Vocabulary Terms

	Expanded Term	Definition	Notes
802.1X		part of the IEEE 802.1 group of networking protocols; provides an authentication mechanism to devices wishing to connect to a LAN or WLAN	
AAA	authentication, authorization, accounting	an architectural framework for configuring a set of three independent security functions (authentication, authorization, and accounting) in a consistent manner.	
AAA session		Period of time a user is connected to the router/network through AAA	
accounting		keeps a record of a user's actions	
ACL	access control list	provides basic traffic filtering capabilities; list of permit/deny statements	
address mapping		Translation of private IPs to public IPs using a NAT table	
ADSM		GUI tool for configuring ASA over HTTP	
ARP	address resolution protocol	used to map IP network addresses to hardware addresses	
AS	autonomous system	a collection of networks within a single company (such as an intranet)	
ASA	adaptive security appliance	special type of router used solely as a firewall	
asynchronous		process continues while awaiting a response	
authentication		verifies a user's identity, usually with a username and password	
authorization		restricts a user's access to certain services	
auxiliary port		connector on a router to allow for a remote terminal connection through a modem	
binary		base 2 number system of 0s and 1s	
bridge		joins 2+ networks	
broadcast		message sent from one device to all to all listening devices	
broadcast domain		group of devices that can receive a broadcast from one another; usually all connected by layer 2 switches in one subnet or all the devices in a VLAN	
CDP	cisco discovery protocol	used to share information about other directly connected devices, such as the OS version and IP	
CIDR notation	classless inter-domain routing	shorter way to write a subnet mask; number refers to number of 1 bits in a subnet mask	ex. /24
Cisco ASA device	adaptive security appliance	security device that combines firewall, antivirus, intrusion prevention, and VPN capabilities	
Cisco secure ACS	access control server	supports AAA and allows for restricted access for users	
client		device requesting information from a server	

Vocabulary Terms

	Expanded Term	Definition	Notes
console cable		also known as a rollover cable; used to connect an end device to a network device for configuration	
console port		connector on a router to allow for a remote terminal connection through an end device	
converged network		modern network that supports multiple functions (phone, web, video)	
copper cross-over		used to interconnect similar devices (ex. router to router)	
copper straight-through		most common type of networking cable; commonly used to connect a host to a switch and a switch to a router	
crypto map		selects data flows that need security processing and defines the policy for these flows and the crypto peer that traffic needs to go to	
default gateway/router		IP address of the node of the router connected to the switch; packets with destination addresses outside the subnet are sent here	aka gateway of last resort; default router is used to refer to the default gateway when given out by DHCP
default route		route taken when more specific info is not provided	
DH	Diffie-Hellman algorithm	basis of most modern automatic key exchange methods and is one of the most common protocols used in networking today	
DHCP	dynamic host configuration protocol	dynamic protocol used to determine IP addresses, subnet masks, and DNS server addresses	
DHCP pool		group of IP addresses to be assigned dynamically	
Directly Connected Static Route		A static route which is specified by the next hop IP address	Contrast Recursive/Fully specified static route
distance-vector		Protocol used to advertise distance and direction of routes	
DMZ	demilitarized zone	portion of a network not contained in a firewall	
DNS	domain name system	translates host names into IP addresses	
dotted-decimal notation		an address written in 4 octets in decimal form	
DTP	dynamic trunking protocol	allows for dynamic assignment of port modes for trunking during initial configuration	
dynamic IP address		an IP address automatically managed by a server	
edge router		router between the internal and external network	
EGP	Exterior Gateway Protocol	a routing protocol which is used to route between different autonomous systems	See autonomous system, compare IGP

Vocabulary Terms

	Expanded Term	Definition	Notes
EIGRP	enhanced interior gateway routing protocol	combines advantages of OSPF and RIP routing	
enable mode		allows usage of commands to manage a device	
encapsulation		used to place data from a higher-level protocol into the next-lower-layer protocol	
end device		a component that is an initial sender or final receiver of data	ex. laptop, server, mobile phone
established connection		two-way connection	TCP only; refers to preexisting connections
GRE	generic routing encapsulation	tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network	
hash		one way function that takes an input message of arbitrary length and produces a fixed-length digest for use in cryptography	
host portion		bits of the IP address that identify individual nodes	
hub		LAN device that provides a centralized connection point for LAN cabling	
ICMP	internet control message protocol	reports errors and provides other info about IP packet processing	
IEEE	institute of electrical and electronics engineers	sets many industry standards for networking	
IGP	Interior Gateway Protocol	a routing protocol which is used to route within a single autonomous system	See autonomous system, compare EGP
IKE	internet key exchange	protocol used to set up a security association in the IPsec protocol suite	
inside/local		interfaces/addresses that are part of the LAN	
interface		a physical port on a device	
IOS Firewall		software that provides an extensive set of security features, allowing for configuration of a simple or elaborate firewall	
IOS image		Cisco’s operating system for most devices	
IP address		a unique string of numbers separated by periods that identify each device	
IPsec	internet protocol security	protocol suite for secure IP communications by authenticating and encrypting each IP packet of a communication session	
IPv4	internet protocol version 4	uses 32-bit addresses; 4.3B possible addresses	
IPv6	internet protocol version 6	uses 128-bit addresses; 3.4 x 10^38 possible addresses	
IPv6 prefix		IPv6 equivalent of a subnet address	

Vocabulary Terms

	Expanded Term	Definition	Notes
ISAKMP	internet security association and key management protocol	establishes security associations and cryptographic keys over the internet	
key		password used in cryptography	
label		tag applied to VPN packets for faster routing	
LAN	local area network	group of devices in an enclosed network	based on physical connections
lease time		amount of time before a dynamically allocated IP expires and must be reassigned	
leased-line		private connection only used for one company's traffic; leased by an ISP	
legacy equipment		devices no longer in production but still in use	
license		software purchased from Cisco to expand an ASA's capacities	
line		point of access for console, auxiliary, SSH, or telnet connections	
link-local		network address that is valid only for communications within the network segment or broadcast domain	
link-state		routing protocol which creates a map of the network used to determine routing tables	
local database		set of users and their info stored on the network device	
MAC address	media access control	layer 2 built-in address that is unique to every device	
management VLAN		used for management data as opposed to user data	default is vlan 1
metric		quantitative value used to measure the distance to a given network	
mode		a level of a access for config/assessment purposes	
multicast		a message sent from one device to a group of devices	
NAT	network address translation	translates local addresses to global addresses to reduce the need for globally unique IP addresses	
native VLAN		VLAN containing the trunk port on a switch	
network address		first address in an IPv4 subnet; used to identify the network	
network device		a component used to connect other devices together	
network object		named set of IPs that can be used in other ASA commands	
network portion		bits of the IP address that identify the subnet	
next hop		the next IP address a packet should be sent to	

Vocabulary Terms

	Expanded Term	Definition	Notes
NIC	network interface card	the component of a computer that allows it to connect to a network	
NTP	network time protocol	synchronizes device time over a network	
object group		named set of objects that can be used in other ASA commands	
octet		a group of 8 binary digits	
octet boundary		subnet created using a /8, /16, or /24 subnet mask	
operator		a keyword used to limit arguments	eq = neq ≠ lt < gt > range
optic fiber		durable cable used for high-speed connections	
OSPF area		a network segment that shares OSPF routing information	
OSPFv2	open shortest path first version 2	uses a link-state database to calculate routing information for IPv4	
OSPFv3	open shortest path first version 3	uses a link-state database to calculate routing information for IPv6	
outside/global		interfaces/addresses that are part of the general Internet	
packet		group of bytes that includes the network layer header and encapsulated data	
packet state		describes if traffic is part of an existing connection or not	
partition		virtual “device” created by virtually separating a device	
passphrase		the use of a space in a password to create a pharse made of many words	used to make strong passwords
passive interface		interface that does not transmit routing information	
PAT	port address translation	allows for one or more global IP addresses to be mapped to multiple private IP addresses using port numbers	
payload		data sent over a VPN	
PFS	perfect forward secrecy	property of secure communication protocols in which compromise of long-term keys does not compromise past sessions	
ping		an ICMP echo message and its reply; used to test reachability in a network	
port number		identifies the application that is sending/receiving data	
PPP	point-to-point protocol	data link protocol used to establish a direct connection between two nodes	
PPPoE	point-to-point protocol over ethernet	specification for connecting multiple computer users on an Ethernet local area network to a remote site	

Vocabulary Terms

	Expanded Term	Definition	Notes
prefix length		the number of 1s in the binary form of the subnet mask	slash/CIDR notation
private address		IP address that can only be used within an internal network	
protocol		standard method of transmitting and processing various kinds of information	ex. tcp, udp, ip, http
public address		IP address that can be used globally	
quiet mode		disables telnet/ssh connections based on an ACL for a period of time after too many unsuccessful logins	
RADIUS	remote authentication dial-in user services	used in AAA as a remote user login database; encrypts user passwords; open standards allow for greater compatibility	UDP based; uses ports 1645-1646 or 1812-1813
Recursive Static Rotue		A static route which is specified by the next hop IP address	Contrast Directly Connected/Fully specified staic route
Relay agent		allows IP addresses to be dynamically allocated throughout multiple broadcast domains	
RIP	routing information protocol	uses distance vector logic and router hop count to calculate routing information for IPv4	
RIPng	routing information protocol new generation	uses distance vector logic and router hop count to calculate routing information for IPv6	
root		user mode with full privileges	
route summarization		consolidates routing commands	
router		a device that determines the next network point a packet should be forwarded to	
router-on-a-stick		a network topology in which a router has a single physical interface that is part of multiple VLANs for use in trunking	
routing table		list of routing information, including destinations and next hops	
SA	security association	establishment of shared security policies between two network devices to support secure communication	
serial connection		used to transfer information between two devices using a serial communication protocol	
server		device sending information to a client	
service object		named set of services that can be used in other ASA commands	
SLAAC	stateless address autoconfiguration	allows for generation of a unique IPv6 address without a DHCP server	
SSH	secure shell	supports encrypted terminal emulation between a client and a server	

Vocabulary Terms

	Expanded Term	Definition	Notes
SSL	secure socket layer	security technology for establishing an encrypted link between a server and client	
stateful		describes a centralized configuration	
stateless		describes a decentralized configuration	
statement		a line of an ACL	
static IP address		an IP address manually managed by an administrator or users	
string		text input/output	
subinterface		one of multiple virtual interfaces on a single physical interface	
subnet		subdivision of a network	
subnet mask		a binary string that describes the format of an IP address in terms of network bits and host bits; determines which subnet a host belongs to	written in dotted-decimal or CIDR format
superview		large view made up of smaller views	
SVI	switch virtual interface	a layer 2 physical port encapsulated by a VLAN into a layer 3 interface	
switch		layer 2 device used to connect end devices to routers	
symmetric crypto ACL		an ACL used to determine which traffic to send through a VPN; another ACL with the source and destination reversed is placed at the other end of the VPN tunnel	
synchronous		process pauses while awaiting a response	
TACACS+	terminal access control access control server plus	used in AAA as a remote user login database; encrypts all user protocols; limited accounting	uses TCP port 49
TCP	transmission control protocol	transport layer protocol that provides reliable data transmission	
telnet		used for remote, unencrypted terminal connection	
transform		protocol/algorithm specified on a gateway to secure data	
trap		automated informational SNMP message	
trunking		link between two network devices that carries multiple VLANs	
tunnel		established VPN	
UDP	user datagram protocol	simple protocol that exchanges datagrams without guaranteed delivery	

Vocabulary Terms

	Expanded Term	Definition	Notes
unicast		communication between two individual devices	
view		set of commands available to a user	
VLAN	virtual local area network	group of devices in a single broadcast domain	based on logical connections; overrides a LAN's broadcast domain
VLSM	variable length subnet mask	dividing a network into subnets of different sizes in order to conserve address space	
VoIP VLAN		A VLAN with special low-latency configurations to support VoIP	
VPN	virtual private network	allows for an encrypted, uninterrupted connection	
VTP	VLAN trunking protocol	distributes VLAN info to all switches on a domain	
WAN	wide area network	large network of devices overseen by a service provider	
wildcard mask		format opposite of a subnet mask; used in ACL, OSPF, and EIGRP commands	
WINS	windows internet name service	a name translation service for NetBIOS computer names	