Glossary

Table D-1 lists acronyms and definitions for terms used in discussions of products from Encore Networks, Inc.[1, 2]

Table D-1. Terms, Acronyms, and Definitions (Sheet 1 of 30)

Term	Acronym	Definition
3DES		*See Triple Data Encryption Standard.*
802.11 wireless	wifi, Wi-Fi™	A set of IEEE specifications for wireless LANs using the 2.4 GHz or 5 GHz frequency bands. *802.11 wireless is sometimes called "wifi."*
access point	AP	A device that provides access (connection) to a wireless network. **Note:** Some access points also have a connection to a wired network (in addition to a connection to a wireless network).
address translation		Conversion of an IP address to another IP address. *Also see network address translation, Private Address Translation™, address translation traversal.*
address translation traversal		Any of several methods of maintaining end-to-end connectivity and security when address translation occurs between the transmission endpoints. *Also see NAT traversal, Encore NAT 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.

1. Entries in Table D-1 are alphabetized character by character. Roman numerals are listed by letter sequence, not by numeric sequence. Other numbers precede letters and are listed by numeric sequence, not character by character. Spaces, hyphens, dashes, apostrophes, quotation marks, parentheses, and other special characters (for example, "&" or "™") are ignored.
2. Foreign words and phrases follow capitalization guidelines for the source languages.

Table D-1. Terms, Acronyms, and Definitions (Sheet 2 of 30)

Term	Acronym	Definition
AES		*See Advanced Encryption Standard.*
aggressive mode		A mode that can be used in phase 1 of an IKEv1 IPsec VPN tunnel. (Phase 1 sets up the VPN tunnel.) Aggressive mode does not hide the identities of the parties while negotiating the security association. Aggressive mode is quicker than main mode. **Note:** Phase 2 (bulk data transfer) of an IKEv1 IPsec VPN tunnel uses quick mode. *Compare main mode, transport mode. Also see tunnel mode.*
AH		*See authentication header.*
anti-replay		An IPsec routine that uses authentication and sequence numbers to thwart replay attacks.
AP		*See access point.*
asymmetric encryption		(Also called public-key cryptography.) 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™ (chassis)		The original tabletop chassis in the family of BANDIT™ products. This model provides support for legacy protocols over IP and provides support for up to 30 IPsec VPNs. *See Broadband Access Network Device for Intelligent Termination™.* **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 3 of 30)

Term	Acronym	Definition
BANDIT™ family		*See BANDIT™ products.*
BANDIT II™ (chassis)		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. **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 II C2C™ (chassis)		A streamlined router in the BANDIT™ family's C2C™ products, developed to support legacy devices (such as modems) migrating from POTS applications to cellular wireless networks. The BANDIT II C2C supports IPsec VPNs and supports legacy protocols over IP networks. *Also see C2C™ (chassis), Copper to Cellular™ (technology).*
BANDIT III™ (chassis)		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. **Note:** Optional brackets for the BANDIT III allow the chassis to be mounted in a standard equipment rack.
BANDIT IP™ (chassis)		A tabletop streamlined router in the BANDIT™ family. The BANDIT IP supports IPsec VPNs. **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.*
BANDIT Mini™ (chassis)		A miniature, streamlined router in the BANDIT™ family. The BANDIT Mini supports IPsec VPNs and supports legacy protocols over IP networks. **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 4 of 30)

Term	Acronym	Definition
BANDIT Plus™ (chassis)		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. **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.* The BANDIT Plus has the option to use one RDU™.
BANDIT™ products		Encore Networks, Inc.'s family of products that support VPNs or support legacy protocols over IP, or both. The product family includes the BANDIT™, C2C™, BANDIT II C2C™, BANDIT II™, BANDIT III™, BANDIT IP™, BANDIT Mini™, BANDIT Plus™, E2C™, 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. **Note:** The BANDIT products include the C2C™ products. *Also 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 chassis in Encore Networks, Inc.'s BANDIT™ products. *See BANDIT™ (chassis).* **Note:** The term "BANDIT" can indicate the entire family of BANDIT™ products (including the C2C™ products) or can indicate a specific chassis (when stipulated): the original BANDIT™, the BANDIT II™, the BANDIT III™, the BANDIT IP™, the BANDIT Mini™, or the BANDIT Plus™.
C2C™ (chassis)		A miniature streamlined router in the BANDIT™ family's C2C™ products, developed to support legacy devices (such as modems) migrating from POTS applications to cellular wireless networks. The C2C is available in commercial and industrial models. The C2C can support IPsec VPNs and can support legacy protocols over IP networks. *Also see BANDIT II C2C™, Copper to Cellular™ (technology).*
C2C™ products		A line of commercial and industrial products featuring support for Copper to Cellular™ migration. The C2C product family includes the C2C™, the E2C™, and the BANDIT II C2C™. The C2C products are part of the family of BANDIT™ products.
C2C™ technology		*See Copper to Cellular™ (technology).*

Table D-1. Terms, Acronyms, and Definitions (Sheet 5 of 30)

Term	Acronym	Definition
CCITT		The acronym for the Comité consultatif international téléphonique et télégraphique, a former French name for the International Telecommunication Union, Telecommunication Standardization Sector. (The English equivalent of the former name was the International Telegraph and Telephone Consultative Committee).
CDM		*See code-division multiplexing.*
CDMA		*See code-division multiple access.*
CEN		*See European Committee for Standardization.*
checksum		An algorithm performed to detect accidental error in data transmission or data storage. Errors in transmission are usually caused by a bad line. **Note:** Checksums cannot detect corruption of data at the source. *Also see cyclic redundancy check, hash function, authentication.*
CIP		*See critical infrastructure protection.*
CISPR		*See Special International Committee on Radio Interference.*
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 Differentiated Services, quality of service, type of service.*
code-division multiple access, code-division multiplexing	CDMA, CDM	A wireless technology that uses spread-spectrum communication. To send a call, CDM uses several frequencies along the spectrum of its radiofrequency band. When the call is received, it is reassembled. *Compare time-division multiplexing, wavelength-division multiplexing.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 6 of 30)

Term	Acronym	Definition
combined cryptography		(Also called hybrid cryptography.) A common practice of using asymmetric encryption and symmetric encryption together. For example, to encrypt a message: • A sender might create a secret key and use it for symmetric encryption of a message. • Then the sender might use asymmetric encryption (choosing the recipient's public key or the sender's private key) to package the encrypted message and its secret key together as a single encrypted document. **Note:** The recipient's public key is the safer choice, because no one except the recipient should know the counterpart private key. To decrypt the message: • The recipient uses the counterpart in the key pair chosen by the sender (that is, the recipient's private key or the sender's public key) to open the document. That decryption reveals the secret key and the still-encrypted message. • Then the recipient uses the secret key to decrypt the message.
Comité consultatif international téléphonique et télégraphique	CCITT	A former French name for the International Telecommunication Union, Telecommunication Standardization Sector. (The equivalent former English name was the International Telegraph and Telephone Consultative Committee.)
Comité européen de normalisation	CEN	The French name for the European Committee for Standardization.
Comité international spécial des perturbations radioélectriques	CISPR	The French name for the Special International Committee on Radio Interference.
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 confidentiality is encryption.

Table D-1. Terms, Acronyms, and Definitions (Sheet 7 of 30)

Term	Acronym	Definition
connection between office and remote location		*See teleworking.*
connectionless (protocol)		A general term for protocols wherein devices do not establish a defined route for data transmission. Instead, the header of each datagram (packet) contains the packet's destination address. A router looks at each packet's header and sends that packet on the best route toward its destination. Because there is no specified route for transmissions, individual packets in a transmission can travel over different routes to the destination. A connectionless protocol, such as IP, does not check for completion of delivery—but it can use other protocols, such as TCP, to check for completion of delivery. *Compare connection-oriented.*
connection-oriented (protocol)		A general term for protocols wherein devices must establish a defined route or session for data transmission. Each packet in the transmission must travel over the defined route to the destination. A connection-oriented protocol, such as TCP, checks for completion of delivery. *Compare connectionless.*
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.
Copper to Cellular™ (technology)	C2C™ (technology)	An Encore Networks implementation that supports legacy equipment migration from copper wire networks to cellular wireless networks. *See C2C™ products, C2C™ (chassis), E2C™ (chassis), BANDIT II C2C™.*
COS, CoS		*See class of service.*
CRC		*See cyclic redundancy check.*
critical infrastructure protection	CIP	A program to prevent and respond to threats to the critical infrastructure of a locality, region, or nation. CIP programs are designed to defend against damage or destruction from natural disasters, accidents, attacks, and similar events. *Also see North American Electric Reliability Corporation.*
cyclic redundancy check	CRC	Any of several checksum algorithms based on cyclic processes.

Table D-1. Terms, Acronyms, and Definitions (Sheet 8 of 30)

Term	Acronym	Definition
data carrier equipment	DCE	A device that sits between a DTE and the network. Modems and routers are examples of DCEs.
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 EN-4000 and several BANDIT™ products 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 reflected, otherwise diverted, or blocked by physical impediments to signal transmission.
Data Encryption Algorithm	DEA	*See Data Encryption Standard.*
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 uses encryption.
data terminal equipment	DTE	An endpoint device in a transmission circuit. A DTE goes through a DCE to reach the network.
DCE		*See data carrier equipment.*
DEA		*See Data Encryption Standard.*
decryption		A process that reverses encryption of a message so that the message content can be discerned. The use of encryption and decryption for data storage or transfer preserves confidentiality and data integrity.
DES		*See Data Encryption Standard.*
destination address		The address of the endpoint device for which a transmission is destined. *Compare source address. Also see security parameter index.*
DH		*See Diffie–Hellman exchange.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 9 of 30)

Term	Acronym	Definition
Differentiated Services	diffserv	A protocol that handles packets by class instead of by individual packet request. *Also see class of service, quality of service, type of service.*
Diffie–Hellman exchange	DH	An algorithm for developing a shared secret between endpoints by combining the endpoints' public keys and then separately combining this result with each endpoint's private key.
diffserv		*See Differentiated Services.*
directive on hazardous substances		*See Restriction of Hazardous Substances.*
diversity antenna		A second antenna, which collects a second set of wireless signals (for data diversity). **Note:** A diversity antenna only receives signals; it does not transmit.
drop and insert		Use of an internal bus to connect network interface resources and to transfer calls from one interface to another.
DTE		*See data terminal equipment.*
dynamic packet filtering		*See stateful inspection.*
dynamic split tunneling		*See split tunneling.*
E2C™ (chassis)		A miniature streamlined router in the BANDIT™ family's C2C™ products, developed to support IP transmissions over cellular wireless networks. The E2C has an Ethernet port and a port on a 3G cellular wireless card. The E2C can support IPsec VPNs. The E2C is available in commercial and ruggedized industrial models. *Also see Ethernet to Cellular™ (technology), C2C™ products.*
E2C™ technology		*See Ethernet to Cellular™ (technology).*
E and M	E&M	*See earth and magneto.*
EAP		*See Extensible Authentication Protocol.*
ear and mouth	E&M	*See earth and magneto.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 10 of 30)

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 (earth, ground) and the M lead (magneto, 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. **Note:** E&M type V is generally preferred; type II is second in preference. Type IV is not used often. E&M is also known as ear and mouth.
EDGE		*See Enhanced Data Rates for GSM Evolution.*
EIA		*See Electronic Industries Alliance.*
Electronic Industries Alliance	EIA	An alliance of U.S. trade organizations that issued standards for electronics manufacturing. The EIA has discontinued operation.
ELIOS™		*See Encore Legacy-to-IP Operating System™.*
E&M		*See earth and magneto.*
EN-1000™ (chassis)		A miniature streamlined router from Encore Networks, Inc. The EN-1000 supports a 3G/4G LTE cellular wireless card, a WAN port, and a LAN port. It also supports VPNs and legacy protocols. The EN-1000 can be managed through a browser window.
EN-2000™ (chassis)		A miniature streamlined router from Encore Networks, Inc. The EN-2000 supports a 3G/4G LTE cellular wireless card, a WAN port, and a LAN port. It supports VPNs and legacy protocols, and can support an 802.11 wireless card. The EN-2000 can be managed through a browser window.
EN-4000™ (chassis)		A miniature streamlined router from Encore Networks, Inc. The EN-4000 can support two 3G/4G cellular wireless cards, an 802.11 wireless card, a WAN port, four LAN ports, and a dual-serial module for two slots. It also supports VPNs and legacy protocols. The EN-4000 can be managed through a browser window or through a command line interface (CLI).
encapsulating		*See encapsulation.*
Encapsulating Security Payload	ESP	An IPsec protocol that encrypts and encapsulates data into IP packets. ESP may be used alone or with AH.

Table D-1. Terms, Acronyms, and Definitions (Sheet 11 of 30)

Term	Acronym	Definition
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:** The EN-4000 and most BANDIT™ products routers can encapsulate several legacy protocols within IP. The routers 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 products.
Encore NAT Traversal™	eNT™	A value-added method of NAT traversal, available from Encore Networks, Inc. Encore's eNT™ can be used with SLE™. **Note:** Use of eNT™ requires BANDIT™ products on both the local side and the remote side of the transmission.
encryption		Conversion of a message into a coded form so that its content cannot be readily discerned. The use of encryption and decryption for data storage or transfer preserves confidentiality and data integrity.
Enhanced Data Rates for GSM Evolution	EDGE	A technology for increased rate and improved reliability in GSM transmissions.
enServer™		A server from Encore Networks, Inc. The enServer can support VPNs and legacy protocols. The enServer can be managed through a browser window or through a command line interface (CLI).
eNT™		*See Encore NAT Traversal™.*
ESP		*See Encapsulating Security Payload.*
Ethernet to Cellular™ (technology)	E2C™ (technology)	An Encore Networks implementation that supports IP transmissions over cellular wireless networks. *Also see E2C™ (chassis), C2C™ products.*
European Committee for Standardization	CEN	A non-profit organization that supports development, maintenance, and distribution of uniform standards and specifications. **Note:** The acronym CEN is from the French name for the committee, Comité européen de normalisation.
European Union ROHS		*See Restriction of Hazardous Substances.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 12 of 30)

Term	Acronym	Definition
EVDO		*See Evolution of Data Optimization.*
Evolution of Data Optimization	EVDO	A third-generation (3G) wireless protocol that improves CDM speeds, improves reliability, and reduces latency.
Extensible Authentication Protocol	EAP	An authentication framework used in VPN connections, other point-to-point connections, and wireless networks. EAP is not a transport protocol; it specifies a structure that a protocol such as IPsec VPN IKE version 2 might use for communication. EAP is defined in RFC 3748.
Federal Information Processing Standard	FIPS	Any standard in the set of standards that NIST develops and issues for use by federal contractors and non-military federal agencies. **Note:** Adherence to these standards is voluntary for private industries that do not hold federal contracts.
fiber optic network		A network that uses light pulses for data transmission. Advantages of fiber optic networks include high speed, high reliability, long distance without significant degradation, no electromagnetic interference or radiofrequency interference, and high security. *Also see optical fiber.*
FIPS		*See Federal Information Processing Standard.*
firewall (electronic)		An interface that regulates traffic between a public network and a private entity (for example, a personal computer or a private network), to protect the security of the private entity. *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. *Compare network access device.*
General Packet Radio Service	GPRS	A system that uses increased speed to support transfer of data packets over GSM.
generated shared secret		*See shared secret, generated.*
generic route encapsulation	GRE	A method of encapsulating any protocol within IP packets. *Also see encapsulation, tunneling.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 13 of 30)

Term	Acronym	Definition
geostationary (orbit), geosynchronous (orbit)	GSO	(Used to describe a satellite or its orbit.) Orbiting in a way that maintains position above the same point of latitude and longitude on the earth's surface. **Note:** Many communications satellites are geostationary (that is, the geosynchronous orbit is at the equator). Most communications satellites are geosynchronous. However, communications satellites at high latitudes—for example, in latitudes beyond the arctic circle or beyond the antarctic circle—may have orbits that are not geosynchronous. GPS satellites are not geosynchronous.
Global Positioning System	GPS	An array of U.S. satellites orbiting the earth, each broadcasting its position, orbit, speed, and correlated time of broadcast. GPS is designed to assist in land, sea, and air navigation at the earth's surface or in the atmosphere. **Note:** GPS signals do not travel far through liquids and cannot support navigation under water. *Also see trilateration.*
Global System for Mobile Communications	GSM	A wireless network based on TDM 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.
GPRS		*See General Packet Radio Service.*
GPS		*See Global Positioning System.*
GRE		*See generic route encapsulation.*
ground and battery		*See earth and magneto.*
GSM		*See Global System for Mobile Communications.*
GSM smartcard		*See Subscriber Identity Module.*
GSO		*See geostationary (orbit), geosynchronous (orbit).*
hash function		Any of several algorithms that map data sets to strings of uniform length. Hashes are generally used to index data. **Note:** In IPsec, a hash is an IKE authentication routine that generates a string of fixed size from a message of variable size. *Also see checksum, Hashed Message Authentication Code, Message Digest 5.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 14 of 30)

Term	Acronym	Definition
Hashed Message Authentication Code	HMAC	An extremely powerful method of employing a hash function.
high-speed downlink packet access	HSDPA	An HSPA protocol for packets downloaded to the end-user device (the customer's device).
high-speed packet access	HSPA	A third-generation group of protocols, based on the Universal Mobile Telecommunications System (UMTS). HSPA provides high speed, high data capacity, and high reliability for packet transmission. *Also see high-speed downlink packet access.*
HMAC		*See Hashed Message Authentication Code.*
HSDPA		*See high-speed downlink packet access.*
HSPA		*See high-speed packet access.*
hybrid cryptography		*See combined cryptography.*
IBR-10™		*See IP Banking Router 10™.*
IDU™		*See Internal Data Unit™.*
IETF®		*See Internet Engineering Task Force.*
IKE		*See Internet Key Exchange.*
IKEv1		Version 1 of the Internet Key Exchange.
IKEv2		Version 2 of the Internet Key Exchange.
ILR-100™		*See IP Legacy Router 100™.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 15 of 30)

Term	Acronym	Definition
Institute of Electrical and Electronics Engineers	IEEE	A professional organization of engineers, scientists, and related industry professionals. IEEE's purposes include science and education in electrical engineering, electronics, and related fields. *Also see IEEE-SA.*
Institute of Electrical and Electronics Engineers Standards Association	IEEE-SA	An organization of IEEE that develops standards in several fields, including telecommunication.
Internal Data Unit™	IDU™	An optional set of four DB-25 serial ports, physically contained in the expanded model of the BANDIT III™ chassis. *Compare Remote Data Unit™.*
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. *Also see International Telecommunication Union, Telecommunication Standardization Sector.*
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 one or more Recommendations. **Note:** ITU-T was formerly known as the International Telegraph and Telephone Consultative Committee (CCITT, Comité consultatif international téléphonique et télégraphique).
International Telegraph and Telephone Consultative Committee	CCITT	A former name for the International Telecommunication Union, Telecommunication Standardization Sector. **Note:** The acronym CCITT derives from the equivalent former French name, 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.

Table D-1. Terms, Acronyms, and Definitions (Sheet 16 of 30)

Term	Acronym	Definition
Internet Key Exchange	IKE (IKEv1, IKEv2)	A protocol that negotiates authentication methods, encryption methods, and keys for IPsec. IKE can also negotiate the length of time that a key is valid before a new key must be implemented. IKE version 1 (IKEv1) and IKE version 2 (IKEv2) use different processes for exchanges: • In IKEv1 IPsec VPNs, the tunnel mode varies during VPN transmission: - IKEv1 can use main mode or aggressive mode to set up the tunnel - Then IKEv1 uses quick mode for communication through the tunnel. • IKEv2 uses only one mode.
Internet Protocol	IP	A connectionless protocol for transport and delivery of packets. IP is the principal protocol in the Internet Protocol suite. *Also see TCP, UDP.*
IP Banking Router 10™ (chassis)	IBR-10™	A router in the BANDIT™ family. The IBR-10 is dedicated to support of legacy protocols over IP networks. **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.*
IP Legacy Router 100™ (chassis)	ILR-100™	A miniature, streamlined router in the BANDIT™ family. The ILR-100 supports IPsec VPNs and supports legacy protocols over IP networks. **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.*
IPsec		*See IP Security Protocol.*
IP Security Protocol	IPsec, IPSEC	A protocol to protect IP transmissions (for example, in VPNs). IPsec comprises two protocols that may be applied separately or together: • Authentication Header (AH) • Encapsulating Security Protocol (ESP) The Internet Key Exchange (IKE) uses different processes for IPsec exchanges in IKE version 1 (IKEv1) and version 2 (IKEv2). An IPsec VPN tunnel can also function in transport mode. *Also see Internet Key Exchange, virtual private network, VPN tunneling.*
ITU		*See International Telecommunication Union.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 17 of 30)

Term	Acronym	Definition
ITU-T		*See International Telecommunication Union, Telecommunication Standardization Sector.*
key pair		An encryption set used in asymmetric encryption. The key pair comprises a private key and its counterpart public key. **Note:** Only the holder of the private key knows the complete key pair.
LAN		*See local area network.*
local area network	LAN	A group of computers, routers, and other electronic devices in the same location and on the same IP network. The size and geographic range of a LAN can vary. A LAN might comprise one household or it might span several floors of a business office. Most LANs lie somewhere between those examples.
main mode		A mode that can be used in phase 1 of an IKEv1 IPsec VPN tunnel. (Phase 1 sets up the VPN tunnel.) Main mode hides the identities of the parties while negotiating the security association. Main mode is more secure than aggressive mode. **Note:** Phase 2 (bulk data transfer) of an IKEv1 IPsec VPN tunnel uses quick mode. *Compare aggressive mode, transport mode. Also see tunnel mode.*
MD5		*See Message Digest 5.*
Message Digest 5	MD5	A hash function that authenticates packet data by creating a 16-byte message digest. Used in AH and ESP.
multimode fiber		An optical fiber that can carry more than one ray of light pulses. Multimode fiber is used for shorter distances than single-mode fiber is. Multimode fiber also has more attenuation than single-mode fiber because the light rays reflect along the fiber core more often.
NAT		*See network address translation.*
National Institute of Standards and Technology	NIST	A U.S. Agency that supports (but does not regulate) measurement, evaluation, and standards for technology. *Also see FIPS.*
NAT traversal		*See network address translation traversal.*
NERC		*See North American Electric Reliability Corporation.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 18 of 30)

Term	Acronym	Definition
network access device		A device that provides connection to a network. *Compare gateway.*
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.*
network address translation traversal	NAT traversal	A method of address translation traversal across NAT. NAT traversal is described in IETF RFC 3947, with reference to RFCs 3948 and 3715. NAT traversal is used primarily to allow routers to build IPsec VPNs or Voice over IP connections through networks that use firewalls and NAT. **Note:** IKEv2 IPsec automatically includes NAT traversal. ***Note:*** *Also see Encore NAT Traversal™.*
NIST		*See National Institute of Standards and Technology.*
North American Electric Reliability Corporation	NERC	A non-profit corporation formed by the electric-utility industry to promote the dependability of electric-power transmission systems in North America. Adherence to NERC standards is mandatory in the United States and in some parts of Canada. NERC includes critical infrastructure protection. **Note:** The prior organization charged with responsibility for electric-power dependability was the North American Electric Reliability Council (also NERC).
offsite connection to office		*See teleworking.*
optical fiber		A solid glass or plastic fiber that carries light pulses for fiber optic networks. Advantages of optical fiber include high speed, high reliability, ability to send transmissions over long distances without significant degradation, immunity to electromagnetic interference and radiofrequency interference, and high security. Optical fiber generally uses an SFP connector. Optical fiber is available in single-mode fiber or multimode fiber.
originating address		*See source address.*
PAT		*See port address translation.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 19 of 30)

Term	Acronym	Definition
PCI		*See Peripheral Component Interconnect.*
PEP		*See performance enhancement proxy.*
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.) *Also see Selective Layer Encryption™.*
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.
PFS		*See perfect forward secrecy.*
PKC		*See public-key cryptography.*
plain old telephone service	POTS	Analog telephone service that, in many areas, connects landline phones and other end-line customer devices to the public switched telephone system (PSTN). Faxes, modems, and many other business devices still use POTS to transmit digital information. **Note:** The terms “POTS” and “PSTN” are often used interchangeably, despite their references to different entities.
port address translation	PAT	Inclusion of port numbers when implementing network address translation. **Note:** NAT methods generally include PAT.
POTS		*See plain old telephone service.*
PrAT™		*See Private Address Translation™.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 20 of 30)

Term	Acronym	Definition
pre-shared key		*See secret key.* **Note:** A pre-shared key is not a generated shared secret.
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 that the holder of a key pair uses for encryption and decryption of communication with others. The private key is never shared. The private key's counterpart is the public key. *Also see asymmetric encryption.*
psophometric weighting		A method of weighting when measuring circuit noise. **Note:** ITU is studying recommendations for psophometric weighting in telecommunication.
PSTN		*See public switched telephone system.*
public key		The key that, when communicating with the holder of a private key, other entities use for encryption and decryption. The public key is freely available to anyone. The private key and its counterpart public key constitute the key pair. *Also see asymmetric encryption.*
public-key cryptography	PKC	*See asymmetric encryption.*
public switched telephone system	PSTN	The global network of the world's public telephone networks. The PSTN's implementation of ITU-T standards for connection and for telephone numbering makes it possible to call any telephone from anywhere in the world. **Note:** In many areas, end-line customer devices (for example, landline telephones) use plain old telephone service (POTS) to connect to the PSTN. The terms "POTS" and "PSTN" are often used interchangeably, despite their references to different entities.
QOS, QoS		*See quality of service.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 21 of 30)

Term	Acronym	Definition
quality of service	QOS, QoS	Guarantee of a specific throughput, achieved by configuring bandwidth, packet priority, and so forth. *Also see class of service, Differentiated Services, type of service.*
quick mode		The mode used for communication in phase 2 of an IKEv1 IPsec VPN tunnel. (Phase 2 is used for the communication payload—for example, data transfer.) **Note:** For phase 1 (setting up the VPN tunnel) of an IKEv1 IPsec VPN tunnel, see main mode or aggressive mode. *Compare transport mode. Also see tunnel mode.*
rack unit (measurement)	U	A measure of vertical distance defined in EIA-310. 1U is equal to 1.75 inches or 4.445 cm.
radiofrequency	RF	Any frequency in the radiowave spectrum used for radio communication.
RADIUS (authentication)		*See Remote Authentication Dial-In User Service.*
RADIUS shared secret		A secret key used in the Remote Authentication Dial-In User Service. **Note:** The RADIUS shared secret is not a generated shared secret used in a key-agreement protocol. *Compare shared secret (generated).*
RDU™		*See Remote Data Unit™.*
re-keying		An IKE feature that sets the interval between encryption key changes. Re-keying increases key security.
Remote Authentication Dial-In User Service	RADIUS	A network service that provides centralized authentication, authorization, and accounting for connections to a network. *Also see RADIUS shared secret.*
remote connection to office		*See teleworking.*
Remote Data Unit™ (peripheral device)	RDU™	A peripheral device for the VSR-1200™ and the BANDIT Plus™, supplying twelve DB-25 serial ports. *Compare Internal Data Unit™.*
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.

Table D-1. Terms, Acronyms, and Definitions (Sheet 22 of 30)

Term	Acronym	Definition
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.
Restriction of Hazardous Substances (directive)	ROHS	A directive set forth by the European Union (EU), specifying standards that restrict or prohibit the use of specified hazardous substances in the manufacture of electric and electronic equipment.
RF		*See radiofrequency.*
RFC		*See Request for Comments.*
Rivest–Shamir–Adleman algorithm	RSA (algorithm)	A public-key algorithm for asymmetric encryption, generally considered secure when sufficiently long keys are used. **Note:** A key of 512 bits is considered insecure; a key of 1024 bits is considered quite secure.
ROHS		*See Restriction of Hazardous Substances.*
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.
RSA		*See Rivest–Shamir–Adleman algorithm.*
SA		*See security association.*
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 generated shared secret.
secret-key cryptography		*See symmetric encryption.*
secure hash algorithm	SHA	A routine that develops a 20-byte hash function 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 *Also see security parameter index.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 23 of 30)

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.
SFP		*See small form-factor pluggable transceiver.*
SHA		*See secure hash algorithm.*
shared key		*See secret key.* **Note:** A shared key is not a generated shared secret.
shared secret, generated		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. A shared secret is sometimes developed in VPN connections. **Note:** A generated shared secret is not a shared key. *Compare RADIUS shared secret.*
shared secret, RADIUS		*See RADIUS shared secret.*
SIM		*See Subscriber Identity Module.*
single-mode fiber		An optical fiber that carries a single ray of light pulses. Single-mode fiber is used for longer distances than multimode fiber is. Single-mode fiber also has less attenuation than multimode fiber because the light rays reflect along the fiber core less often.
SLE™		*See Selective Layer Encryption™.*
SMA		*See sub-miniature coaxial connector, type A.*
small form-factor pluggable transceiver	SFP (transceiver)	A transceiver for optical fiber connections. **Note:** An SFP transceiver can be inserted into or removed from a port in a router's Fiber Optic Card while the router is running.
smartcard (for GSM)		*See Subscriber Identity Module.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 24 of 30)

Term	Acronym	Definition
source address		(Also called originating address.) The address of the device that initiates a transmission. *Compare destination address.*
Special International Committee on Radio Interference	CISPR	A committee that sets standards for controlling interference from electromagnetic emissions. CISPR is part of the International Electrotechnical Commission (IEC). **Note:** The acronym CISPR is from the French name for the committee, Comité international spécial des perturbations radioélectriques.
SPI		*See security parameter index.*
split tunneling		The ability to route VPN traffic through VPN tunnels and to route non-VPN traffic outside these tunnels, on the same line. **Note:** Encore Networks' VPN products perform split tunneling automatically and 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.
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.*
TCP		*See Transmission Control Protocol.*
TDEA		*See Triple Data Encryption Standard.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 25 of 30)

Term	Acronym	Definition
TDM		*See time-division multiplexing.*
TDMA		*See time-division multiple access.*
Telecommunication Standardization Sector		*See International Telecommunication Union, Telecommunication Standardization Sector.*
telecommuting		*See teleworking.*
teleworking		Performance of employment responsibilities by means of a remote connection to the central network. The remote site can connect to the central site in one of several ways—for example, through a VPN tunnel. Teleworking (also called telecommuting) saves time and provides convenience for business travelers, employees working at home, and other remote users.
TFTP		*See Trivial File Transfer Protocol.*
throughput		The data transfer rate.
time-division multiple access, time-division multiplexing	TDMA, TDM	A wireless technology that divides a network's radiofrequency band into timeslots and allocates the timeslots to calls. This allows one radiofrequency band to support several simultaneous calls. *Compare code-division multiplexing, wavelength-division multiplexing.*
timeslot		One of several subchannels allocated to carry data in time-division multiplexing.
TOS, ToS		*See type of service.*
traffic analysis		Analysis of network traffic in order to infer information—for example, source address, destination address, frequency of transmission, or packet size.
transceiver		A combined transmitter and receiver. The term is used to specify a type of SFP for optical fiber connections.
Transmission Control Protocol	TCP	A protocol layer used in the Internet Protocol suite. TCP checks for packet receipt and packet order. *Compare User Datagram Protocol.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 26 of 30)

Term	Acronym	Definition
transport mode		A mode in which the endpoints of an IPsec VPN connection perform their own encryption. The VPN gateway functions solely as the transport, encapsulating (thus protecting) the upper layer payload and reusing the IP header. *Compare main mode, aggressive mode, quick mode. Also see tunnel mode.*
triangulation		A method of calculating position, in Cartesian coordinates *x* and *y*, by means of distances and angles from static points whose positions are known (or by means of distances and angles from points whose positions are in motion and by relating each position to a specific time *t*). Triangulation uses the law of sines in one plane (for coordinates *x* and *y*), and requires at least one known distance and two known angles. Collection of this information requires at least two reference points (for example, static towers for cellular wireless networks), so that a triangle is formed by the positions of any two reference points and the position being calculated. **Note:** GPS does not use triangulation; GPS uses trilateration. However, when GPS signals are weak, triangulation might be useful instead of trilateration to determine position. For details and examples of triangulation, please see the non-GPS navigation literature. *Compare trilateration.*
trilateration		A method of calculating position, in Cartesian coordinates *x*, *y*, and *z*, by means of distances from static points whose positions are known (or by means of distances from points whose positions are in motion and by relating each position to a specific time *t*). Trilateration works with three reference points (for example, satellites). In GPS, data are needed from four satellites, because one of the computations solves for real time. (A GPS satellite includes its clock time with each set of spatial coordinates it broadcasts. The signal delay caused by travel through the atmosphere must be resolved in terms of real time.) Data from four satellites allow simultaneous solution for four variables (time *t* and coordinates *x*, *y*, and *z*) in four linear equations. If the value of one variable is already known (for example, at sea level, altitude *z* is zero), data are sufficient from three satellites. **Note:** For details and examples of trilateration, please see the GPS navigation literature. *Compare triangulation.*
Triple Data Encryption Algorithm	TDEA	*See Triple Data Encryption Standard.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 27 of 30)

Term	Acronym	Definition
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 protocol for transferring files. TFTP is based on UDP.
tunneling		Use of encapsulation to send one protocol through a network that uses a different protocol. *Also see tunnel mode, VPN tunneling.*
tunnel mode		In IKEv1, the type of tunneling used in a transmission. For example, an IKEv1 IPsec VPN might use *main mode or aggressive mode, then quick mode*; or it might use only *transport mode*. *Also see tunneling, VPN 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. *Contrast with class of service. Also see Differentiated Services, quality of service.*
U (a unit of measure)		*See rack unit.*
UDP		*See User Datagram Protocol.*
User Datagram Protocol	UDP	A protocol layer used in the Internet Protocol suite. UDP does not check for packet order or packet receipt. **Note:** TFTP is based on UDP. *Compare Transmission Control Protocol.*
VBRS™		*See Virtual Broadband Redundancy System™.*
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.

Table D-1. Terms, Acronyms, and Definitions (Sheet 28 of 30)

Term	Acronym	Definition
Virtual Broadband Redundancy System™	VBRS™	A value-added system (from Encore Networks, Inc.) providing host-to-host physical and logical redundancy for continuous management of the Remote Data Unit™. VBRS is used only in the VSR-1200™ and the BANDIT Plus™. **Note:** VBRS and VRRP are sometimes confounded but are unrelated. Both processes provide redundancy, but in different ways.
Virtual LAN		*See virtual local area network.*
virtual local area network	VLAN	A group of devices within a LAN (or a group of devices located in two or more LANs) selected to receive broadcasts intended only for that group. Use of VLANs reduces the amount of traffic broadcast to the entire LAN. **Note:** VLANs are described in IEEE standards 802.1q and 802.1p. *Also see VLAN broadcast.*
virtual private network	VPN	Use of encryption, authentication, and tunneling across a public network to ensure secure communication between private endpoints. A VPN can implement one or more technologies to accomplish secure private communication—for example, IPsec or SLE™. **Note:** 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 *Also see VPN tunneling.*
Virtual Private Network Consortium	VPN Consortium, VPNC	A trade association for manufacturers and vendors of VPN products. The VPN Consortium tests products for VPN compliance and interoperability. The VPNC supports development of standards for VPNs, but the VPNC itself does not develop standards. **Encore Networks, Inc., is a member of the VPN Consortium.** *For a list of RFCs applicable to VPNs, see the VPN Consortium's website:* www.vpnc.org/vpn-standards.html
Virtual Router Redundancy Protocol	VRRP	A protocol for providing continuous router support to a network. VRRP and VBRS™ are sometimes confounded but are unrelated. Both processes provide redundancy, but in different ways.
VLAN		*See virtual local area network.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 29 of 30)

Term	Acronym	Definition
VLAN broadcast		A broadcast directed to a specified VLAN. **Note:** VLAN broadcasts reduce the amount of traffic sent to the entire LAN.
VPN		*See virtual private network.*
VPNC		*See Virtual Private Network Consortium.*
VPN Consortium		*See Virtual Private Network Consortium.*
VPN Satellite Router™ products	VSR™ products	A group of routers in the BANDIT™ products that support VPNs over ground-based networks and, via Selective Layer Encryption™, support VPNs over satellite networks. The VSR product line includes the VSR-30™ and the VSR-1200™.
VPN tunneling		The use of tunneling on a VPN. **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, IP Security Protocol.*
VRRP		*See Virtual Router Redundancy Protocol.*
VSAT		*See very-small-aperture terminal.*
VSR-30™ (chassis)		A router in the VSR™ group, supporting IPsec VPNs over ground-based networks and satellite networks, and featuring IPsec VPNs with SLE™. The VSR-30 can support up to 30 VPN tunnels. **Note:** This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. *For more information, see the BANDIT Product Document Set.*
VSR-1200™ (chassis)		A router in the VSR™ group, supporting IPsec VPNs over ground-based networks and satellite networks, and featuring IPsec VPNs with SLE™. The VSR-1200 can support up to 1200 VPN tunnels. The VSR-1200 also has the option to use one or two RDUs.
VSR™ products		*See VPN Satellite Router™ products.*
wavelength-division multiple access, wavelength-division multiplexing	WDMA, WDM	A technology sometimes used in fiber optic networks. WDM sends several wavelengths across one optical fiber, increasing the fiber's carrying capacity. WDM also allows bidirectional transmission over an optical fiber. *Compare code-division multiplexing, time-division multiplexing.*

Table D-1. Terms, Acronyms, and Definitions (Sheet 30 of 30)

Term	Acronym	Definition
WDM		*See wavelength-division multiplexing.*
WDMA		*See wavelength-division multiple access.*
weighting		Adding emphasis to some data in order to make properties or relationships more apparent. For example, a criterion under study can be given priority by weighting it. This allows the effect of the criterion to be better analyzed and understood. *Also see psophometric weighting.*
wifi		*See 802.11 wireless.*
wireless fidelity	wifi	*See 802.11 wireless.*
working off site		*See teleworking.*