WHAT IS CLAIMED IS:

1. An autonomous network comprising:

a plurality of switches, each switch including a plurality of network interfaces, and configured to:

receive a data packet addressed to a device located outside the network;

obtain from a header of the received outgoing data packet data indicative of a network interface over which to transmit the outgoing data packet; and

transmit the outgoing data packet over the network interface indicated in the data obtained from the header;

a data packet processor, located remotely from the plurality of switches, configured, for an outgoing packet, to:

identify one of the plurality of switches of the autonomous network to transmit the outgoing data packet out of the network and a network interface of the identified switch over which the identified switch is to transmit the outgoing data packet;

add an indication of the identified switch and the identified network interface to a header of the outgoing data packet; and

forward the outgoing data packet to the identified switch;

a controller configured to:

determine routing paths for routing data packets; and

provide routing information, associated with the determined routing paths, to the data packet processor, sufficient for the data packet processor to identify switches and network interfaces of switches to transmit outgoing data packets.

2. The autonomous network of claim 1, wherein in determining the routing paths, the controller is further configured to:

collect information from network elements of the network; and

determine the routing paths based on the collected information.

3. The autonomous network of claim 2, wherein in collecting the information, the controller is further configured to collect information regarding Internet routing paths from a border gateway protocol (BGP) module.

4. The autonomous network of claim 2, wherein in collecting the information, the controller is further configured to collect information regarding internal routing paths from backbone network elements of the autonomous network.

5. The autonomous network of claim 4, wherein the information regarding the internal routing paths includes at least one of information about the volume of traffic across the paths, the service classes supported across the paths, and quality of the paths.

6. The autonomous network of claim 1, wherein in adding an indication of the identified switch and the identified network interface, the data packet processor is further configured to encapsulate the data packet with a general routing encapsulation (GRE) header or to add a multiprotocol label switching (MPLS) label to the header of the data packet.

7. The autonomous network of claim 1, wherein the data packet processor is further configured to filter data packets originating outside the network.

8. The autonomous network of claim 7, wherein filtering includes at least one of access control list (ACL) filtering and dynamic denial of service (DoS) filtering.

9. The autonomous network of claim 1, wherein the data packet processor is further configured to, in response to receiving a synchronize (SYN) data packet from a device located outside of the network, generate a secure SYN acknowledgement for transmission to a device originating the SYN data packet.

10. The autonomous network of claim 1, wherein in transmitting the outgoing data packet, a switch of the plurality of switches is configured to:

remove the indication of the identified switch and the identified network interface; and

transmit the data packet, with the indication removed, over the network interface indicated in the data obtained from the header.

11. The autonomous network of claim 1, wherein the data packet processor is a general purpose processor.

12. The autonomous network of claim 1, wherein the data packet processor includes a cache memory, and is further configured to store the routing formation received from the controller in the cache memory.

13. A method for handling data packets in an autonomous network, comprising:

receiving, by a switch of a plurality of switches, a data packet addressed to a device located outside the network, each switch of the plurality of switches including a plurality of network interfaces;

obtaining, by the switch, from a header of the received outgoing data packet data indicative of a network interface over which to transmit the outgoing data packet; and

transmitting, by the switch, the outgoing data packet over the network interface indicated in the data obtained from the header;

identifying, by a data packet processor located remotely from the plurality of switches of the autonomous network, one of the plurality of switches to transmit the outgoing data packet out of the network and a network interface of the identified switch over which the identified switch is to transmit the outgoing data packet;

adding, by the data packet processor, an indication of the identified switch and the identified network interface to a header of the outgoing data packet; and

forward, by the data packet processor, the outgoing data packet to the identified switch;

determining, by a controller, routing paths for routing data packets;

providing, by the controller, routing information, associated with the determined routing paths, to the data packet processor, sufficient for the data packet processor to identify switches and network interfaces of switches to transmit outgoing data packets.

14. The method of claim 13, wherein determining the routing paths includes:

collecting information from network elements of the network; and

determining the routing paths based on the collected information.

15. The method of claim 14, wherein collecting the information includes collecting information regarding Internet routing paths from a border gateway protocol (BGP) module.

16. The method of claim 14, wherein collecting the information includes collecting information regarding internal routing paths from backbone network elements of the network.

17. The method of claim 16, wherein the information regarding the internal routing paths includes at least one of information about the volume of traffic across the paths, the service classes supported across the paths, and quality of the paths.

18. The method of claim 14, wherein adding an indication of the identified switch and the identified network interface includes encapsulating the data packet with a general routing encapsulation (GRE) header or adding a multiprotocol label switching (MPLS) label to the header of the data packet.

19. The method of claim 13 further comprising filtering, by the data packet processor, data packets originating outside the network.

20. The method of claim 19, wherein filtering includes at least one of access control list (ACL) filtering and dynamic denial of service (DoS) filtering.

21. The method of claim 13 further comprising, in response to receiving a synchronize (SYN) data packet from a device located outside the network, generating, by the data packet processor, a secure SYN acknowledgement for transmission to a device originating the SYN data packet.

22. The method of claim 13, wherein transmitting the outgoing data packet over the network interface includes:

removing the indication of the identified switch and the identified network interface; and

transmitting the data packet, with the indication removed, over the network interface indicated in the data obtained from the header.

23. The method of claim 13, wherein the data packet processor is a general purpose processor.

24. The method of claim 13 further comprising storing, by the data packet processor, the routing formation received from the controller in a cache memory of the data packet processor.

25. A computer-readable medium with computer code instructions stored thereon, the computer code instructions, when executed by a processor, are configured to cause an apparatus to:

identify, based on routing information received from a controller, one of a plurality of switches to transmit an outgoing data packet out of a network and a network interface of the identified switch over which the identified switch is to transmit the outgoing data packet;

add an indication of the identified switch and the identified network interface to a header of the outgoing data packet; and

forward the outgoing data packet to the identified switch.