

Integrated Networking

The dynamic nature of network connectivity dictates that whatever solutions enterprises choose, must interoperate with their existing infrastructure. Juniper Networks solutions can easily fit into a switched environment with Transport mode, which allows enterprises to deploy the device without having to change the network. Juniper's entire line of integrated firewall/IPSec VPN solutions supports a robust set of routing protocols to easily integrate with existing solutions while simultaneously providing enterprises with the flexibility to quickly change configurations without impacting the budget.

Through support for industry standard routing protocols such as BGP, OSPF and RIPv2, Juniper's entire product line can quickly be integrated into an existing routing infrastructure while performing common routing functions. An added benefit of the integrated networking capabilities is the fact that it will provide enterprises with increased redundancy and support for multiple ISPs.

When combined with integrated FW/VPN security features, dynamic routing facilitates:

- Route based VPNs: The ability to define multiple VPN tunnels and based upon a routing decision, the best VPN tunnel will be used for traffic.
- Subnet additions: Flexibility of routing protocol support simplifies the addition of subnets, requiring less administrative effort when network configurations change.
- Multiple ISP Support: Dynamic routing, when combined with path monitoring, enables automatic connection failover to an alternate route and/or ISP.
- Network level High Availability: Dynamic routing helps make the Juniper Networks High Availability solution one of the most comprehensive on the market by automatically finding the open route in a fully meshed configuration.

Adding to the multiple levels of device redundancy and reliability, the Juniper Networks firewall/VPN appliances integrate dynamic routing with OSPF and BGP. While not designed for core Internet routing functions, dynamic routing allows a Juniper Networks device to integrate with the routing infrastructure for both firewall and VPN functions.

Juniper Networks integrated networking protocol support not only simplifies network integration, it also facilitates built-in High Availability and route-based VPN functionality.

Neighbor: To begin configuring a BGP network, administrators need to establish a connection between the current device and a counterpart, adjacent device known as a neighbor or peer. While this may seem like unneeded information at first, it is actually central to the way BGP works. Unlike RIP or OSPF, administrators now have to configure two devices, both the current router and its neighbor, for BGP to work. While this requires more work, it enables networking to occur on a larger scale as BGP eludes deploying the limited advertising techniques inherent to interior networking standards. There are two types of BGP neighbors: **internal neighbors** which are in the same autonomous system and **external neighbors** which are in different autonomous systems. A reliable connection is required between neighbors and is achieved by creating a TCP connection between the two. The handshake that occurs between the two prospect neighbors evolves through a series of phases or states before a true connection can be made. A reliable connection is required between neighbors and is achieved by creating a TCP connection between the two. The handshake that occurs between the two prospect neighbors evolves through a series of phases or states before a true connection can be made.

Dynamic Routing Protocol (DRP) – Inter-router communications that enable routers to automatically exchange and update information about known routes. Examples include Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP).

Open Shortest Path First (OSPF) – Popular DRP used in Enterprise routing. “Open” refers to the fact that this protocol is an Open Standard – not proprietary (like some other protocols such as Cisco's IGRP and EIGRP). OSPF is a link state protocol (as opposed to vector-based such as RIP and RIP v2) in that it keeps track of routes by which links are active, and assigns costs to egress links to enable it to calculate the best route. RFC 1583 describes OSPF v2.

OSPF Area – All routers in an OSPF Area share a common database of subnets and links and determine the best routes collectively. OSPF routers form an Adjacency with Neighbors to determine routing peers. This is done with OSPF Hello Packets – a Multicast packet addressed to OSPF routers only.

Border Gateway Protocol (BGP) – Popular DRP used in inter-ISP routing (technically, an inter-Autonomous System routing protocol). In BGP, clusters of common networks are grouped into Autonomous Systems (AS). BGP then exchanges information between these AS as to what subnets belong to what AS, and by what paths different AS communicate. BGP is an extremely flexible and advanced protocol. The entire BGP protocol set is not supported by NetScreen ScreenOS, and Juniper Networks integrated firewall/IPSec VPN devices should not be used as a Border Gateway Router. BGP is included in ScreenOS in order for it to learn routes from a Border Gateway Router. RFC 1771 describes BGP v4, while RFC's 1772-1774 go into more detail about the protocol.

BGP Autonomous System – An Autonomous System is a collection of CIDR IP address prefixes under common technical management.

Network Convergence – The period of time it takes for all routers in a routing area to agree on the same routes. Some DRP's can take many minutes to converge. While the route-map is out of synch, routing errors can occur, which cause portions of the network to lose connectivity with each other. Generally, event-driven DRP's (like OSPF) can react faster to network changes than periodic DRP's (like RIP).

Routing protocols - Administrators can configure a router statically by manually configuring route entries one-by-one. They can also configure a router to learn routes dynamically from neighboring routers using a routing protocol such as OSPF or BGP. While static routing offers the most control, it is not as flexible as dynamic routing. With static routing, any change to the network topology (for example, an interface that becomes inoperable) usually requires the intervention of a network administrator. With dynamic routing, a router can automatically update its route table without the help of an administrator whenever a change to the network topology occurs.