CCNP ISCW Notes

1 Apr 2008

Chapter 1: Describing Network Requirements

Intelligent Information Network (IIN)

The IIN is a model designed to demonstrate how networks evolve to meet business needs.

The IIN is comprised of four road maps, each suiting a particular business type:

Service-Oriented Network Architecture (SONA)

Service Provider Architecture (IP Next Generation Networks, IP-NGN)

Commercial Architecture

Consumer Architecture

IIN has three phases:

Integrated transport - The network serves as a common pathway for all communications traffic

Integrated services - Services are moved from dedicated hardware to flexible virtualization

Integrated applications - Application-Oriented Networking (AON); per-application network optimization

SONA

SONA has three layers:

1. **Application Layer** - Composed of applications for business and collaboration
2. **Interactive Services Layer** - Flexible virtualization of services
3. **Networked Infrastructure Layer** - Provides transport shared by all resources

Cisco Network Models

Campus network

Branch network

Data center

Enterprise edge

WAN/MAN

Teleworker

Chapter 2: Topologies for Teleworker Connectivity

Remote Connection Options

Traditional Layer 2 Connections

Layer 2 technologies include frame relay and ATM

Relatively secure (separate from the Internet), but not flexible

Not typically available to residential premises

Service Provider MPLS VPN

Requires a layer 2 connection to ride

Provides security and QoS

Site-to-site VPN over Public Internet

Most popular solution (most easily available, cheapest)

A secure layer 3 VPN is formed across existing public infrastructure

Infrastructure Options

DSL

Cable

Fiber (limited availability)

Chapter 3: Using Cable to Connect to a Central Site

Cable System Standards

National Television Standards Committee (NTSC) - North America

Phase Alternating Line (PAL) - Europe, Asia, Africa, Australia, Brazil, and Argentina

Systeme Electronic Couleur avec Memoire (SECAM) - France and Eastern Europe

Cable System Components

Antenna Site - The site at which a cable provider's main receiving antennas are located

Headend - A master facility where signals are processed and distributed over the cable network

Transportation network - Connects remote antenna sites to the headend(s)

Distribution network - Distributes signals to end users; often contains a *Hybrid Fiber-Coaxial (HFC)* infrastructure

Subscriber drop - Connects the subscriber to the distribution network

The *Radio Frequency (RF)* range is 5 MHz to 1 GHz.

Data-Over-Cable Service Interface Specifications (DOCSIS)

Downstream frequencies: 50 - 860 MHz

Upstream frequencies: 5-42 MHz

DOCSIS allows for channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, 3.2 MHz, and 6.4 MHz.

DOCSIS 1.0 and 1.1 utilize TDMA; DOCSIS 2.0 can utilize TDMA or *synchronous code division multiple access (S-CDMA)*.

Media access control is done on a request/grant system, minimizing collisions.

Cable Modem Termination System (CMTS) - Responsible for signal (de)modulation; typically resides in the headend

Cable Modem (CM) - CPE (de)modulation device

DOCSIS 2.0 provides for up to 40 Mbps downstream and 30 Mbps upstream. DOCSIS 3.0 is capable of up to 160/120 Mbps.

Cable modem boot process

1. Downstream setup
2. Upstream setup
3. Layer 1 and 2 establishment
4. IP address allocation (DHCP)
5. TFTP DOCSIS configuration file
6. Register QoS with CMTS
7. IP network initialization

Chapter 4: Using DSL to Connect to a Central Site

Terminology

ATU-C - ADSL Transmission Unit - Central office; a subscriber-facing modem in the CO

ATU-R - ADSL Transmission Unit - remote; a provider-facing modem at a remote location

DSL Access Multiplexer (DSLAM) - A group of ATU-C units in a single chassis

Line code - Technique used to encode a digital signal onto the wire

Microfilter - Low-pass filter to prevent noise from reaching traditional analog equipment on a DSL line

Network Interface Device (NID) - The CPE device terminating the local loop

Limitations

ADSL can typically reach only 18,000 feet from the CO.

Load coils placed to extend voice signals disrupt data signals.

Bridge taps (unterminated wire split) introduce additional interference.

Crosstalk occurs between pairs within a cable bundle.

DSL Types

Asymmetric Types

Asymmetric DSL (ADSL) - Offers 1.5 - 8 Mpbs down, 16 Kbps - 1 Mbps up, up to 18,000 feet

G.Lite ADSL - Allows for 1.5/512 without the use of filters for analog equipment

Rate-Adaptive DSL (RADSL) - Nonstandard implementation which automatically adjusts connection speed to match line quality

Very-high-bitrate DSL (VDSL) - Offers 13 - 55 Mbps down, up to 4500 feet; Cisco LRE is based on VDSL

Symmetric Types

Symmetric DSL (SDSL) - Provides identical downstream and upstream speeds from 128 Kbps to 2.32 Mbps; 768 Kbps is typical; reaches up to 21,000 feet

Symmetric High-Data-rate DSL (G.SHDSL) - Defined in ITU-T G.991.2; offers 192 Kbps - 2.3 Mbps up to 26,000 feet

High-data-rate DSL (HDSL) - Provides T1 or E1 data rates; cannot coexist with analog telephone service

HDSL2 - Uses only one pair (HDSL uses two pairs)

ISDN DSL (IDSL) - Up to 144 Kbps (2x 64K + 1x 16K); can be augmented up to 45,000 feet with repeaters

ADSL Modulation

Carrierless Amplitude Phase (CAP)

CAP operates with three frequency bands:

Voice - 0 to 4 kHz

Upstream - 25 kHz to 160 kHz

Downstream - 240 kHz to 1.1 MHz

CAP is based on *quadrature amplitude modulation (QAM)*.

CAP is legacy and nonstandard, giving way to DMT.

Discrete Multi-Tone (DMT)

DMT uses *orthogonal frequency-division multiplexing (OFDM)* and operates on multiple carriers (channels) within each frequency range.

The available frequency range of 0 to 1.1 MHz is divided into 256 channels of 4.312 kHz each.

Channels are dynamically allocated to find the combination of channels with the least interference.

Data Transmission over ADSL

RFC 1483/2684 Bridging

Simple multi-protocol encapsulation over ATM, defined in the RFCs **1483** and **2684**.

PPP over Ethernet (PPPoE)

Defined in **RFC 2516**.

Connection setup occurs in two phases:

Discovery

PPP Session

Discovery Phase

The CPE router performs the discovery phase to determine the MAC address of its peer.

1. The client broadcasts a *PPPoE Active Discovery Initiation (PADI)* packet requesting service.
2. The aggregation router responds with a *PPPoE Active Discovery Offer (PADO)*.
3. The client sends a unicast *PPPoE Active Discovery Response (PADR)* requesting to move on to the session phase.
4. The aggregation router sends a *PPPoE Active Discovery Session-Confirmation* with a session ID.

PPPoE frame structure:

VER (4 bits) - Version; always 0x1

TYPE (4 bits) - Type; always 0x1

CODE (8 bits) - Determines stage of the discovery process; always 0x00 during session phase

SESSION_ID (16 bits) - Carries the PPP session ID (once established); constant for the duration of the session

LENGTH (16 bits) - Length of the payload

Session Phase

The session phase consists of normal PPP operation; LCP and NCP negotiation.

RFC 2516 defines a *Maximum Receivable Unit (MRU)* (MTU) of 1492 (6-byte PPPoE header + a 2-byte PPP protocol ID field).

PPP over ATM (PPPoA)

PPPoA uses *ATM Adaptation Layer 5 (AAL5)* and *Logical Link Control/Subnetwork Access Protocol (LLC/SNAP)* for encapsulation on virtual circuits.

Ethernet frames are appended with an 8-byte *segmentation and reassembly (SAR)* trailer and padding so that their length extends to a multiple of 48, then split into 53-bye ATM cells for transmission.

Virtual circuits are specified as a pairing of a *Virtual Path Identifier (VPI)* (8 bits) and a *Virtual Circuit Identifier (VCI)* (16 bits).

PPPoA also performs discovery and session phases similar to PPPoE.

Chapter 5: Configuring DSL Access with PPPoE

Several components of PPPoE over DSL need to be configured:

Ethernet/ATM interface

Dialer interface configuration

PAT configuration

DHCP service configuration

Static default route configuration

Provider-facing Ethernet/ATM Interface Configuration

Ethernet interface:

```
interface Ethernet0/0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
```

ATM interface:

```
interface ATM0/0
 no ip address
 dsl operating-mode auto
 pvc 8/35
 pppoe-client dial-pool-number 1
```

Dialer Interface Configuration

```
interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
```

Port Address Translation Configuration

```
interface Ethernet0/0
 ip nat inside
!
interface Dialer0
 ip nat outside
```

```
!
ip nat inside source list 100 interface dialer0 overload
access-list 100 permit ip 172.16.0.0 0.0.255.255 any
```

DHCP Service Configuration for LAN Clients

```
ip dhcp exclude-address 172.16.0.1 172.16.0.9
!
ip dhcp pool LAN
 import all
 network 172.16.0.0 255.255.0.0
 default-router 172.16.0.1
```

Static Default Route Configuration

```
ip route 0.0.0.0 0.0.0.0 interface dialer0
```

Verification

`show pppoe session all` can be used to verify active PPPoE sessions.

Chapter 6: Configuring DSL Access with PPPoA

PPPoA is defined in **RFC 2364** as *PPP over AAL5*.

PPPoA Types

Three types of PPPoA are available:

- Virtual circuit multiplexed PPP over AAL5 (AAL5MUX) (RFC 2364)
- LLC encapsulated PPP over AAL5 (AAL5SNAP) (RFC 2364) (default)
- Cisco PPP over ATM (PPPoA) (Cisco proprietary)

VC-Multiplexed PPP over AAL5

Provides a separate virtual circuit for each routed protocol to be transported.

Configuration:

```
interface ATM0/0
```

```
 no ip address
 dsl operating-mode auto
 pvc 8/35
  encapsulation aal5mux ppp Virtual-Template1
!
interface Virtual-Template1
 encapsulation ppp
 ip address negotiated
 ppp authentication chap
 ...
```

LLC Encapsulated PPP over AAL5

Provides a single virtual circuit for all higher-layer protocols.

AAL5SNAP is the default method.

An LLC header is inserted at the beginning of the PDU.

The LLC header contains the following information:

> **Destination Service Access Point (DSAP)** - Set to `0xFE for` SNAP
>
> **Source Service Access Point (SSAP)** - `Set to 0xFE` for SNAP
>
> **Frame Type** (Control) - `0x03` (unnumbered)

Configured with `encapsulation aal5snap`.

Cisco PPPoA

Allows for multiple PVCs on multiple subinterfaces.

Cisco equipment is required end-to-end.

Configured with `encapsulation ciscoppp`.

Chapter 7: DSL Connection Troubleshooting

Physical Layer

Layer 1 has two sublayers: the *transmission convergence (TC)* and *physical medium dependent (PMD)* layers.

Framing is the process of ordering bits for transmission.

Line coding is the process of transmitting bits.

RJ-11/RJ-14 pinout:

1. (empty)
2. Black (Tip)
3. Red (Ring)
4. Green (Tip)
5. Yellow (Ring)
6. (empty)

Supported DSL Operating Modes

`auto` - Automatic negotiation

`ansi-dmt` - ANSI T1.413

`itu-dmt` - G.992.1

`splitterless` - G.992.2 or G.Lite

Carrierless Amplitude Phase (CAP) cannot be autonegotiated.

ATM Debugging

`debug atm events` - Displays the allocated VPI/VCI pair

`debug atm packet` - Displays VPI/VCI and packet type (MUX vs SNAP)

An ATM ping can be performed to test the ATM circuit:

```
Router# ping atm interface atm0/0 8 35 seg-loopback
```

PPP Operation

PPP phases:

1. Link Control phase
2. Authentication phase (optional)
3. Network Control phase

Monitoring:

```
debug ppp negotiation
debug ppp authentication
```

Chapter 8: The MPLS Conceptual Model

Multiprotocol Label Switching (MPLS) is defined in **RFC 3031**.

Terminology

Label - Identifies a group of networks sharing a common destination

Label stack - An ordered set of independent labels attached to a packet header

Label swap - Forwarding operation based on label lookups

Label-Switched Hop (LSH) - The hop between two MPLS nodes ***Label-Switched Path (LSP)** - The path taken through multiple LSRs

Label Switching Router (LSR) - An MPLS node capable of forwarding labeled packets

MPLS Features

Label switching is not dependent on L3 routing functionality.

MPLS is designed to forward packets on the minimum amount of information required (a short label rather than an entire IP header).

Packets are grouped by destination into *Forwarding Equivalence Classes (FECs)*.

Packets are assigned to an FEC by applying a label at the ingress MPLS node. Packets are relabeled at each *Label Switching Router (LSR)*.

Service providers use MPLS technologies to isolate each customers' routing information, forming an MPLS VPN.

A *Penultimate Hop Pop (PHP)* occurs when an LSR directly before the egress edge LSR remove the label, so that the egress edge LSR only has to make a routing decision (versus a label *and* routing decision).

Router Switching Mechanisms

Process Switching - Each packet is processed individually; very resource intensive

Cache-driven (Fast) Switching - The first packet to a destination is process-switched and the routing decision is cached; subsequent packets are forwarded based on the cache entry

Topology-driven (CEF) Switching - A *Forwarding Information Base (FIB)* is built in parallel to the routing table; provides high-speed layer 3 switching

MPLS is CEF switched.

Chapter 9: MPLS Architecture

MPLS Components

Control plane - Maintains routing and label information exchange between neighbors

Data plane - Forwards traffic

Label Stacking

MPLS label structure:

Label (20 bits) - Label values 0 through 15 are reserved; 16 is the first value available for use.

Experimental CoS (3 bits) - The Experimental CoS field is undefined in **RFC 3031**; Cisco uses this field for class of service (taken from IP precedence values).

Bottom of Stack Indicator (1 bit) - Indicates end of the label stack

TTL (8 bits) - Time to live

In *frame mode* MPLS, labels are inserted between the layer 2 and layer 3 headers.

In *cell mode* MPLS (over ATM), VPI/VCI fields are used to carry label information.

Some instances require stacked labels:

MPLS VPN - *Multi-Protocol BGP (MPBGP)* propagates VPN information, which is added to packets preceding the original MPLS label.

MPLS TE - MPLS Traffic Engineering relies on information conveyed by RSVP to establish tunnels, and added to packets as a label preceding the original label.

MPLS VPN and TE - A label is added for VPN and for TE, resulting in a stack of at least three labels in the packet.

MPLS identifies the upper-layer protocol by replacing the layer 2 header field with an MPLS-specific value. For example, in Ethernet, `0x0800` (IP) would be replaced with `0x8847` (MPLS-IP).

Label Allocation

Label Distribution Protocol (LDP) is used to advertise labels to neighboring LSRs (functioning as a routing protocol).

Label Information Base (LIB) - Stores label-to-prefix tables; control plane

Label Forwarding Information Base (LFIB) - Maintains forwarding database from LIB; data plane, comparable to the FIB

Label distribution can occur in two ways:

Unsolicited - An update is triggered by a convergence event

On-demand - An LSR actively requests an update from its neighbor

Interim packet propagation occurs when an LSR has no label associated with a packet's destination, and falls back to CEF switching (IP routing).

Penultimate Hop Popping (PHP) occurs when an LSR realizes it is the second-to-last router in the LSP, and assigns a packet the reserved label value of 3 (`imp-null`, implicit null). When the next LSR receives the packet, it knows immediately to discard the label and perform a CEF lookup.

Chapter 10: Configuring Frame Mode MPLS

Configuring CEF

```
Router(config)# ip cef [distributed]
```

CEF operation can be verified with `show ip cef`.

Configuring MPLS

MPLS is enabled by default on routers which support it. It can be disabled with `no mpls ip`.

MPLS and *Label Distribution Protocol (LDP)* must be enabled per interface.

```
Router(config-if)# mpls label protocol ldp
Router(config-if)# mpls ip
```

Configuring MTU Size

The MTU on an MPLS interface must be raised by four bytes for each potential label in a stack.

```
Router(config-if)# mpls mtu 1512
```

Setting the MTU with `mpls mtu` only modifies the MTU for MPLS packets, rather than all interface traffic.

All intermediate devices must support jumbo frames as well.

Verification

The status of LDP neighbors can be verified with `show mpls ldp neighbor`.

Chapter 11: MPLS VPN Technologies

VPN Types

Layer 1 Overlay - Dedicated physical circuits

Layer 2 Overlay - Traditional WAN services (Frame Relay, HDLC, etc); virtual circuits

Layer 3 Overlay - GRE/IPsec tunnels

Peer-to-Peer - Layer 3 connectivity serviced by provider

VPN Architecture

C network - A customer's private network

CE router - Customer edge router which connects to a PE router

P network - The provider's shared network composed of MPLS routers

PE router - Provider edge router which connects to one or more customers

Different customer networks can be logically separated using *Virtual Routing and Forwarding (VRF)*, a private routing table on the provider's routers.

A *route distinguisher (RD)* is a 64-bit prefix prepended to an IPv4 address to create a globally unique VPNv4 address. Each customer is assigned its own RD or RDs.

VPNv4 addresses are communicated between PE routers using MPBGP.

A *route target (RT)* is an attribute appended to a VPNv4 BGP route to indicate VPN membership.

Chapter 12: IPsec Overview

IPsec features:

Data confidentiality

Data integrity

Data origin authentication (peer authentication)

Anti-replay

IPsec Protocols

Internet Key Exchange (IKE)

IKE handles secure exchange of keys and other information over a nonsecure channel.

Rides TCP port 500.

Encapsulating Security Payload (ESP)

Provides for both data encryption and integrity.

DES, 3DES, or AES can be used for encryption.

Hash-based Message Authentication Code (HMAC) provides data integrity, using either SHA-1 or MD5.

Defined as IP protocol 50.

Authentication Header (AH)

Does not provide for data encryption.

Like ESP, uses HMAC to provide data integrity.

Defined as IP protocol 51.

IPsec Modes

Transport mode - An ESP or AH header is inserted between the IP header and layer 4 header

Tunnel mode - A new IP header is generated, followed by ESP/AH and the entire original packet (which is encrypted if ESP is used)

Peer Authentication

IPsec can use any of the following methods to authenticate a peer:

Username and password

One-time password (OTP)

Biometrics

Preshared keys

Digital certificates

Internet Key Exchange (IKE)

IKE Protocols

Internet Secure Association and Key Management Protocol (ISAKMP) - Manages security associations, parameter negotiation, and peer authentication

Oakley - Uses the Diffie-Hellman algorithm to exchange keys

IKE Phases

Phase 1

A bidirectional *security association (SA)* is established between peers, and peers may optionally be authenticated.

Phase 1 is accomplished in either *main mode* or *aggressive mode*.

Parameters such as hash methods and transform sets are negotiated.

Phase 1.5 (Optional)

Xauth (Extended Authentication) can optionally authenticate the user of the IPsec endpoint.

Phase 2

Unidirectional SA's are set up between endpoints in IKE *quick mode* using the parameters agreed upon in phase 1. Separate keys are used for each direction.

IKE Modes

Main Mode

Six messages are exchanged, in three pairs:

IPsec parameters and security policy - The initiator sends one or more proposals, and the responder selects the appropriate one.

Diffie-Hellman public key exchange - Public keys are exchanged

ISAKMP session authentication - Each end is authenticated by the other

Aggressive Mode

An abbreviated version of main mode:

The initiator sends all its configuration data

The responder authenticates the packet and replies with its configuration data

The initiator authenticates the packet

IKE Quick Mode

Used only in phase 2, to setup unidirectional SA's over an established bidirectional SA.

Other IKE Functions

Dead peer detection - Keepalives

NAT traversal - NAT existence and support are determined in IKE phase 1; NAT traversal is accomplished by UDP encapsulation and negotiated in phase 2

Mode configuration - Pushing IPsec configuration details to the remote client

Xauth - Optional user authentication in phase 1.5

Encryption Algorithms

Symmetric algorithms:

DES - 56-bit key

3DES - Three instances of DES using three different keys

AES - Originally termed Rijndael, uses 128-, 192-, or 256-bit keys

Asymmetric algorithms:

RSA - Minimum key length of 1024 bits; can be used for encryption and digital signatures

Public Key Infrastructure (PKI)

Peers - End hosts with the need for secure communication

Certification Authority (CA) - Grants and maintains digital certificates

Digital certificate - Used to identify and authenticate a peer

Registration authority (RA) - An optional entity which handles certificate requests for the CA

Distribution mechanism - A means to distribute *certification revocation lists (CRLs)*

Chapter 13: Site-to-Site VPN Operations

Life cycle of an IPsec VPN

Step 1: Specify interesting traffic

An ACL is use to specify which types of traffic are to be placed into the VPN tunnel.

If the VPN tunnel has not yet been established, the first packet of interesting traffic will trigger its setup.

Step 2: IKE phase 1

IKE phase 1 is performed in either main mode or aggressive mode.

IKE transform set negotiation, Diffie-Hellman public key exchange, and peer authentication take place in this step.

IKE transform sets are composed of the following parameters:

- IKE encryption algorithm (DES, 3DES, or AES)
- IKE authentication algorithm (MD5 or SHA-1)
- IKE key (preshared, RSA signatures, or nonces)
- Diffie-Hellman version (1, 2, or 5)
- IKE tunnel lifetime (time and/or byte count)

Candidate transform sets are selected by lowest policy number.

Step 3: IKE phase 2

IKE quick mode is used to negotiate IPsec transform sets and establish unidirectional IPsec security associations (SAs) in both directions.

IKE also monitors and reestablishes SAs as needed.

Optionally, IKE quick mode can also perform additional Diffie-Hellman key exchanges when active keys expire.

IPsec transform sets (similar to IKE transform sets) include the following parameters:

- IPsec protocol (ESP or AH)
- IPsec encryption type (DES, 3DES, or AES)
- IPsec authentication (MD5 or SHA-1)
- IPsec mode (tunnel or transport)
- IPsec SA lifetime (seconds or kilobytes)

The *Security Association Database (SAD)* maps SAs to peers by their *Security Parameter Index (SPI)*.

The *Security Policy Database (SPD)* contains the security parameters (transform set) that were agreed upon for each SA.

Step 4: Secure Data Transfer

Interesting traffic is encrypted and/or authenticated through the IPsec tunnel.

Step 5: IPsec tunnel termination

If the SA key has expired, the SA is torn down and a new one is established if more traffic needs to be passed.

Tunnels can also be manually deleted by an administrator.

Upon tunnel termination, all SA information for that tunnel is removed from the SAD and SPD.

IPsec Configuration

Step 1: Configure the ISAKMP policy

Define an IKE transform set:

```
crypto isakmp policy 10
 encryption des
 hash md5
 authentication pre-share
 group 1
 lifetime 3600
!
crypto isakmp key 0 <secret key> address 192.168.100.1
```

Step 2: Configure the IPsec transform sets

An example defining ESP with 256-bit AES encryption and SHA-1 authentication in tunnel mode:

```
crypto ipsec transform-set Foo esp-aes 256 esp-sha-mac
 mode tunnel
```

Optionally, a lifetime for the SA can be configured:

```
crypto ipsec security-association lifetime seconds 1800
```

Step 3: Configure the crypto ACL

An extended ACL is configured to match interesting traffic.

```
access-list 123 172.16.0.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Step 4: Configure the crypto map

```
crypto map Tyler 10 ipsec-isakmp
 match address 123
 set peer 1.2.3.4
 set transform-set Foo
```

Step 5: Apply the crypto map to an interface

```
interface Serial 0/0
 ip address 192.168.200.1
 crypto map Tyler
```

Step 6: Configure the interface ACL

Optionally configure ACLs on public-facing interfaces to only accept IPsec traffic from expected sources.

Chapter 14: GRE Tunneling over IPsec

GRE over IPsec is primarily used to facilitate routing protocols within tunnels.

GRE is stateless.

GRE adds a new 20-byte IP header and its own 4-byte header, and up to 12 bytes of options:

Bit 0: Checksum present - Adds an optional 4-byte checksum field

Bit 2: Key present - Adds an optional 4-byte encryption key

Bit 3: Sequence number present - Adds an optional 4-byte sequence number

Bits 13-15: GRE version - 0 is basic GRE, 1 is used for PPTP

Bits 16-31: Protocol field - Identifies layer 3 protocol being transported

GRE Tunnel Configuration

Basic configuration components:

- Tunnel source
- Tunnel destination
- Tunnel mode (GRE/IP is default)

Basic GRE/IP configuration:

```
Router(config)# interface tunnel0
Router(config-if)# ip address 192.168.0.1 255.255.255.252
Router(config-if)# tunnel source s0/0
Router(config-if)# tunnel destination 10.1.2.3
! GRE/IP is default
Router(config-if)# tunnel mode gre ip
```

GRE over IPsec configuration under the SDM involves the following steps:

1. Create the GRE tunnel
2. Create a backup GRE tunnel (optional)
3. Select the IPsec VPN authentication method
4. Select the IPsec VPN IKE proposals
5. Select the IPsec VPN transform sets
6. Select the routing method for the tunnel
7. Validate the configuration

Chapter 15: IPsec High Availability Options

Common Sources of Failure

Access link failure - Failure of a physical interface or cable

Remote peer failure - Failure at the distant end

Device failure - Failure of some intermediary device in the VPN path

Path failure - A routing or circuit issue between VPN endpoints

IPsec Stateless Failover

In a stateless failover configuration, routers do not directly track the status of tunnels.

Dead Peer Detection (DPD)

DPD can operate in either *periodic mode* or *on-demand mode*.

Periodic mode:

- Keepalive messages are sent between VPN peers periodically
- Keepalives are only sent in the absence of normal data traffic
- Keepalives are sent in addition to regular IPsec rekey messages

On-demand mode (default):

- Keepalives are only sent when the health of the peer is suspect
- Less overhead than periodic mode
- Might not detect a dead peer until the IPsec SA expires and needs to be rekeyed

DPD configuration:

```
Router(config)# crypto isakmp keepalive <seconds> [<retries>] [periodic | on-demand]
```

IGP Within a GRE over IPsec Tunnel

An IGP such as EIGRP or OSPF is run between peers, treating the tunnels like normal layer 3 links.

HSRP

HSRP is used on a pair of routers facing a peer, so that either will answer for the VPN peer address.

The HSRP group on an interface must be designated as providing IPsec redundancy with the `redundancy` command appended to the interface `crypto map` specification:

```
crypto map central-office 10 dynamic from-remote
!
interface FastEthernet1/0
 ip address 192.168.0.3
 standby 1 ip 192.168.0.1
 standby 1 name vpn-remote
 crypto map central-office redundancy vpn-remote
```

IPsec Stateful Failover

Stateful failover uses identical active and backup devices running HSRP and Stateful Switchover (SSO).

Inside and outside interfaces on the devices must be LAN interfaces.

Both modes of DPD (periodic and on-demand) are supported.

The HSRP configuration of an interface is similar to the stateless configuration, but with the addition of `stateful` to the interface `crypto map` specification:

```
crypto map central-office 10 dynamic from-remote
!
interface FastEthernet1/0
 ip address 192.168.0.3
 standby 1 ip 192.168.0.1
 standby 1 name vpn-remote
 crypto map central-office redundancy vpn-remote stateful
```

SSO is enabled by specifying the HSRP group as follows:

```
redundancy inter-device
 scheme standby vpn-remote
```

Inter-device Communication Protocol (IPC) facilitates inter-device communication:

```
ipc zone default
 association 1
 protocol sctp
  local-port 12321
 local-ip 10.10.10.1
 retransmit-timeout 300 10000
 path-retransmit 10
 assoc-retransmit 20
  remote-port 12321
 remote-ip 10.10.20.1
```

Stream Control Transmission Protocol (SCTP) is used as the transport protocol. Local and remote port numbers must match.

Chapter 16: Configuring Cisco Easy VPN

Easy VPN modes:

Client - NAT/PAT is used to enable remote hosts to use a separate IP space

Network Extension - Server IP space is extended through the tunnel to the remote network

Network Extension Plus - Network extension mode with the added capability of issuing an IP address to the remote for use on a loopback interface

Easy VPN connection establishment:

1. IKE phase 1
2. Establishing an ISAKMP SA
3. SA proposal acceptance
4. Easy VPN user authentication
5. Mode configuration
6. Reverse route injection
7. IPsec quick mode

Chapter 18: Cisco Device Hardening

Potential Vulnerabilities

Unnecessary Services and Interfaces

Disable unused interfaces

Disable BOOTP server (`no ip bootp server`)

Disable CDP (`no cdp run`)

Disable automatic configuration download (`no service config`) (disabled by default)

Disable FTP server (`no ftp-server enable`) (disabled by default)

Disable TFTP server (`no tftp-server enable`) (disabled by default)

Disable PAD (`no service pad`)

Disable minor TCP and UDP services (`no service tcp-small-servers` and `no service udp-small-servers`)

Disable MOP (`no mop enable`) (disabled by default)

Common Management Services

Disable SNMP if not used (`no snmp-server enable`)

Disable HTTP(S) if not used (`no ip http server` and/or `no ip http secure-server`)

Disable DNS queries (`no ip domain-lookup`)

Path Integrity Mechanisms

Disable ICMP redirects (`no ip icmp redirect`)

Disable IP source routing (`no ip source-route`)

Probes and Scans

Disable finger service (`no service finger`)

Disable ICMP unreachables (`no ip unreachables`)

Disable ICMP mask reply (`no ip mask-reply`) (disabled by default)

Disable directed broadcasts (`no ip directed-broadcast`) (disabled by default)

Terminal Access Security

Disable identd (`no ip identd`)

Enable TCP keepalives (`service tcp-keepalives-in` and `service tcp-keepalives-out`)

Gratuitous and Proxy ARP

Disable gratuitous ARP (`no ip arp gratuitous`)

Disable proxy ARP (`no ip arp proxy`)

AutoSecure

```
Router# auto secure [management | forwarding] [no-interact | full] [login | ntp |
 ssh | firewall | tcp-intercept]
```

Chapter 19: Securing Administrative Access

Security Measures

Login Limitations

Example base *Authentication, Authorization and Accounting (AAA)* configuration:

```
Router(config)# aaa new-model
```

```
Router(config)# aaa authentication attempts login 5
Router(config)# aaa authentication login default local
```

Authentication failure logging generates a syslog message after a number of failed attempts within one minute, and prevents future logins for 15 seconds:

```
Router(config)# security authentication failure rate <attempts> log
```

Login blocking:

```
Router(config)# login block-for <seconds> attempts <number> within <seconds>
```

Failed login delay:

```
Router(config)# login delay <seconds>
```

Success and failure logging:

```
Router(config)# login on-success log
Router(config)# login on-failure log
```

Quiet mode maps an access class matching origins exempt from these login restrictions:

```
Router(config)# login quiet-mode access-class <ACL>
```

Login restrictions can be viewed with `show login`.

Line Protections

An access-class can be applied to restrict logins to permitted sources:

```
Router(config)# line vty 0 15
Router(config-line)# access-class 10 in
```

An idle timeout can be enforced:

```
Router(config-line)# exec-timeout <minutes> [<seconds>]
```

Setting the `exec-timeout` to 0 disabled the idle timer.

Minimum Password Lengths

```
Router(config)# security passwords min-length <characters>
```

Password Encryption

```
Router(config)# service password-encryption
```

Banners

A *message of the day (MOTD)* banner can be defined to advertise policy:

```
Router(config)# banner motd #
*** Unauthorized users will be shot. ***
#
```

Custom Privilege Levels

There are 16 privilege levels (0 through 15).

Level 0 is user mode, level 15 is privileged mode, and levels 1 through 14 are customizable.

```
Router(config)# privilege <mode> level <level> <command>
Router(config)# enable secret level <level> <password>
```

Role-based CLI

Role-based CLI allows for users to belong to multiple *views* rather than a privilege level.

```
Router(config)# parser view <name>
Router(config-view)# secret <password>
Router(config-view)# commands <type> {include | exclude | include-exclusive}
 {<line> | all}
```

```
Router# enable view <name>
```

Superviews link individual views:

```
Router(config)# parser view <name> superview
Router(config-view)# secret <password>
Router(config-view)# view <name>
```

Mitigating Physical Access

Password recovery can be disabled to prevent someone with physical access to a device from rebooting into ROMMON:

```
Router(config)# no service password-recovery
```

Chapter 20: Using AAA to Scale Access Control

AAA

Authentication, Authorization, and Accounting (AAA) has two access modes:

Character Mode - Used on VTY, auxiliary, and console lines to access the CLI

Packet Mode - Used on physical interfaces and dialer profiles for inter-device authentication (PPP, Arap, or NASI)

TACACS+

Developed by Cisco, defined in **RFC 1492**.

TACACS+ uses TCP.

TACACS+ allows for encryption of the entire packet body.

TACACS+ separates authentication and authorization, allowing a different backend to be used for each.

TACACS+ has better multiprotocol support than RADIUS.

Only TACACS+ provides command-specific authorization.

Configuration example:

```
aaa new-model
tacacs-server host 10.18.0.27
tacacs-server key SharedSecret
username Steve secret <hash>
aaa authentication ppp dial-list tacacs+ local
aaa authorization commands 15 tacacs+ if-authenticated none
aaa accounting network start-stop tacacs+
```

RADIUS

Defined in **RFC 2865**

RADIUS uses UDP.

RADIUS only encrypts passwords within an access-request packet.

RADIUS combines authentication and authorization.

Configuration example:

```
aaa new-model
radius-server host 10.18.0.27
radius-server key SharedSecret
username Steve secret <hash>
aaa authentication ppp dial-list radius local
aaa authorization network radius local
aaa accounting network mynetwork start-stop group radius
```

Debugging

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug radius
debug tacacs
```

Chapter 21: Cisco IOS Threat Defense Features

Firewall Technologies

Packet Filtering - *Access Control Lists (ACLs)* are used to restrict traffic to and from certain addresses and port numbers.

Application Layer Gateway (ALG) - An ALG operates at the application layer and sits between a client and server (example: HTTP proxy).

Stateful Packet Filtering - Packet filtering with the added capability of tracking session state.

IOS Firewall Features

IOS Firewall

Permits/denies TCP and UDP traffic

Maintains a state table

Dynamically modifies ACLs

Denial of Service (DoS) mitigation

Packet inspection

Authentication Proxy

Provides authentication and authorization for services via TACACS+ or RADIUS.

Supported protocols:

HTTP

HTTPS

FTP

Telnet

IOS Intrusion Prevention System (IPS)

Responds to suspect traffic with one or more actions:

Drop - Drop the packet

Block - Blocks origin IP for a specified amount of time

Reset - Terminates the TCP session

Alarm - Logs an alarm

Chapter 22: Implementing Cisco IOS Firewalls

Cisco IOS Firewall Configuration

Step 1: Choose an interface to inspect

Apply ACL and inspection rules in the inbound direction on untrusted interfaces.

Step 2: Configure an ACL

Example to allow SMTP and HTTP inbound to their respective servers:

```
ip access-list extended FROM_OUTSIDE
 permit tcp any host 10.0.24.89 eq 25
 permit tcp any host 10.0.22.103 eq 80
 deny ip any any log
```

Step 3: Define the inspection rules

```
Router(config)# ip inspect name <name> <protocol> [alert {on | off}]
 [audit-trail {on | off}] [timeout <seconds>]
```

The default timeout between alerts is 10 seconds.

Step 4: Apply the ACL and inspection rule

Enable audit trail tracking via syslog:

```
Router(config)# ip inspect audit-trail
Router(config)# logging on
```

To turn on real-time alerts (default):

```
Router(config)# no ip inspect alert-off
```

Apply the ACL and inspect rule:

```
Router(config)# ip access-group FROM_OUTSIDE in
Router(config)# ip inspect SMTP-AND-HTTP in
```

Step 5: Verify the configuration

```
show ip inspect [name <name> | config | interface | session | statistics |
all]
```

```
debug ip inspect ...
```

Chapter 23: Implementing Cisco IDS and IPS

Concepts

Intrusion Detection System (IDS) - Does not sit in the traffic path; cannot block traffic itself

Intrusion Prevention System (IPS) - Sits in the traffic path; configured to actively deny malicious traffic

IDS/IPS categories:

Network (NIDS/NIPS) - A dedicated device on the network; unable to assess the effectiveness of an attack

Host (HIDS/HIPS) - Software running on end hosts

Signature-based - Matches a specific byte pattern or content

Policy-based - Configurable policy to allow or deny certain traffic types and sources/destinations

Anomaly-based - Looks for traffic patterns which deviate from the norm

A *honeypot* is a device deployed with the intention of attracting attackers, possibly to distract them from legitimate devices.

Attack categories:

Denial of Service (DoS) - An attack on resources such as bandwidth and CPU power

Distributed DoS (DDoS) - A DoS attack sourced from multiple, likely spoofed sources

Reconnaissance - An attempt to gather information about the network

Signatures:

Exploit - A signature built to match a unique exploit

Connection - Matches unusual connection characteristics or events

String - Use regular expressions to check for patterns in packets

DoS - Tailored to detect denial of service attacks

Cisco IOS uses signatures stored in **Signature Definition Files (SDFs)**. SDFs can be moved, modified, and merged together.

Signature reaction:

Generate an alarm - Via syslog or SNMP; usually accompanied by other actions

Drop the packet - Traffic is blocked

Reset the connection - Only works with connection-oriented protocols (TCP)

Time-limited block from source - All traffic from the source IP is blocked for a specified amount of time

Time-limited block on connection - Blocks all traffic in a particular TCP session

Configuration

Specify the location of the SDF:

```
Router(config)# ip ips sdf {builtin | location}
```

Configure the failure parameter:

```
Router(config)# ip ips fail closed
```

Create an IPS rule:

```
Router(config)# ip ips name <name> [list <ACL>]
```

Apply the IPS rule to an interface:

```
Router(config-if)# ip ips <name> {in | out}
```

Verification

```
show ip ips configuration
```