

# Glossary

Table B-1 lists acronyms and definitions for terms used in discussions of products from Encore Networks, Inc.<sup>1,2</sup>

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

Term	Acronym	Definition
3DES		See <i>Triple Data Encryption Standard</i> .
3rd Generation Partnership Project	3GPP	An organization that directs standards for technology used in mobile telephony.
802.11 wireless	wifi	A set of <a href="#">IEEE</a> specifications for wireless LANs using the 2.4 GHz or 5 GHz frequency bands. <i>802.11 wireless is sometimes called "wifi."</i>
access point	AP	A device that provides access (connection) to a wireless network. <b>Note:</b> 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. <i>Also see <a href="#">network address translation</a>, <a href="#">Private Address Translation™</a>, <a href="#">address translation traversal</a>.</i>
address translation traversal		Any of several methods of maintaining end-to-end connectivity and security when <a href="#">address translation</a> occurs between the transmission endpoints. <i>Also see <a href="#">NAT traversal</a>, <a href="#">Encore NAT Traversal™</a>.</i>

1. Entries in [Table B-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 by character sequence. Spaces, hyphens, dashes, apostrophes, quotation marks, parentheses, and other special characters (for example, "&" or "™") are ignored.

2. A non-English name of an organization follows capitalization guidelines for the source language.

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

Term	Acronym	Definition
<b>Advanced Encryption Standard</b>	AES	An <a href="#">encryption</a> standard, <a href="#">FIPS 197</a> , that <a href="#">NIST</a> proposes to replace <a href="#">DES</a> . AES uses the Rijndael symmetric <a href="#">block cipher</a> , and supports 128-bit, 192-bit, and 256-bit keys.
<b>AES</b>		See <a href="#">Advanced Encryption Standard</a> .
<b>aggressive mode</b>		A mode that can be used in phase 1 of an <a href="#">IKEv1 IPsec VPN</a> tunnel. (Phase 1 sets up the VPN tunnel.) Aggressive mode does not hide the identities of the parties while negotiating the <a href="#">security association</a> . Aggressive mode is quicker than <a href="#">main mode</a> . <b>Note:</b> Phase 2 (bulk data transfer) of an IKEv1 IPsec VPN tunnel uses <a href="#">quick mode</a> . Compare <a href="#">main mode</a> , <a href="#">transport mode</a> . Also see <a href="#">tunnel mode</a> .
<b>AH</b>		See <a href="#">authentication header</a> .
<b>anti-replay</b>		An <a href="#">IPsec</a> routine that uses <a href="#">authentication</a> and sequence numbers to thwart <a href="#">replay attacks</a> .
<b>AP</b>		See <a href="#">access point</a> .
<b>asymmetric encryption</b>		(Also called public-key cryptography.) Use of a paired <a href="#">private key</a> and <a href="#">public key</a> for <a href="#">encryption</a> and <a href="#">decryption</a> . 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 <a href="#">authentication</a> , including non-repudiation. <a href="#">RSA</a> is an example of asymmetric encryption. <b>Note:</b> 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 <a href="#">symmetric encryption</a> . Also see <a href="#">combined cryptography</a> .
<b>authentication</b>		Verification that the declared sender is the actual sender, and that the data received are the data that were sent.
<b>authentication header</b>	AH	An <a href="#">IPsec</a> protocol that performs <a href="#">authentication</a> . AH may be applied alone or with <a href="#">ESP</a> .

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

Term	Acronym	Definition
BANDIT™ (chassis)		<p>The original tabletop chassis in the family of <a href="#">BANDIT™ products</a>. This model provides support for legacy protocols over IP and provides support for up to 30 <a href="#">IPsec VPNs</a>.</p> <p>See <a href="#">Broadband Access Network Device for Intelligent Termination™</a>.</p> <p><b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product.</p> <p><i>For more information, see the BANDIT Product Document Set.</i></p>
BANDIT™ family		<p>See <a href="#">BANDIT™ products</a>.</p>
BANDIT II™ (chassis)		<p>An environmentally hardened (“ruggedized”) <a href="#">ROHS-compliant</a> miniature desktop model in the <a href="#">BANDIT™</a> family, providing legacy-protocol support and <a href="#">IPsec VPNs</a> using <a href="#">DES</a>, <a href="#">3DES</a>, or <a href="#">AES</a>. It is available in a commercial chassis or in an industrially hardened chassis.</p> <p><b>Note:</b> 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.</p>
BANDIT II C2C™ (chassis)		<p>A streamlined router in the BANDIT™ family’s <a href="#">C2C™ products</a>, developed to support legacy devices (such as modems) migrating from <a href="#">POTS</a> applications to cellular wireless networks. The BANDIT II C2C supports <a href="#">IPsec VPNs</a> and supports legacy protocols over IP networks.</p> <p><i>Also see <a href="#">C2C™ (chassis)</a>, <a href="#">Copper to Cellular™ (technology)</a>.</i></p>
BANDIT III™ (chassis)		<p>An environmentally hardened (ruggedized) <a href="#">ROHS-compliant</a> full-featured tabletop model in the <a href="#">BANDIT™</a> family, providing legacy-protocol support and providing <a href="#">IPsec VPNs</a> using <a href="#">DES</a>, <a href="#">3DES</a>, or <a href="#">AES</a>.</p> <p>The BANDIT III has an external expansion port and an optional internal wireless card. It also can include an <a href="#">Internal Data Unit™</a>, which provides four additional serial ports, or it can include an internal <a href="#">E&amp;M</a> card for a pulse-code modulated (PCM) voice network, which provides two audio ports and eight relay ports.</p> <p><b>Note:</b> Optional brackets for the BANDIT III allow the chassis to be mounted in a standard equipment rack.</p>
BANDIT IP™ (chassis)		<p>A tabletop streamlined router in the <a href="#">BANDIT™</a> family. The BANDIT IP supports <a href="#">IPsec VPNs</a>.</p> <p><b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product.</p> <p><i>For more information, see the BANDIT Product Document Set.</i></p>

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

Term	Acronym	Definition
<b>BANDIT Mini™</b> (chassis)		<p>A miniature, streamlined router in the <a href="#">BANDIT™</a> family. The BANDIT Mini supports <a href="#">IPsec VPNs</a> and supports legacy protocols over IP networks.</p> <p><b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product.</p> <p><i>For more information, see the BANDIT Product Document Set.</i></p>
<b>BANDIT Plus™</b> (chassis)		<p>A full-featured rackmounted model in the <a href="#">BANDIT™</a> family, providing legacy-protocol support and providing up to 100 <a href="#">IPsec VPN</a> tunnels that use DES or 3DES. The BANDIT Plus has the option to use one <a href="#">RDU™</a>.</p> <p><b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product.</p> <p><i>For more information, see the BANDIT Product Document Set.</i></p>
<b>BANDIT™</b> products		<p>Encore Networks, Inc.'s family of products that support <a href="#">VPNs</a> or support legacy protocols over IP, or both. The product family includes the <a href="#">BANDIT™</a>, <a href="#">C2C™</a>, <a href="#">BANDIT II™</a>, <a href="#">BANDIT II C2C™</a>, <a href="#">BANDIT III™</a>, <a href="#">BANDIT IP™</a>, <a href="#">BANDIT Mini™</a>, <a href="#">BANDIT Plus™</a>, <a href="#">E2C™</a>, <a href="#">IBR-10™</a>, <a href="#">ILR-100™</a>, <a href="#">VSR-30™</a>, and <a href="#">VSR-1200™</a> chassis. It also includes the <a href="#">RDU™</a>, a peripheral device for optional use with the BANDIT Plus or the VSR-1200.</p> <p><b>Note:</b> The BANDIT products include the <a href="#">C2C™ products</a>. <i>Also see <a href="#">Broadband Access Network Device for Intelligent Termination™</a>.</i></p>
block cipher		Encryption of data into blocks of a fixed size.
<b>Broadband Access Network Device for Intelligent Termination™</b>	BANDIT™	<p>The original chassis in Encore Networks, Inc.'s <a href="#">BANDIT™ products</a>. <i>See <a href="#">BANDIT™ (chassis)</a>.</i></p> <p><b>Note:</b> The term "BANDIT" can indicate the entire family of <a href="#">BANDIT™ products</a> (including the <a href="#">C2C™ products</a>) or can indicate a specific chassis (when stipulated): the original <a href="#">BANDIT™</a>, the <a href="#">BANDIT II™</a>, the <a href="#">BANDIT III™</a>, the <a href="#">BANDIT IP™</a>, the <a href="#">BANDIT Mini™</a>, or the <a href="#">BANDIT Plus™</a>.</p>
<b>C2C™</b> (chassis)		<p>A miniature streamlined router in the <a href="#">BANDIT™</a> family's <a href="#">C2C™ products</a>, developed to support legacy devices (such as modems) migrating from <a href="#">POTS</a> applications to cellular wireless networks.</p> <p>The C2C is available in commercial and industrial models. The C2C can support <a href="#">IPsec VPNs</a> and can support legacy protocols over IP networks.</p> <p><i>Also see <a href="#">BANDIT II C2C™</a>, <a href="#">Copper to Cellular™ (technology)</a>.</i></p>

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

Term	Acronym	Definition
C2C™ products		A line of commercial and industrial products featuring support for <a href="#">Copper to Cellular™</a> migration. The C2C product family includes the C2C™, the E2C™, and the <a href="#">BANDIT II C2C™</a> . The C2C products are part of the family of <a href="#">BANDIT™ products</a> .
C2C™ technology		See <a href="#">Copper to Cellular™ (technology)</a> .
CA		See <a href="#">certificate authority</a> .
CCITT		The acronym for the Comité consultatif international téléphonique et télégraphique, a former French name for the <a href="#">International Telecommunication Union, Telecommunication Standardization Sector</a> . (The English equivalent of the former name was the International Telegraph and Telephone Consultative Committee.)
CDM		See <a href="#">code-division multiplexing</a> .
CDMA		See <a href="#">code-division multiple access</a> .
CEN		See <a href="#">European Committee for Standardization</a> .
certificate authority	CA	Use of digital certificates to identify and authenticate trusted clients and servers in a connection.
checksum		An algorithm performed to detect accidental error during data transmission or during data storage. <b>Note:</b> Errors in transmission are usually caused by a bad line. <i>Also see <a href="#">cyclic redundancy check</a>, <a href="#">hash function</a>, <a href="#">authentication</a>.</i>
CIP		See <a href="#">critical infrastructure protection</a> .
CISPR		See <a href="#">Special International Committee on Radio Interference</a> .
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. <i>Also see <a href="#">Differentiated Services</a>, <a href="#">quality of service</a>, <a href="#">type of service</a>.</i>

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

Term	Acronym	Definition
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 <a href="#">radiofrequency</a> band. When the call is received, it is reassembled. <i>Compare <a href="#">time-division multiplexing</a>, <a href="#">wavelength-division multiplexing</a>.</i>
combined cryptography		(Also called hybrid cryptography.) A common practice of using <a href="#">asymmetric encryption</a> and <a href="#">symmetric encryption</a> together. For example, to encrypt a message: <ul style="list-style-type: none"> <li>• A sender might create a <a href="#">secret key</a> and use it for symmetric encryption of a message.</li> <li>• Then the sender might use asymmetric encryption (choosing the recipient's <a href="#">public key</a> or the sender's <a href="#">private key</a>) to package the encrypted message and its secret key together as a single encrypted document. <b>Note:</b> The recipient's public key is the safer choice, because no one except the recipient should know the counterpart private key.</li> </ul> To decrypt the message: <ul style="list-style-type: none"> <li>• The recipient uses the counterpart in the <a href="#">key pair</a> chosen by the sender (that is, the recipient's private key or the sender's public key) to open the document. That <a href="#">decryption</a> reveals the secret key and the still-encrypted message.</li> <li>• Then the recipient uses the secret key to decrypt the message.</li> </ul>
Comité consultatif international téléphonique et télégraphique	CCITT	A former French name for the <a href="#">International Telecommunication Union, Telecommunication Standardization Sector</a> . (The equivalent former English name was the International Telegraph and Telephone Consultative Committee.)
Comité européen de normalisation	CEN	The French name for the <a href="#">European Committee for Standardization</a> .
Comité international spécial des perturbations radioélectriques	CISPR	The French name for the <a href="#">Special International Committee on Radio Interference</a> .
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 <a href="#">encryption</a> .

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

Term	Acronym	Definition
connection between office and remote location		See <a href="#">teleworking</a> .
connectionless (protocol)		<p>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.</p> <p>Because there is no specified route for transmissions, individual packets in a transmission can travel over different routes to the destination.</p> <p>A connectionless protocol, such as <a href="#">IP</a>, does not check for completion of delivery—but it can use other protocols, such as <a href="#">TCP</a>, to check for completion of delivery.</p> <p>Compare <a href="#">connection-oriented</a>.</p>
connection-oriented (protocol)		<p>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.</p> <p>A connection-oriented protocol, such as <a href="#">TCP</a>, checks for completion of delivery.</p> <p>Compare <a href="#">connectionless</a>.</p>
cookie		A cipher, generated and assigned by the host, that identifies clients without using comprehensive <a href="#">authentication</a> . As used in <a href="#">IKE</a> , cookies conserve CPU resources yet offer some protection against <a href="#">replay attacks</a> .
Copper to Cellular™ (technology)	C2C™ (technology)	<p>An Encore Networks implementation that supports legacy equipment migration from copper wire networks to cellular wireless networks.</p> <p>See <a href="#">C2C™ products</a>, <a href="#">C2C™ (chassis)</a>, <a href="#">E2C™ (chassis)</a>, <a href="#">BANDIT II C2C™</a>.</p>
COS, CoS		See <a href="#">class of service</a> .
CRC		See <a href="#">cyclic redundancy check</a> .
critical infrastructure protection	CIP	<p>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.</p> <p>Also see <a href="#">North American Electric Reliability Corporation</a>.</p>
cyclic redundancy check	CRC	Any of several <a href="#">checksum</a> algorithms based on cyclic processes.

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

Term	Acronym	Definition
<b>data carrier equipment</b>	DCE	A device that sits between a <a href="#">DTE</a> and the network. Modems and routers are examples of DCEs.
<b>data diversity</b>		<p>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 <a href="#">diversity antenna</a>. The EN-4000 and several <a href="#">BANDIT™ products</a> can use diversity antennas.)</p> <p>Data diversity permits a larger number of calculations, contributing to more accurate resolution of information from the signals.</p> <p>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.</p>
<b>Data Encryption Algorithm</b>	DEA	See <a href="#">Data Encryption Standard</a> .
<b>Data Encryption Standard</b>	DES	<p>A standard <a href="#">block cipher encryption</a> algorithm that uses the same 56-bit key for encryption and decryption.</p> <p><b>Note:</b> Because its short key length makes DES vulnerable to persistent attack, <a href="#">3DES</a> can be used, providing longer key lengths for additional security.</p>
<b>data integrity</b>		<p>Use of a <a href="#">checksum</a> to ensure that data have been transmitted from endpoint to endpoint without error.</p> <p>The checksum in <a href="#">IPsec</a> uses <a href="#">encryption</a>.</p>
<b>data terminal equipment</b>	DTE	<p>An endpoint device in a transmission circuit. A DTE goes through a <a href="#">DCE</a> to reach the network.</p> <p>A management console is an example of a DTE.</p>
<b>DCE</b>		See <a href="#">data carrier equipment</a> .
<b>DEA</b>		See <a href="#">Data Encryption Standard</a> .
<b>decryption</b>		<p>A process that reverses <a href="#">encryption</a> of a message so that the message content can be discerned.</p> <p>The use of encryption and decryption for data storage or for data transfer preserves <a href="#">confidentiality</a> and <a href="#">data integrity</a>.</p>
<b>DES</b>		See <a href="#">Data Encryption Standard</a> .
<b>destination address</b>		<p>The address of the endpoint device for which a transmission is destined.</p> <p>Compare <a href="#">source address</a>. Also see <a href="#">security parameter index</a>.</p>
<b>DH</b>		See <a href="#">Diffie–Hellman exchange</a> .



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

Term	Acronym	Definition
Differentiated Services (protocol)	diffserv	A protocol that handles packets by class instead of by individual packet request. <i>Also see <a href="#">class of service</a>, <a href="#">quality of service</a>, <a href="#">type of service</a>.</i>
Diffie–Hellman exchange	DH	An algorithm for developing a <a href="#">shared secret</a> between endpoints by combining the endpoints' <a href="#">public keys</a> and then separately combining this result with each endpoint's <a href="#">private key</a> .
diffserv		See <a href="#">Differentiated Services</a> .
directive on hazardous substances		See <a href="#">Restriction of Hazardous Substances</a> .
diversity antenna		A second antenna, which collects a second set of wireless signals (for <a href="#">data diversity</a> ). <b>Note:</b> 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 <a href="#">data terminal equipment</a> .
dynamic packet filtering		See <a href="#">stateful inspection</a> .
dynamic split tunneling		See <a href="#">split tunneling</a> .
E2C™ (chassis)		A miniature streamlined router in the BANDIT™ family's <a href="#">C2C™ products</a> , 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 <a href="#">IPsec VPNs</a> . The E2C is available in commercial and ruggedized industrial models. <i>Also see <a href="#">Ethernet to Cellular™ (technology)</a>, <a href="#">C2C™ products</a>.</i>
E2C™ technology		See <a href="#">Ethernet to Cellular™ (technology)</a> .
E and M	E&M	See <a href="#">earth and magneto</a> .
EAP		See <a href="#">Extensible Authentication Protocol</a> .
ear and mouth	E&M	See <a href="#">earth and magneto</a> .

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

Term	Acronym	Definition
earth and magneto (ground and battery)	E&M	<p>Signaling leads, traditionally used in the North American telecommunications industry, on a voice tie-line. This supervisory line signaling uses separate leads, called the E lead (also called earth or ground) and the M lead (magneto, battery).</p> <p>E&amp;M signaling uses two states: On hook and Off hook. Off hook sends a signal from the M lead to the E lead.</p> <p>There are E&amp;M standards with 2, 4, 6, or 8 wires. The BANDIT III supports 4-wire E&amp;M types I through V.</p> <p><b>Note:</b> E&amp;M type V is generally preferred; type II is second in preference. Type IV is not used often.</p> <p>E&amp;M is sometimes known as ear and mouth.</p>
EDGE		See <a href="#">Enhanced Data Rates for GSM Evolution</a> .
EIA		See <a href="#">Electronic Industries Alliance</a> .
Electronic Industries Alliance	EIA	<p>An alliance of U.S. trade organizations that issued standards for electronics manufacturing.</p> <p><b>Note:</b> The EIA has discontinued operation.</p>
ELIOS™		See <a href="#">Encore Legacy-to-IP Operating System™</a> .
E&M		See <a href="#">earth and magneto</a> .
EN-1000™ (chassis)		<p>A miniature streamlined router from Encore Networks, Inc. The EN-1000 supports a 3G/4G <a href="#">LTE</a> cellular wireless card, a WAN port, and a LAN port. It also supports <a href="#">VPNs</a> and legacy protocols.</p> <p>The EN-1000 can be managed through a browser window or via <a href="#">enCloud™</a>.</p>
EN-2000™ (chassis)		<p>A miniature streamlined router from Encore Networks, Inc. The EN-2000 supports a 3G/4G <a href="#">LTE</a> cellular wireless card, a WAN port, and a LAN port. It supports <a href="#">VPNs</a> and legacy protocols, and can support an <a href="#">802.11 wireless</a> card.</p> <p>The EN-2000 can be managed through a browser window or via <a href="#">enCloud™</a>.</p>
EN-4000™ (chassis)		<p>A miniature streamlined router from Encore Networks, Inc. The EN-4000 can support two 3G/4G cellular wireless cards, an <a href="#">802.11 wireless</a> card, a WAN port, four LAN ports, and a dual-serial module for two slots. It also supports IPsec <a href="#">VPNs</a> and legacy protocols.</p> <p>The EN-4000 can be managed through a browser window, through a command line interface (CLI), or via <a href="#">enCloud™</a>.</p>
EN-9000™ (server)		<p>A server from Encore Networks, Inc. The EN-9000 can support IPsec <a href="#">VPNs</a> and legacy protocols.</p> <p>The EN-9000 can be managed through a browser window or through a command line interface (CLI) or via <a href="#">enSite™</a>.</p>

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

Term	Acronym	Definition
encapsulate		See <a href="#">encapsulation</a> .
Encapsulating Security Payload	ESP	An <a href="#">IPsec</a> protocol that encrypts and encapsulates data into IP packets. ESP may be used alone or with <a href="#">AH</a> .
encapsulation		<p>Packaging information of one protocol within packets of another protocol. Encapsulation is generally used to carry information across a network that does not support the encapsulated protocol.</p> <p><b>Note:</b> The EN-4000 and most <a href="#">BANDIT™ products</a> routers can encapsulate several legacy protocols within IP. The routers can also encapsulate some protocols within Frame Relay.</p> <p>Also see <a href="#">tunneling</a>, <a href="#">generic route encapsulation</a>.</p>
enCloud™ Management System		A cloud management system from Encore Networks, Inc., for management of EN™ Routers via the internet.
Encore Legacy-to-IP Operating System™	ELIOS™	The operating system software in the <a href="#">BANDIT™ products</a> , used when configuring and managing the products.
Encore NAT Traversal™	eNT™	<p>A value-added method of <a href="#">NAT traversal</a>, available from Encore Networks, Inc.</p> <p>Encore's eNT™ can be used with Encore's <a href="#">SLE™</a>.</p> <p><b>Note:</b> Use of eNT™ requires <a href="#">BANDIT™ products</a> on both the local side and the remote side of the transmission.</p>
encryption		<p>Conversion of a message into a coded form so that its content cannot be readily discerned.</p> <p>The use of encryption and <a href="#">decryption</a> for data storage or transfer preserves <a href="#">confidentiality</a> and <a href="#">data integrity</a>.</p>
Enhanced Data Rates for GSM Evolution	EDGE	A technology for increased rate and improved reliability in <a href="#">GSM</a> transmissions.
enServer™		See <a href="#">EN-9000™</a> .
enSite™ Management System		The <a href="#">enCloud™ Management System</a> , modified for use in a closed, private network.
eNT™		See <a href="#">Encore NAT Traversal™</a> .
ESP		See <a href="#">Encapsulating Security Payload</a> .

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

Term	Acronym	Definition
Ethernet to Cellular™ (technology)	E2C™ (technology)	An Encore Networks implementation that supports IP transmissions over cellular wireless networks. <i>Also see <a href="#">E2C™ (chassis)</a>, <a href="#">C2C™ products</a>.</i>
European Committee for Standardization	CEN	A non-profit organization that supports development, maintenance, and distribution of uniform standards and specifications. <b>Note:</b> The acronym CEN is from the French name for the committee, Comité européen de normalisation.
European Union ROHS		<i>See <a href="#">Restriction of Hazardous Substances</a>.</i>
EVDO		<i>See <a href="#">Evolution of Data Optimization</a>.</i>
Evolution of Data Optimization	EVDO	A third-generation (3G) wireless protocol that improves <a href="#">CDM</a> speeds, improves reliability, and reduces latency.
Extensible Authentication Protocol	EAP	An authentication framework used in <a href="#">VPN</a> 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 <a href="#">IKE</a> version 2 might use for communication. EAP is defined in <a href="#">RFC 3748</a> .
Federal Information Processing Standard	FIPS	Any standard in the set of standards that <a href="#">NIST</a> develops and issues for use by federal contractors and non-military federal agencies. <b>Note:</b> 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. <i>Also see <a href="#">optical fiber</a>.</i>
FIPS		<i>See <a href="#">Federal Information Processing Standard</a>.</i>
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. <i>Also see <a href="#">stateful inspection</a>.</i>
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. <i>Compare <a href="#">network access device</a>.</i>

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

Term	Acronym	Definition
General Packet Radio Service	GPRS	A system that uses increased speed to support transfer of data packets over <a href="#">GSM</a> .
generated shared secret		See <a href="#">shared secret</a> , <a href="#">generated</a> .
generic route encapsulation	GRE	A method of encapsulating any protocol within IP packets. <i>Also see <a href="#">encapsulation</a>, <a href="#">tunneling</a>.</i>
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. <b>Note:</b> Most communications satellites are geosynchronous. Many communications satellites are geostationary (that is, the geosynchronous orbit is at the equator). 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. <a href="#">GPS</a> 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. <b>Note:</b> GPS signals do not travel far through liquids and cannot support navigation under water. <i>Also see <a href="#">trilateration</a>.</i>
Global System for Mobile Communications	GSM	A wireless network based on <a href="#">TDM</a> technology. <b>Note:</b> Each GSM device uses a region-specific or country-specific <a href="#">SIM</a> to enable use of the GSM device in that region or country.
GPRS		See <a href="#">General Packet Radio Service</a> .
GPS		See <a href="#">Global Positioning System</a> .
GRE		See <a href="#">generic route encapsulation</a> .
ground and battery		See <a href="#">earth and magneto</a> .
GSM		See <a href="#">Global System for Mobile Communications</a> .
GSM smartcard		See <a href="#">Subscriber Identity Module</a> .
GSO		See <a href="#">geostationary (orbit)</a> , <a href="#">geosynchronous (orbit)</a> .

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

Term	Acronym	Definition
hash function		Any of several algorithms that map data sets to strings of uniform length. Hashes are generally used to index data. <b>Note:</b> In <i>IPsec</i> , a hash is an <i>IKE</i> authentication routine that generates a string of fixed size from a message of variable size. <i>Also see <a href="#">checksum</a>, <a href="#">Hashed Message Authentication Code</a>, <a href="#">Message Digest 5</a>.</i>
Hashed Message Authentication Code	HMAC	An extremely powerful method of employing a <a href="#">hash function</a> .
high-speed downlink packet access	HSDPA	An <i>HSPA</i> 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. <i>Also see <a href="#">high-speed downlink packet access</a>.</i>
HMAC		<i>See <a href="#">Hashed Message Authentication Code</a>.</i>
HSDPA		<i>See <a href="#">high-speed downlink packet access</a>.</i>
HSPA		<i>See <a href="#">high-speed packet access</a>.</i>
hybrid cryptography		<i>See <a href="#">combined cryptography</a>.</i>
IBR-10™		<i>See <a href="#">IP Banking Router 10™</a>.</i>
IDU™		<i>See <a href="#">Internal Data Unit™</a>.</i>
IEEE		<i>See <a href="#">Institute of Electrical and Electronics Engineers</a>.</i>
IEEE-SA		<i>See <a href="#">Institute of Electrical and Electronics Engineers Standards Association</a>.</i>
IETF®		<i>See <a href="#">Internet Engineering Task Force</a>.</i>
IKE		<i>See <a href="#">Internet Key Exchange</a>.</i>
IKEv1		Version 1 of the <a href="#">Internet Key Exchange</a> .
IKEv2		Version 2 of the <a href="#">Internet Key Exchange</a> .
ILR-100™		<i>See <a href="#">IP Legacy Router 100™</a>.</i>

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

Term	Acronym	Definition
<b>Institute of Electrical and Electronics Engineers</b>	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. <i>Also see <a href="#">IEEE-SA</a>.</i>
<b>Institute of Electrical and Electronics Engineers Standards Association</b>	IEEE-SA	An organization of <a href="#">IEEE</a> that develops standards in several fields, including telecommunication.
<b>Internal Data Unit™</b>	IDU™	An optional set of four DB-25 serial ports, physically contained in the expanded model of the <a href="#">BANDIT III™</a> chassis. <i>Compare <a href="#">Remote Data Unit™</a>.</i>
<b>International Telecommunication Union</b>	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. <i>Also see <a href="#">International Telecommunication Union, Telecommunication Standardization Sector</a>.</i>
<b>International Telecommunication Union, Telecommunication Standardization Sector</b>	ITU-T	An <a href="#">ITU</a> 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. <b>Note:</b> ITU-T was formerly known as the International Telegraph and Telephone Consultative Committee (CCITT, Comité consultatif international téléphonique et télégraphique).
<b>International Telegraph and Telephone Consultative Committee</b>	CCITT	A former name for the <a href="#">International Telecommunication Union, Telecommunication Standardization Sector</a> . <b>Note:</b> The acronym CCITT derives from the equivalent former French name, Comité consultatif international téléphonique et télégraphique.
<b>Internet Engineering Task Force</b>	IETF®	An international organization concerned with the function and development of the internet. IETF maintains a series of <a href="#">RFCs</a> . RFC 3935 describes IETF's purpose.

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

Term	Acronym	Definition
Internet Key Exchange	IKE (IKEv1, IKEv2)	<p>A protocol that negotiates <a href="#">authentication</a> methods, <a href="#">encryption</a> methods, and keys for <a href="#">IPsec</a>. IKE can also negotiate the length of time that a key is valid before a new key must be implemented.</p> <p><b>Note:</b> IKE version 1 (IKEv1) and IKE version 2 (IKEv2) use different processes for exchanges:</p> <ul style="list-style-type: none"> <li>In IKEv1 IPsec VPNs, the <a href="#">tunnel mode</a> varies during VPN transmission: <ul style="list-style-type: none"> <li>IKEv1 can use <a href="#">main mode</a> or <a href="#">aggressive mode</a> to set up the tunnel</li> <li>Then IKEv1 uses <a href="#">quick mode</a> for communication through the tunnel.</li> </ul> </li> <li>IKEv2 uses only one mode.</li> </ul>
Internet Protocol	IP	<p>A <a href="#">connectionless</a> protocol for transport and delivery of packets.</p> <p>IP is the principal protocol in the Internet Protocol suite.</p> <p><i>Also see <a href="#">TCP</a>, <a href="#">UDP</a>.</i></p>
IP Banking Router 10™ (chassis)	IBR-10™	<p>A router in the <a href="#">BANDIT™</a> family. The IBR-10 is dedicated to support of legacy protocols over IP networks.</p> <p><b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product.</p> <p><i>For more information, see the <a href="#">BANDIT Product Document Set</a>.</i></p>
IP Legacy Router 100™ (chassis)	ILR-100™	<p>A miniature, streamlined router in the <a href="#">BANDIT™</a> family. The ILR-100 supports <a href="#">IPsec VPNs</a> and supports legacy protocols over IP networks.</p> <p><b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product.</p> <p><i>For more information, see the <a href="#">BANDIT Product Document Set</a>.</i></p>
IPsec		<i>See <a href="#">IP Security Protocol</a>.</i>
IP Security Protocol	IPsec, IPSEC	<p>A protocol to protect IP transmissions (for example, in <a href="#">VPNs</a>). IPsec comprises two protocols that may be applied separately or together:</p> <ul style="list-style-type: none"> <li>Authentication Header (<a href="#">AH</a>)</li> <li>Encapsulating Security Protocol (<a href="#">ESP</a>)</li> </ul> <p><b>Note:</b> The <a href="#">Internet Key Exchange</a> (IKE) uses different processes for IPsec exchanges in IKE version 1 (IKEv1) and version 2 (IKEv2).</p> <p><i>Also see <a href="#">Internet Key Exchange</a>, <a href="#">virtual private network</a>, <a href="#">VPN tunneling</a>.</i></p>
ITU		<i>See <a href="#">International Telecommunication Union</a>.</i>



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

Term	Acronym	Definition
ITU-T		See <a href="#">International Telecommunication Union, Telecommunication Standardization Sector</a> .
key pair		An <a href="#">encryption</a> set used in <a href="#">asymmetric encryption</a> . The key pair comprises a <a href="#">private key</a> and its counterpart <a href="#">public key</a> . <b>Note:</b> Only the holder of the private key knows the complete key pair.
LAN		See <a href="#">local area network</a> .
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.
Long-Term Evolution	LTE	A standard specified by the <a href="#">3rd Generation Partnership Project</a> (3GPP) for mobile wireless communication.
LTE smartcard		See <a href="#">Subscriber Identity Module</a> .
main mode		A mode that can be used in phase 1 of an <a href="#">IKEv1 IPsec VPN</a> tunnel. (Phase 1 sets up the VPN tunnel.) Main mode hides the identities of the parties while negotiating the <a href="#">security association</a> . Main mode is more secure than <a href="#">aggressive mode</a> . <b>Note:</b> Phase 2 (bulk data transfer) of an IKEv1 IPsec VPN tunnel uses <a href="#">quick mode</a> . <i>Compare <a href="#">aggressive mode</a>, <a href="#">transport mode</a>. Also see <a href="#">tunnel mode</a>.</i>
MD5		See <a href="#">Message Digest 5</a> .
Message Digest 5	MD5	A <a href="#">hash function</a> that authenticates packet data by creating a 16-byte message digest. Used in <a href="#">AH</a> and <a href="#">ESP</a> .
multimode fiber		An <a href="#">optical fiber</a> that can carry more than one ray of light pulses. Multimode fiber is used for shorter distances than <a href="#">single-mode fiber</a> is. Multimode fiber also has more attenuation than single-mode fiber because the light rays reflect along the fiber core more often.
NAT		See <a href="#">network address translation</a> .
National Institute of Standards and Technology	NIST	A U.S. Agency that supports (but does not regulate) measurement, evaluation, and standards for technology. <i>Also see <a href="#">FIPS</a>.</i>

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

Term	Acronym	Definition
NAT traversal		See <a href="#">network address translation traversal</a> .
NERC		See <a href="#">North American Electric Reliability Corporation</a> .
network access device		A device that provides connection to a network. Compare <a href="#">gateway</a> .
network address translation	NAT	An <a href="#">address translation</a> 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: <ul style="list-style-type: none"> <li>• Use a single public IP address for several connections.</li> <li>• Use a greater number of internal IP addresses.</li> <li>• Hide internal IP addresses.</li> </ul> Also see <a href="#">port address translation</a> , <a href="#">Private Address Translation™</a> , <a href="#">NAT traversal</a> .
network address translation traversal	NAT traversal	A method of <a href="#">address translation traversal</a> 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 <a href="#">IPsec VPNs</a> or Voice over IP connections through networks that use <a href="#">firewalls</a> and NAT. <b>Note:</b> <a href="#">IKEv2</a> IPsec VPNs automatically include NAT traversal. <b>Note:</b> Also see <a href="#">Encore NAT Traversal™</a> .
NIST		See <a href="#">National Institute of Standards and Technology</a> .
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 <a href="#">critical infrastructure protection</a> . <b>Note:</b> The prior organization charged with responsibility for electric-power dependability was the North American Electric Reliability Council (also NERC).
offsite connection to office		See <a href="#">teleworking</a> .
OpenVPN®	OVPN	A <a href="#">virtual private network</a> based on <a href="#">certificate authority</a> . For information, see <a href="https://openvpn.net">https://openvpn.net</a> .

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

Term	Acronym	Definition
optical fiber		A solid glass or plastic fiber that carries light pulses for <a href="#">fiber optic networks</a> . 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 <a href="#">SFP</a> connector. Optical fiber is available in <a href="#">single-mode fiber</a> or <a href="#">multimode fiber</a> .
originating address		See <a href="#">source address</a> .
OVPN		See <a href="#">OpenVPN®</a> .
PAT		See <a href="#">port address translation</a> .
PCI		See <a href="#">Peripheral Component Interconnect</a> .
PEP		See <a href="#">performance enhancement proxy</a> .
perfect forward secrecy	PFS	Use of uniquely derived keys. PFS is part of <a href="#">IKE</a> . PFS comprises the following principles: <ul style="list-style-type: none"> <li>• Material used to derive one key cannot be used to derive additional keys.</li> <li>• A key cannot be used to derive another key.</li> <li>• Discovery of a key can endanger only transmissions protected by that key.</li> </ul>
performance enhancement proxy	PEP	A routine that satellite groundstations use to mitigate the delay in satellite networks. PEPs spoof <a href="#">TCP</a> 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.) <i>Also see <a href="#">Selective Layer Encryption™</a>.</i>
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. <b>Note:</b> Using 32 bits at 33 MHz, PCI has a throughput of 133 Mbytes/sec.
PFS		See <a href="#">perfect forward secrecy</a> .
PKC		See <a href="#">public-key cryptography</a> .

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

Term	Acronym	Definition
plain old telephone service	POTS	Analog telephone service that, in many areas, connects landline phones and other end-line customer devices to the <a href="#">public switched telephone system</a> (PSTN). Faxes, modems, and many other business devices still use POTS to transmit digital information. <b>Note:</b> 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 <a href="#">network address translation</a> . <b>Note:</b> NAT methods generally include PAT.
POTS		See <a href="#">plain old telephone service</a> .
PrAT™		See <a href="#">Private Address Translation™</a> .
pre-shared key		See <a href="#">secret key</a> . <b>Note:</b> A pre-shared key is not a generated <a href="#">shared secret</a> .
Private Address Translation™	PrAT™	A value-added <a href="#">address translation</a> routine from Encore Networks, Inc., for devices on private networks. Also see <a href="#">network address translation</a> .
private key		The key that the holder of a <a href="#">key pair</a> uses for <a href="#">encryption</a> and <a href="#">decryption</a> of communication with others. The private key is never shared. The private key’s counterpart is the <a href="#">public key</a> . Also see <a href="#">asymmetric encryption</a> .
psophometric weighting		A method of <a href="#">weighting</a> when measuring circuit noise. <b>Note:</b> ITU is studying recommendations for psophometric weighting in telecommunication.
PSTN		See <a href="#">public switched telephone system</a> .
public key		The key that, when communicating with the holder of a <a href="#">private key</a> , other entities use for <a href="#">encryption</a> and <a href="#">decryption</a> . The public key is freely available to anyone. The private key and its counterpart public key constitute the <a href="#">key pair</a> . Also see <a href="#">asymmetric encryption</a> .
public-key cryptography	PKC	See <a href="#">asymmetric encryption</a> .

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

Term	Acronym	Definition
public switched telephone system	PSTN	The global network of the world's public telephone networks. The PSTN's implementation of <a href="#">ITU-T</a> standards for connection and for telephone numbering makes it possible to call any telephone from anywhere in the world. <b>Note:</b> In many areas, end-line customer devices (for example, landline telephones) use <a href="#">plain old telephone service</a> (POTS) to connect to the PSTN. The terms "POTS" and "PSTN" are often used interchangeably, despite their references to different entities.
QOS, QoS		See <a href="#">quality of service</a> .
quality of service	QOS, QoS	Guarantee of a specific <a href="#">throughput</a> , achieved by configuring bandwidth, packet priority, and so forth. <i>Also see <a href="#">class of service</a>, <a href="#">Differentiated Services</a>, <a href="#">type of service</a>.</i>
quick mode		The mode used for communication in phase 2 of an IKEv1 <a href="#">IPsec VPN</a> tunnel. (Phase 2 is used for the communication payload—for example, data transfer.) <b>Note:</b> For phase 1 (setting up the VPN tunnel) of an IKEv1 <a href="#">IPsec VPN</a> tunnel, see <a href="#">main mode</a> or <a href="#">aggressive mode</a> . <i>Compare <a href="#">transport mode</a>. Also see <a href="#">tunnel mode</a>.</i>
rack unit (measurement)	U	A measure of vertical distance defined in <a href="#">EIA-310</a> . 1U is equal to 1.75 vertical inches or 4.445 vertical cm.
radiofrequency	RF	Any frequency in the radiowave spectrum used for radio communication.
RADIUS (authentication)		See <a href="#">Remote Authentication Dial-In User Service</a> .
RADIUS shared secret		A <a href="#">secret key</a> used in the <a href="#">Remote Authentication Dial-In User Service</a> . <b>Note:</b> The RADIUS shared secret is not a generated <a href="#">shared secret</a> used in a key-agreement protocol. <i>Compare <a href="#">shared secret (generated)</a>.</i>
RDU™		See <a href="#">Remote Data Unit™</a> .
re-keying		An <a href="#">IKE</a> 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. <i>Also see <a href="#">RADIUS shared secret</a>.</i>

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

Term	Acronym	Definition
remote connection to office		See <a href="#">teleworking</a> .
Remote Data Unit™ (peripheral device)	RDU™	A peripheral device for the <a href="#">VSR-1200™</a> and the <a href="#">BANDIT Plus™</a> , supplying twelve DB-25 serial ports. Compare <a href="#">Internal Data Unit™</a> .
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 <a href="#">IETF</a> , 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 <a href="#">radiofrequency</a> .
RFC		See <a href="#">Request for Comments</a> .
Rivest–Shamir–Adleman algorithm	RSA (algorithm)	A public-key algorithm for <a href="#">asymmetric encryption</a> , generally considered secure when sufficiently long keys are used. <b>Note:</b> A key of 512 bits is considered insecure; a key of 1024 bits is considered quite secure.
ROHS		See <a href="#">Restriction of Hazardous Substances</a> .
router		A device, generally a network <a href="#">gateway</a> , that determines the optimal path for each packet to reach its destination and sends the packet along that route.
RSA		See <a href="#">Rivest–Shamir–Adleman algorithm</a> .
SA		See <a href="#">security association</a> .
secret key		(Also called <a href="#">pre-shared key</a> or <a href="#">shared key</a> .) A key used in <a href="#">symmetric encryption</a> . The key can be pre-shared, requiring a trusted delivery mechanism, or can be sent via <a href="#">combined cryptography</a> . <b>Note:</b> A secret key is not a generated <a href="#">shared secret</a> .
secret-key cryptography		See <a href="#">symmetric encryption</a> .

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

Term	Acronym	Definition
secure hash algorithm	SHA	A routine that develops a 20-byte <a href="#">hash function</a> to authenticate data. SHA gives up speed in order to gain greater resistance to attack. Used in <a href="#">AH</a> and <a href="#">ESP</a> .
security association	SA	Information associated with setting up a specific secure connection. The security association comprises the following elements: <ul style="list-style-type: none"> <li>• The security protocol</li> <li>• The <a href="#">authentication</a> protocol</li> <li>• The <a href="#">encryption</a> protocol</li> </ul> <i>Also see <a href="#">security parameter index</a>.</i>
security parameter index	SPI	An index correlated against the <a href="#">destination address</a> to determine a specific <a href="#">security association</a> .
Selective Layer Encryption™	SLE™	A value-added technology (patent pending), developed by Encore Networks, Inc., that allows <a href="#">IPsec VPNs</a> to function more effectively over satellite networks that are <a href="#">PEP</a> -enabled.
SFP		<i>See <a href="#">small form-factor pluggable transceiver</a>.</i>
SHA		<i>See <a href="#">secure hash algorithm</a>.</i>
shared key		<i>See <a href="#">secret key</a>.</i> <b>Note:</b> A shared key is not a generated <a href="#">shared secret</a> .
shared secret, generated		A secret that the <a href="#">Diffie–Hellman exchange</a> algorithm develops from endpoints' <a href="#">public keys</a> and <a href="#">private keys</a> and that the endpoints use for part of the security in their communication. A shared secret is sometimes developed in <a href="#">VPN</a> connections. <b>Note:</b> A generated shared secret is not a <a href="#">shared key</a> . <i>Compare <a href="#">RADIUS shared secret</a>.</i>
shared secret, RADIUS		<i>See <a href="#">RADIUS shared secret</a>.</i>
SIM		<i>See <a href="#">Subscriber Identity Module</a>.</i>
single-mode fiber		An <a href="#">optical fiber</a> that carries a single ray of light pulses. Single-mode fiber is used for longer distances than <a href="#">multimode fiber</a> is. Single-mode fiber also has less attenuation than multimode fiber because the light rays reflect along the fiber core less often.

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

Term	Acronym	Definition
SLE™		See <a href="#">Selective Layer Encryption™</a> .
SMA		See <a href="#">sub-miniature coaxial connector, type A</a> .
small form-factor pluggable transceiver	SFP (transceiver)	A <a href="#">transceiver</a> for <a href="#">optical fiber</a> connections. <b>Note:</b> 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 or LTE)		See <a href="#">Subscriber Identity Module</a> .
source address		(Also called originating address.) The address of the device that initiates a transmission. <i>Compare <a href="#">destination address</a>.</i>
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). <b>Note:</b> The acronym CISPR is from the French name for the committee, Comité international spécial des perturbations radioélectriques.
SPI		See <a href="#">security parameter index</a> .
split tunneling		The ability to route <a href="#">VPN</a> traffic through VPN tunnels and to route non-VPN traffic outside these tunnels, on the same line. <b>Note:</b> Encore Networks' VPN products perform split tunneling automatically and dynamically.
stateful inspection		A <a href="#">firewall</a> 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 <a href="#">BANDIT™ products</a> , used to connect an antenna to the wireless module.
Subscriber Identity Module	SIM	(Also called a <a href="#">GSM</a> smartcard or an <a href="#">LTE</a> smartcard.) A removable card, specific to a region or country, used in a GSM smartphone or an LTE-capable smartphone to identify and authenticate a subscriber within that region or country.



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

Term	Acronym	Definition
symmetric encryption		(Also called secret-key encryption.) Use of a <a href="#">secret key</a> , shared by both sides of a connection, for <a href="#">encryption</a> and <a href="#">decryption</a> . (The same key is used both for encryption and for decryption.) A quick algorithm, such as <a href="#">DES</a> , 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 <a href="#">authentication</a> . <i>Compare <a href="#">asymmetric encryption</a>. Also see <a href="#">combined cryptography</a>.</i>
TCP		See <a href="#">Transmission Control Protocol</a> .
TDEA		See <a href="#">Triple Data Encryption Standard</a> .
TDES		See <a href="#">Triple Data Encryption Standard</a> .
TDM		See <a href="#">time-division multiplexing</a> .
TDMA		See <a href="#">time-division multiple access</a> .
Telecommunication Standardization Sector		See <a href="#">International Telecommunication Union, Telecommunication Standardization Sector</a> .
telecommuting		See <a href="#">teleworking</a> .
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 <a href="#">VPN</a> tunnel. Teleworking (also called telecommuting) saves time and provides convenience for business travelers, employees working at home, and other remote users.
TFTP		See <a href="#">Trivial File Transfer Protocol</a> .
Third Generation Partnership Project		See <a href="#">3rd Generation Partnership Project</a> .
throughput		The data transfer rate.
time-division multiple access, time-division multiplexing	TDMA, TDM	A wireless technology that divides a network's <a href="#">radiofrequency</a> band into <a href="#">timeslots</a> and allocates the timeslots to calls. This allows one radiofrequency band to support several simultaneous calls. <i>Compare <a href="#">code-division multiplexing</a>, <a href="#">wavelength-division multiplexing</a>.</i>

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

Term	Acronym	Definition
timeslot		One of several subchannels allocated to carry data in <a href="#">time-division multiplexing</a> .
TOS, ToS		See <a href="#">type of service</a> .
traffic analysis		Analysis of network traffic in order to infer information—for example, <a href="#">source address</a> , <a href="#">destination address</a> , frequency of transmission, or packet size.
transceiver		A combined transmitter and receiver. The term is used to specify a type of <a href="#">SFP</a> for <a href="#">optical fiber</a> connections.
Transmission Control Protocol	TCP	A protocol layer used in the <a href="#">Internet Protocol</a> suite. TCP checks for packet receipt and packet order. <i>Compare <a href="#">User Datagram Protocol</a>.</i>
transport mode		A mode in which the endpoints of an <a href="#">IPsec VPN</a> connection perform their own <a href="#">encryption</a> . The VPN <a href="#">gateway</a> functions solely as the transport, <a href="#">encapsulate</a> (thus protecting) the upper layer payload and reusing the IP header. <i>Compare <a href="#">main mode</a>, <a href="#">aggressive mode</a>, <a href="#">quick mode</a>. Also see <a href="#">tunnel mode</a>.</i>
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. <b>Note:</b> <a href="#">GPS</a> does not use triangulation; <a href="#">GPS</a> uses <a href="#">trilateration</a> . However, when <a href="#">GPS</a> signals are weak, triangulation might be useful instead of trilateration to determine position. For details and examples of triangulation, see the non- <a href="#">GPS</a> navigation literature. <i>Compare <a href="#">trilateration</a>.</i>

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

Term	Acronym	Definition
<b>trilateration</b>		<p>A method of calculating position, in Cartesian coordinates <math>x</math>, <math>y</math>, and <math>z</math>, 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 <math>t</math>).</p> <p>Trilateration works with three reference points (for example, satellites). In <b>GPS</b>, 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.)</p> <p>Data from four satellites allow simultaneous solution for four variables (time <math>t</math> and coordinates <math>x</math>, <math>y</math>, and <math>z</math>) in four linear equations. If the value of one variable is already known (for example, at sea level, altitude <math>z</math> is zero), data are sufficient from three satellites.</p> <p><b>Note:</b> For details and examples of trilateration, see the <b>GPS</b> navigation literature.</p> <p>Compare <a href="#">triangulation</a>.</p>
<b>Triple Data Encryption Algorithm</b>	TDEA	See <a href="#">Triple Data Encryption Standard</a> .
<b>Triple Data Encryption Standard</b>	3DES TDES	<p>An <a href="#">encryption</a> method incorporating three iterations of <b>DES</b>, each with a different key, for added security:</p> <ul style="list-style-type: none"> <li>• Encryption</li> <li>• Decryption</li> <li>• Another encryption</li> </ul> <p>Some versions of 3DES use two DES keys (112 bits) in each iteration. Some versions use three DES keys (168 bits) in each iteration.</p>
<b>Trivial File Transfer Protocol</b>	TFTP	A simple protocol for transferring files. TFTP is based on <a href="#">UDP</a> .
<b>tunneling</b>		<p>Use of <a href="#">encapsulation</a> to send one protocol through a network that uses a different protocol.</p> <p>Also see <a href="#">tunnel mode</a>, <a href="#">VPN tunneling</a>.</p>
<b>tunnel mode</b>		<p>In <b>IKEv1</b>, the type of <a href="#">tunneling</a> used in a transmission. For example, an IKEv1 <b>IPsec VPN</b> might use <a href="#">main mode</a> or <a href="#">aggressive mode</a>, then <a href="#">quick mode</a>; or it might use only <a href="#">transport mode</a>.</p> <p>Also see <a href="#">tunneling</a>, <a href="#">VPN tunneling</a>.</p>
<b>type of service</b>	TOS, ToS	<p>Use of bits in a packet's IP header to indicate specific priority and service type for the packet.</p> <p>Contrast with <a href="#">class of service</a>. Also see <a href="#">Differentiated Services</a>, <a href="#">quality of service</a>.</p>

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

Term	Acronym	Definition
U (a unit of measure)		See <a href="#">rack unit</a> .
UDP		See <a href="#">User Datagram Protocol</a> .
User Datagram Protocol	UDP	A protocol layer used in the <a href="#">Internet Protocol</a> suite. UDP does not check for packet order or packet receipt. <b>Note:</b> <a href="#">TFTP</a> is based on UDP. Compare <a href="#">Transmission Control Protocol</a> .
VBRS™		See <a href="#">Virtual Broadband Redundancy System™</a> .
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 (from Encore Networks, Inc.) providing host-to-host physical and logical redundancy for continuous management of the <a href="#">Remote Data Unit™</a> . VBRS™ is used only in the <a href="#">VSR-1200™</a> and the <a href="#">BANDIT Plus™</a> . <b>Note:</b> VBRS™ and <a href="#">VRRP</a> are sometimes confounded but are unrelated. Both processes provide redundancy, but in different ways.
Virtual LAN		See <a href="#">virtual local area network</a> .
virtual local area network	VLAN	A group of devices within a <a href="#">LAN</a> (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. <b>Note:</b> VLANs are described in IEEE standards 802.1q and 802.1p. Also see <a href="#">VLAN broadcast</a> .
virtual private network	VPN	Use of <a href="#">encryption</a> , <a href="#">authentication</a> , and <a href="#">tunneling</a> across a public network to ensure secure communication between private endpoints. A VPN can implement one or more technologies—for example, <a href="#">IPsec</a> —to accomplish secure private communication. <b>Note:</b> There are several <a href="#">IETF RFCs</a> that address VPNs. All routers from Encore Networks, Inc., can use <a href="#">IPsec</a> VPNs. The <a href="#">EN-1000™</a> and the <a href="#">EN-2000™</a> can also use <a href="#">OpenVPN®</a> . Also see <a href="#">VPN tunneling</a> .

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

Term	Acronym	Definition
Virtual Private Network Consortium	VPN Consortium, VPNC	A former trade association for manufacturers and vendors of IPsec VPN products. The VPN Consortium tested products for VPN compliance and interoperability. The VPNC supported development of standards for VPNs, but the VPNC itself did not develop standards. <b>Note:</b> The VPN consortium has discontinued operation.
Virtual Router Redundancy Protocol	VRRP	A protocol for providing continuous router support to a network. VRRP and VBRSTM are sometimes confounded but are unrelated. Both processes provide redundancy, but in different ways.
VLAN		See <i>virtual local area network</i> .
VLAN broadcast		A broadcast directed to a specified VLAN. <b>Note:</b> VLAN broadcasts reduce the amount of traffic sent to the entire LAN.
VPN		See <i>virtual private network</i> .
VPNC		See <i>Virtual Private Network Consortium</i> .
VPN Consortium		See <i>Virtual Private Network Consortium</i> .
VPN Satellite Router™ products	VSR™ products	A group of routers (in the BANDIT™ family) 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. <b>Note:</b> VPN tunneling includes the ability, if desired, to encrypt the source address, destination address, and data in order to provide protection for encapsulated packets. <i>Also see tunnel mode, IP Security Protocol.</i>
VRRP		See <i>Virtual Router Redundancy Protocol</i> .
VSAT		See <i>very-small-aperture terminal</i> .
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. <b>Note:</b> This chassis is no longer manufactured. Support is available from Encore Networks, Inc., for customers using this product. <i>For more information, see the BANDIT Product Document Set.</i>

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

Term	Acronym	Definition
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 <i>VPN Satellite Router™ products</i> .
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.  <i>Compare code-division multiplexing, time-division multiplexing.</i>
WDM		See <i>wavelength-division multiplexing</i> .
WDMA		See <i>wavelength-division multiple access</i> .
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.  <i>Also see psophometric weighting.</i>
wifi		See <i>802.11 wireless</i> .
wireless fidelity	wifi	See <i>802.11 wireless</i> .
working off site		See <i>teleworking</i> .