 to the applicable output access port 305. In such a case, where the sender and addressee are each members of a LAN connected to the same switch, there is no need to add a VLAN header to the communication before directing it to output port 305. However, if such a communication is to be multicast transmitted to one or more LANs within the applicable VLAN that are directly connected to other switches by access ports, the communication output from the trunk port 315 of the applicable switch will, of course, be tagged by the tagger before transmission via the trunk 265 as discussed above. Rijhsinghani at 9:30-45: The NMS 290' is capable of configuring VLANs of differing types. More particularly, the NMS 290' can configure or define VLANs which are port-based, address-based, protocol-based, port and protocol-based, and address and protocol-based. The NMS 290' instructs the switches 270'-280' as to the configurations of the different types of VLANs. Each of the switches 270'-280' is programmed to consider the applicable characteristics of each communication received, via an access port, in order to determine the appropriate VLAN tag to add to the communication before transmission via the trunk port 315 to the high speed LAN backbone or trunk 265. These instructions may be stored in the memory 286 of the switch, as depicted in FIG. 8, and utilized by the switch control module 284 in determining which tag to add to a communication received at an access port 305. Rijhsinghani at 10:55-63: In step 1320, the control module 288, in accordance with the programmed instructions stored in the memory 286, determines one or more VLAN matches, i.e. determines one or more VLANs with which the communication may be appropriately associated. Depending on the instruction, this

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	determination may be based upon the receive port and protocol considered jointly, the receive port, the source address and protocol considered jointly, the address, and the protocol. Rijhsinghani at 11:11-40: For example, referring to FIG. 9, the following steps would be performed at switch 275' when a system user at address U on LAN 240 transmits a communication packet with a protocol identifier for P1 addressed to a system user at address L on LAN 220, and the system is programmed to identify packets with a protocol identifier for protocol P1 with protocol-based VLAN 1000. First, switch 275' receives the packet at an access port 305. Second, detector 284 b of the control module 288 of switch 275' detects the receive port, the source address U of the packet, and the protocol identifier for P1 of the packet. Third, the control module 288 of switch 275', in accordance with the programmed instructions stored on the memory 286, determines five VLAN matches. Specifically, the control module determines that the packet may be appropriately associated with port-based VLAN 800 because the receive port at which LAN 240 is connected is a member of VLAN 800, the packet may be appropriately associated with address-based VLAN 900 because the source address U is a member of VLAN 900, the packet may be appropriately associated with protocol-based VLAN 1000 because the protocol identifier of the packet is for P1, the packet may be appropriately associated with port and protocol-based VLAN 1100 because the receive port at which LAN 240 is connected is a member of VLAN 1100 when the protocol identifier of the packet is for P1, and the packet may be appropriately associated with address and protocol-based VLAN 1200 because the source address U is a member of VLAN 1200 when the protocol identifier of the packet is for P1.
[1.f] identify, based on the rules, a received packet;	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute instructions to identify, based on the rules, a received packet. <i>See, e.g.:</i> Rijhsinghani at Fig. 10:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

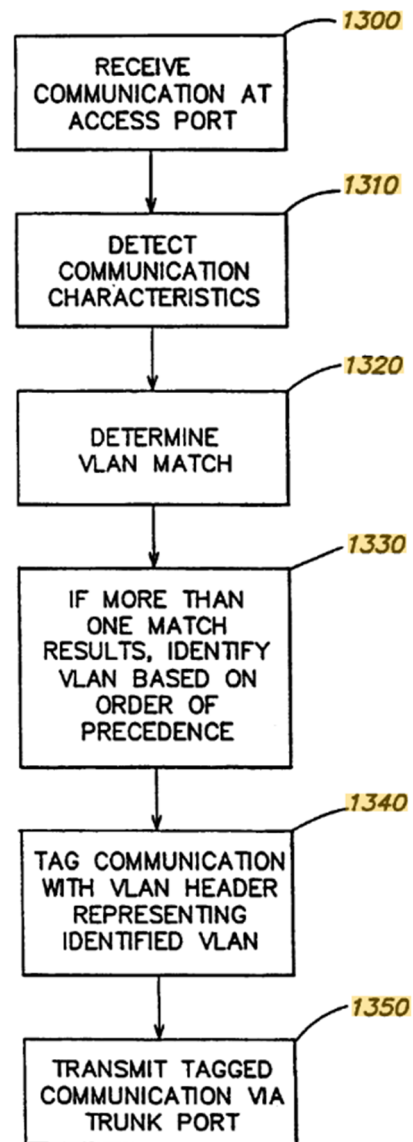


FIG. 10

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 7:41-43: FIG. 10 is a flow chart of the steps performed by the switch depicted in FIG. 8 in accordance with the present invention; and Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received. For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 6:25-7:15: Accordingly, the present invention provides rules of precedence for directing communications within different types of VLANs, in order to provide for predictable and desirable network behavior when there are areas of the network in which there is overlap in VLAN configurations, and to allow conflict resolutions by switches in the VLAN system. Advantageously, switches are provided that route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, based upon predefined rules of precedence. Advantageously, switches route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, in a secure manner. Physical security is ensured by giving a higher precedence to port-based VLAN classifications than to other types of VLAN classifications. In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-ported reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (I) the port and protocol-based virtual networks precedence over the port-based virtual networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks. Typically, the communication will include at least a source address and a protocol identifier, which the switch control detects, along with the port at which the communication is received, to identify the VLAN. After the VLAN has been identified, the switch control adds a VLAN tag representing the identified VLAN to form a VLAN communication. The switch control then directs the VLAN communication to the second communication port for transmission over the identified virtual local area network. In accordance with other aspects of the invention, a virtual communications system can be implemented using multiple switches of the type described above. A network manager, interconnected to the multiple switches, is capable of configuring virtual local area networks of differing types a described above. Rijhsinghani at 10:64-11:4: In step 1330, in the case of more than one VLAN match, the applicable switch 270'-280' identifies which of the VLAN type matches has the highest priority based upon the order of precedence described above, i.e., port and protocol-based over port-based, port-based over address and protocol-based, address and protocol-based over address-based, and address-based over protocol-based, as shown in FIG. 11.
[1.g] duplicate a part of a header of the identified packet as an additional	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute instructions to duplicate a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
header when the identified packet comprises a target of encapsulation;	<i>See, e.g.:</i> Rijhsinghani at Fig. 3:

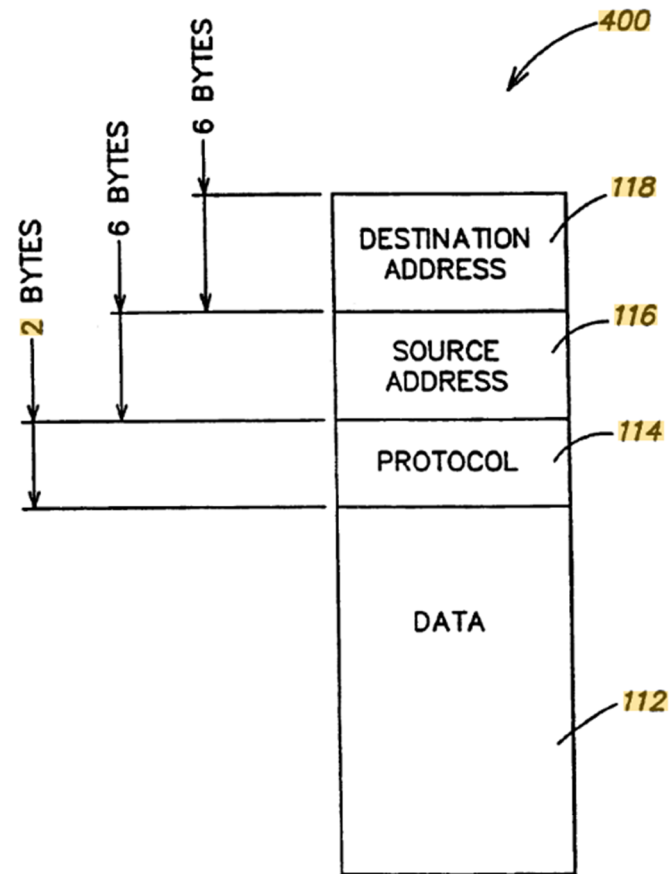


FIG. 3

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at Fig. 4:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

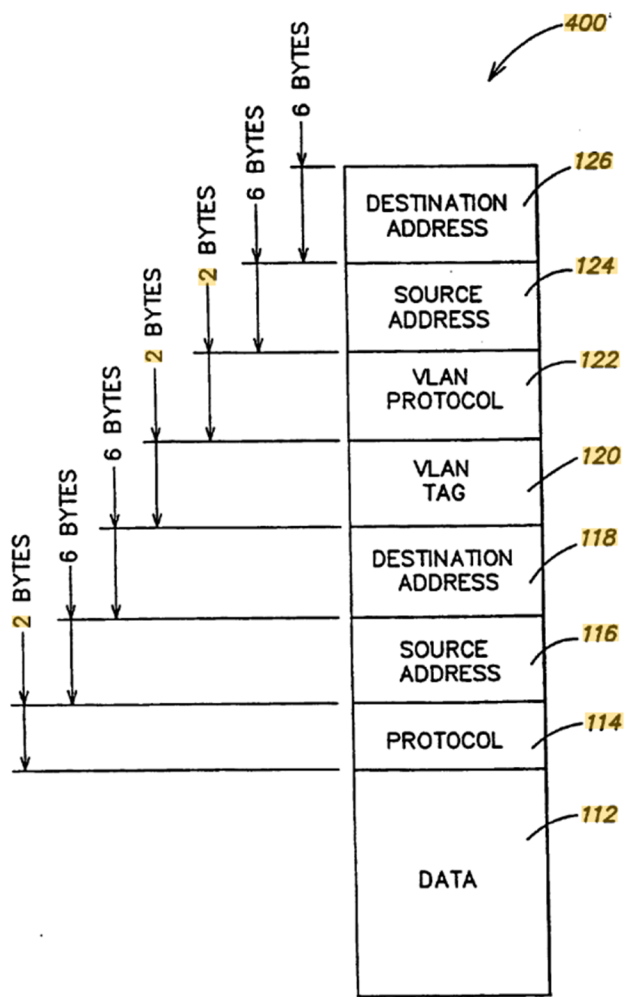
Asserted Claims	Rijhsinghani
	 FIG. 4

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at Fig. 10:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

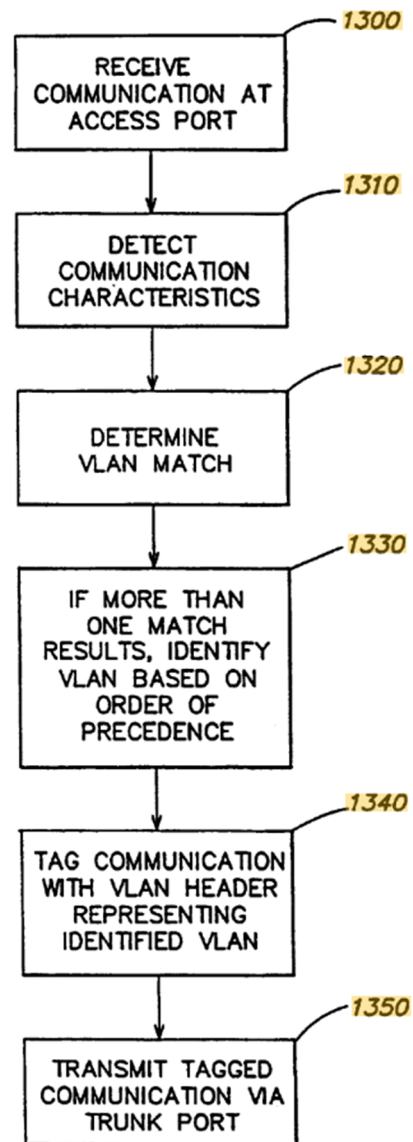


FIG. 10

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 7:41-43: FIG. 10 is a flow chart of the steps performed by the switch depicted in FIG. 8 in accordance with the present invention; and Rijhsinghani at 3:22-67: FIG. 4 depicts a VLAN communications packet 400' which is similar to the LAN communications packet 400 depicted in FIG. 3, except that a VLAN header has been added to the packet. The VLAN header is added by the initial switch to which the message packet is directed. The VLAN header identifies the resulting packet as a "VLAN" or "tagged" packet, and represents the particular VLAN from which the packet originated. The VLAN header, as shown, includes a destination address 126 which is the same address as the destination address 118, a source address 124 which is the same as source address 116, a protocol identifier 122, and a VLAN tag 120 identifying the applicable VLAN. For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet 400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Because switch 280 lacks any access ports connected to LANs within the applicable VLAN, switch 280 discards the packet 400'. Switch 275, however, identifies the VLAN header of packet 400' as associated with a VLAN which includes LAN 230. The switch 275 accordingly removes the VLAN header and directs the packet, which now appears as packet 400 of FIG. 3, to LAN 230 over which the member I receives the message. Many trunk stations, such as trunk station 285, are incapable of recognizing VLAN headers. Further, since no programmable switch is disposed between a trunk station and the trunk, communications, i.e. packets, with a VLAN header will be ignored and/or discarded by the trunk station. Hence, in a

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	conventional VLAN system, such as that shown in FIG. 5, the trunk stations, e.g., trunk station 285, form part of a default group. The default group is a group of system users or end stations not within any VLAN. For a communication packet sent by a system user within the default group, the initial switch to which the packet is directed determines that the system user does not fall within any VLAN, and consequently does not add a VLAN header. Rijhsinghani at 5:13-54: In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200. In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100. Although it is known to configure different types of VLANs within a VLAN system based upon characteristics such as those previously described, problems arise in attempting to implement such systems. More particularly, under certain circumstances, overlap of VLANs may occur such as depicted in FIG. 6. Overlap occurs when a communication packet received at a switch can be

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	identified with more than one VLAN. When overlap occurs, a switch may become confused as to which VLAN of multiple VLANs of different types should be identified for transmission of a received communication. Consequently, the switch will be confused as to which VLAN header should be added to the communication. Rijhsinghani at 8:60-9:6: The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. Rijhsinghani at 9:23-29: Accordingly, all communications between LANs within configured VLANs are forwarded to the appropriate addressee LAN. This is accomplished by identifying communications between LANs within configured VLANs and tagging the communications, except for those between LANs connected by an access port to the same switch, with a VLAN header. Rijhsinghani at 9:46-10:34: Each of the switches 270'-280' is programmed to utilize an order of precedence to identify with certainty the appropriate VLAN for transmission of the received communication. More particularly, each of the switches 270'-280' is programmed so as to operate to tag the communication with the VLAN header, i.e., the VLAN tag, representing the VLAN which is port and protocol-based over any other VLAN. Hence, if a communication received from one of the LANs is identified as potentially

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	associated with a port and protocol-based or other type of VLAN, the switch will give precedence to the port and protocol-based VLAN over the other possible associated VLANs. For example, referring to FIG. 9, if the switch 280' receives a communication with a protocol identifier for protocol P1 from a user on LAN 250, the switch identifies the communication as being associated with both a port and protocol-based and protocol-based VLAN. The switch 280', in accordance with the order of precedence established by its programmed instructions, will identify the communication as being associated with the port and protocol-based VLAN 1100, rather than with the protocol-based VLAN 1000, and will, accordingly, tag the communication with a VLAN header representing VLAN 1100. Each of the switches 270'-280' is further programmed to give precedence to an identification of a possible association with a port-based VLAN over all other types of VLANs except port and protocol-based VLANs. For example, if switch 270' receives a communication at an access port 305 from LAN 215 that includes a source address within address-based VLAN 900, e.g., address V, the switch 270' will give precedence to the fact that the communication was received at a port 305 configured within port-based VLAN 800 and will tag the communication with a VLAN header representing VLAN 800 rather than VLAN 900. It will be recognized by those skilled in the art that establishing port and protocol-based VLANs, as well as just port-based VLANs, at the highest levels within the order of precedence not only ensures that the communication is transmitted via the correct VLAN, but also enhances security because protocol-based and address-based VLANs are inherently less secure than port-based VLANs. The switches 270'-280' are further programmed such that address and protocol-based VLANs are given precedence over address-based VLANs and protocol-based VLANs. For example, if switch 280' receives a communication at an access port 305 from a system user at address T of LAN 260, and the communication has an identified protocol corresponding to the protocol associated with protocol-based LAN 1000, P1, the switch 280' will prioritize and give precedence to the correspondence of the communication to the address and protocol-based VLAN 1200 over address-based VLAN 900 and protocol-based VLAN 1000. Accordingly, switch 280' will tag the communication with the VLAN header representing VLAN 1200. Rijhsinghani at 11:5-10:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	In step 1340, the communication is tagged with the VLAN header representing the highest priority identified VLAN. In step 1350, the tagged communication is transmitted via the trunk port 315 from the switch and from there forwarded to the appropriate addressee or addressees in the conventional manner. Rijhsinghani at 11:46-51: Fifth, the tagger 284 c of switch 275' tags the packet with the VLAN header representing VLAN 1100. Last, the switch 275' transmits the tagged packet via the trunk port 315 onto the high-speed backbone 265 to be forwarded to system user at address V in the conventional manner.
[1.h] encapsulate the identified packet by the additional header; and	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute instructions to encapsulate the identified packet by the additional header. <i>See, e.g.:</i> Rijhsinghani at 3:22-67: FIG. 4 depicts a VLAN communications packet 400' which is similar to the LAN communications packet 400 depicted in FIG. 3, except that a VLAN header has been added to the packet. The VLAN header is added by the initial switch to which the message packet is directed. The VLAN header identifies the resulting packet as a "VLAN" or "tagged" packet, and represents the particular VLAN from which the packet originated. The VLAN header, as shown, includes a destination address 126 which is the same address as the destination address 118, a source address 124 which is the same as source address 116, a protocol identifier 122, and a VLAN tag 120 identifying the applicable VLAN. For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly,

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet 400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Because switch 280 lacks any access ports connected to LANs within the applicable VLAN, switch 280 discards the packet 400'. Switch 275, however, identifies the VLAN header of packet 400' as associated with a VLAN which includes LAN 230. The switch 275 accordingly removes the VLAN header and directs the packet, which now appears as packet 400 of FIG. 3, to LAN 230 over which the member I receives the message. Many trunk stations, such as trunk station 285, are incapable of recognizing VLAN headers. Further, since no programmable switch is disposed between a trunk station and the trunk, communications, i.e. packets, with a VLAN header will be ignored and/or discarded by the trunk station. Hence, in a conventional VLAN system, such as that shown in FIG. 5, the trunk stations, e.g., trunk station 285, form part of a default group. The default group is a group of system users or end stations not within any VLAN. For a communication packet sent by a system user within the default group, the initial switch to which the packet is directed determines that the system user does not fall within any VLAN, and consequently does not add a VLAN header. Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 5:13-54: In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200. In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100. Although it is known to configure different types of VLANs within a VLAN system based upon characteristics such as those previously described, problems arise in attempting to implement such systems. More particularly, under certain circumstances, overlap of VLANs may occur such as depicted in FIG. 6. Overlap occurs when a communication packet received at a switch can be identified with more than one VLAN. When overlap occurs, a switch may become confused as to which VLAN of multiple VLANs of different types should be identified for transmission of a received communication. Consequently, the switch will be confused as to which VLAN header should be added to the communication. Rijhsinghani at 8:60-9:6: The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. Rijhsinghani at 9:23-29: Accordingly, all communications between LANs within configured VLANs are forwarded to the appropriate addressee LAN. This is accomplished by identifying communications between LANs within configured VLANs and tagging the communications, except for those between LANs connected by an access port to the same switch, with a VLAN header. Rijhsinghani at 9:46-10:34: Each of the switches 270'-280' is programmed to utilize an order of precedence to identify with certainty the appropriate VLAN for transmission of the received communication. More particularly, each of the switches 270'-280' is programmed so as to operate to tag the communication with the VLAN header, i.e., the VLAN tag, representing the VLAN which is port and protocol-based over any other VLAN. Hence, if a communication received from one of the LANs is identified as potentially associated with a port and protocol-based or other type of VLAN, the switch will give precedence to the port and protocol-based VLAN over the other possible associated VLANs. For example, referring to FIG. 9, if the switch 280' receives a communication with a protocol identifier for protocol P1 from a user on LAN 250, the switch identifies the communication as being associated with both a port and protocol-based and protocol-based VLAN. The switch 280', in accordance with the order of precedence established by its programmed instructions, will identify the communication as being associated with the port and protocol-based VLAN 1100, rather than with the protocol-based VLAN 1000, and will, accordingly, tag the communication with a VLAN header representing VLAN 1100. Each of the switches 270'-280' is further programmed to give precedence to an identification of a possible association with a port-based VLAN over all other types of VLANs except port and protocol-based VLANs. For example, if switch 270' receives a communication at an access port 305 from LAN 215 that includes a source address within address-based VLAN 900, e.g., address V, the

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	switch 270' will give precedence to the fact that the communication was received at a port 305 configured within port-based VLAN 800 and will tag the communication with a VLAN header representing VLAN 800 rather than VLAN 900. It will be recognized by those skilled in the art that establishing port and protocol-based VLANs, as well as just port-based VLANs, at the highest levels within the order of precedence not only ensures that the communication is transmitted via the correct VLAN, but also enhances security because protocol-based and address-based VLANs are inherently less secure than port-based VLANs. The switches 270'-280' are further programmed such that address and protocol-based VLANs are given precedence over address-based VLANs and protocol-based VLANs. For example, if switch 280' receives a communication at an access port 305 from a system user at address T of LAN 260, and the communication has an identified protocol corresponding to the protocol associated with protocol-based LAN 1000, P1, the switch 280' will prioritize and give precedence to the correspondence of the communication to the address and protocol-based VLAN 1200 over address-based VLAN 900 and protocol-based VLAN 1000. Accordingly, switch 280' will tag the communication with the VLAN header representing VLAN 1200. Rijhsinghani at 11:5-10: In step 1340, the communication is tagged with the VLAN header representing the highest priority identified VLAN. In step 1350, the tagged communication is transmitted via the trunk port 315 from the switch and from there forwarded to the appropriate addressee or addressees in the conventional manner. Rijhsinghani at 11:46-51: Fifth, the tagger 284 c of switch 275' tags the packet with the VLAN header representing VLAN 1100. Last, the switch 275' transmits the tagged packet via the trunk port 315 onto the high-speed backbone 265 to be forwarded to system user at address V in the conventional manner.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
[1.i] process, based on the actions, the identified packet.	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute instructions to process, based on the actions, the identified packet. <i>See, e.g.:</i> Rijhsinghani at Fig. 10:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

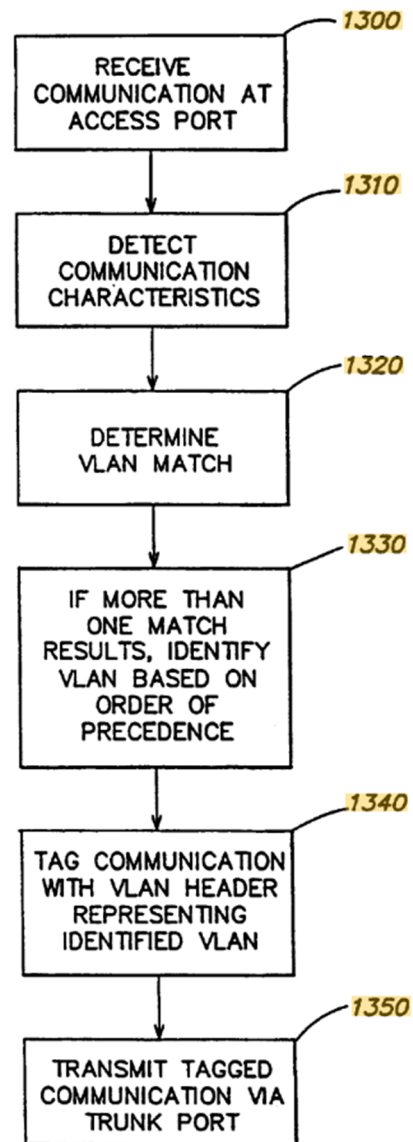


FIG. 10

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 7:41-43: FIG. 10 is a flow chart of the steps performed by the switch depicted in FIG. 8 in accordance with the present invention; and Rijhsinghani at 3:34-44: For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet 400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received. For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 5:13-54: In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200. In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100. Although it is known to configure different types of VLANs within a VLAN system based upon characteristics such as those previously described, problems arise in attempting to implement such systems. More particularly, under certain circumstances, overlap of VLANs may occur such as depicted in FIG. 6. Overlap occurs when a communication packet received at a switch can be identified with more than one VLAN. When overlap occurs, a switch may become confused as to which VLAN of multiple VLANs of different types should be identified for transmission of a received communication. Consequently, the switch will be confused as to which VLAN header should be added to the communication. Rijhsinghani at 6:25-7:15: Accordingly, the present invention provides rules of precedence for directing communications within different types of VLANs, in order to provide for predictable and desirable network behavior when there are areas of the network in which there is overlap in VLAN configurations, and to allow conflict resolutions by switches in the VLAN system. Advantageously, switches are provided that route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, based upon predefined rules of precedence.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Advantageously, switches route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, in a secure manner. Physical security is ensured by giving a higher precedence to port-based VLAN classifications than to other types of VLAN classifications. In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-ported reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g. a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (I) the port and protocol-based virtual networks precedence over the port-based virtual networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks. Typically, the communication will include at least a source address and a protocol identifier, which the switch control detects, along with the port at which the communication is received, to identify the VLAN. After the VLAN has been identified, the switch control adds a VLAN tag representing the identified VLAN to form a VLAN communication. The switch control then directs the VLAN communication to the second communication port for transmission over the identified virtual local area network. In accordance with other aspects of the invention, a virtual communications system can be implemented using multiple switches of the type described above. A network manager, interconnected to the multiple switches, is capable of configuring virtual local area networks of differing types a described above.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 8:60-9:6: The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. Rijhsinghani at 9:23-29: Accordingly, all communications between LANs within configured VLANs are forwarded to the appropriate addressee LAN. This is accomplished by identifying communications between LANs within configured VLANs and tagging the communications, except for those between LANs connected by an access port to the same switch, with a VLAN header. Rijhsinghani at 9:46-10:34: Each of the switches 270'-280' is programmed to utilize an order of precedence to identify with certainty the appropriate VLAN for transmission of the received communication. More particularly, each of the switches 270'-280' is programmed so as to operate to tag the communication with the VLAN header, i.e., the VLAN tag, representing the VLAN which is port and protocol-based over any other VLAN. Hence, if a communication received from one of the LANs is identified as potentially associated with a port and protocol-based or other type of VLAN, the switch will give precedence to the port and protocol-based VLAN over the other possible associated VLANs. For example, referring to FIG. 9, if the switch 280' receives a communication with a protocol identifier for protocol P1 from a user on LAN 250, the switch identifies the communication as being

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	associated with both a port and protocol-based and protocol-based VLAN. The switch 280', in accordance with the order of precedence established by its programmed instructions, will identify the communication as being associated with the port and protocol-based VLAN 1100, rather than with the protocol-based VLAN 1000, and will, accordingly, tag the communication with a VLAN header representing VLAN 1100. Each of the switches 270'-280' is further programmed to give precedence to an identification of a possible association with a port-based VLAN over all other types of VLANs except port and protocol-based VLANs. For example, if switch 270' receives a communication at an access port 305 from LAN 215 that includes a source address within address-based VLAN 900, e.g., address V, the switch 270' will give precedence to the fact that the communication was received at a port 305 configured within port-based VLAN 800 and will tag the communication with a VLAN header representing VLAN 800 rather than VLAN 900. It will be recognized by those skilled in the art that establishing port and protocol-based VLANs, as well as just port-based VLANs, at the highest levels within the order of precedence not only ensures that the communication is transmitted via the correct VLAN, but also enhances security because protocol-based and address-based VLANs are inherently less secure than port-based VLANs. The switches 270'-280' are further programmed such that address and protocol-based VLANs are given precedence over address-based VLANs and protocol-based VLANs. For example, if switch 280' receives a communication at an access port 305 from a system user at address T of LAN 260, and the communication has an identified protocol corresponding to the protocol associated with protocol-based LAN 1000, P1, the switch 280' will prioritize and give precedence to the correspondence of the communication to the address and protocol-based VLAN 1200 over address-based VLAN 900 and protocol-based VLAN 1000. Accordingly, switch 280' will tag the communication with the VLAN header representing VLAN 1200. Rijhsinghani at 11:5-10: In step 1340, the communication is tagged with the VLAN header representing the highest priority identified VLAN. In step 1350, the tagged communication is transmitted via the trunk port 315 from

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	the switch and from there forwarded to the appropriate addressee or addressees in the conventional manner. Rijhsinghani at 11:46-51: Fifth, the tagger 284 c of switch 275' tags the packet with the VLAN header representing VLAN 1100. Last, the switch 275' transmits the tagged packet via the trunk port 315 onto the high-speed backbone 265 to be forwarded to system user at address V in the conventional manner.
2. The switch apparatus according to claim 1, wherein the processor is further configured to execute the instructions to send header information to the control apparatus when the identified packet comprises an encapsulated packet.	Rijhsinghani discloses, expressly and/or inherently, the switch apparatus according to claim 1, wherein the processor is further configured to execute the instructions to send header information to the control apparatus when the identified packet comprises an encapsulated packet. <i>See claim 1.</i> <i>See, e.g.:</i> Rijhsinghani at 2:8-26: For example, as shown in FIG. 2, individual LANs 10, 20, 30, 40, 50, 60, 70, 80, 90 (10-90) are interconnected by layer 2 switches 5', 15', 25', 35', 45', (5'-55'). A network management station (NMS) 290 controls the interconnection of the individual LANs such that LANs can be easily bridged to other LANs on a long term or short term basis without the need to rewire the network. As depicted in FIG. 2, the NMS 290 has configured two VLANs by instructing, e.g., programming, and thereby configuring the switches 5'-55' such that LANs 10-60 are bridged together by switches 5', 15', 55', 35' to form VLAN 100' and LANs 70-90 are bridged together by switches 45' and 55' to form VLAN 200'. This is possible because, unlike the bridges 5-35 of FIG. 1, which include only two ports, and accordingly are able to only transfer information from one LAN to another LAN, the switches 5'-55'

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	are multi-ported and programmable by the NMS 290 such that the network can be configured and reconfigured in any desired manner by simply changing the switch instructions. Rijhsinghani at 2:36-56: If it becomes desirable to change the network configuration, this is easily accomplished by issuing commands from NMS 290 to the applicable switches 5'-55'. For example, if desired, user H could be easily added to VLAN 100' by simply reconfiguring VLAN 100' from the NMS 290. The NMS 290 issues an instruction to switch 55', instructing switch 55' to allow communications to flow between users A-D and E and user H via switch 55', i.e., to include LAN 90 in VLAN 100' and remove it from VLAN 200'. Because the switches 5'-55' are layer 2 switches, a bridge formed by the switch is transparent to the users within the VLAN. Hence, the transmission delays normally associated with routers, such as the router 300 of FIG. 1, are avoided. The flexibility of the VLAN lies in its' ability to have its' network configuration controlled through software on the NMS 290. More particularly, in accordance with its' programmed instructions, the NMS 290 generates and transmits signals to instruct the switches 5'-55' to form the desired VLAN configurations. Rijhsinghani at 2:62-3:22: FIG. 5 is a schematic of a conventional VLAN system. The VLAN system includes LANs 205-260 which are connected by switches 270-280 to a high-speed LAN backbone or trunk 265. An NMS 290 is interconnected to the switches 270-280 via LAN 260. The NMS 290 is interconnected via LAN 260 as an example and could be interconnected to switches 270-280 via any of the LANs 205-260. A trunk station 285 is connected to the high-speed LAN backbone 265 via a trunk port 315. The LANs 205-215, and 230-235 have designated members F-J. LANs connect to each of the switches 270-280 by a plurality of access ports 305. For example, switch 270 is connected via access ports 305 to LANs 205-220. Each switch is capable of interconnecting a LAN connected via an access port 305 with another LAN connected via an access port 305. For example, switch 270 can be instructed by the NMS 290 to

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	interconnect LAN 205 to LAN 215 by configuring a VLAN including LANs 205 and 215, thereby enabling communications between members F and H. Each switch is also capable of interconnecting a LAN connected by an access port 305 with a LAN connected to another switch by an access port 305 via high-speed LAN backbone 265. For example, Switches 270 and 275 can be instructed by the NMS 290 to interconnect LANs 205 and 230 by configuring a VLAN including LANs 205 and 230, thereby enabling communications between member E of LAN 205 and member I of LAN 230. Rijhsinghani at 3:34-44: For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet 400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name "protocol-based" implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 7:49-8:5: FIG. 7 depicts a virtual communications system or network in accordance with the present invention. The network includes multiple Local Area Networks (LANs) 205-260 interconnected by multiple multi-ported reconfigurable switches 270', 275' and 280' all of which are connected by a high speed backbone LAN 265, often referred to as the trunk. Each LAN, other than the backbone LAN 265 is

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	connected to one of the switches 270', 275' or 280' by an access port 305, while the backbone LAN 265 is connected to each switch by a trunk port 315. A network management station (NMS) 290', which may be a workstation having network management software loaded thereon, manages the network by configuring the network via the switches 270', 275' and 280' to form one or more virtual local area networks (VLANs). A trunk station 285 is connected to the backbone LAN 265 via a trunk port 315. The trunk stations 285 may, for example, be a network server or other network resource to which some or all of the members of the LANs 205-260 may require high speed access from time to time or on a continuous basis as is known in the art. Each of the switches 270', 275' and 280' is capable of linking, via the backbone LAN 265, members of each of the LANs 205-260 to members of the one or more other LANs within the VLANs configured by the NMS 290'. Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 8:34-40: For the network depicted in FIG. 8, communications from NMS 290' are detected differently. The detectors 284 b of switches 270' and 275' detect communications from NMS 290' via the backbone LAN 265 at a trunk port 315, while the detector 284 b of switch 280' detects communications from the NMS 290' at the access port 305 connected to LAN 260. Rijhsinghani at 8:41-9:22:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	The detector 284 b of a switch detects all communications over the backbone LAN 265, which the control module 284 handles in the following manner. If a detected communication is deliverable to a network addressee on any of the LANs connected to an access port of the applicable switch, the controller 284 a of the applicable switch controls the switching device 282 to transmit the communication from the trunk port 315 to the applicable access port 305. More specifically, if the detected communication is properly addressed to the addressee and forwarded from an authorized member of the system, the controller 284 a of the applicable switch controls the switching device 282 to transmit the message to the applicable LAN. An authorized member is a member of the VLAN that includes the addressee. In the case where the addressee is a member of the default group, however, an authorized member is any other member of the system because the member is not a member of any VLAN. The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. If the detected communication has been received via an access port 305 of the switch and is properly addressed and deliverable to a network addressee on any of the other LANs connected to the switch, the controller 284 a of the switch controls the switching device 282 to transmit the message from the input access port 305 to the applicable output access port 305. In such a case, where the sender and addressee are each members of a LAN connected to the same switch, there is no need to add a VLAN header to the communication before directing it to output port 305. However, if such a communication is to be multicast transmitted to one or more LANs within the applicable VLAN that are directly connected to other switches by access ports, the communication output from the trunk port 315 of the applicable switch will, of course, be tagged by the tagger before transmission via the trunk 265 as discussed above. Rijhsinghani at 9:30-45:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	The NMS 290' is capable of configuring VLANs of differing types. More particularly, the NMS 290' can configure or define VLANs which are port-based, address-based, protocol-based, port and protocol-based, and address and protocol-based. The NMS 290' instructs the switches 270'-280' as to the configurations of the different types of VLANs. Each of the switches 270'-280' is programmed to consider the applicable characteristics of each communication received, via an access port, in order to determine the appropriate VLAN tag to add to the communication before transmission via the trunk port 315 to the high speed LAN backbone or trunk 265. These instructions may be stored in the memory 286 of the switch, as depicted in FIG. 8, and utilized by the switch control module 284 in determining which tag to add to a communication received at an access port 305. Rijhsinghani at 10:55-63: In step 1320, the control module 288, in accordance with the programmed instructions stored in the memory 286, determines one or more VLAN matches, i.e. determines one or more VLANs with which the communication may be appropriately associated. Depending on the instruction, this determination may be based upon the receive port and protocol considered jointly, the receive port, the source address and protocol considered jointly, the address, and the protocol. Rijhsinghani at 11:11-40: For example, referring to FIG. 9, the following steps would be performed at switch 275' when a system user at address U on LAN 240 transmits a communication packet with a protocol identifier for P1 addressed to a system user at address L on LAN 220, and the system is programmed to identify packets with a protocol identifier for protocol P1 with protocol-based VLAN 1000. First, switch 275' receives the packet at an access port 305. Second, detector 284 b of the control module 288 of switch 275' detects the receive port, the source address U of the packet, and the protocol identifier for P1 of the packet. Third, the control module 288 of switch 275', in accordance with the programmed instructions stored on the memory 286, determines five VLAN matches. Specifically, the control module determines that the packet may be appropriately associated with port-based VLAN 800

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	because the receive port at which LAN 240 is connected is a member of VLAN 800, the packet may be appropriately associated with address-based VLAN 900 because the source address U is a member of VLAN 900, the packet may be appropriately associated with protocol-based VLAN 1000 because the protocol identifier of the packet is for P1, the packet may be appropriately associated with port and protocol-based VLAN 1100 because the receive port at which LAN 240 is connected is a member of VLAN 1100 when the protocol identifier of the packet is for P1, and the packet may be appropriately associated with address and protocol-based VLAN 1200 because the source address U is a member of VLAN 1200 when the protocol identifier of the packet is for P1.
3. The switch apparatus according to claim 2, wherein the header information includes the additional header.	Rijhsinghani discloses, expressly and/or inherently, the switch apparatus according to claim 2, wherein the header information includes the additional header. <i>See claim 2.</i> <i>See, e.g.:</i> Rijhsinghani at 3:22-67: FIG. 4 depicts a VLAN communications packet 400' which is similar to the LAN communications packet 400 depicted in FIG. 3, except that a VLAN header has been added to the packet. The VLAN header is added by the initial switch to which the message packet is directed. The VLAN header identifies the resulting packet as a "VLAN" or "tagged" packet, and represents the particular VLAN from which the packet originated. The VLAN header, as shown, includes a destination address 126 which is the same address as the destination address 118, a source address 124 which is the same as source address 116, a protocol identifier 122, and a VLAN tag 120 identifying the applicable VLAN. For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Because switch 280 lacks any access ports connected to LANs within the applicable VLAN, switch 280 discards the packet 400'. Switch 275, however, identifies the VLAN header of packet 400' as associated with a VLAN which includes LAN 230. The switch 275 accordingly removes the VLAN header and directs the packet, which now appears as packet 400 of FIG. 3, to LAN 230 over which the member I receives the message. Many trunk stations, such as trunk station 285, are incapable of recognizing VLAN headers. Further, since no programmable switch is disposed between a trunk station and the trunk, communications, i.e. packets, with a VLAN header will be ignored and/or discarded by the trunk station. Hence, in a conventional VLAN system, such as that shown in FIG. 5, the trunk stations, e.g., trunk station 285, form part of a default group. The default group is a group of system users or end stations not within any VLAN. For a communication packet sent by a system user within the default group, the initial switch to which the packet is directed determines that the system user does not fall within any VLAN, and consequently does not add a VLAN header. Rijhsinghani at 5:13-54: In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100. Although it is known to configure different types of VLANs within a VLAN system based upon characteristics such as those previously described, problems arise in attempting to implement such systems. More particularly, under certain circumstances, overlap of VLANs may occur such as depicted in FIG. 6. Overlap occurs when a communication packet received at a switch can be identified with more than one VLAN. When overlap occurs, a switch may become confused as to which VLAN of multiple VLANs of different types should be identified for transmission of a received communication. Consequently, the switch will be confused as to which VLAN header should be added to the communication. Rijhsinghani at 8:60-9:6: The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. Rijhsinghani at 9:23-29: Accordingly, all communications between LANs within configured VLANs are forwarded to the appropriate addressee LAN. This is accomplished by identifying communications between LANs

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	within configured VLANs and tagging the communications, except for those between LANs connected by an access port to the same switch, with a VLAN header. Rijhsinghani at 9:46-10:34: Each of the switches 270'-280' is programmed to utilize an order of precedence to identify with certainty the appropriate VLAN for transmission of the received communication. More particularly, each of the switches 270'-280' is programmed so as to operate to tag the communication with the VLAN header, i.e., the VLAN tag, representing the VLAN which is port and protocol-based over any other VLAN. Hence, if a communication received from one of the LANs is identified as potentially associated with a port and protocol-based or other type of VLAN, the switch will give precedence to the port and protocol-based VLAN over the other possible associated VLANs. For example, referring to FIG. 9, if the switch 280' receives a communication with a protocol identifier for protocol P1 from a user on LAN 250, the switch identifies the communication as being associated with both a port and protocol-based and protocol-based VLAN. The switch 280', in accordance with the order of precedence established by its programmed instructions, will identify the communication as being associated with the port and protocol-based VLAN 1100, rather than with the protocol-based VLAN 1000, and will, accordingly, tag the communication with a VLAN header representing VLAN 1100. Each of the switches 270'-280' is further programmed to give precedence to an identification of a possible association with a port-based VLAN over all other types of VLANs except port and protocol-based VLANs. For example, if switch 270' receives a communication at an access port 305 from LAN 215 that includes a source address within address-based VLAN 900, e.g., address V, the switch 270' will give precedence to the fact that the communication was received at a port 305 configured within port-based VLAN 800 and will tag the communication with a VLAN header representing VLAN 800 rather than VLAN 900. It will be recognized by those skilled in the art that establishing port and protocol-based VLANs, as well as just port-based VLANs, at the highest levels within the order of precedence not only ensures that the communication is transmitted via the correct VLAN, but also enhances security because protocol-based and address-based VLANs are inherently less secure than port-based VLANs.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	The switches 270'-280' are further programmed such that address and protocol-based VLANs are given precedence over address-based VLANs and protocol-based VLANs. For example, if switch 280' receives a communication at an access port 305 from a system user at address T of LAN 260, and the communication has an identified protocol corresponding to the protocol associated with protocol-based LAN 1000, P1, the switch 280' will prioritize and give precedence to the correspondence of the communication to the address and protocol-based VLAN 1200 over address-based VLAN 900 and protocol-based VLAN 1000. Accordingly, switch 280' will tag the communication with the VLAN header representing VLAN 1200. Rijhsinghani at 11:5-10: In step 1340, the communication is tagged with the VLAN header representing the highest priority identified VLAN. In step 1350, the tagged communication is transmitted via the trunk port 315 from the switch and from there forwarded to the appropriate addressee or addressees in the conventional manner. Rijhsinghani at 11:46-51: Fifth, the tagger 284 c of switch 275' tags the packet with the VLAN header representing VLAN 1100. Last, the switch 275' transmits the tagged packet via the trunk port 315 onto the high-speed backbone 265 to be forwarded to system user at address V in the conventional manner.
4. The switch apparatus according to claim 3, wherein the processor is further configured to execute further instructions to decapsulate the encapsulated packet.	Rijhsinghani discloses, expressly and/or inherently, the switch apparatus according to claim 3, wherein the processor is further configured to execute further instructions to decapsulate the encapsulated packet. <i>See claim 3.</i> <i>See, e.g.:</i>

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 2:8-26: For example, as shown in FIG. 2, individual LANs 10, 20, 30, 40, 50, 60, 70, 80, 90 (10-90) are interconnected by layer 2 switches 5', 15', 25', 35', 45', (5'-55'). A network management station (NMS) 290 controls the interconnection of the individual LANs such that LANs can be easily bridged to other LANs on a long term or short term basis without the need to rewire the network. As depicted in FIG. 2, the NMS 290 has configured two VLANs by instructing, e.g., programming, and thereby configuring the switches 5'-55' such that LANs 10-60 are bridged together by switches 5', 15', 55', 35' to form VLAN 100' and LANs 70-90 are bridged together by switches 45' and 55' to form VLAN 200'. This is possible because, unlike the bridges 5-35 of FIG. 1, which include only two ports, and accordingly are able to only transfer information from one LAN to another LAN, the switches 5'-55' are multi-ported and programmable by the NMS 290 such that the network can be configured and reconfigured in any desired manner by simply changing the switch instructions. Rijhsinghani at 2:36-56: If it becomes desirable to change the network configuration, this is easily accomplished by issuing commands from NMS 290 to the applicable switches 5'-55'. For example, if desired, user H could be easily added to VLAN 100' by simply reconfiguring VLAN 100' from the NMS 290. The NMS 290 issues an instruction to switch 55', instructing switch 55' to allow communications to flow between users A-D and E and user H via switch 55', i.e., to include LAN 90 in VLAN 100' and remove it from VLAN 200'. Because the switches 5'-55' are layer 2 switches, a bridge formed by the switch is transparent to the users within the VLAN. Hence, the transmission delays normally associated with routers, such as the router 300 of FIG. 1, are avoided. The flexibility of the VLAN lies in its' ability to have its' network configuration controlled through software on the NMS 290. More particularly, in accordance with its' programmed instructions, the NMS 290 generates and transmits signals to instruct the switches 5'-55' to form the desired VLAN configurations.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 2:62-3:22: FIG. 5 is a schematic of a conventional VLAN system. The VLAN system includes LANs 205-260 which are connected by switches 270-280 to a high-speed LAN backbone or trunk 265. An NMS 290 is interconnected to the switches 270-280 via LAN 260. The NMS 290 is interconnected via LAN 260 as an example and could be interconnected to switches 270-280 via any of the LANs 205-260. A trunk station 285 is connected to the high-speed LAN backbone 265 via a trunk port 315. The LANs 205-215, and 230-235 have designated members F-J. LANs connect to each of the switches 270-280 by a plurality of access ports 305. For example, switch 270 is connected via access ports 305 to LANs 205-220. Each switch is capable of interconnecting a LAN connected via an access port 305 with another LAN connected via an access port 305. For example, switch 270 can be instructed by the NMS 290 to interconnect LAN 205 to LAN 215 by configuring a VLAN including LANs 205 and 215, thereby enabling communications between members F and H. Each switch is also capable of interconnecting a LAN connected by an access port 305 with a LAN connected to another switch by an access port 305 via high-speed LAN backbone 265. For example, Switches 270 and 275 can be instructed by the NMS 290 to interconnect LANs 205 and 230 by configuring a VLAN including LANs 205 and 230, thereby enabling communications between member E of LAN 205 and member I of LAN 230. Rijhsinghani at 3:34-44: For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet 400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 3:45-53: Because switch 280 lacks any access ports connected to LANs within the applicable VLAN, switch 280 discards the packet 400'. Switch 275, however, identifies the VLAN header of packet 400' as associated with a VLAN which includes LAN 230. The switch 275 accordingly removes the VLAN header and directs the packet, which now appears as packet 400 of FIG. 3, to LAN 230 over which the member I receives the message. Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received. For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 7:49-8:5: FIG. 7 depicts a virtual communications system or network in accordance with the present invention. The network includes multiple Local Area Networks (LANs) 205-260 interconnected by multiple multi-ported reconfigurable switches 270', 275' and 280' all of which are connected by a high speed backbone LAN 265, often referred to as the trunk. Each LAN, other than the backbone LAN 265 is connected to one of the switches 270', 275' or 280' by an access port 305, while the backbone LAN 265 is connected to each switch by a trunk port 315. A network management station (NMS) 290', which may be a workstation having network management software loaded thereon, manages the network by configuring the network via the switches 270', 275' and 280' to form one or more virtual local area networks (VLANs). A trunk station 285 is connected to the backbone LAN 265 via a trunk port 315. The trunk stations 285 may, for example, be a network server or other network resource to which some or all of the members of the LANs 205-260 may require high speed access from time to time or on a continuous basis as is known in the art. Each of the switches 270', 275' and 280' is capable of linking, via the backbone LAN 265, members of each of the LANs 205-260 to members of the one or more other LANs within the VLANs configured by the NMS 290'.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305. Rijhsinghani at 8:34-40: For the network depicted in FIG. 8, communications from NMS 290' are detected differently. The detectors 284 b of switches 270' and 275' detect communications from NMS 290' via the backbone LAN 265 at a trunk port 315, while the detector 284 b of switch 280' detects communications from the NMS 290' at the access port 305 connected to LAN 260. Rijhsinghani at 8:41-9:22: The detector 284 b of a switch detects all communications over the backbone LAN 265, which the control module 284 handles in the following manner. If a detected communication is deliverable to a network addressee on any of the LANs connected to an access port of the applicable switch, the controller 284 a of the applicable switch controls the switching device 282 to transmit the communication from the trunk port 315 to the applicable access port 305. More specifically, if the detected communication is properly addressed to the addressee and forwarded from an authorized member of the system, the controller 284 a of the applicable switch controls the switching device 282 to transmit the message to the applicable LAN. An authorized member is a member of the VLAN that includes the addressee. In the case where the addressee is a member of the default group, however, an authorized member is any other member of the system because the member is not a member of any VLAN.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. If the detected communication has been received via an access port 305 of the switch and is properly addressed and deliverable to a network addressee on any of the other LANs connected to the switch, the controller 284 a of the switch controls the switching device 282 to transmit the message from the input access port 305 to the applicable output access port 305. In such a case, where the sender and addressee are each members of a LAN connected to the same switch, there is no need to add a VLAN header to the communication before directing it to output port 305. However, if such a communication is to be multicast transmitted to one or more LANs within the applicable VLAN that are directly connected to other switches by access ports, the communication output from the trunk port 315 of the applicable switch will, of course, be tagged by the tagger before transmission via the trunk 265 as discussed above. Rijhsinghani at 9:30-45: The NMS 290' is capable of configuring VLANs of differing types. More particularly, the NMS 290' can configure or define VLANs which are port-based, address-based, protocol-based, port and protocol-based, and address and protocol-based. The NMS 290' instructs the switches 270'-280' as to the configurations of the different types of VLANs. Each of the switches 270'-280' is programmed to consider the applicable characteristics of each communication received, via an access port, in order to determine the appropriate VLAN tag to add to the communication before transmission via the trunk port 315 to the high speed LAN backbone or trunk 265. These instructions may be stored in the memory 286 of the switch, as depicted in FIG. 8, and utilized by the switch control module 284 in determining which tag to add to a communication received at an access port 305.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 10:55-63: In step 1320, the control module 288, in accordance with the programmed instructions stored in the memory 286, determines one or more VLAN matches, i.e. determines one or more VLANs with which the communication may be appropriately associated. Depending on the instruction, this determination may be based upon the receive port and protocol considered jointly, the receive port, the source address and protocol considered jointly, the address, and the protocol. Rijhsinghani at 11:11-40: For example, referring to FIG. 9, the following steps would be performed at switch 275' when a system user at address U on LAN 240 transmits a communication packet with a protocol identifier for P1 addressed to a system user at address L on LAN 220, and the system is programmed to identify packets with a protocol identifier for protocol P1 with protocol-based VLAN 1000. First, switch 275' receives the packet at an access port 305. Second, detector 284 b of the control module 288 of switch 275' detects the receive port, the source address U of the packet, and the protocol identifier for P1 of the packet. Third, the control module 288 of switch 275', in accordance with the programmed instructions stored on the memory 286, determines five VLAN matches. Specifically, the control module determines that the packet may be appropriately associated with port-based VLAN 800 because the receive port at which LAN 240 is connected is a member of VLAN 800, the packet may be appropriately associated with address-based VLAN 900 because the source address U is a member of VLAN 900, the packet may be appropriately associated with protocol-based VLAN 1000 because the protocol identifier of the packet is for P1, the packet may be appropriately associated with port and protocol-based VLAN 1100 because the receive port at which LAN 240 is connected is a member of VLAN 1100 when the protocol identifier of the packet is for P1, and the packet may be appropriately associated with address and protocol-based VLAN 1200 because the source address U is a member of VLAN 1200 when the protocol identifier of the packet is for P1.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
5. The switch apparatus according to claim 1, wherein the processor is further configured to execute the instructions for translation of first header data of a head of the received packet into second header data.	Rijhsinghani discloses, expressly and/or inherently, the switch apparatus according to claim 1, wherein the processor is further configured to execute the instructions for translation of first header data of a head of the received packet into second header data. <i>See claim 1.</i> <i>See, e.g.:</i> Rijhsinghani at 4:1-5:29: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. The depiction of VLANs 100 and 1200 in FIG. 6 is for description purposes only because the VLAN is also determined by the protocol P1. For a packet transmitted from one of the LANs 235-250 to be identified with port and protocol-based VLAN 1100, the packet must include a protocol identifier for protocol P1. Similarly, for a packet transmitted from one of the addresses K, L, M, U, Q, or T to be identified with address and protocol-based VLAN 1200, the packet must include a protocol identifier for protocol P1. LANs 1100 and 1200 are depicted as such in FIG. 6 to illustrate the configuration of different types of VLANs. As can be seen from the system of FIG. 6, some of the VLANs overlap. For example, a packet transmitted from address K will be identified with address-based VLAN 900, and port-based VLAN 800 because address K resides on LAN 210, which is included in VLAN 800. Furthermore, if a packet transmitted from address K includes a protocol identifier for protocol P1, the packet may be identified with VLAN 1000. Another example of overlap affects packets transmitted from LAN 240 which will be identified with port-based VLAN 800 and may be also identified with protocol-based VLAN 1000 and port and protocol-based VLAN 1100 if the packet includes a protocol identifier for protocol P1. The problems associated with overlap are discussed below. In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100.
6. The switch apparatus according to claim 5, wherein the instructions to encapsulate the identified packet includes notifying the controller of the first header data before the translation and the second header data after the translation.	Rijhsinghani discloses, expressly and/or inherently, the switch apparatus according to claim 5, wherein the instructions to encapsulate the identified packet includes notifying the controller of the first header data before the translation and the second header data after the translation. <i>See claim 5.</i> <i>See, e.g.:</i> Rijhsinghani at 3:22-67: FIG. 4 depicts a VLAN communications packet 400' which is similar to the LAN communications packet 400 depicted in FIG. 3, except that a VLAN header has been added to the packet. The VLAN header is added by the initial switch to which the message packet is directed. The VLAN header identifies the resulting packet as a "VLAN" or "tagged" packet, and represents the particular VLAN from which the packet originated. The VLAN header, as shown, includes a destination address 126 which is the same address as the destination address 118, a source address 124 which is the same as source address 116, a protocol identifier 122, and a VLAN tag 120 identifying the applicable VLAN. For example, if LANs 205, 220 and 230 of FIG. 5 are within a single VLAN and member E of LAN 205 desires to communicate with member I of LAN 230, the message 400 of FIG. 3 is directed to access port 305 of the switch 270. The switch determines, based upon instructions previously received from the NMS 290, that the LAN 205 falls within the applicable VLAN and, accordingly, adds the appropriate VLAN header to the packet to form packet 400', as shown in FIG. 4. The packet

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	400' is then directed via trunk port 315 to the high-speed backbone LAN 265 and detected by switches 275 and 280. Because switch 280 lacks any access ports connected to LANs within the applicable VLAN, switch 280 discards the packet 400'. Switch 275, however, identifies the VLAN header of packet 400' as associated with a VLAN which includes LAN 230. The switch 275 accordingly removes the VLAN header and directs the packet, which now appears as packet 400 of FIG. 3, to LAN 230 over which the member I receives the message. Many trunk stations, such as trunk station 285, are incapable of recognizing VLAN headers. Further, since no programmable switch is disposed between a trunk station and the trunk, communications, i.e. packets, with a VLAN header will be ignored and/or discarded by the trunk station. Hence, in a conventional VLAN system, such as that shown in FIG. 5, the trunk stations, e.g., trunk station 285, form part of a default group. The default group is a group of system users or end stations not within any VLAN. For a communication packet sent by a system user within the default group, the initial switch to which the packet is directed determines that the system user does not fall within any VLAN, and consequently does not add a VLAN header. Rijhsinghani at 4:1-5:29: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. The depiction of VLANs 100 and 1200 in FIG. 6 is for description purposes only because the VLAN is also determined by the protocol P1. For a packet transmitted from one of the LANs 235-250 to be identified with port and protocol-based VLAN 1100, the packet must include a protocol identifier for protocol P1. Similarly, for a packet transmitted from one of the addresses K, L, M, U, Q, or T to be identified with address and protocol-based VLAN 1200, the packet must include a protocol identifier for protocol P1. LANs 1100 and 1200 are depicted as such in FIG. 6 to illustrate the configuration of different types of VLANs. As can be seen from the system of FIG. 6, some of the VLANs overlap. For example, a packet transmitted from address K will be identified with address-based VLAN 900, and port-based VLAN 800 because address K resides on LAN 210, which is included in VLAN 800. Furthermore, if a packet transmitted from address K includes a protocol identifier for protocol P1, the packet may be identified with VLAN 1000. Another example of overlap affects packets transmitted from LAN 240 which will be identified with port-based VLAN 800 and may be also identified with protocol-based VLAN 1000 and port and protocol-based VLAN 1100 if the packet includes a protocol identifier for protocol P1. The problems associated with overlap are discussed below.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200. In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100. Rijhsinghani at 5:13-54: In view of the different types of VLANs, each of the switches 270-280 must be programmed to consider all of the various communications characteristics which are necessary to associate a communication packet received at an access port. For example, switch 270 is programmed to consider the port, the address, as well as the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, or 1200. Switch 275 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 800, 900, 1000, 1100, or 1200. Switch 280 must be programmed to consider the port, the address, and the protocol to determine if a communication received via one of its access ports should be tagged with a VLAN header representing VLAN 900, 1000, 1100, or 1200. In each case presented above, it should be noted that switches must be programmed to consider some characteristics jointly. For example, switches 270 and 280 must be programmed to consider jointly

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	the address and protocol to ensure that communications received from address K or addresses Q and T are properly tagged with a VLAN header representing VLAN 1200. Switches 275 and 280 must be programmed to consider jointly the port and protocol to ensure that communications received from LANs 235 and 240, or 245 and 250, respectively, are properly tagged with a VLAN header representing VLAN 1100. Although it is known to configure different types of VLANs within a VLAN system based upon characteristics such as those previously described, problems arise in attempting to implement such systems. More particularly, under certain circumstances, overlap of VLANs may occur such as depicted in FIG. 6. Overlap occurs when a communication packet received at a switch can be identified with more than one VLAN. When overlap occurs, a switch may become confused as to which VLAN of multiple VLANs of different types should be identified for transmission of a received communication. Consequently, the switch will be confused as to which VLAN header should be added to the communication. Rijhsinghani at 8:60-9:6: The control module 284 also includes a tagger 284 c for tagging communications received via an access port 305 for transmission from one member to another member of a configured VLAN by adding a VLAN header thereto. The tagger 284 c also removes the VLAN header from a communication received from the switch's trunk port 315 that is to be forwarded to a member of a LAN connected to the switch by an access port. More particularly, the tagger 284 c discards the tag by removing the VLAN header from the communication, prior to the communication being transmitted to the appropriate output port 305, i.e., prior to the controller 284 a controlling the switching device 282 to transmit the communication from the trunk port 315 to the access port 305. Rijhsinghani at 9:23-29: Accordingly, all communications between LANs within configured VLANs are forwarded to the appropriate addressee LAN. This is accomplished by identifying communications between LANs

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	within configured VLANs and tagging the communications, except for those between LANs connected by an access port to the same switch, with a VLAN header. Rijhsinghani at 9:46-10:34: Each of the switches 270'-280' is programmed to utilize an order of precedence to identify with certainty the appropriate VLAN for transmission of the received communication. More particularly, each of the switches 270'-280' is programmed so as to operate to tag the communication with the VLAN header, i.e., the VLAN tag, representing the VLAN which is port and protocol-based over any other VLAN. Hence, if a communication received from one of the LANs is identified as potentially associated with a port and protocol-based or other type of VLAN, the switch will give precedence to the port and protocol-based VLAN over the other possible associated VLANs. For example, referring to FIG. 9, if the switch 280' receives a communication with a protocol identifier for protocol P1 from a user on LAN 250, the switch identifies the communication as being associated with both a port and protocol-based and protocol-based VLAN. The switch 280', in accordance with the order of precedence established by its programmed instructions, will identify the communication as being associated with the port and protocol-based VLAN 1100, rather than with the protocol-based VLAN 1000, and will, accordingly, tag the communication with a VLAN header representing VLAN 1100. Each of the switches 270'-280' is further programmed to give precedence to an identification of a possible association with a port-based VLAN over all other types of VLANs except port and protocol-based VLANs. For example, if switch 270' receives a communication at an access port 305 from LAN 215 that includes a source address within address-based VLAN 900, e.g., address V, the switch 270' will give precedence to the fact that the communication was received at a port 305 configured within port-based VLAN 800 and will tag the communication with a VLAN header representing VLAN 800 rather than VLAN 900. It will be recognized by those skilled in the art that establishing port and protocol-based VLANs, as well as just port-based VLANs, at the highest levels within the order of precedence not only ensures that the communication is transmitted via the correct VLAN, but also enhances security because protocol-based and address-based VLANs are inherently less secure than port-based VLANs.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	The switches 270'-280' are further programmed such that address and protocol-based VLANs are given precedence over address-based VLANs and protocol-based VLANs. For example, if switch 280' receives a communication at an access port 305 from a system user at address T of LAN 260, and the communication has an identified protocol corresponding to the protocol associated with protocol-based LAN 1000, P1, the switch 280' will prioritize and give precedence to the correspondence of the communication to the address and protocol-based VLAN 1200 over address-based VLAN 900 and protocol-based VLAN 1000. Accordingly, switch 280' will tag the communication with the VLAN header representing VLAN 1200. Rijhsinghani at 11:5-10: In step 1340, the communication is tagged with the VLAN header representing the highest priority identified VLAN. In step 1350, the tagged communication is transmitted via the trunk port 315 from the switch and from there forwarded to the appropriate addressee or addressees in the conventional manner. Rijhsinghani at 11:46-51: Fifth, the tagger 284 c of switch 275' tags the packet with the VLAN header representing VLAN 1100. Last, the switch 275' transmits the tagged packet via the trunk port 315 onto the high-speed backbone 265 to be forwarded to system user at address V in the conventional manner.
[7.pre] 7. A communication system, comprising:	Dell takes no position in these Invalidity Contentions on whether the entirety of the preamble of this claim is a limitation. To the extent it is a limitation, Rijhsinghani discloses, expressly and/or inherently, a communication system. <i>See, e.g.:</i> Rijhsinghani at 6:25-67:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Accordingly, the present invention provides rules of precedence for directing communications within different types of VLANs, in order to provide for predictable and desirable network behavior when there are areas of the network in which there is overlap in VLAN configurations, and to allow conflict resolutions by switches in the VLAN system. Advantageously, switches are provided that route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, based upon predefined rules of precedence. Advantageously, switches route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, in a secure manner. Physical security is ensured by giving a higher precedence to port-based VLAN classifications than to other types of VLAN classifications. In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-ported reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g. a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (I) the port and protocol-based virtual networks precedence over the port-based virtual networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks. Rijhsinghani at 7:10-15: In accordance with other aspects of the invention, a virtual communications system can be implemented using multiple switches of the type described above. A network manager,

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	interconnected to the multiple switches, is capable of configuring virtual local area networks of differing types a described above. <i>See</i> Rijhsinghani claims 13-36.
[7.a] a control apparatus configured to control a plurality of switch apparatuses; and	Rijhsinghani discloses, expressly and/or inherently, a control apparatus configured to control a plurality of switch apparatuses. <i>See, e.g.:</i> Rijhsinghani at Fig 5:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

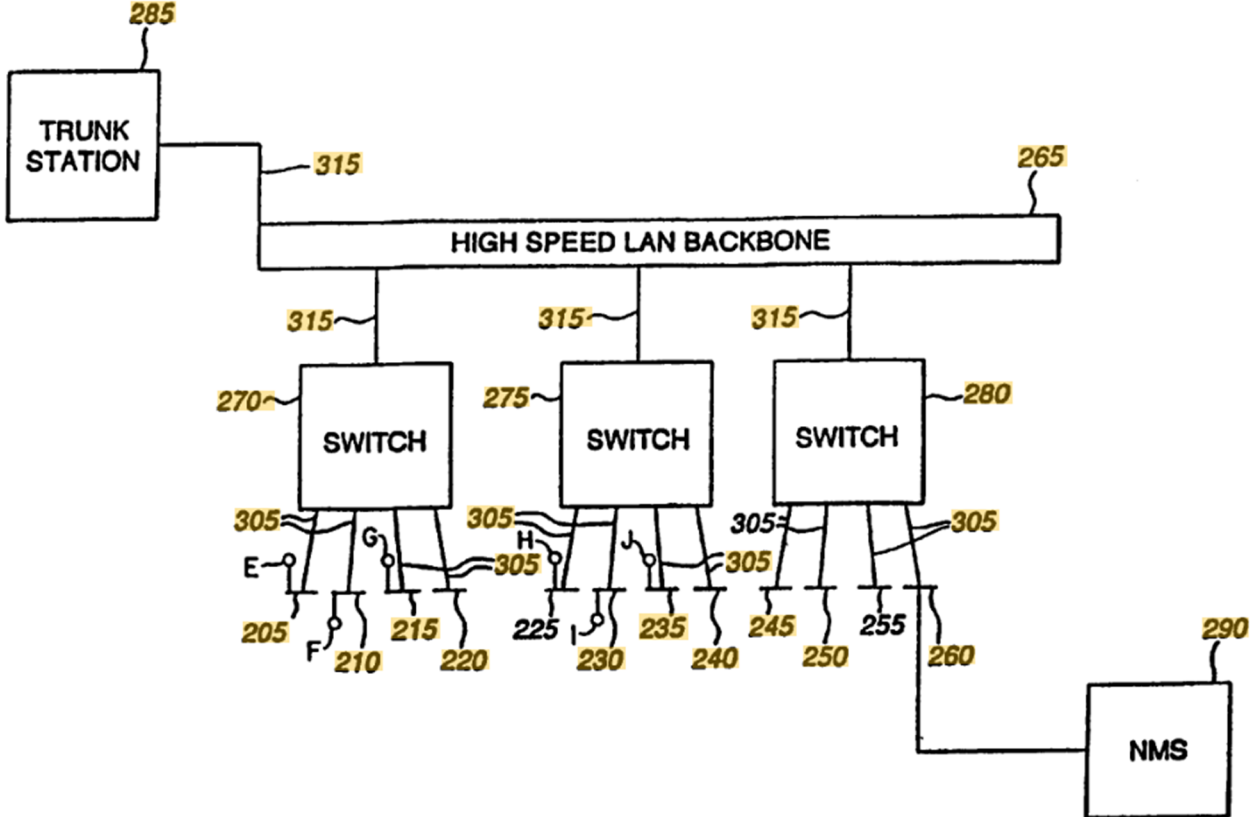
Asserted Claims	Rijhsinghani
	 FIG. 5 Rijhsinghani at 7:29-30:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

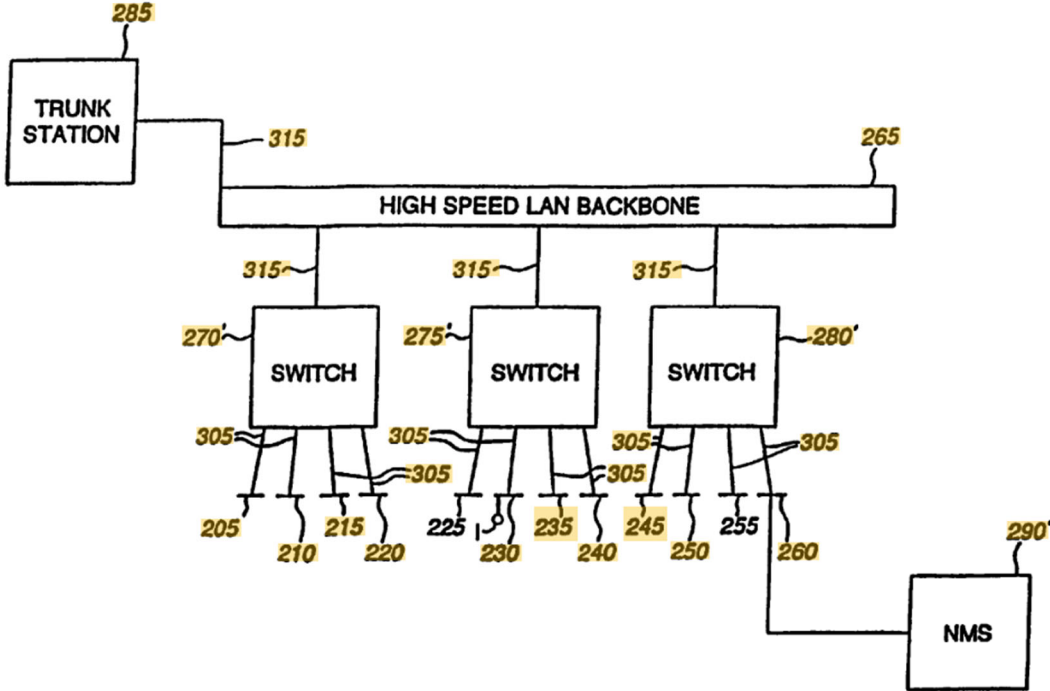
Asserted Claims	Rijhsinghani
	FIG. 5 depicts a schematic diagram of a conventional VLAN system; Rijhsinghani at Fig. 7:  FIG. 7 Rijhsinghani at 7:33-34 FIG. 7 depicts a VLAN system in accordance with the present invention;

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	Rijhsinghani at 4:1-54: The NMS 290 of the system shown in FIG. 5 is capable of configuring different types of VLANs as is understood by those skilled in the art. For example, VLANs may be port-based, address-based, protocol-based, port and protocol-based, or address and protocol-based. When the NMS 290 configures a VLAN, the NMS instructs the appropriate switches to identify the VLAN for packets received at the switch. Identifying the appropriate VLAN for a packet enables the switch to transmit the packet over the appropriate VLAN. For a port-based VLAN, the NMS configures the VLAN to include LANs connected at certain access ports 305 of certain switches. The NMS instructs each certain switch to identify the VLAN for a packet based upon the access port at which the packet is received. For an address-based VLAN, the NMS configures the VLAN to include certain addresses. If a switch is connected to a LAN at an access port 305 that includes one of the certain addresses, the NMS instructs the switch to identify the VLAN for a packet when received at the access port based upon the source address 116 included in the packet. For a protocol-based VLAN, the NMS 290 configures the VLAN based upon a system user's ability to transmit and receive communications following a particular protocol, whether that protocol is proprietary or open. The NMS instructs the switches to identify the VLAN based upon the protocol identifier 114 included in the packet received at an access port 305. For port and protocol-based VLANs, the NMS 290 instructs the switches that include certain access ports to identify the VLAN for a packet based upon the access port at which the packet is received and the protocol identifier 114 included in the packet received. For address and protocol-based VLANs, the NMS 290 instructs the switches connected to certain addresses to identify the VLAN for the packet based on the source address 116 and the protocol identifier 114 included in the packet. FIG. 6 depicts a system with various LANs 205-260 configured into a number of different types of VLANs 800-1200 by the NMS 290 in a conventional manner. VLAN 800 is a port-based VLAN including LANs 210, 235, and 240. VLAN 900 is an address-based VLAN including addresses K, V, L, N, U, Q, R, S, and T. VLAN 1000 is a protocol-based VLAN including protocol P1. Protocol-based VLAN 1000 is not explicitly depicted in FIG. 6 because any packet may be identified with

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	VLAN 1000 if the packet includes a protocol identifier for protocol P1. As the name “protocol-based” implies, VLAN 1000 is independent of the address of the system user, or the port connected to the LAN on which the system user resides. VLAN 1100 is a port and protocol-based VLAN including LANs 235, 240, 245, and 250 and protocol P1. Finally, VLAN 1200 is an address and protocol-based VLAN including addresses K, L, M, U, Q, T and protocol P1. Rijhsinghani at 6:25-7:15: Accordingly, the present invention provides rules of precedence for directing communications within different types of VLANs, in order to provide for predictable and desirable network behavior when there are areas of the network in which there is overlap in VLAN configurations, and to allow conflict resolutions by switches in the VLAN system. Advantageously, switches are provided that route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, based upon predefined rules of precedence. Advantageously, switches route communications to addressees, within a VLAN system capable of configuring multiple types of VLANs, in a secure manner. Physical security is ensured by giving a higher precedence to port-based VLAN classifications than to other types of VLAN classifications. In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-ported reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g. a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (I) the port and protocol-based virtual networks precedence over the port-based virtual

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks. Typically, the communication will include at least a source address and a protocol identifier, which the switch control detects, along with the port at which the communication is received, to identify the VLAN. After the VLAN has been identified, the switch control adds a VLAN tag representing the identified VLAN to form a VLAN communication. The switch control then directs the VLAN communication to the second communication port for transmission over the identified virtual local area network. In accordance with other aspects of the invention, a virtual communications system can be implemented using multiple switches of the type described above. A network manager, interconnected to the multiple switches, is capable of configuring virtual local area networks of differing types a described above. Rijhsinghani at 7:49-8:5: FIG. 7 depicts a virtual communications system or network in accordance with the present invention. The network includes multiple Local Area Networks (LANs) 205-260 interconnected by multiple multi-ported reconfigurable switches 270', 275' and 280' all of which are connected by a high speed backbone LAN 265, often referred to as the trunk. Each LAN, other than the backbone LAN 265 is connected to one of the switches 270', 275' or 280' by an access port 305, while the backbone LAN 265 is connected to each switch by a trunk port 315. A network management station (NMS) 290', which may be a workstation having network management software loaded thereon, manages the network by configuring the network via the switches 270', 275' and 280' to form one or more virtual local area networks (VLANs). A trunk station 285 is connected to the backbone LAN 265 via a trunk port 315. The trunk stations 285 may, for example, be a network server or other network resource to which some or all of the members of the LANs 205-260 may require high speed access from time to time or on a continuous basis as is known in the art. Each of the switches 270', 275' and 280' is

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	capable of linking, via the backbone LAN 265, members of each of the LANs 205-260 to members of the one or more other LANs within the VLANs configured by the NMS 290'. Rijhsinghani at 10:64-11:4: In step 1330, in the case of more than one VLAN match, the applicable switch 270'-280' identifies which of the VLAN type matches has the highest priority based upon the order of precedence described above, i.e., port and protocol-based over port-based, port-based over address and protocol-based, address and protocol-based over address-based, and address-based over protocol-based, as shown in FIG. 11.
[7.b] a switch apparatus of the switch apparatuses comprising:	Rijhsinghani discloses, expressly and/or inherently, a switch apparatus of the switch apparatuses. <i>See, e.g.:</i> Rijhsinghani at Fig. 8:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 Rijhsinghani at 7:35-38:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 depicts a switch which can be utilized in the VLAN system depicted in FIG. 7 in accordance with the present invention; Rijhsinghani at 6:42-67: In accordance with the present invention, a switch is provided for use in a virtual communications system having multiple local area networks interconnected by multiple switches so as to be configurable into different types of virtual local area networks. The different types of virtual local area networks may include, for example, port-based networks, address-based networks, protocol-based networks, port and protocol-based networks, and address and protocol-based networks. The switch is preferably a multi-ported reconfigurable switch and includes a first communications port, e.g. an access port, connected directly to a local area network and a second communications port, e.g. a trunk port, interconnected with other system switches typically via a backbone LAN or trunk. A switch control detects a communication from the local area network at the first port and identifies a virtual local area network over which the communication is to be transmitted based upon rules of precedence for different types of virtual local area networks. The rules of precedence preferably provide (i) the port and protocol-based virtual networks precedence over the port-based virtual networks, (ii) the port-based virtual networks precedence over the address and protocol-based virtual networks, (iii) the address and protocol-based virtual networks precedence over the address-based virtual networks, and (iv) the address-based virtual networks precedence over the protocol-based virtual networks.
[7.c] a storage storing a table, the table including rules and actions corresponding to the rules; and	Rijhsinghani discloses, expressly and/or inherently, a storage storing a table, the table including rules and actions corresponding to the rules. <i>See claim 1.a.</i>
[7.d] a controller comprising:	Rijhsinghani discloses, expressly and/or inherently, a controller. <i>See claim 1.b.</i>

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
[7.e] a memory storing instructions; and	Rijhsinghani discloses, expressly and/or inherently, a memory storing instructions. <i>See claim 1.c.</i>
[7.f] a processor configured to execute the instructions to:	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute the instructions. <i>See claim 1.d.</i>
[7.g] receive the rules and the actions from a controller;	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute the instructions to receive the rules and the actions from a controller. <i>See claim 1.e.</i>
[7.h] identify, based on the rules, a received packet;	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute the instructions to identify, based on rules, a received packet. <i>See claim 1.f.</i>
[7.i] duplicate a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation;	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute the instructions to duplicate a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation. <i>See claim 1.g.</i>
[7.j] encapsulate the identified packet by the additional header; and	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute the instructions to encapsulate the identified packet by the additional header. <i>See claim 1.h.</i>

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
[7.k] process, based on the actions, the identified packet.	Rijhsinghani discloses, expressly and/or inherently, a processor configured to execute the instructions to process, based on actions, the identified packet. <i>See claim 1.i.</i>
8. The communication system according to claim 7, wherein the processor is further configured to execute the instructions to send header information to the control apparatus when the identified packet comprises an encapsulated packet.	Rijhsinghani discloses, expressly and/or inherently, the communication system according to claim 7, wherein the processor is further configured to execute the instructions to send header information to the control apparatus when the identified packet comprises an encapsulated packet. <i>See claims 2, 7.</i>
9. The communication system according to claim 8, wherein the header information includes the additional header.	Rijhsinghani discloses, expressly and/or inherently, the communication system according to claim 8, wherein the header information includes the additional header. <i>See claims 3, 8.</i>
10. The communication system according to claim 9, wherein the processor is further configured to execute further instructions to decapsulate the encapsulated packet.	Rijhsinghani discloses, expressly and/or inherently, the communication system according to claim 9, wherein the processor is further configured to execute further instructions to decapsulate the encapsulated packet. <i>See claims 4, 9.</i>
11. The communication system according to claim 7, wherein the processor is	Rijhsinghani discloses, expressly and/or inherently, the communication system according to claim 7, wherein the processor is further configured to execute the instructions for translation of the first header data of a head of the received packet into the second header data.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
further configured to execute the instructions for translation of the first header data of a head of the received packet into the second header data.	<i>See claims 5, 7.</i>
12. The communication system according to claim 11, wherein the instructions to encapsulate the identified packet includes notifying the controller of first header data before the translation and second header data after the translation.	Rijhsinghani discloses, expressly and/or inherently, the communication system according to claim 11, wherein the instructions to encapsulate the identified packet includes notifying the controller of first header data before the translation and second header data after the translation. <i>See claims 6, 11.</i>
[13.pre] 13. A communication method, comprising:	Dell takes no position in these Invalidity Contentions on whether the entirety of the preamble of this claim is a limitation. To the extent it is a limitation, Rijhsinghani discloses, expressly and/or inherently, a communication method. <i>See claim 7.pre.</i>
[13.a] receiving rules and actions from a controller;	Rijhsinghani discloses, expressly and/or inherently a communication method comprising receiving rules and actions from a controller. <i>See claims 1.e, 7.g.</i>
[13.b] identifying, based on the rules, a received packet;	Rijhsinghani discloses, expressly and/or inherently a communication method comprising identifying, based on the rules, a received packet.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	<i>See</i> claims 1.f, 7.h.
[13.c] duplicating a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation;	Rijhsinghani discloses, expressly and/or inherently a communication method comprising duplicating a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation. <i>See</i> claims 1.g, 7.i.
[13.d] encapsulating the identified packet by the additional header; and	Rijhsinghani discloses, expressly and/or inherently a communication method comprising encapsulating the identified packet by the additional header. <i>See</i> claims 1.h, 7.j.
[13.e] processing, based on the actions, the identified packet.	Rijhsinghani discloses, expressly and/or inherently a communication method comprising processing, based on the actions, the identified packet. <i>See</i> claims 1.i, 7.k.
14. The communication method according to claim 13, further comprising: sending header information to a controller when the identified packet comprises an encapsulated packet.	Rijhsinghani discloses, expressly and/or inherently, the communication method according to claim 13, further comprising sending header information to a controller when the identified packet comprises an encapsulated packet. <i>See</i> claims 2, 8, 13.
15. The communication method according to claim 14, wherein the header information includes the additional header.	Rijhsinghani discloses, expressly and/or inherently, the communication method according to claim 14, wherein the header information includes the additional header. <i>See</i> claims 3, 9, 14.

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
16. The communication method according to claim 15, further comprising: executing further instructions to decapsulate the encapsulated packet.	Rijhsinghani discloses, expressly and/or inherently, the communication method according to claim 15, further comprising executing further instructions to decapsulate the encapsulated packet. <i>See claims 4, 10, 15.</i>
17. The communication method according to claim 14, further comprising: translating first header data of a head of the received packet into second header data.	Rijhsinghani discloses, expressly and/or inherently, the communication method according to claim 14, further comprising translating first header data of a head of the received packet into second header data. <i>See claims 5, 11, 14.</i>
18. The communication method according to claim 17, further comprising: notifying the controller of the first header data before the translating and the second header data after the translating.	Rijhsinghani discloses, expressly and/or inherently, the communication method according to claim 17, further comprising notifying the controller of the first header data before the translating and the second header data after the translating. <i>See claims 6, 12, 17.</i>
[19.pre] 19. A non-transitory recording medium recording a program which when executed causes a switch to perform a method, the method comprising:	Dell takes no position in these Invalidity Contentions on whether the entirety of the preamble of this claim is a limitation. To the extent it is a limitation, Rijhsinghani discloses, expressly and/or inherently a non-transitory recording medium recording a program which when executed causes a switch to perform a method. <i>See, e.g.:</i> Rijhsinghani at Fig. 8:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

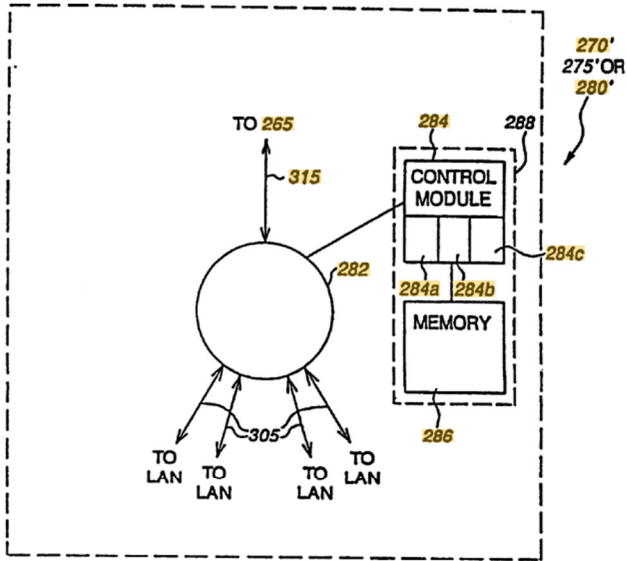
Asserted Claims	Rijhsinghani
	 FIG. 8 Rijhsinghani at 7:35-38:

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
	FIG. 8 depicts a switch which can be utilized in the VLAN system depicted in FIG. 7 in accordance with the present invention; Rijhsinghani at 8:6-15: As shown in FIG. 8, each of the switches 270', 275' and 280' includes a control console 288 having a control module 284 and a memory 286 for storing and processing control and VLAN configuration instructions. This data may be initially programmed into the switch or transmitted to the switch by the NMS 290'. The control module 284 includes a controller 284 a to control the switching device 282. A detector 284 b detects a communication packet received from the backbone 265 via a trunk port 315 or from a LAN directly connected to the switch via an access port 305.
[19.a] receiving rules and actions from a controller;	Rijhsinghani discloses, expressly and/or inherently, a method comprising receiving rules and actions from a controller. <i>See claims 1.e, 7.g, 13.a.</i>
[19.b] identifying, based on the rules, a received packet;	Rijhsinghani discloses, expressly and/or inherently, a method comprising identifying, based on the rules, a received packet. <i>See claims 1.f, 7.h, 13.b.</i>
[19.c] duplicating a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation;	Rijhsinghani discloses, expressly and/or inherently, a method comprising duplicating a part of a header of the identified packet as an additional header when the identified packet comprises a target of encapsulation. <i>See claims 1.g, 7.i, 13.c.</i>

Exhibit C6 – Rijhsinghani Invalidity Claim Chart for the '177 Patent

Asserted Claims	Rijhsinghani
[19.d] encapsulating the identified packet by the additional header; and	Rijhsinghani discloses, expressly and/or inherently, a method comprising encapsulating the identified packet by the additional header. <i>See claims 1.h, 7.j, 13.d.</i>
[19.e] processing, based on the actions, the identified packet.	Rijhsinghani discloses, expressly and/or inherently, a method comprising processing, based on the actions, the identified packet. <i>See claims 1.i, 7.k, 13.e.</i>
[20.pre] 20. The non-transitory recording medium, according to claim 19, the method further comprising: sending header information to the controller when the identified packet comprises an encapsulated packet,	Rijhsinghani discloses, expressly and/or inherently, the non-transitory recording medium according to claim 19, the method further comprising sending header information to the controller when the identified packet comprises an encapsulated packet. <i>See claims 2, 8, 14, 19.</i>
[20.a] wherein the header information includes the additional header.	Rijhsinghani discloses, expressly and/or inherently, the non-transitory recording medium according to claim 19, the method further comprising sending header information to the controller when the identified packet comprises an encapsulated packet wherein the header information includes the additional header. <i>See claims 3, 9, 15.</i>