Appendix B

Glossary

This appendix lists definitions and acronyms for products in the BANDIT™ product family.

Table B-1. Acronyms and Definitions *(1 of 20)*

Term	Acronym	Definition
access point	AP	A device that provides access to a wireless network. **Note:** Most access points also connect to a wired network.
address translation		Conversion of an IP address to another IP address. (Also see network address translation, Private Address Translation™, address translation traversal.)
Advanced Encryption Standard	AES	An encryption standard, FIPS 197, that NIST proposes to replace DES. AES uses the Rijndael symmetric block cipher, and supports 128-bit, 192-bit, and 256-bit keys.

Table B-1. Acronyms and Definitions *(2 of 20)*

Term	Acronym	Definition
aggressive mode		A mode used in phase 1 of setting up a VPN tunnel. Aggressive mode does not hide the identities of the parties during SA negotiation. Aggressive mode is quicker than main mode. **Note:** Phase 2 (bulk data transfer) uses quick mode. (Compare transport mode. Also see tunnel mode.)
anti-replay		An IPsec routine that uses authentication and sequence numbers to thwart replay attacks.
asymmetric encryption		(Also called public-key encryption.) Use of a paired private key and public key for encryption and decryption. The private key is used only by its owner. The corresponding public key is used by all other parties when encrypting or decrypting communication with the private key's owner. Asymmetric encryption is used for authentication, including non-repudiation. RSA is an example of asymmetric encryption. **Note:** Because asymmetric encryption consumes significant resources, it is not used to encrypt the bulk of a message and it is not used for data transfer. (Compare symmetric encryption. Also see combined cryptography.)
authentication		Verification that the declared sender is the actual sender, and that the data received are the data that were sent.
authentication header	AH	An IPsec protocol that performs authentication. AH may be applied alone or with ESP.
BANDIT™		The original tabletop model in the family of BANDIT™ products. This model provides support for legacy protocols over IP and provides support for up to 30 IPsec VPNs. (Also see Broadband Access Network Device for Intelligent Termination™.)

Top Doc
TOC

Table B-1. Acronyms and Definitions (3 of 20)

Term	Acronym	Definition
BANDIT II™		An environmentally hardened (ruggedized) ROHS-compliant miniature desktop model in the BANDIT™ family, providing legacy-protocol support and IPsec VPNs using DES, 3DES, or AES. It is available in a commercial chassis or in an industrially hardened chassis. (For more information, see the BANDIT II, BANDIT III, and VSR-1200 Document Set.) **Note:** Optional brackets for the BANDIT II allow the chassis to be mounted in a corner or against a wall, typically in a field utility shed.
BANDIT III™		An environmentally hardened (ruggedized) ROHS-compliant full-featured tabletop model in the BANDIT™ family, providing legacy-protocol support and providing IPsec VPNs using DES, 3DES, or AES. The BANDIT III has an external expansion port and an optional internal wireless card. It also can include an Internal Data Unit™, which provides four additional serial ports, or it can include an internal E&M card (for a PCM voice network), which provides two audio ports and eight relay ports. (For more information, see the BANDIT II, BANDIT III, and VSR-1200 Document Set.) **Note:** Brackets for the BANDIT III allow the chassis to be mounted in a standard equipment rack.
BANDIT IP™		A tabletop streamlined router in the BANDIT™ family. The BANDIT IP supports IPsec VPNs.
BANDIT Mini™		A miniature, streamlined router in the BANDIT™ family. The BANDIT Mini supports IPsec VPNs and supports legacy protocols over IP networks.
BANDIT Plus™		A full-featured rackmounted model in the BANDIT™ family, providing legacy-protocol support and providing up to 100 IPsec VPN tunnels that use DES or 3DES. The BANDIT Plus has the option to use one RDU™.

Table B-1. Acronyms and Definitions *(4 of 20)*

Term	Acronym	Definition
BANDIT™ products		Encore Networks, Inc.'s family of products that provide VPN support, or legacy protocol over IP support, or both. The product family includes the BANDIT™, BANDIT II™, BANDIT III™, BANDIT IP™, BANDIT Mini™, BANDIT Plus™, IBR-10™, ILR-100™, VSR-30™, and VSR-1200™ chassis. It also includes the RDU™, a peripheral device for optional use with the BANDIT Plus or the VSR-1200. (See Broadband Access Network Device for Intelligent Termination™.)
block cipher		Encryption of data into blocks of a fixed size.
Broadband Access Network Device for Intelligent Termination™	BANDIT™	The original product in Encore Networks, Inc.'s family of BANDIT™ products that provide VPN support, or legacy protocol over IP support, or both. **Note:** The name "BANDIT" can indicate the entire product family or, when stipulated, can indicate a specific chassis: the original BANDIT™, the BANDIT II™, the BANDIT III™, the BANDIT IP™, the BANDIT Mini™, or the BANDIT Plus™. (Also see BANDIT™ entry.)

Table B-1. Acronyms and Definitions *(5 of 20)*

Term	Acronym	Definition
checksum		An algorithm performed on random data, to detect accidental error in data transmission or storage. Although not absolute, the probability is high that: • If checksums performed before and after transmission match, the data have not been accidentally corrupted. • If the checksums do not match, the data have been accidentally corrupted. Errors in transmission are usually caused by a bad line. **Note:** Use of checksums cannot indicate intentional corruption of data. Because of the nature of a checksum, intentionally altered data can be manipulated to generate a checksum that matches the checksum of the original data. However, *encryption* of checksums may provide some protection against intentional alteration. (An encrypted checksum verifies that data have been transmitted without error and without alteration—or that, if alteration has occurred, it is detected.) To protect data integrity, use a good encryption algorithm (to guard against intentional alteration) and make sure the transmission line is clear (to guard against accidental alteration). The most commonly used checksum is the cyclic redundancy check.
class of service	CoS, COS	A field in the packet's IP header that specifies traffic priorities. CoS operates at the data-link layer (layer 2) of the protocol stack. (Also see diffserv, QoS, ToS.)
Code Division Multiple Access	CDMA	A wireless technology that uses spread-spectrum communication. To send a call, CDMA uses several frequencies along the spectrum of its radiofrequency band. When the call is received, it is reassembled.

Table B-1. Acronyms and Definitions *(6 of 20)*

Term	Acronym	Definition
combined cryptography		(Also called hybrid cryptography.) A common practice of using asymmetric encryption and symmetric encryption together. For example, a sender may create a secret key (symmetric encryption) to encrypt a message, and then use the sender's private key or the recipient's public key (asymmetric encryption) to encrypt the secret key and the message together as one document. The recipient decrypts the document, revealing the secret key. Then the recipient uses the secret key to decrypt the message.
confidentiality		Privacy of communication—that is, the principle that a party that is not intended to know the content of a transmission will not be able to determine the content of the transmission. The principal method used for safeguarding security is encryption.
cookie		A cipher, generated and assigned by the host, that identifies clients without using comprehensive authentication. As used in IKE, cookies conserve CPU resources yet offer some protection against replay attacks.
data carrier equipment	DCE	A device that sits between the DTE and the network. Examples of DCEs are modems and routers.
data diversity		Use of more than one set of wireless signals. The signals are collected at the same time through more than one antenna. (An antenna used for this purpose is a diversity antenna. The BANDIT II and the BANDIT III can use diversity antennas.) Data diversity permits a larger number of calculations, contributing to more accurate resolution of information from the signals. Data diversity is important when signals might be delayed by travel through the atmosphere or when signals might be diverted or reflected by physical impediments to signal transmission.

Top Doc
TOC

Table B-1. Acronyms and Definitions (7 of 20)

Term	Acronym	Definition
Data Encryption Standard	DES	A standard block cipher encryption algorithm that uses the same 56-bit key for encryption and decryption. **Note:** Because its short key length makes DES vulnerable to persistent attack, 3DES can be used, providing longer key lengths for additional security.
data integrity		Use of a checksum to ensure that data have been transmitted from endpoint to endpoint without error. In IPsec, the checksum is encrypted.
data terminal equipment	DTE	An endpoint device in a transmission circuit. A DTE goes through a DCE to reach the network.
destination address		The address of the endpoint device for which a transmission is destined. (Compare source address.)
Differentiated Services	diffserv	A protocol that handles packets by class instead of by individual packet request. (Also see CoS, QoS, ToS.)
Diffie–Hellman exchange	DH	An algorithm for developing a shared secret between endpoints by combining the endpoints' public keys and then combining this result with each endpoint's private key, separately.
drop [a packet]		To discard a transmission packet, for any of several reasons, without comment or report. Compare reject [a packet].
drop and insert		Use of an internal bus to connect network interface resources and to transfer calls from one interface to another.
dynamic packet filtering		(See stateful inspection.)
dynamic split tunneling		(See split tunneling.)

Table B-1. Acronyms and Definitions *(8 of 20)*

Term	Acronym	Definition
Earth and Magneto (Ground and Battery)	E&M	Signaling leads, traditionally used in the North American telecommunications industry, on a voice tieline. This supervisory line signaling uses separate leads, called the E lead (ground) and the M lead (battery). E&M signaling uses two states: On hook and Off hook. Off hook sends a signal from the M lead to the E lead. There are E&M standards with 2, 4, 6, or 8 wires. The BANDIT III supports 4-wire E&M Types I through V. E&M is also known as Ear and Mouth.
Encapsulating Security Payload	ESP	An IPsec protocol that encrypts and encapsulates data into IP packets. ESP may be used alone or with AH.
encapsulation		Packaging information of one protocol into packets of another protocol. Encapsulation is generally used to carry information across a network that does not support the encapsulated protocol. **Note:** Most BANDIT™ products can encapsulate several legacy protocols within IP. They can also encapsulate some protocols within Frame Relay. (Also see tunneling, generic route encapsulation.)
Encore Legacy-to-IP Operating System™	ELIOS™	The operating system software in the BANDIT™ products, used when configuring and managing the devices.
encryption		Conversion of a message into a coded form so that its contents cannot be readily discerned. Encryption preserves confidentiality and data integrity.
Enhanced Data Rates for GSM Evolution	EDGE	A technology for increased rate and improved reliability in GSM transmissions. EDGE is used only in the BANDIT II, the BANDIT III, and the BANDIT Plus.

Table B-1. Acronyms and Definitions (9 of 20)

Term	Acronym	Definition
Evolution of Data Optimization	EVDO	A third-generation (3G) wireless protocol that improves CDMA speeds, improves reliability, and reduces latency. EVDO is used only in the BANDIT II and the BANDIT III.
Federal Information Processing Standard	FIPS	A standard (in the set of standards) that NIST develops and issues, for use by federal contractors and non-military federal agencies. Adherence to these standards is voluntary for private industries that do not hold federal contracts.
firewall		An interface that regulates traffic between a private network and a public network, to protect the security of the private network. (Also see stateful inspection.)
gateway		An interface between networks. In addition to routing packets to destinations, a gateway usually provides security and converts transmission speeds, protocols, or other processes between the networks.
General Packet Radio Service	GPRS	A system that uses increased speed to support transfer of data packets over GSM.
generic route encapsulation	GRE	A method of encapsulating any protocol within IP packets. (Also see encapsulation, tunneling.)
geostationary		(Used to describe a satellite or its orbit.) Orbiting in a way that maintains position above the same point (latitude and longitude) on the earth's surface. **Note:** Most communications satellites are geostationary. However, communications satellites at high latitudes—for example, in latitudes beyond the arctic circle or beyond the antarctic circle—may have non-geostationary orbits.

Table B-1. Acronyms and Definitions *(10 of 20)*

Term	Acronym	Definition
Global System for Mobile Communications	GSM	A wireless network based on TDMA technology. **Note:** Each GSM device uses a region-specific or country-specific SIM (smartcard) to enable use of the GSM device in that region or country.
Ground and Battery		(See E&M.)
GSM smartcard		(See SIM.)
hash		An IKE authentication routine that generates a string of fixed size from a message of variable size.
Hashed Message Authentication Code	HMAC	An extremely powerful method of employing a hash function.
hybrid cryptography		(See combined cryptography.)
IBR-10™		(See IP Banking Router 10™.)
ILR-100™		(See IP Legacy Router 100™.)
International Telecommunication Union	ITU	A United Nations autonomous specialized agency studying information technology, including communication. Membership in ITU is open to governmental and private entities interested in developments in communication.

Table B-1. Acronyms and Definitions (11 of 20)

Term	Acronym	Definition
International Telecommunication Union, Telecommunication Standardization Sector	ITU-T	An ITU group that coordinates development of international standards. ITU-T releases Recommendations, which are not mandatory standards. However, individual governments can require adherence to a Recommendation. **Note:** ITU-T was formerly known as the International Telegraph and Telephone Consultative Committee (CCITT, Comité consultatif international téléphonique et télégraphique).
Internet Engineering Task Force	IETF®	An international organization concerned with the function and development of the internet. IETF maintains a series of RFCs. RFC 3935 describes IETF's purpose.
Internet Key Exchange	IKE	A protocol that negotiates authentication methods, encryption methods, and keys. It also negotiates the length of time that a key is valid before a new key must be implemented.
IP Banking Router 10™	IBR-10™	A router in the BANDIT™ family. The IBR-10 is dedicated to support of legacy protocols over IP networks.
IP Legacy Router 100™	ILR-100™	A miniature, streamlined router in the BANDIT™ family. The ILR-100 supports IPsec VPN and supports legacy protocols over IP networks.
IP Security Protocol	IPsec	A protocol to protect IP transmissions. IPsec comprises two protocols that may be applied separately or together: • Authentication Header (AH) • Encapsulating Security Protocol (ESP)
key pair		The set of a private key and its public key; the set is used in asymmetric encryption. **Note:** Only the holder of the private key knows the complete key pair.

Table B-1. Acronyms and Definitions (12 of 20)

Term	Acronym	Definition
main mode		A mode used in phase 1 of setting up a VPN tunnel. Main mode hides the identities of the parties during negotiation of the security association. Main mode is more secure than aggressive mode. **Note:** Phase 2 (bulk data transfer) uses quick mode. (Compare transport mode. Also see tunnel mode.)
Message Digest 5	MD5	A hash that authenticates packet data by creating a 16-byte message digest. Used in AH and ESP.
National Institute of Standards and Technology	NIST	A U.S. Agency that supports (but does not regulate) measurement, evaluation, and standards for technology.
network access device		A device that provides connection to a network.
network address translation	NAT	An address translation routine, described but not standardized in IETF RFC 3022, that lets a private network use one set of IP addresses for internal traffic and another set for external traffic. Use of NAT makes it possible for an organization to do the following: • Use a single public IP address for several connections. • Use a greater number of internal IP addresses. • Hide internal IP addresses. (Also see port address translation, Private Address Translation™, NAT traversal.)
originating address		(See source address.)

Table B-1. Acronyms and Definitions (13 of 20)

Term	Acronym	Definition
perfect forward secrecy	PFS	Use of uniquely derived keys. PFS is part of IKE. PFS comprises the following principles: • Material used to derive one key cannot be used to derive additional keys. • A key cannot be used to derive another key. • Discovery of a key can endanger only transmissions protected by that key.
performance enhancement proxy	PEP	A routine that satellite groundstations use to mitigate the delay in satellite networks. PEPs spoof TCP sessions with endpoints outside the satellite network, thereby mitigating the delays inherent in satellite networks. (500 ms is a typical TCP roundtrip response time over a satellite network without PEP.)
Peripheral Component Interconnect	PCI	A standard for a 64-bit local bus (generally implemented as a 32-bit bus) that runs at 33 MHz or 66 MHz. Developed by Intel Corporation but not specific to any line of microprocessors, PCI is a widely used standard for expansion cards. **Note:** Using 32 bits at 33 MHz, PCI has a throughput of 133 Mbytes/sec.
pre-shared key		(See secret key.)
port address translation	PAT	Inclusion of port numbers when implementing NAT. **Note:** NAT methods generally include PAT.
Private Address Translation™	PrAT™	A value-added address translation routine, from Encore Networks, Inc., for devices on private networks. (Also see network address translation.)
private key		The key used by the holder of a key pair for encryption and decryption in communication with everyone else. The private key is never shared. (Compare public key. Also see asymmetric encryption.)

Table B-1. Acronyms and Definitions *(14 of 20)*

Term	Acronym	Definition
public key		The key used for encryption and decryption by everyone except the holder of a key pair, to communicate with the holder of the key pair. The public key is freely available to anyone. (Compare private key. Also see asymmetric encryption.)
public-key cryptography	PKC	(See asymmetric encryption.)
quality of service	QoS, QOS	Guarantee of a specific throughput, achieved by configuring bandwidth, packet priority, and so forth. (Also see CoS, diffserv, ToS.)
quick mode		The mode used for communication in phase 2 of a VPN tunnel. (Phase 2 is used for the communication payload—for example, data transfer.) **Note:** For phase 1 (setting up the VPN tunnel), see main mode or aggressive mode. (Compare transport mode. Also see tunnel mode.)
radiofrequency	RF	A frequency (in the band of frequencies in the radiowave spectrum) used for radio communication.
reject [a packet]		To discard a transmission packet, for any of several reasons, and to transmit a comment or report about the rejected packet. Compare drop [a packet].
re-keying		An IKE feature that sets the interval between encryption key changes. Re-keying increases key security.
Remote Data Unit™	RDU™	A peripheral device for the BANDIT Plus™ and the VSR-1200™, supplying 12 DB-25 serial ports.

Table B-1. Acronyms and Definitions *(15 of 20)*

Term	Acronym	Definition
replay attack		Interception and recording of a transmission, with the purpose of sending the transmission later to a recipient unaware that the transmission is no longer legitimate. A replay attack is a type of denial-of-service attack.
Request for Comments	RFC	A working paper in a series maintained by IETF, to circulate and discuss proposed protocols and other ideas for telecommunication and the internet.
Rivest–Shamir–Adleman	RSA	A public-key algorithm for asymmetric encryption, generally considered secure when sufficiently long keys are used. (A key of 512 bits is considered insecure; a key of 1024 bits is considered quite secure.)
router		A device, generally a network gateway, that determines the optimal path for each packet to reach its destination, and sends the packet along that route.
secret key		(Also called pre-shared key or shared key.) A key used in symmetric encryption. The key can be pre-shared, requiring a trusted delivery mechanism, or can be sent via combined cryptography. **Note:** A secret key is not a shared secret.
secret-key cryptography		(See symmetric encryption.)
secure hash algorithm	SHA	A routine that develops a 20-byte hash to authenticate data. SHA gives up speed in order to gain greater resistance to attack. Used in AH and ESP.
security association	SA	Information associated with setting up a specific secure connection. The security association comprises the following elements: • The security protocol • The authentication protocol • The encryption protocol

Table B-1. Acronyms and Definitions *(16 of 20)*

Term	Acronym	Definition
security parameter index	SPI	An index correlated against the destination address to determine a specific security association.
Selective Layer Encryption™	SLE™	A value-added technology (patent pending), developed by Encore Networks, Inc., that allows IPsec VPNs to function more effectively over satellite networks that are PEP-enabled.
shared key		(See secret key.) **Note:** A shared key is not a shared secret.
shared secret		A secret that the Diffie–Hellman exchange algorithm develops from endpoints' public keys and private keys and that the endpoints use for part of the security in their communication. **Note:** A shared secret is not a shared key.
smartcard (for GSM)		(See Subscriber Identity Module, or SIM.)
source address		The address of the device that initiates a transmission. (Also called originating address. Compare destination address.)
split tunneling		The ability to route VPN traffic through VPN tunnels and to route non-VPN traffic outside these tunnels, on the same line. The BANDIT VPN products do this dynamically.
stateful inspection		A firewall inspection of each packet's state. This inspection examines a packet's header information and its information up through several layers. To be allowed into the network, the packet must pass defined filtering rules and must conform to the context (state) established by previous packet traffic.
sub-miniature coaxial connector, type A	SMA	An external connector on wireless modules in the BANDIT products, used to connect an antenna to the wireless module.

Table B-1. Acronyms and Definitions (17 of 20)

Term	Acronym	Definition
Subscriber Identity Module	SIM	(Also called a GSM smartcard.) A removable card used in GSM to identify a subscriber in a GSM region. With insertion of various SIMs, a GSM device—for example, a GSM cellphone—can be used virtually throughout the world.
symmetric encryption		(Also called secret-key encryption.) Use of a secret key, shared by both sides of a connection, for encryption and decryption. (The same key is used both for encryption and for decryption.) A quick algorithm, such as DES, is used to support symmetric encryption. Symmetric encryption is used for bulk encryption—for example, for a message or data transfer. Symmetric encryption is not used for authentication. (Compare asymmetric encryption. Also see combined cryptography.)
telecommuting		(See teleworking.)
teleworking		Performance of employment responsibilities by means of a remote connection to the central network. As an example, this connection can be through a VPN tunnel. Teleworking (also called telecommuting) includes business travelers, employees working at home, and other remote users.
throughput		The data transfer rate.
Time Division Multiple Access	TDMA	A wireless technology that divides a network's radiofrequency band into timeslots and allocates the timeslots to calls. This allows one RF band to support several simultaneous calls.
traffic analysis		Analysis of network traffic in order to infer information—for example, source address, destination address, frequency of transmission, or packet size.
Transmission Control Protocol	TCP	A protocol layer used in IP. TCP checks for packet receipt and packet order. (Compare UDP.)

Table B-1. Acronyms and Definitions *(18 of 20)*

Term	Acronym	Definition
transport mode		A mode in which the endpoints of a VPN connection perform their own encryption. The VPN gateway functions solely as the transport, encapsulating (thus protecting) the upper layer payload (e.g., TCP or UDP) and reusing the IP header. (Compare main mode, aggressive mode, quick mode. Also see tunnel mode.)
Triple Data Encryption Standard	3DES	An encryption method incorporating three iterations of DES, each with a different key, for added security: • Encryption • Decryption • Another encryption Some versions of 3DES use two DES keys (112 bits) in each iteration. Some versions use three DES keys (168 bits) in each iteration.
Trivial File Transfer Protocol	TFTP	A simple file transfer protocol, based on UDP.
tunneling		Use of encapsulation to send one protocol through a network that uses a different protocol. **Note:** VPN tunneling includes the ability, if desired, to encrypt the source address, destination address, and data in order to provide protection for encapsulated packets. (Also see tunnel mode.)
tunnel mode		The type of tunneling used to create and send data across a VPN. VPN tunneling can use main mode or aggressive mode to set up the tunnel, then quick mode for communication through the tunnel. A VPN tunnel can also function in transport mode. (Also see tunneling.)
type of service	ToS, TOS	Use of bits in a packet's IP header to indicate specific priority and service type for the packet. ToS contrasts with class of service. (Also see CoS, diffserv, QoS.)

Table B-1. Acronyms and Definitions (19 of 20)

Term	Acronym	Definition
User Datagram Protocol	UDP	A protocol layer used in IP. UDP does not check for packet order or packet receipt. (Compare TCP.)
very-small-aperture terminal	VSAT	A small satellite dish, ranging from 2 ft. to 15 ft. (0.6 m to 4.6 m) in diameter. The size of the VSAT depends on the site and uses. The principal advantage in using VSATs is that a network can be developed without reliance on landlines, permitting a branch site to be placed where it is needed, no matter how remote.
Virtual Broadband Redundancy System™	VBRS™	A value-added system of Encore Networks, Inc., for continuous management of the Remote Data Unit™, supplying host-to-host physical and logical redundancy. VBRS is used only in the BANDIT Plus™ and the VSR-1200™.
virtual local area network	VLAN	A smaller grouping of devices within a LAN (or a grouping of devices located in two or more LANs) selected to receive VLAN broadcasts. Use of VLANs reduces traffic broadcast to the entire LAN. **Note:** VLANs are described in IEEE standards 802.1q and 802.1p.
virtual private network	VPN	Use of encryption, authentication, and tunneling across a public network to ensure secure communication between private endpoints. There are several IETF RFCs that address VPNs; for a list of RFCs applicable to VPNs, see the VPN Consortium's website: *www.vpnc.org/vpn-standards.html*
Virtual Private Network Consortium	VPN Consortium, VPNC	A trade association for manufacturers and vendors of VPN products. VPNC tests products for VPN compliance and interoperability. VPNC supports development of standards for VPNs, but VPNC itself does not develop standards.

Table B-1. Acronyms and Definitions *(20 of 20)*

Term	Acronym	Definition
Virtual Router Redundancy Protocol	VRRP	A protocol for providing continuous router support to a network.
VPN Satellite Router™	VSR™	A type of router in the BANDIT™ family, providing support of VPNs over ground-based networks and, via Selective Layer Encryption™, over satellite networks. The VSR product line includes the VSR-30™ and the VSR-1200™.
VPN Satellite Router 30™	VSR-30™	A router in the VSR™ group, supporting IPsec VPNs over ground-based and satellite networks, and featuring IPsec VPNs with SLE™. The VSR-30 can support up to 30 VPN tunnels.
VPN Satellite Router 1200™	VSR-1200™	A router in the VSR™ group, supporting IPsec VPNs over ground-based and satellite networks, and featuring IPsec VPNs with SLE™. (For more information, see the BANDIT II, BANDIT III, and VSR-1200 Document Set.) The VSR-1200 can support up to 1200 VPN tunnels. The VSR-1200 also has the option to use one or two RDUs.