IPsec and VPN

IPSec Basics

IPSec allows the establishment of a secure connection between two hosts. The IPSec protocol sets up a unidirectional SA (security association between the two endpoints). Because the association is unidirectional, an SA is created on both ends, resulting in two SAs per IPSec tunnel.

IPSec tunnels are often used as a backup to a WAN link failure. If a point-to-point WAN circuit drops, an IPSec tunnel can be configured to automatically be established over the internet to the remote site. When the primary WAN circuit comes back up, the IPSec tunnel is disconnected.

Floating Static Routes

Configuring an IPSec tunnel to activate when a primary link drops is commonly inplemented as a floating static route. The idea is to configure the IPSec VPN as a static route, but with an administrative distance higher than that of the WAN routing protocol's.

If the primary route is active, the backup link is not placed into the routing table because it has a higher administrative distance. If the primary route goes down, the static route becomes active.

To configure a floating static route, make sure you define a higher administrative distance value at the end of the statement:

```
R1(conf)# ip route prefix mask address|interface distance_value
```

VPN Tunnels

One major problem with standard IPSec sessions is that they do not support broadcast or multicast traffic. If you want to use an IPSec VPN in an "always on" fashion, then the tunnel needs to allow routing information to pass through. Of course dynamic routing protocols use broadcast or multicast to send hellos and updates, which creates a problem.

To get around this issue, a "tunnel within a tunnel" approach can be used. A generic tunnel can be configured within the IPSec tunnel to allow routing protocol information (along with all the other traffic). There are generally four ways to do this paired with IPSec:

DMVPN and GET VPN

Both allow the creation of secure, "on-demand", multipoint tunnels.

Virtual Tunnel Interface (VTI)

A secure, "always-on" tunnel that supports multicast traffic. This allows routing protocols to operate within it.

Generic Routing Encapsulation (GRE)
GRE tunnels may be the most common of the bunch – they are also the default tunnel mode on Cisco routers. GRE tunnels support many layer 3 protocols but perhaps most importantly allow multicast traffic accross the tunnel – permitting dynamic routing protocol traffic. *Be aware that GRE tunnels add an additional 20 byte IP header as well as a 4 byte GRE tunnel header.*

Branch Office Connectivity
The CCNP ROUTE exam covers several unusual topics related to managing and configuring the connectivity between an HQ site and a branch office. You need to be familiar with some of the underlying technologies used.Cisco ISR routers are often a good choice for branch sites as they support a wide variety of incoming services. In smaller offices, a single ISR may be used for a both remote connectivity and inter-VLAN routing. In that case, know that an Ethernet Switch Module would be required for the ISR router.

DSL

DSL, or Digital Subscriber Line, can be used as a backup WAN connection to a branch office. DSL uses frequencies not used by TDM phone systems on a phone line – allowing the extra bandwidth to be used for data connectivity.**Asymetrical DSL** has higher downstream bandwidth than upstream, while with **symetric DSL** they are both the same rate.

There are two primary methods for pushing L2 data across a DSL line:

PPPoE
Point-to-Point Protocol over Ethernet is the most common method and encapsulates PPP traffic into Ethernet frames.

PPoA
Point-to-Point Protocol over ATM is less common and routes PPP traffic over an ATM network between the customer and the DSL service provider. Both options can be configured on a Cisco router to terminate the DSL connectivity. PPPoE is especially helpful because it frees the local office's computers from running PPPoE
Cable

Broadband cable providers also provide internet connectivity which can be used for WAN backup or provide internet connectivity for telecommuters. The internet signal is carried on the same line that the television is carried, but a cable modem allows the data traffic to be separated.The international standard for sending data over a cable system is Data Over Cable Service Interface Specification (or DOCSIS). Many different versions of the standard are used throughout the world. Cable system connections are typically not terminated directly into a Cisco router. Instead, a cable modem demodulates the incoming signal and converts the traffic to Ethernet frames, which a router can process.