

Section 9

Cable and DSL Technologies

Cable and DSL technologies have changed the remote access world dramatically. Without them, remote and Internet access would be limited to the 56 kbps typical of dialup. In order to bring high-speed Internet access to as many users as possible as quickly as possible, technologies had to be developed to leverage existing infrastructure. Broadband cable and DSL are those technologies. Broadband cable uses the RF modulation techniques of cable television. DSL provides high-speed Internet and remote access over existing telephone service. DSL uses either Carrierless Amplitude Phase (CAP) or Discrete Multi-Tone (DMT) to transmit data without interfering with voice communications.

The flashcards in this chapter test and expand your knowledge of these technologies. Recently added to the BCRAN exam, this knowledge is critical to your successful completion of the CCNP certification.

Question 1

What does the abbreviation DOCSIS stand for?

Question 2

What is the current version of the DOCSIS standard?

Question 1 Answer

The abbreviation DOCSIS stands for Data Over Cable Service Interface Specification. DOCSIS is the standardized method of transmitting and receiving data over a cable television network.

Question 2 Answer

DOCSIS is presently at version 2.0. Previous versions of DOCSIS include 1.1, which is very widely deployed, and 1.0.

Question 3

What are the two primary hardware components of a broadband cable deployment?

Question 4

What type of information is included in a DOCSIS-compliant cable modem configuration file?

Question 3 Answer

A Cable Modem Termination System (CMTS) is installed at the cable head end and is used to service many cable modems installed at customer locations.

Question 4 Answer

The following types of information are included in a DOCSIS cable modem configuration file:

- Radio frequency configuration
- Class of service information
- Management information
- Vendor-specific information

Question 5

What protocol does a cable modem use to download its configuration and system image?

Question 6

What are the two modes in which a cable modem can operate?

Question 5 Answer

Cable modems use TFTP to download their configurations. Software downloads also utilize TFTP.

Question 6 Answer

Cable modems can be configured in either a bridging or routing mode. In bridging mode, Layer 2 frames are simply bridged from a cable modem's Ethernet interface to its cable interface. In routing mode, IP packets are routed by the cable modem.

Question 7

In which cable modem operational mode might NAT be used?

Question 8

In a broadband cable network bandwidth is dedicated to individual users. True or false?

Question 7 Answer

Because Layer 3 handling of packets only takes place when the CPE is routing, NAT only makes sense in that type of configuration.

Question 8 Answer

False. Because cable networks were built around a shared infrastructure, data bandwidth is shared among several users.

Question 9

Why are PPP over Ethernet and PPP over ATM typically deployed?

Question 10

What type of WAN connection is used at the central site to support DSL connectivity?

Question 9 Answer

PPP over Ethernet and PPP over ATM provide three major benefits: user authentication, service selection, and address management.

Question 10 Answer

Although implementations may vary, remote DSL users are typically provided central site connectivity over an ATM PVC terminated on a customer owned router.

Question 11

Which of the following is not a type of DSL?

- Asymmetric
- Symmetric
- Variable

Question 12

DSL is not limited by distance. True or false?

Question 11 Answer

Variable is not a type of DSL. Asymmetric refers to DSL variants in which the upstream speed is different than the downstream speed. Symmetric refers to DSL variants where the upstream and downstream speeds are identical.

Question 12 Answer

False. In order for DSL to operate correctly, the total length of the local loop must typically be less than 15,000 feet.

Question 13

DSL technologies fall into two broad categories. What are they?

Question 14

In a DSL implementation, what piece of equipment terminates the copper connection from the CPE?

Question 13 Answer

The two categories of DSL variants are symmetric and asymmetric. In symmetric DSL, the upstream and downstream data rates are identical. With asymmetric DSL, the downstream data rate is higher than the upstream rate.

Question 14 Answer

Within the phone company central office, a DSL Access Multiplexer (DSLAM) is used to terminate many customer connections. The DSLAM performs aggregation to one or two ATM backbone connections.

Question 15

What two pieces of equipment terminate each end of a DSL connection?

Question 16

What are two modulation methods used with ADSL?

Question 15 Answer

CPE is used to terminate DSL connection in the customer's residence or business. The DSL provider uses a DSL Access Multiplexer to terminate many customer connections.

Question 16 Answer

The two modulation methods typical in ADSL deployments are Carrierless Amplitude Phase (CAP) and Discrete Multi-Tone (DMT). CAP is not an industry standard, while DMT is. Although widely deployed, CAP is not typically used in new DSL deployments.

Question 17**How large is an ATM cell?**

- 37 bytes
- 53 bytes
- 69 bytes
- 101 bytes

Question 18**What does RFC 1483 detail?**

Question 17 Answer

An ATM cell is 53 bytes in length. 48 of the 53 bytes are used for cell payload with the remaining 5 bytes serving as a cell header.

Question 18 Answer

RFC 1483 discusses how to transport connectionless LAN data across an ATM network. This RFC offers two types of connections: bridged and routed.

Question 19

When configuring an ATM interface, the VCI must be in what range?

Question 20

What interface configuration command links a PVC to an ATM interface?

Question 19 Answer

Valid VCI values include 0 through 65535. However, values 0 through 31 have been reserved. Therefore, any configured VCI must be between 32 and 65535.

Question 20 Answer

The interface configuration command `pvc` links a PVC to an ATM interface or subinterface. The complete syntax for the `pvc` command is `pvc [number] vpi vci`.

Question 21

What encapsulation type should be used on an ADSL ATM connection?

Question 22

What command configures the largest frame that can be sent or received on an interface?

Question 21 Answer

AAL5SNAP encapsulation is used on asymmetric DSL ATM PVCs.

Question 22 Answer

The interface configuration command `ip mtu mtu` is used to configure the largest packet that can be sent or received on an interface.

Question 23

What type of authentication server is used with PPP over Ethernet or PPP over ATM?

Question 24

What authentication protocols are used to authenticate PPP over Ethernet or PPP over ATM users?

Question 23 Answer

A RADIUS server is used by the DSL service provider to authenticate PPP over Ethernet and PPP over ATM users.

Question 24 Answer

PPP over Ethernet and PPP over ATM can use either PAP or CHAP to authenticate users. CHAP provides an additional level of security as passwords are never sent over the network.

Question 25

Why must an Ethernet interface using PPP over Ethernet have an MTU less than or equal to 1492 bytes?

Question 26

Which ETHER_TYPE values represent PPP over Ethernet?

Question 25 Answer

PPP over Ethernet (PPPoE) adds a total of 8 bytes to an Ethernet frame; the PPPoE header is 6 bytes and the PPP protocol ID field is 2 bytes. These 8 bytes must be included in every frame and reduce the effective MTU from 1500 bytes to 1492 bytes.

Question 26 Answer

PPP over Ethernet (PPPoE) uses two ETHER_TYPE fields. A value of 0x8863 represents the PPPoE Discovery phase while 0x8864 represents the PPPoE Session phase.

Question 27

What mechanism is used to transmit data over a broadband cable network?

Question 28

When configuring an ATM connection, the VPI must fall in what range?

Question 27 Answer

Broadband cable networks use an RF transmission scheme identical to that used to transmit television programming. Downstream transmissions use the 55 MHz to 750 MHz band while upstream transmissions use the 5 MHz to 42 MHz band.

Question 28 Answer

Valid VPI values range from 0 to 255.

Question 29

Which RFC documents PPP over ATM encapsulation?

Question 30

Which RFC documents PPP over Ethernet encapsulation?

Question 29 Answer

RFC 2364, “PPP over AAL5,” describes PPP over ATM.

Question 30 Answer

RFC 2516, “A Method for Transmitting PPP over Ethernet (PPPoE),” describes the operation of PPP over Ethernet.

Question 31

What are the frequency bands used by a cable modem and CMTS to communicate?

Question 32

Which of the following is not a valid PPP over Ethernet packet?

- PADI
- PADV
- PADR
- PADS

Question 31 Answer

Downstream (to CPE) uses the 55 MHz to 750 MHz band, while upstream (to CMTS) uses the 5 MHz to 42 MHz band.

Question 32 Answer

PADV is not a valid PPP over Ethernet (PPPoE) packet. There are five valid PPPoE packets: the PPPoE Active Discovery Initiation (PADI), the PPPoE Active Discovery Offer (PADO), the PPPoE Active Discovery Request (PADR), the PPPoE Active Discovery Session confirmation (PADS), and the PPPoE Active Discovery Terminate (PADT) packet.

Question 33

What are the valid PPP over Ethernet session discovery and initiation packets and in what order are they sent and received during session establishment?

Question 34

Why use PPP over ATM instead of PPP over Ethernet?

Question 33 Answer

The four PPP over Ethernet (PPPoE) session discovery and initiation packets are

PPPoE Active Discovery Initiation (PADI)

PPPoE Active Discovery Offer (PADO)

PPPoE Active Discovery Request (PADR)

PPPoE Active Discovery Session (PADS) confirmation

Question 34 Answer

PPP over ATM is used when the CPE is configured for a routed DSL connection. PPP over Ethernet requires that the customer client computer have Layer 2 connectivity with the service provider's PPP access concentrator.

Question 35

What CPE functionality is required to support PPP over Ethernet?

Question 36

What asymmetric DSL modulation technique, Carrierless Amplitude Phase (CAP) or Discrete Multi-Tone (DMT), is an industry standard?

Question 35 Answer

Since the customer computer must have Layer 2 connectivity to the service provider access concentrator, the CPE must be configured for RFC 1483 bridging.

Question 36 Answer

Although CAP was once dominant, DMT is an industry standard and is, therefore, the preferred modulation technique for new asymmetric DSL installations.

Question 37

How can cable modem software images be standardized by a broadband cable service provider?

Cable and DSL
Technologies

Question 38

Does PPP over Ethernet or PPP over ATM require that software be installed on the client computer?

Cable and DSL
Technologies

Question 37 Answer

A DOCSIS-compliant cable modem downloads its configuration file during power-on. Within the configuration file it is possible to specify that a software image should be downloaded on power-on and where that image should come from.

Question 38 Answer

PPP over Ethernet (PPPoE) requires that client software or native PPPoE support be present on the client computer. Since PPP over ATM terminates on the CPE and not the client computer, no client computer support is required.

Question 39

In which PPP over Ethernet session initiation and discovery packet is the Session ID transmitted?

Cable and DSL
Technologies**Question 40**

What series of commands enables an IOS router to serve as a PPP over ATM client?

Cable and DSL
Technologies

Question 39 Answer

The PPP over Ethernet (PPPoE) Session ID is transmitted in the PPPoE Active Discovery Session (PADS) confirmation packet. This is the last packet used during PPPoE session establishment.

Question 40 Answer

The commands below enable the PPP over ATM client functionality on a Cisco router.

vpdn-group *group_name*

request-dialin

protocol pppoe

Interface configuration must take place in addition to these commands.

Question 41

An Ethernet interface using PPP over Ethernet can have an MTU no larger than what?

Question 41 Answer

The largest MTU that can be supported with PPP over Ethernet (PPPoE) is 1492 bytes. This is reduced from the standard Ethernet MTU by 8 bytes due to the addition of the 6-byte PPPoE header and the 2 byte PPP protocol ID field.

Section 10

Understanding Virtual Private Networks

Virtual private networks (VPNs) are an excellent mechanism to secure IP communications. VPNs fall into two categories: remote-access VPNs and site-to-site VPNs. Remote-access VPNs provide remote users secure access to information on a corporate or central network. To the benefit of the central site administrators, remote-access VPNs provide extensive options for remote-user authentication. Site-to-site VPNs are used to link sites across a less secure network, typically the Internet. These secure connections can also provide a significant cost savings by obviating the need for a traditional WAN. Regardless of the type of VPN, there are several common protocols that make up any IPsec VPN. Knowledge of these protocols is critical to becoming a successful CCNP.

The flashcards in this chapter challenge and expand your understanding of both types of IPsec VPNs. They cover not only the mechanisms used by the protocols but also their configuration.

Question 1

What is IKE?

Question 2

How many phases take place during a successful IKE negotiation?

Question 1 Answer

The Internet Key Exchange (IKE) protocol is used to negotiate, create, and exchange information needed to establish an IPSec connection. This negotiated information is called a security association (SA).

Question 2 Answer

There are two phases to an IKE negotiation. The first phase has two modes: aggressive mode and main mode. The second phase has a single mode named quick mode.

Question 3

How are main mode and aggressive mode different?

Question 4

How can you authenticate remote devices in a site-to-site VPN scenario?

Question 3 Answer

A successful main mode negotiation is made up of exactly six messages. First the keying material is negotiated. This keying material is used to encrypt the remaining messages.

Aggressive mode is less secure because the keying material and options are negotiated simultaneously using only three messages.

Question 4 Answer

There are the three options for site-to-site VPN authentication:

- Preshared keys
- RSA encrypted nonces
- RSA signatures

Question 5

Is it necessary that the ISAKMP policy and IPSec transform be configured to use the same encryption algorithm?

Question 6

What is the difference between tunnel mode and transport mode IPSec?

Question 5 Answer

No, it is possible to use one encryption algorithm for IKE and another for IPSec.

Question 6 Answer

In tunnel mode IPSec, the Cisco default, the entire original IP packet is encapsulated in a new IP packet. All routing takes place based on information in the outer most IP header—in essence hiding the internal IP addresses.

In transport mode IPSec, a new ESP header is placed between the existing Layer 3 and Layer 4 headers. The source and destination IP address of the original packet are used for routing the encrypted packet.

Question 7

Can AH and ESP be used at the same time?

Question 8

When AH and ESP are used together, what is the numeric value present in the protocol field of the IP packet?

Question 7 Answer

Yes. When AH and ESP are used together, the AH header is the outer most Layer 4 header. This is important to consider when designing access control lists that affect IPSec traffic.

Question 8 Answer

Since AH is the first Layer 4 header, its protocol value is in the Layer 3 IP header. The protocol value for AH is 51.

Question 9

Is it necessary that both ends of a site-to-site VPN have static IP addresses?

Question 10

How can a site-to-site VPN be established when one site acquires its IP address dynamically?

Question 9 Answer

No, a dynamic crypto map can be used when the remote peer has a dynamic IP address. Only one end of a site-to-site VPN configuration may use a dynamic crypto map.

Question 10 Answer

Dynamic crypto maps can be used when a single end of a site-to-site VPN uses a dynamic IP address. The dynamic crypto map must be configured on the IPSec peer with a static IP address.

Question 11

What command assigns a single ISAKMP key to all IPsec peers?

Question 12

What configuration commands create and apply crypto transform sets?

Question 11 Answer

To create a wildcard ISAKMP key, use the global configuration command **crypto isakmp key *key* address 0.0.0.0**.

Question 12 Answer

IPSec transform sets are created with the global configuration command **crypto ipsec transform-set** and are applied to crypto maps via the **set transform-set** command.

Question 13

What encryption algorithms are available for use with IPSec?

Question 14

What IP protocol values represent AH, ESP, and GRE?

Question 13 Answer

You can use one of the following encryption algorithms with IPSec:

- DES (56 bit)
- 3DES (168 bit)
- AES (128 or 256 bit)

Question 14 Answer

The IP protocol values for these protocols are

- AH: 51
- ESP: 50
- GRE: 47

Question 15

What command enables transport mode IPSec?

Question 16

Can multiple crypto maps be applied to a single router interface?

Question 15 Answer

Transport mode IPsec is enabled by issuing the **mode transport** command in transform-set configuration mode. The following is an example of a transform set configured for transport mode:

```
crypto ipsec transform-set TRANSFORM esp-des esp-sha-hmac
mode transport
```

Question 16 Answer

No. However, it is possible to have multiple instances of the same crypto map. Similar to the configuration of route maps, each crypto map instance is given a unique numeric tag. When encrypting traffic, crypto map instances are evaluated in order, starting at tag 1. The tag value can range from 1 to 65535. Multiple instances are used when multiple remote peers exist in a site-to-site VPN configuration.

Question 17

How can routing protocols be used over a site-to-site VPN?

Question 18

What Layer 4 protocol and port are used for ISAKMP communications?

Question 17 Answer

To use a routing protocol in a site-to-site VPN environment, GRE tunnels must be utilized. With GRE tunnels, a virtual tunnel interface is used to represent the logical connection between peers. It is on this tunnel interface that a routing protocol can be utilized.

Question 18 Answer

ISAKMP uses UDP with source and destination ports equal to 500.

It should be noted that some implementations—especially remote-access implementations—use UDP source ports other than 500.

Question 19

When two peers begin IKE negotiations, how do they identify themselves?

Question 20

What command is used to configure the ISAKMP identity of a router?

Question 19 Answer

Either IP address or host name can be used as the IKE identity. The identity value supplied must match the ISAKMP key configured on the peer.

The global configuration command **crypto isakmp identity {hostname | address}** configures which identity is used.

Question 20 Answer

The global configuration command **crypto isakmp identity {hostname | address}** configures which identity is used during IKE negotiations.

Question 21

What is the difference between authentication provided by ESP and AH?

Question 22

How can you authenticate remote-access VPN connections?

Question 21 Answer

The authentication provided by ESP computes a hash based solely on a packet's payload. In contrast, the hash associated with AH is computed on the entire packet, headers included (this excludes fields like TTL that legitimately change in transit). AH, therefore, provides greater security by ensuring that the entire packet has not changed.

Question 22 Answer

Remote-access VPN connections can be authenticated using one of the following options:

- Preshared keys
- RSA signatures

In addition to the above options, remote-access users can be further authenticated using Extended Authentication (XAUTH). With XAUTH, users are authenticated against an external RADIUS server, such as Cisco ACS or Microsoft IAS.

Question 23

Within the context of certificates, what is a CRL?

Question 24

Can the same crypto map instance be used with multiple IPSec peers?

Question 23 Answer

A Certificate Revocation List (CRL) is used to verify that a certificate has not been revoked. If a certificate's serial number is listed on the CRL, it has been revoked and is no longer valid for any authentication purposes and is rejected.

Question 24 Answer

Yes, one crypto map instance can have multiple peers as long as both peers share an identical configuration. This is often used at a remote site to specify a redundant VPN device at the central site.

Question 25

Can different encryption algorithms be used with the same crypto map instance?

Question 26

How does the router determine which traffic to encrypt?

Question 25 Answer

No, a crypto map instance is associated with exactly one IPSec transform set, which is where the encryption algorithm is configured.

Question 26 Answer

An ACL is created and associated with a crypto map instance. This ACL, known as the crypto ACL, is used to select traffic that is to be encrypted. Traffic that is not selected by the crypto ACL (as permit entries) is not encrypted.

Question 27

What happens if the router receives traffic that matches a crypto ACL but is not encrypted?

Question 28

What is Perfect Forward Secrecy?

Question 27 Answer

Inbound traffic that should be encrypted and is not (as determined by evaluating the crypto ACL in reverse) is silently dropped.

Question 28 Answer

Diffie-Hellman Perfect Forward Secrecy (PFS) is used to generate new keying material for IPSec security associations. Without PFS, the IPSec keying material is derived from the IKE keying material.

Question 29

What does the command group 2 enable?

Question 30

What types of security associations exist?

Question 29 Answer

The **group 2** ISAKMP policy configuration command enables 1024-bit Diffie-Hellman key exchange during IKE negotiations. The default setting is **group 1**, which uses 768-bit encryption. It should be noted that larger keys require additional router CPU resources.

Question 30 Answer

There are two types of security associations (SAs): the ISAKMP SA and the IPsec SA. An SA is made up of a unidirectional connection and all of its associated security parameters. After the successful establishment of an IPsec session, each device has four SAs—an ISAKMP SA in each direction and an IPsec SA in each direction.

Question 31

What is an SPI?

Question 32

What command displays the number of existing ISAKMP security associations? What other information does this command display?

Question 31 Answer

A Security Parameters Index (SPI), is an index into the Security Parameters Database (SPD). Each security association has an SPI for each protocol (AH or ESP) in each direction (inbound and outbound).

Question 32 Answer

The EXEC command `show crypto isakmp sa` displays the number of existing ISAKMP security associations (SAs). In addition, this command displays the source and destination IP address of each SA.

Question 33

What is the name of the second IKE negotiation phase?

Question 34

When creating an IPSec transform set, you have selected the esp-sha-hmac option. What does this enable?

Question 33 Answer

The second IKE phase, called quick mode, is used to negotiate IPSec transform sets and establish IPSec security associations.

Question 34 Answer

This option enables ESP message authentication using the SHA hashing algorithm. Message authentication using MD5 can be enabled with the `esp-md5-hmac` option.

Question 35

What command links a crypto map with a crypto ACL?

Question 36

What command applies a crypto map to an interface?

Question 35 Answer

The crypto map configuration command **match address** *acl* is used to link an ACL to a crypto map.

Question 36 Answer

The interface configuration command **crypto map** *crypto-map-name* applies a crypto map to an interface.

Question 37

When creating an ISAKMP policy, which command enables the use of certificates for peer authentication?

Question 38

What settings make up the default ISAKMP policy?

Question 37 Answer

The ISAKMP policy configuration command **authentication rsa-sig** enables RSA digital signatures for the authentication of VPN peers.

Question 38 Answer

The following items make up the default ISAKMP policy:

- Authentication: rsa-sig
- Encryption: DES
- Diffie-Hellman: group 1
- Hash: SHA
- Lifetime: 86,400 seconds

Question 39

What are the main benefits associated with VPN technologies?

Question 40

Cisco offers two hashing algorithms for use with IPSec. What are they and which is more secure?

Question 39 Answer

VPNs have the following benefits:

- Reduced cost
- Improved data security
- Remote-access user authentication

Question 40 Answer

The two hashing algorithms available are SHA, which produces a hash 160 bits in length, and MD5, which produces a 128-bit hash. It is generally regarded that MD5 provides higher performance but, due to its larger resultant hash, that SHA is more secure.

Understanding DSL and Broadband Cable Technologies

Technology Goals

Although DSL and cable infrastructures are very different in their implementation, their goals are nearly identical. The following table lists goals and how each technology attains those goals.

Goal	DSL	Cable
Provide Internet or enterprise remote access	Provides Internet access or remote access to the enterprise	Provides Internet access only but can be teamed with a VPN solution for remote access to enterprise resources
Utilize existing facilities to reach as many potential customers as possible	Delivered over an existing telephone service to residential or business customers	Takes advantage of an existing cable television network that reaches nearly all potential customers

Modulation Techniques

ADSL uses one of two modulation techniques to allow the simultaneous transmission of voice and data over the same cable pair: CAP or DMT.

DSL Modulation Technique	Overview
Carrierless Amplitude Phase (CAP)	Data transmission uses one of two bands: 2.5 kHz to 160 kHz for upstream communications and 240 kHz to 1.5 MHz for downstream communications. Not an industry standard but widely deployed.
Discrete MultiTone (DMT)	Available bandwidth is divided into 256 4,312.5 kHz channels. The DMT devices monitor the channels in use and utilize of channels that provide cleaner transmissions.

In a broadband cable network, the existing RF modulation technique transmits data as well as television programming.

Devices in the Network

A DSL or cable network consists of several devices, which are summarized in the following table.

DSL Access Multiplexer (DSLAM)	DSL	Aggregates many customer connections to a few ATM connections
DSL Customer Premise Equipment (CPE)	DSL	Provides Ethernet connectivity to the user within their residence or business
Cable Modem Termination System (CMTS)	Cable	Services many customer connections from the cable network
Cable Modem	Cable	Provides Ethernet connectivity from customer devices to the cable network

The DOCSIS Standard

The Data over Cable Service Interface Specification (DOCSIS) is a standard for cable modem CPE to CMTS communication over a cable network. DOCSIS has three versions: 1.0, 1.1 (widely deployed), and 2.0.

As part of DOCSIS, the cable modem downloads its configuration and, optionally, its software image from a centralized TFTP server. The following information is part of a DOCSIS-compliant configuration file:

- Radio frequency information
- Configuration details
- Vendor-specific information
- Management specifics
- Software upgrade information

RFC-Defined Standards

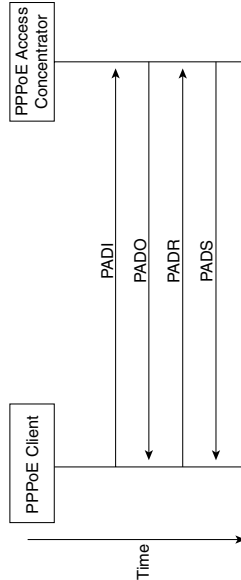
The following table lists the RFCs that are relevant to the configuration and deployment of DSL.

RFC **Relevance**

1483	Details the transmission of connectionless LAN data across an ATM network. Defines two modes of operation: bridged and routed. This is the basis of many legacy DSL CPE implementations.
2364	Defines PPP over ATM (PPPoA). PPPoA provides device authentication and service selection in a routed CPE configuration. With PPPoA, PPT terminates on CPE.
2516	Defines PPP over Ethernet (PPPoE). With PPPoE, a LAN-connected client can be authenticated and utilize the service selection capabilities inherent with PPP. Unlike PPPoA, PPPoE terminates PPP on the client computer and requires the CPE to be in a bridging mode.

PPP over Ethernet Session Establishment

The PPPoE session establishment process consists of four PPPoE packets: the PPPoE Active Discovery Initiation (PADI), the PPPoE Active Discovery Offer (PADO), the PPPoE Active Discovery Request (PADR), and the PPPoE Active Discovery Session (PADS) confirmation packet.



A fifth PPPoE packet is the PPPoE Active Discovery Terminate (PADT) packet. This is used to terminate an active PPPoE session. PPPoE packets use one of the following ETHER_TYPE fields.

ETHER_TYPE Field	Use
0x8863	PPPoE Discovery phase
0x8864	PPPoE Session phase

ATM Operating Parameters

When configuring an ATM interface, it is important to consider the following points:

Item	Valid Settings	Comments
Encapsulation	AAL5SNAP	All DSL CPEs should use this type of encapsulation. This becomes important when configuring the ATM PVC.
VPC	32-65535	Values 0-31 are reserved and are not used for PVCs. This is relevant when configuring a PVC.

VPI

0-255

This is relevant when configuring a PVC.

Understanding Virtual Private Networks

Types of VPNs

- Remote Access
- Site-to-Site

Remote Access VPNs

A Remote Access VPN allows remote users to securely access resources within an organization. The goals of a Remote Access VPN are simple:

- Secure access to internal resources
- User authentication and authorization
- Data confidentiality and authentication
- Cost savings through the utilization of local Internet connections

Site-to-Site VPNs

A site-to-site VPN provides secure connectivity between two networks over a less secure network, usually the Internet. The benefits of a site-to-site VPN include

- Secure access to remote resources
- Seamless access across sites
- Data confidentiality and authentication
- Cost savings through the utilization of local Internet connections

IPSec Protocols

The following protocols are relevant to the configuration of an IPSec solution:

- Internet Key Exchange (IKE)
- IPSec
- Encapsulated Security Payload (ESP)
- Authentication Header (AH)
- Generic Routing Encapsulation (GRE)

Layer 4 Protocols

The table below details the Layer 4 protocols that are relevant to an IPSec solution.

Protocol Name	Protocol Number	Description
Authentication Header	51	Verifies that a packet's contents have not been altered. This verification is computed based on the entire IP packet (legitimately changing fields [TTL, for example] ignored). This is enabled with the ah-md5-hmac or ah-sha-hmac transform set options.
Encapsulated Security Payload	50	Encrypts and authenticates information as it traverses the network. Authentication is provided on the Layer 4 payload only. ESP is enabled via the esp-des or esp-3des transform set options. ESP authentication is configured using the esp-md5-hmac or esp-sha-hmac transform set options.

Generic Routing Encapsulation

47

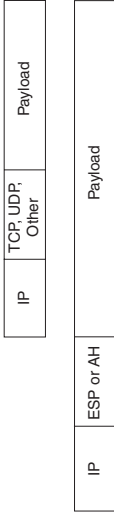
Creates a virtual point-to-point interface between IPSec peers. This interface aids in the deployment of routing protocols and redundancy.

Internet Key Exchange

The Internet Key Exchange (IKE) protocol negotiates IPSec security association information necessary to build an IPSec connection. IKE consists of two phases: phase one and phase two. Phase one has two modes: aggressive mode and main mode. In aggressive mode, IKE keying material is negotiated simultaneously with the IKE security associations. Aggressive mode uses three messages as opposed to the six used by main mode negotiations. In main mode, security is enhanced by first exchanging the keying material used by IKE and by then encrypting the remaining negotiations. Phase two of IKE negotiations has a single mode known as quick mode. In phase two, negotiations take place to establish the IPSec security associations. The following table details the default IKE policy configuration.

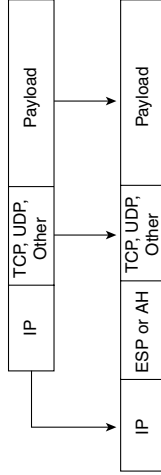
IPSec Tunnel Mode

IPSec has two operation modes: tunnel mode and transport mode. In tunnel mode, the Cisco default, each packet is completely encapsulated into a new IP packet with either an ESP or AH Layer 4 header. The following figure shows this encapsulation.



IPSec Transport Mode

In transport mode, a new Layer 4 header is added for either AH or ESP. This new header is inserted between the existing Layer 3 and 4 headers. The following figure shows how a packet is changed during transport mode operation.



Configuring a Site-to-Site IPSec VPN

First, an access control list (ACL) must be created to select the traffic to be encrypted. This ACL, known as the *crypto ACL*, controls exactly which packets are encrypted. The following crypto ACL encrypts all IP traffic from the 192.168.1.0/24 subnet to the 192.168.2.0/24 subnet:

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

After creating the crypto ACL, the IKE policy must be configured. The following commands enable IKE and configure a policy with 3DES encryption, MD5 hashing, and authentication using preshared keys:

```
crypto isakmp enable
crypto isakmp policy 10
```

Characteristic	Default Setting
Authentication	RSA Signatures
DH group	Group 1
Encryption	DES
Hashing	SHA
Lifetime	86,400 seconds

The following table lists the options available for each of the IKE policy configuration items following table.

Characteristic	Available Settings
Authentication	Preshared Keys, RSA Encrypted Nonces, RSA Signatures
DH group	Group 1, Group 2
Encryption	DES, 3DES, AES
Hashing	SHA, MD5
Lifetime	Time in Seconds, or Data in KB

Hashing Protocols

Hashing Protocol	Characteristics
SHA	Generates a 160-bit hash from a message of any length. Considered more secure than MD5 due to the decreased likelihood of collisions.
MD5	Produces a 128-bit hash from an arbitrary length message. Considered to impose less of a performance hit than SHA.

```

authentication preshared
hash md5
encryption 3des

```

Next, a transform set is created that defines the IPsec encryption and hashing to be used:

```
crypto ipsec transform-set TRANSFORM esp-3des esp-md5-hmac
```

Now, create an IKE key for the remote peer. The following example creates a key for the peer at 10.1.1.2:

```
crypto isakmp key cisco address 10.1.1.2
```

After the crypto ACL, the IKE policy, and the transform set have been created and a key is assigned to the peer, they are all linked together using the crypto map:

```

crypto map CRYPTOMAP 10 ipsec-isakmp
set peer 10.1.1.2
set transform-set TRANSFORM
match address 100

```

Now that everything has been created, the crypto map is applied to an interface with the following commands:

```

interface FastEthernet 0/0
crypto map CRYPTOMAP

```

Verification of VPN Functionality

The following commands verify and troubleshoot IPsec VPN functionality:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **show access-list**
- **show crypto ipsec sa**
- **show crypto ipsec transform-set**
- **show crypto isakmp policy**
- **show crypto isakmp sa**
- **show crypto map**