

Building

A World of Choice

with

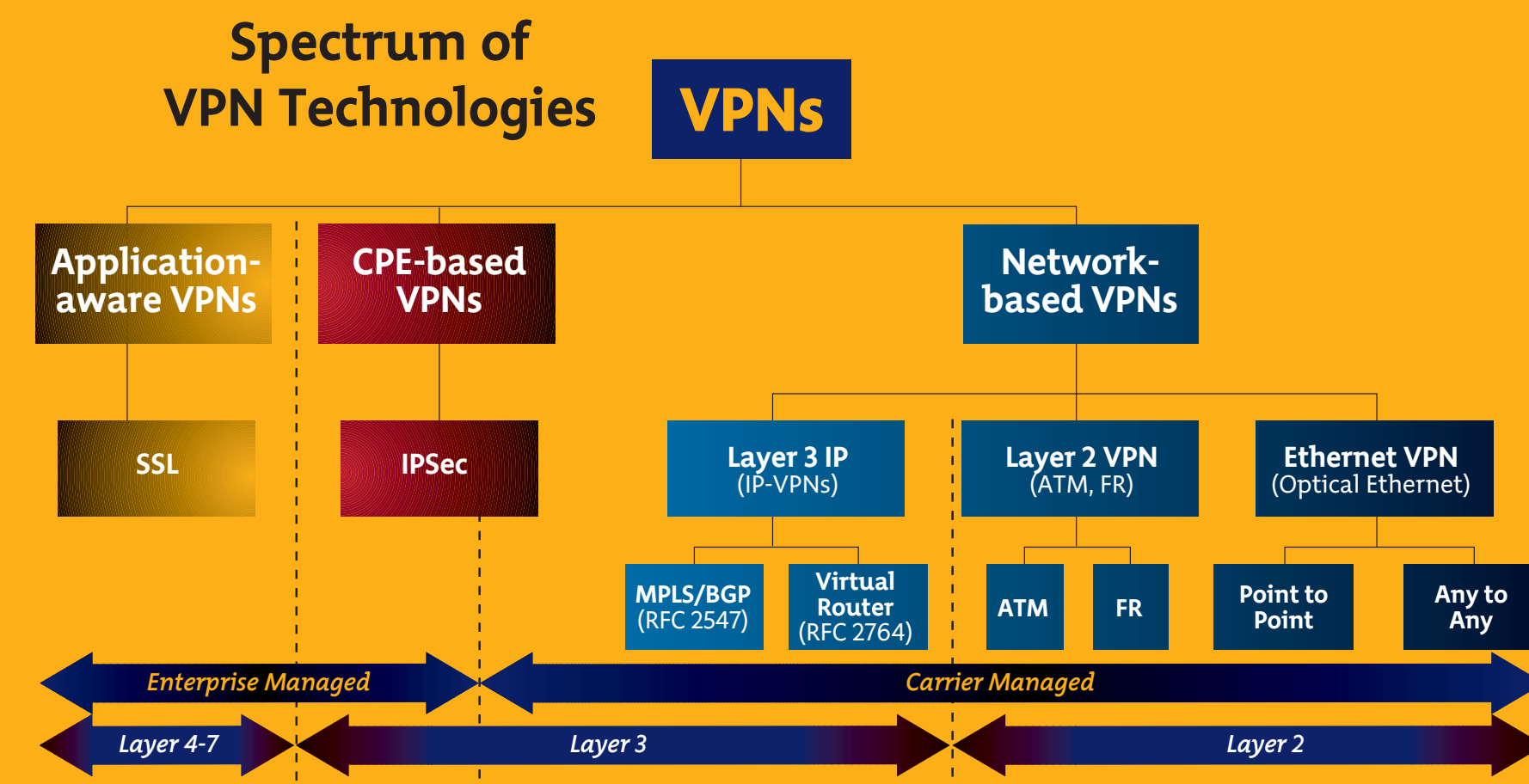
**NORTEL NETWORKS™**

www.nortelnetworks.com



## Nortel Networks VPN Solutions

Enabling secure, scalable, reliable and feature-rich VPN services over any type of infrastructure via any type of access.



### Contivity Secure IP Services Gateways

> Contivity 600, 1010, 1050, 1100, 1700, 2700 and 5000  
Platforms that deliver IP-VPN, routing, firewall, bandwidth management, encryption, authentication and data integrity for secure connectivity across managed IP networks and the Internet. They can connect remote users, branch offices, suppliers and customers with the cost and performance advantages of shared IP networks and the security and control of private networks.



### Shasta 5000 Broadband Service Node

An industry-leading convergence platform geared toward data service providers and enterprises. It delivers scalable, reliable and cost-effective advanced IP services and subscriber aggregation regardless of the access and network transport technologies/protocols. Capabilities of the platform extend to virtualized firewalls, IP-VPNs (Intranet, extranet, remote access, MPLS), advanced QoS, network address translation (NAT), policy routing and personalized content delivery.



### Passport Multiservice Switches

> Passport 6400, 7400, 15000 and 20000  
High-performance, flexible and reliable platforms that deliver highly available, cost effective, multi-service networking. A variety of multi-service protocols are supported on a single switch, including Frame Relay, ATM, MPLS, IP, IP-VPN, Layer 2 VPN, wireless transport, packet voice and circuit emulation. Passport's exceptional CoS and QoS capabilities have helped make it a leader in global WAN networking.



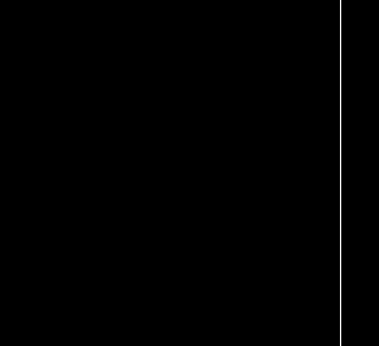
### Alteon SSL VPN Gateway

Securely addresses remote access and extends the reach of enterprise applications to mobile workers, telecommuters, partners and customers. By using secure sockets layer (SSL) as the underlying security protocol, the Alteon SSL VPN allows for truly unrestricted remote access, using the Internet for remote connectivity and the ubiquitous Web browser as the primary client interface.



### OPTera Metro Portfolio

OPTera Metro harnesses the power of DWDM and SONET/SDH technology to extend the value of optical networks. This enables service providers to offer innovative and profitable voice, multimedia and data services to their customers and gives enterprises access to these industry-leading services.

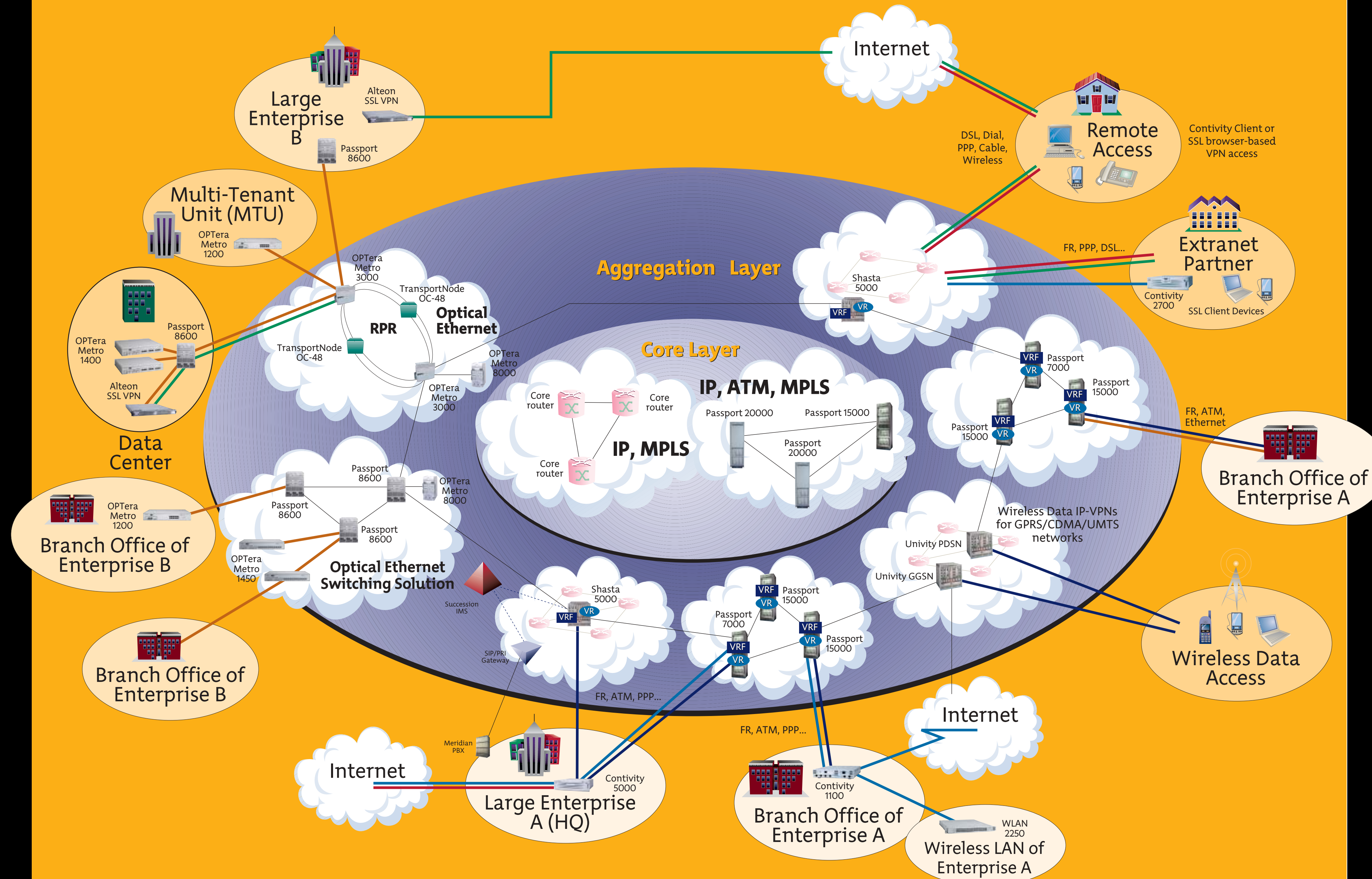


**OPTera Metro 1000 Ethernet Services Module:** Carrier-class edge device that simplifies the delivery of all types of Ethernet services by enabling simple and rapid provisioning.

**OPTera Metro 8000 Services Switch:** MPLS-based Ethernet switch supports any-to-any transparent LAN and VPN service on Layer 2 Ethernet networks.

**OPTera Metro 3000/4000 Multiservice Platforms:** A family of next-generation SONET/SDH products that enable the evolution and enhancement of existing metro networks, while setting a new economic benchmark for network efficiency and increasing broadband service capability.

**Passport 8600 Routing Switch:** High-density, high-performance Layer 2-Layer 7 switching, routing and traffic classification for enterprise, service provider and carrier customers.



### BGP/MPLS VPN

Also known as RFC2547bis—or more commonly referred to as RFC2547—is an Internet Engineering Task Force (IETF) draft specification for building a provider-provisioned IP-VPN using BGP and Multiprotocol Label Switching (MPLS). The Provider Edge router (PE), as defined for MPLS, maintains multiple forwarding table instances while running only a single routing protocol instance, thereby allowing the PE device to support full and private separation of customer IP-VPN traffic from all other traffic. Nortel Networks Passport Multiservice Switches and Shasta 5000 BSN support RFC2547.

### Network-based IP-VPN architecture using virtual routers

Also known as VR-based VPNs—consistent with RFC2764—is an IETF draft specification for building a provider-provisioned IP-VPN using the concept of virtual routers. A virtual router is a software and hardware based emulation of a physical router that inherits all of its various attributes. In the context of a VPN, virtual routers have independent IP routing and forwarding tables that are isolated from each other, enabling one platform to support numerous IP-VPNs with full and private separation of customer traffic. Nortel Networks Passport Multiservice Switches and Shasta 5000 BSN support RFC2764.

### IPSec

IPSec provides encryption, authentication and protection at the network layer, based on standards set forth by the IETF. It allows the sender to encrypt each IP packet, ensuring confidentiality, data integrity and authentication. Technologies include Diffie-Hellman key exchanges, Data Encryption Standard (DES), Advanced Encryption Standard (AES), keyed hash algorithms for authenticating packets and digital certificates for validating public keys. Nortel Networks Contivity and Shasta platforms support IPSec encryption.

### IPSec client

An IPSec tunnel can be initiated from a remote terminal, provided that the terminal possesses the appropriate software client. The tunnel provides a secure, encrypted link between the remote device and the terminating VPN device. Client tunneling is a point-to-point capability that links one remote user to one terminating VPN device. Nortel Networks Contivity and Shasta platforms both support Contivity IPSec client.

### L2TP

The Layer 2 Tunneling Protocol is defined in the IETF's RFC 2661 as a way to tunnel PPP connections across a network. It was primarily aimed at enabling dial-up users to make a local call, which could be transparently extended to a remote access server over a Frame Relay or Internet backbone, avoiding long-distance charges and telephone network congestion. L2TP Version 3 is being defined in the IETF's L2TP Extensions Working Group as a more modular general-purpose tunneling protocol capable of transporting and multiplexing a variety of Layer 2 "pseudowires" (Ethernet, Frame Relay, ATM, etc.).

### SSL

Secure sockets layer (SSL) secures communication by providing authentication, encryption and data integrity at the transport and application layers. SSL has been integrated into all modern Web browsers and servers to become a universally deployed protocol for securing web applications across the Internet. SSL can be used with session proxies to provide secure remote access to virtually all enterprise applications without the need to deploy lower-layer tunneling software on client PCs. Nortel Networks Alteon SSL VPN uses this approach for a clientless VPN solution.

### Optical Ethernet

Optical Ethernet VPNs use Ethernet as the frame format and protocol to move data across the physical links in the network. Optical Ethernet can be carried over many kinds of physical link types including SONET, SDH, dark fiber, DWDM and CWDM. There are a number of different switching or VPN technologies that can be employed in Optical Ethernet including Multiprotocol Label Switching (MPLS), native Ethernet and Resilient Packet Ring. Nortel Networks OPTera Metro family of products support Optical Ethernet VPNs.

- Key**
- Remote client access (IPSec)
  - Clientless access (SSL)
  - Site-to-site tunnel (IPSec, L2TP, PPTP...)
  - WAN access (FR, PPP, ATM, DSL...)
  - Ethernet access
  - Virtual Router (RFC 2764)
  - VPN Routing and Forwarding Table (BGP/MPLS)