

Nortel Networks IP-VPN Services on Passport Multiservice Platforms

With dramatic increases in eBusiness, leading enterprises are looking for service providers to supply new networking environments that support personalized customer relationships.

To answer these needs, Nortel Networks offers a full portfolio of solutions that provide an agile subscriber-aware environment based on advanced IP services. One critical component is the Passport IP-VPN, which provides the necessary infrastructure with all the features of a private network, but with more flexibility and lower cost.

If you're a current Passport customer or a service provider planning to build new networks based on Passport, all you need is a software upgrade to enter this market. And as your business grows, you can easily evolve to a complete IP-VPN solution.

According to IDC, total IP-VPN service revenues will grow from \$5.2 billion in 2001 to \$21.3 billion in 2005 for a compound annual growth rate (CAGR) of 41.9 percent. Leading service providers are building networks and offering services to capture early market share. To meet service provider needs, Nortel Networks offers a complete portfolio of IP-VPN solutions.

Nortel Networks delivers a range of IP-VPN services

Nortel Networks has a full portfolio of solutions enabling service providers to offer IP-VPN services. These can operate over a range of data networks and can be configured for intranet, extranet, Internet, and a variety of access options.

What is an IP-VPN?

A managed IP service offered to an enterprise by a service provider over a shared public network infrastructure, which provides secure and reliable connectivity, management, and addressing equivalent to that of a private network.

IP-VPNs fall into two categories, depending on who implements them—the enterprise customer or the service provider.

Enterprise VPNs are based on customer premises equipment (CPE) owned and operated by the enterprise. The CPE device or VPN gateway uses standards-based tunnels over a public IP network. The enterprise handles all provisioning and management. CPE-based VPNs may operate over the Internet or a service provider's IP network. Nortel Networks Contivity is the market-leading solution for this service.

Service-provider VPNs are based on provider-managed equipment located either on the customer premises (CLE) or in the service provider's central office (CO). These are often referred to as network-based VPNs.

CLE-based VPNs are identical in operation to CPE-based VPNs, but the equipment is owned and operated by the service provider.

CO-based VPNs are implemented at the subscriber network edge and operate over the service provider's public IP network. Nortel Networks Passport and Shasta—managed by Preside Multiservice Data Manager—are market-leading examples of network-based VPN solutions.

Passport provides a network-based intranet service now

If you already own a Passport multi-service network, you currently have intranet IP-VPN capabilities. You need only the appropriate software to take advantage of this cost-effective market-entry strategy.

Passport IP-VPN is ideal for medium-to-large enterprises that want their service provider to supply flexible, reliable, low-cost site-to-site connectivity using dynamic routing protocols, IP Quality of Service (QoS), and the industry's largest breadth and depth of interfaces including IP over PPP, IP over frame relay, IP over Ethernet, and IP over ATM.

Passport delivers high-value IP-VPN services

Service providers can further differentiate their service offering and generate incremental revenues by complementing and expanding their Passport IP-VPN service with a remote access or secure, managed IPsec CPE VPN via Contivity and high-value, network-based IP services such as firewall and network address translation (NAT) with the Shasta 5000 Broadband Service Node (BSN). Passport, combined with other Nortel Networks products, enables a full range of IP-VPN services. In addition to intranet service, service providers can offer:

Internet-access VPN—A secure service allowing users of a VPN to access the Internet, or conversely, to access their VPN from the Internet. Key technologies offered by Shasta for this service are firewall and NAT.

Extranet VPN—The same key technologies that enable Internet-access VPN also enable extranet VPN, permitting enterprises to share network resources securely with their business partners. Extranet services facilitate global virtual corporations, eCommerce to the global customer base, and shared development with partners.

Access VPN—Enables all types of user access to the VPN. Options available today include WAN access (via leased lines, IP over frame relay, IP over ATM, or IP over PPP), dial access, cable modem access, or wireless access. Access VPN services can be offered separately from Internet-access VPNs and depend on technologies such as encryption, authentication, and packet steering.

What makes Passport IP-VPN services exceptional?

Passport's renowned reliability, smooth migration design, and scalable architecture—combined with Preside Multi-service Data Manager, an integrated network, service, and policy management software platform—make Passport IP-VPN exceptional in the industry for delivering truly business-grade IP-VPN services.

Powerful IP-VPN service

The Passport architecture offers a revolutionary, cost-effective way of creating multiple, segregated IP-VPNs within a shared environment. Virtual routers (VRs)—on Passport 7400, 15000, and 20000 platforms—are routing engines that provide the functions of physical routers, as well as the ability to separate traffic from different VPNs. Using VRs, service providers can allow enterprises to retain their own private IP

addressing structures, while retaining secure separation between different enterprise VPNs—all without capital- and labor-intensive physical routers.

VRs are fully compatible with physical routers, use standards-based routing protocols, and can operate over existing service provider Layer 2 networks without modification. This gives service providers the ability to seamlessly interwork their IP-VPN service with existing frame relay services—providing flexibility in customer service deployment and migration options. Enterprise customers can test out the service on new sites and then phase in remaining ones as they gain confidence that the service can meet their needs with the same service and availability levels.

Integrated IP Quality of Service

IP networks have traditionally not provided any Quality of Service (QoS) capabilities or guarantees. They are normally described as "best effort" networks where packets may be delayed and even dropped if they experience congestion. Furthermore, the network elements (routers, switches) make no distinction between one packet and another when deciding which packets to drop, so more important traffic may be dropped while less important traffic is forwarded.

These traditional IP networks are not suitable for delivering true "business-grade" IP-VPN services that carry many types of traffic—including voice or video, which require timely and guaranteed delivery. Passport's integrated IP QoS solution, compliant with RFC2474, provides for classification, marking, and queuing of the IP flows to the required DiffServ treatment. IP CoS is translated to Layer 2 media that delivers the desired QoS to the IP flow. In addition to being able to offer IP differentiated services, Passport allows

service providers to dedicate bandwidth per VPN or group of VPNs. This permits the carrier to offer end-to-end bandwidth guarantees to IP-VPN customers.

High-service availability with proven Passport architecture

Passport offers service providers the highest levels of reliability, allowing them to build their business on this platform with confidence. Passport is deployed successfully in many of the largest data networks in the world. Its reputation as the most reliable multiservice carrier-grade switch is renowned—exemplified by it being one of the only packet-core switches to be deployed in regulated voice environments. Passport continues to build on its reputation for reliability and raises the bar with new carrier-grade IP routing capabilities that provide non-stop service availability and IP data forwarding even in the event of equipment failures or switchovers.

Business-grade IP-VPN services with QoS and SLAs

The ability to differentiate services and offer enterprise customers unique value is a key benefit of IP-VPNs. Service Level Agreements (SLAs) can be established with each customer to meet particular needs, and are complemented by applications allowing customers to verify that service providers are meeting their commitments.

Passport SLAs are based on quality of service (QoS) attributes such as bandwidth required, acceptable level of packet loss, network transit delays, and security levels for different types of customer traffic. These parameters permit customers to detail how different types of traffic are processed based on user, application, or traffic type. QoS requirements for each of these traffic types can be mapped onto frame relay, ATM, or MPLS.

Preside Multiservice Data Manager service management applications allow service providers to meet enterprise service needs in a highly granulated way and enable customers to rigorously verify SLA compliance.

Consolidate service rules into a policy for each enterprise

The complete set of rules governing how a particular enterprise's traffic will be treated is termed policy. The ability to deal explicitly with policy and reflect the exact needs of the enterprise is a hallmark of the most advanced IP-VPN services, providing a rich source of service differentiation.

For example, a policy might include the urgency of a traffic stream, its degree of criticality to the business, and its security requirements. Also, an enterprise may have specific accounting or billing requirements and overall service requirements, such as availability and time to repair.



**Passport
15000**

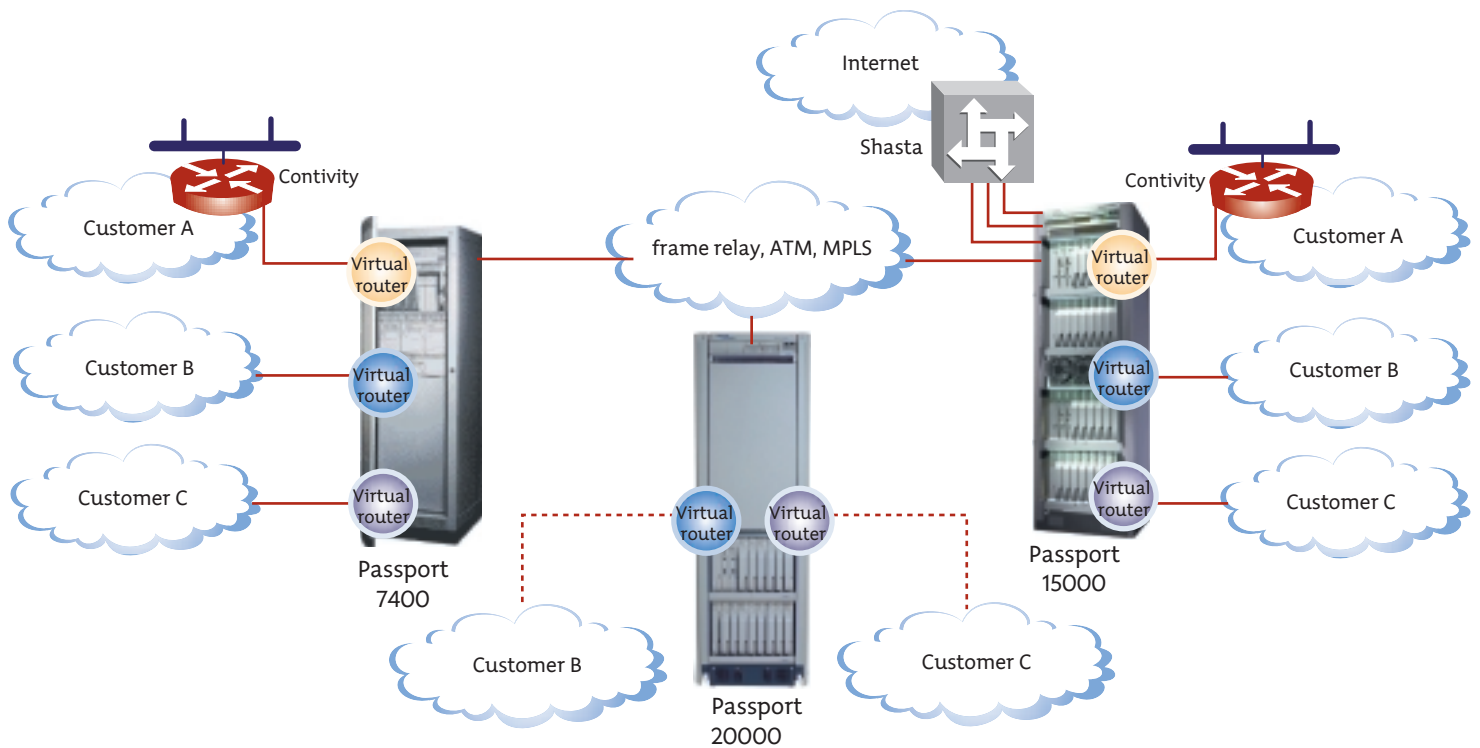


Figure 1: *Passport provides network-based intranet IP-VPNs today. When combined with other Nortel Networks products such as Contivity and Shasta, Passport enables service providers to add unique, high-value services such as firewalls; network address translation; virus detection; intrusion detection; and managed and unmanaged, secure customer premises equipment (CPE)-based IP-VPN services.*

In addition to its customers' policies, a service provider may have its own set of policies for the operation of its IP-VPN service. Effective policy management is an essential requirement of an IP-VPN service, particularly to support mass deployment.

Preside Multiservice Data Manager offers a full range of policy management features for Passport IP networks.

Enjoy complete service and network management

Preside Multiservice Data Manager provides network management services such as device/network configuration and provisioning, element alarm control, and fault surveillance.

Preside Multiservice Data Manager helps service providers expand their focus beyond network infrastructure management to service delivery and

creating personalized relationships with their customers. Preside Multiservice Data Manager delivers integrated service provisioning, accounting mediation, service performance and SLA management, and service control applications for IP-based service types. Rapidly delivering premium IP-VPN services moves networking up the value chain and increases revenue opportunities, while simplifying operations and reducing costs.

Be confident of high security and scalability

A Passport network is a secure network. Passport operates as a set of separate, independent VRs linked by separate logical trunks, so that data from each customer or VPN is kept separate from all other data flows.

With the introduction of the VPN Extender Cards (XC), Passport 7400, 15000, and 20000 switches are able to scale to thousands of VPNs per node. Additionally, engineering the network for revenue-generating multiservice traffic (including frame relay, ATM, CES, and voice) is greatly simplified. This high degree of security and scalability enables providers to offer IP-VPN service to a wide range of medium-to-large enterprises.

Core independence ensures compatibility with your network

The Passport IP-VPN service operates independently of the core network technology. It can be offered over frame relay, ATM, or MPLS infrastructures. Core independence allows providers to implement IP-VPNs now on their existing frame relay or ATM infrastructures, and then smoothly migrate these to MPLS when needed.

Key technical specifications

IP Services

- IP-VPNs for intranet service, VPN access, and extranet
- RFC 2764 (Virtual Routers), RFC 2547
- IP class of service/quality of service/DiffServ (RFC 2597, 2598, 2474)
- Routing protocols: OSPF, RIP V2, BGP-4, MPBGP-4, IS-IS, Static
- IP-VPN over ATM or MPLS, including LDP, CR-LDP and RSVP-TE
- IP-VPN Accounting
- VPN Membership Auto-discovery

Core Network Technologies

- Frame Relay
- ATM
- MPLS

Evolve your network easily— when you're ready

If you are currently running a Passport frame relay network, you have a network that supports robust Layer 2 VPNs and scales easily. For these networks, Nortel Networks continues to offer improvements in function and cost, plus specific IP-aware features that can be rapidly deployed to enhance operations and service offerings.

And, if you plan to evolve your service portfolio, with Passport you have a smooth migration path from frame relay to full Layer 3 IP-VPNs, with no need for flash cutovers of WAN or CPE equipment. For a large network, this migration can even take place incrementally.

For a fast, low-investment, low-risk way to offer IP-VPNs today, you can deploy Passport-only intranet services simply with a software upgrade—without modifying your network infrastructure or changing existing systems. Service can be rolled out within days; not months.

As service demand evolves, you can introduce the Shasta 5000 BSN into the network to further extend the range of IP-VPN services. These high-value, network-based services—such as network address translation, stateful firewalls, IPsec encryption, captive portals, and intrusion detection—enable a wide range of profitable applications, including secure Internet access, extranets, and flexible access networks.

Passport IP-VPN is business-ready now

Passport IP-VPN is available today. Leading service providers—such as Deutsche Telekom in Germany and Telstra in Australia—have chosen Passport IP-VPN services to gain early entry into this competitive market.

The logo for Nortel Networks, featuring the word "NORTEL" in a bold, blue, sans-serif font with a stylized globe icon integrated into the letter "O". Below it, the word "NETWORKS" is written in a similar bold, blue, sans-serif font with a trademark symbol (TM) to its upper right.

NORTEL NETWORKS™

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Metro Networks, Wireless Networks, and Optical Long Haul Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the web at:

www.nortelnetworks.com

In the United States:

Nortel Networks
35 Davis Drive
Research Triangle Park,
North Carolina 27709
USA

In Canada:

Nortel Networks
8200 Dixie Road,
Suite 100
Brampton, Ontario L6T 5P6
Canada

In Europe:

Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead Berkshire SL6 3QH
UK

In Asia:

Nortel Networks
6/F Cityplaza 4,
Taikooshing,
12 Taikoo Wan Road,
Hong Kong
Tel:(852)21002888

For more information, contact your Nortel Networks representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

Contivity, Nortel, Nortel Networks, the Nortel Networks corporate logo, the globemark design, Preside Multiservice Data Manager, Passport, Shasta, and are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2002 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

87003.22/05-02