

CramSession

The Original Study Guide



Over
4 Million
Downloaded

Cisco

CCIE

Security Written Qualification Exam

350-018 350-018 350-018 350-018 350-018

Written by **Subject
Matter Experts**

Your **Trusted
Study Resource** for
Technical Certification

The **Most Popular
Study Guide** on the web

Table of Contents

Security Protocols	5
Remote Authentication Dial In User Service (RADIUS)	5
<i>Basics of AAA</i>	5
<i>AAA (Authentication, Authorization and Accounting)</i>	5
<i>Authentication</i>	5
<i>Authorization</i>	6
<i>Accounting</i>	8
<i>RADIUS (Remote Authentication Dial-In User Service)</i>	8
Terminal Access Controller Access Control System Plus (TACACS+)	10
<i>TACACS+ (Terminal Access Controller Access Control System Plus)</i>	10
Kerberos.....	12
Virtual Private Dial-up Networks (VPDN/Virtual Profiles)	14
Data Encryption Standard (DES).....	15
<i>Encryption</i>	15
Triple DES (DES3).....	15
IP Secure (IPSec)	16
<i>IPSec</i>	16
<i>IPSec Glossary</i>	17
<i>Configuration of IPSec in Cisco IOS</i>	19
Internet Key Exchange (IKE)	20
Certificate Enrollment Protocol (CEP) (aka SCEP)	23
Point to Point Tunneling Protocol (PPTP).....	24
Layer 2 Tunneling Protocol (L2TP).....	25
Operating Systems	26
UNIX.....	26
You should be knowledgeable of basic Unix security practices and terminology.	26
<i>File Permissions</i>	26
Windows (NT/95/98/2000)	31
Application Protocols	33
Domain Name System (DNS).....	33
Trivial File Transfer Protocol (TFTP)	34
File Transfer Protocol (FTP)	34
Hypertext Transfer Protocol (HTTP)	35
Secure Socket Layer (SSL)	35
Simple Mail Transfer Protocol (SMTP)	36

Network Time Protocol (NTP)	37
Secure Shell (SSH)	37
Lightweight Directory Access Protocol (LDAP).....	38
Active Directory	38
General Networking.....	38
Networking Basics	38
<i>General Networking Theory</i>	38
OSI Models.....	38
MAC Addressing	39
General Routing Concepts	39
Standards	40
Protocol Mechanics	40
Transmission Control Protocol (TCP)	40
TCP/IP.....	42
IP Addressing	42
Subnetting	43
Subnetting Tricks.....	43
Route Summarization.....	44
Switching and Bridging (including: VLANs, Spanning Tree, etc.).....	44
Bridging and LAN Switching.....	44
Transparent Bridging (TB).....	44
LAN Switching	45
Switching Technique Types	45
Trunking.....	46
Virtual LAN (VLAN)	46
VLAN Trunk Protocol (VTP)	46
Spanning-Tree Protocol (STP).....	47
Root Bridges and Switches	47
Bridge Protocol Data Units (BPDUs).....	47
How STP Works	48
STP Timers	48
Routed Protocols	49
Routing Protocol Concepts.....	49
Distance-Vector Routing Protocols	50
Link State Routing Protocols.....	50
Hybrid Routing Protocols.....	50
Distribution Lists.....	50

<i>Routing Loops</i>	51
<i>Administrative Distance</i>	51
<i>Policy Routing</i>	52
<i>Route Dampening</i>	52
Routing Protocols (including: RIP, EIGRP, OSPF, BGP)	52
<i>Routing Information Protocol (RIP)</i>	52
<i>Enhanced Interior Gateway Routing Protocol (EIGRP)</i>	53
<i>Tables</i>	54
<i>Tables</i>	55
<i>Choosing Routes</i>	55
<i>Open Shortest Path First (OSPF)</i>	56
<i>Area 0</i>	57
<i>OSPF Area Types:</i>	57
<i>Stub and Totally Stubby Area Similarities</i>	57
<i>Stub and Totally Stubby Area Differences</i>	57
<i>Router Types</i>	58
<i>Traffic Types</i>	58
<i>NMBA Networks</i>	58
<i>LSA Types:</i>	58
<i>Border Gateway Protocol (BGP)</i>	59
<i>Synchronization/Full Mesh</i>	59
<i>Next-Hop-Self Command</i>	60
<i>BGP Path Selection</i>	60
<i>Scalability Problems (and Solutions) with IBGP</i>	60
<i>BGP Security</i>	61
Point to Point Protocol (PPP).....	62
IP Multicast.....	62
<i>Addressing</i>	64
<i>Translate Multicast Addresses into Ethernet MAC Addresses</i>	64
<i>Internet Group Management Protocol (IGMP) and Cisco Group Management Protocol (CGMP)</i>	65
<i>IGMP</i>	65
<i>CGMP</i>	66
Integrated Services Digital Network (ISDN).....	66
Integrated Services Digital Network (ISDN).....	67
<i>ISDN Specifics</i>	67
<i>Channels</i>	68
<i>Flavors of ISDN</i>	68

Async 69

Access Devices (for example: Cisco AS 5300 series)..... 69

Security Technologies 69

 Concepts..... 69

 Packet Filtering 70

Access Control Lists (ACL) 70

 Proxies 72

 Port Address Translation (PAT)..... 73

 Network Address Translation (NAT) 73

 Firewalls..... 74

 Active Audit..... 75

 Content Filters..... 76

Content-Based Application Recognition (CBAC)..... 76

Committed Access Rate (CAR)..... 76

Network-Based Application Recognition (NBAR)..... 77

Configuring NBAR..... 78

 Public Key Infrastructure (PKI)..... 78

 Authentication Technologies..... 79

 Virtual Private Networks (VPN)..... 79

Cisco Security Applications 80

 Cisco Secure UNIX 80

 Cisco Secure NT 80

 Cisco Secure PIX Firewall 80

 Cisco Secure Policy Manager (formerly Cisco Security Manager)..... 81

 Cisco Secure Intrusion Detection System (formerly NetRanger) 81

 Cisco Secure Scanner (formerly NetSonar) 81

 IOS® Firewall Feature Set..... 81

Security General 82

 Policies..... 82

 Standards Bodies..... 84

 Incident Response Teams 84

 Vulnerability discussions..... 84

 Attacks and Common Exploits 84

Common Attacks and Exploits 84

Unicast Reverse Path Forwarding 85

 Intrusion Detection..... 85

Cisco General 86

IOS Specifics	86
<i>Command-Line Interface (CLI)</i>	86

Security Protocols

Remote Authentication Dial In User Service (RADIUS)

Basics of AAA

AAA (Authentication, Authorization and Accounting)

AAA is a set of software security tools that can be used to identify when users are logged into a router, and what they do while they're there. These tools are also used to control each user's authority level and monitor user activity while providing tracking information, the breakdown being:

- ❖ **Authentication** - Validating the claimed identity of an end user or a device, such as a host, server, switch or router.
- ❖ **Authorization** - Granting access rights to a user, group of users, system, or a process.
- ❖ **Accounting** - Tracking who, or what, performed a certain action, such as user connection and logging system users.

You can learn about [AAA at this Cisco Link](#).

Authentication

- ❖ AAA is enabled on an IOS router with the command,


```
aaa new-model
```
- ❖ A local database (local authentication) is setup by defining usernames and passwords, locally on the router. An example is:


```
username test password cisco1234
```
- ❖ If you are going to setup authentication, accounting, or authorization, you would be configuring RADIUS or TACACS, most likely. All possible router authentication methods are:


```
enable, krb5, krb5-telnet, line, local, local-case, none, group radius, group tacacs+, group {group-name}, auth-guest, guest, if-needed
```
- ❖ Something special to note is the "if-needed" parameter. This tells the authentication process to only authenticate the user if the user has not already been authenticated (for a TTY line).
- ❖ These methods are not available on all services. Possibilities for services are:

Login – Login authentication to the router, itself

NASI – NetWare Asynchronous Serial Interface clients

Enable – To access the privilege level of the router

ARAP – AppleTalk Remote Access Protocol

PPP – Point to Point Protocol

For instance, krb5-telnet is only available for login authentication, not for PPP.

- ❖ You would apply these methods and services with the following command:

```
aaa authentication <service> default <method1> [method2 ... ]
```

For example, to configure RADIUS login authentication you would type:

```
aaa authentication login default group radius
```

And then you would have to define the radius server with:

```
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
```

- ❖ You can configure multiple rules such that if one isn't available, it will try the next. Here is an example of trying, first, RADIUS, then local.

```
aaa authentication login default group radius local
```

You can learn about [Cisco Authentication at this link](#).

Authorization

- ❖ Command authorization is allowing only certain users to perform certain commands. This is done with the command:

```
aaa authorization <service> default <method1> [method2 ...]
```

- ❖ As with authentication, there are a variety of services and methods to choose from. The services are:

Auth-proxy – Security policies on a per-user basis

Commands – Sets authorization for IOS commands that you choose

EXEC – Sets authorization for a user's exec command-line session

Network – Sets authorization for network sessions, like PPP or SLIP

Reverse access – Reverse telnet sessions

Configuration – Authorization for downloading configuration from an AAA server

IP Mobile – Authorization for IP mobile

❖ The methods are:

TACACS+ - via a TACACS+ server

If-Authenticated – User can perform the commands if they have already been authenticated

None – No authorization is required

Local – Local authorization is used

RADIUS – Via a RADIUS server

❖ Something special to note is the “if-authenticated” parameter. This tells the authorization process to allow the user to run the command if the user has already been authenticated.

❖ For example, to configure authorization to login and access the router via exec mode, you would do:

```
aaa new-model
```

```
aaa authentication login default group radius
```

```
aaa authorization exec default group radius
```

You would also have to define your RADIUS server.

You can learn about [Cisco Authorization at this link](#).

Take Your Exam for Less!

Discount Exam Vouchers from PrepLogic
Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

[Buy Your Voucher Now](#)

PrepLogic
Be Prepared. Be Confident. Get Certified!

and many more

Accounting

- ❖ Cisco supports accounting only when used with a RADIUS or TACACS+ server.
- ❖ There are six different accounting types: network, connection, exec, system, command, and resource.
- ❖ You must also define how accounting will work. It will be one of the following:

start-stop – Sends information at the beginning and end of every event.

stop-only – Only sends information at the end of an event

wait-start – The router's accounting process waits for an acknowledgement from the accounting server before the router's user can do whatever is being accounted for

none – No accounting is used on that interface or line

The command takes the format:

```
aaa accounting {system | network | exec | connection | commands | resource level } {default | list-name}
{start-stop | stop-only | wait-start | none} [method1 [method2 ...] ]
```

For instance, if you wanted to turn on accounting on an interface for PPP, you would run the following:

```
ppp accounting default
```

Learn about [accounting at the following link](#).

RADIUS (Remote Authentication Dial-In User Service)

Radius is a non-proprietary protocol that provides authentication and accounting for networked devices. Because RADIUS uses UDP, it is generally considered a connectionless service. It is the protocol of choice for enterprise ISPs because it works with a variety of vendors, consumes fewer CPU cycles and is less memory intensive than TACACS+.

RADIUS uses an MD5 algorithm to encrypt passwords sent across the data network. Notice that RADIUS only encrypts the password, not the entire body of the packet like TACACS+ does.

The client passes user information to designated RADIUS servers, which can be either Windows NT or Unix platforms. The servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client device to deliver services to the user. It can use either PAP or CHAP authentication.

- ❖ RADIUS is defined in [RFC2865](#).
- ❖ RADIUS uses UDP, not TCP like TACACS+.

- ❖ As it uses UDP, the timing of communications is very important. There cannot be high latency on the network.
- ❖ RADIUS uses port 1812 but older versions can use port 1645.
- ❖ RADIUS communications are in clear-text except for the password that is encrypted.
- ❖ The password goes through an encryption process that includes MD5 encryption.
- ❖ There are six primary types of RADIUS packets:
 - Access-request
 - Access-accept
 - Access-reject
 - Access-challenge
- ❖ Network access servers (NAS) send access-request packages and the RADIUS server can respond with one of the other three.
- ❖ If the RADIUS server sends an access-accept message, this packet can contain the authorization attribute value (AV) pairs for that particular user.
- ❖ There is a long list of the IETF attributes that are supported by RADIUS. Included in this list is the vendor specific attribute (VSA) number 26. This allows different hardware vendors to support their own specific settings for their hardware. Cisco's vendor type is 9. The supported VSA option is type 1 or "cisco-avpair". These AV pairs would be stored on the RADIUS server in the format:

protocol : attribute sep value *

- ❖ Basically, you should be familiar with the format of these and what a "good" versus "bad" one would look like. A valid VSA would look like this:

cisco-avpair= "shell:priv-lvl=15"

This would set the user that it was configured for to automatically have access to privilege level 15.

- ❖ Also, don't forget that you must turn on support for these VSAs on the NAS (or router) with the following command:

radius-server vsa send [accounting | authentication]

- ❖ You will need to configure your RADIUS server on the NAS with the command:

radius-server host {hostname | ip-address}

- ❖ Then, make sure you configure a key (or password) to be used on each side with the command:

radius server key

- ❖ You can configure AAA server groups, for both RADIUS and TACACS+, with these commands:

```
aaa group server {radius | tacacs+} groupname
```

Then, inside (config-*sg*)# mode, you can configure the servers:

```
server ip-address [auth-port port-number] [acct-port port-number]
```

- ❖ Accounting in RADIUS is supported and uses UDP port 1813.
- ❖ RADIUS [RFC2866](#) defines RADIUS Accounting.

Learn more about [Cisco RADIUS at the following link](#).

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ (Terminal Access Controller Access Control System Plus)

TACACS+ is a Cisco proprietary centralized validation service for user names and password pairs. It uses TCP for transport (older versions of TACACS use UDP), requires AAA (although earlier versions of TACACS did not), and supports all three AAA functions separately. The most common services supported by TACACS+ are PPP for IP, with either PAP or CHAP authentication.

TACACS+ can log every command that is entered at the router exec command line, and provides two ways to control the authorization of router commands: per-user or per-group.

TACACS+ supports router command authorization integration with advanced authentication mechanisms, such as Data Encryption Standard (DES) and a One-Time Password (OTP) key. The complete bodies of TACACS+ packets are encrypted if there is a shared key on the router and server. Notice that TACACS+ can encrypt the entire body of the packet, unlike RADIUS, which only encrypts the password.

- ❖ TACACS+ uses port number 49.
- ❖ Usually, each TACACS+ session has separate TCP connections but they can also be multiplexed on a single TCP connection.
- ❖ As TACACS+ uses TCP, it works better on congested networks or WAN links, it isn't as time-sensitive as RADIUS, and it offers immediate notification for a down TACACS+ server as TCP provides a connection between the NAS and server. With a down RADIUS server, the NAS can only wait for the timeout to expire.

- ❖ Like RADIUS, TACACS+ uses an encryption process that includes MD5. However, as mentioned above, the entire TACACS+ packet, beyond the header, is encrypted, not just the password, as with RADIUS.
- ❖ Also like RADIUS, you should use a pre-shared key between the NAS and Server. This will be used in the encryption process.
- ❖ TACACS+ authentication has three types of packets: START, REPLY, and CONTINUE.
- ❖ These can receive a reply of: ACCEPT, REJECT, ERROR, or CONTINUE.
- ❖ Configure TACACS+ on an IOS router by doing the following:

```
tacacs-server host {hostname} [single-connection] [port integer] [timeout integer] [key string]
```

(The default port is 49)

You can also configure the host and key separately, like this:

```
tacacs-server host {host IP}
```

```
tacacs-server key {key}
```

- ❖ As with RADIUS, you can configure AAA server groups, with these commands:

```
aaa group server {radius | tacacs+} groupname
```

Then, inside (config-sg)# mode, you can configure the servers:

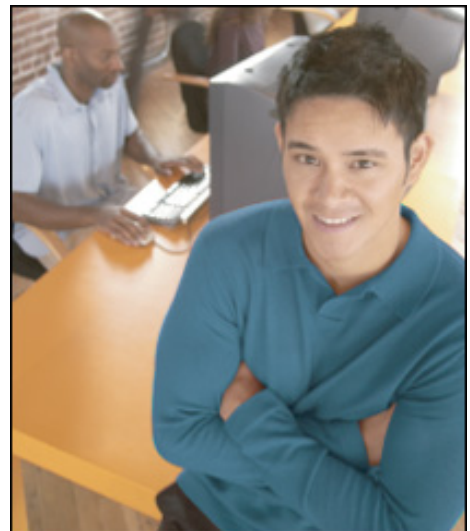
```
server ip-address [auth-port port-number] [acct-port port-number]
```

- ❖ TACACS+ authorization works by the NAS sending a REQUEST packet, and the server replying with a FAIL, PASS_ADD, PASS-REPL, ERROR, or FOLLOW packet.
- ❖ Just as with AAA and RADIUS, mentioned above, you configure authentication, authorization, and accounting the same way but substitute the radius parameter for the TACACS parameter. TACACS+ supports all of the AAA pieces, previously mentioned, including things like av-pair and VSA.
- ❖ TACACS+ has a number of security weaknesses. One of them is that TACACS lacks virtually all resistance to replay attacks, as all TACACS+ sessions start with a sequence number of 1 and increment from there. Learn more about [TACACS+ security weaknesses at this link](#).

You can learn more about [TACACS+ at this Cisco link](#) and [mores detail at this Cisco link](#).

Kerberos

- ❖ Kerberos is a network authentication protocol, developed at MIT.
- ❖ Kerberos performs authentication and encryption.
- ❖ Kerberos does **NOT** do authorization and accounting (the full AAA).
- ❖ A trusted third-party is what verifies users and services. This trusted third-party is called the Key Distribution Center (KDC).
- ❖ Kerberos issues tickets to users (instead of usernames/passwords) so that they users can verify their identity.
- ❖ Cisco supports Kerberos 5, which can interact with Unix and Windows implementations.
- ❖ Only these services are supported by Kerberos on the Cisco IOS:
 - telnet
 - rlogin
 - rsh
 - rcp
- ❖ Note that an end-user application that supports Kerberos is know as an application that is “kerberized”.
- ❖ To configure your router for Kerberos, you will need the hostname or IP of the KDC server, the port number, and the Kerberos realm that it serves.
- ❖ To add a new Kerberos user on the KDC, use this command to add a user in krb5_edit mode:
 - **ank** *user/instance@REALM*
- ❖ To add a privileged instance user, use this command:
 - **ank** *[user@REALM](#)*
- ❖ The most important item that a SRVTAB contains is the passwords for the “users” in the KDC.



Who Do You Trust for Your Certification Training?

PrepLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

PrepLogic Comprehensive Training Tools:

- CBT • Practice Exams • Audio Training
- Mega Guides • Discount Exam Vouchers

For Free Product Demos,
[Click Here.](#)

PrepLogic

Be Prepared. Be Confident. Get Certified.

- ❖ All routers authenticating to the KDC must have a SRVTAB created and extracted for them. To create the SRVTAB, on the KDC in the krb5_edit mode, enter the command:
 - **ark** [*SERVICE/HOSTNAME@REALM*](#)
 - Example: ark [*host/myrouter.brainbuzz.com@BRAINBUZZ.COM*](#)
 - Next, you must extract the SRVTAB with this command:
 - **xst** *router-name host*
- ❖ Now, to configure a Cisco router to use Kerberos, configure the following:
 - **kerberos local-realm** *kerberos-realm*
 - **kerberos server** *kerberos-realm {hostname | IP Add} [port]*
 - *(the default port number is 88)*
- ❖ You must copy the SRVTAB that was created, on the KDC, to the router. Use the following command, on the router:
 - **kerberos srvtab remote** *{hostname | IP Add} filename*
- ❖ Time is very important in Kerberos. All hosts should be running the Network Time protocol (NTP) as they must interact with each other within a certain period of time.
- ❖ In Unix, the Kerberos configuration file is called *krb.conf*
- ❖ To now enable Kerberos as the authentication method on the router for login authentication, do:
 - **aaa authentication login default krb5_telnet**
- ❖ You could also use kerberized-telnet so that the passwords are not sent in clear-text.

Learn more about Kerberos at the [official MIT site with this link](#).

Learn more about [Cisco Kerberos at this link](#).

Virtual Private Dial-up Networks (VPDN/Virtual Profiles)

- ❖ VPDN (Virtual Private Dial Networks) are VPN networks that are periodically connected, typically through some dialup method. For instance, say a laptop user is traveling, dials up to an ISP, then uses a “Dial Up Networking” VPN connection to connect, over the Internet, to his/her company network. This is an example of a VPDN network.
- ❖ Do not confuse a VPDN network with a dedicated VPN network. A dedicated VPN network is different as it is more of a permanent network connection between two networks, tunneled/transported through another network.
- ❖ Associate VPDN as the server portion of your typical VPN Client connection, typically found on a PC.
- ❖ You could use Cisco's VPDN functions on your router to give VPN Clients access to your network. A popular alternative to this is for an ISP to provide VPN connectivity to your network as a service to you, using the VPDN functions.
- ❖ Of course, VPDN connections should be authenticated properly. As we are talking about Security, AAA is an especially important aspect of VPDN.

A sample VPDN configuration looks like this:

```

vpdn enable
vpdn incoming NAS mynew virtual-template 1
interface Loopback0
ip address 192.168.1.1 255.255.255.0
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool mypool
ppp authentication pap
ip local pool mypool 172.16.1.1 172.16.1.32
vpdn-group 1
! Default PPTP VPDN group
accept-dialin
protocol pptp
virtual-template 1

```

- ❖ One of the important, but frequently forgotten, commands is “vpdn enable”
- ❖ VPDN's can use either of these three Layer 2 tunneling protocols: PPTP, L2TP, or L2F. PPTP is Microsoft proprietary, L2F is Cisco proprietary, and L2TP is an IETF standard.
- ❖ Mainly, just be familiar with the function of a VPDN. If you were to configure your router, or PIX, to be able to provide a periodic VPN connection to it or to a network that is connected to it, you would probably use VPDN.

Learn more about [VPDN at this link](#).

Data Encryption Standard (DES)

Encryption

Encryption is the scrambling of data during transmission to reduce the possibility of an unauthorized person accessing the information on route. This scrambling is accomplished through the use of a cryptography algorithm run on the actual data before it is sent; the same algorithm then decrypts the message at the destination. Remember that encryption can add significant overhead to both the routing platforms.

A Key (or cipher) is a variable added to the algorithm that both sides must have for the message to be properly encoded and decoded. To pass data a public key is generated from a private key known only to the source and destination. The public key cannot be used to decipher data encrypted without the private keys. The public key can then be transmitted securely, because the key itself must be deciphered before it can be used to decipher the actual data.

Data Encryption Standard (DES) is a common encryption standard. It is the standard encryption-key algorithm used by the U.S. government. The original standard called for 56-bit encryption domestically, and 40-bit encryption for export.

- ❖ The keys used for DES are the same keys on each side, or symmetric keys.
- ❖ If I asked you how many bits the key for DES is, the answer is 56. This means that you can calculate the number of possible keys as 2^{56} or $2^{56} = 72057594037927936$ possible keys.

You can read [more than you ever wanted to know about DES at this link](#).

Triple DES (DES3)

Triple DES – DES3 encrypts the original data three times over with the 56-bit keys, making the equivalent of up to a 168-bit key, while maintaining backward compatibility with the original DES standard.

- ❖ If I asked you how many bits the key for 3DES is, the answer is 168. This means that you can calculate the number of possible keys as 2^{168} or $2^{168} = 3.7414441915671114706014331717537e+50$ possible keys. That is a lot of keys.
- ❖ 3DES encryption software is not exportable outside the United States.

IP Secure (IPSec)

IPSec

IPSec is a framework of open standards developed by the IETF to provide security for transmission of sensitive information over unprotected networks, such as the Internet. It allows data to be routed across a public network without fear of observation, modification, or spoofing. Its primary use is to allow secure Virtual Private Networks (VPNs), which can be used to allow Intranets, Extranets, and remote access for users.

IPSec provides services that are similar to those provided by the earlier proprietary Cisco Encryption Technology (CET), but IPSec is more robust and has the advantage of being an open standard. It also provides data authentication and anti-replay, in addition to data confidentiality services, while CET provides only data confidentiality services.

IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers. It has two primary advantages over previous tunneling and encryption technologies:

- ❖ **Multivendor support** – The IPSec standard is supported by many vendors for use in routers, firewalls, and client desktop products.
- ❖ **Scalability** - IPSec was designed to support large enterprises, and has "built-in" key management not found in previous security protocols.

IPSec provides the following optional network security services. In general, the local security policy will dictate the use of one or more of these services:

- ❖ **Data Confidentiality** - The IPSec sender can encrypt packets before transmitting them across a network.
- ❖ **Data Integrity** - The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- ❖ **Data Origin Authentication** - The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- ❖ **Anti-Replay** - The IPSec receiver can detect and reject replayed packets.

The most important IPSec standard sub-protocol is IKE (Internet Key Exchange). IKE is only used to establish Security Associations (SA) for IPSec, which it does by negotiating an ISAKMP SA relationship with a defined peer. Because IKE negotiates the policy, it is possible to configure multiple policies in different configurations, then let the two ISAKMP peers come to an agreement. The features ISAKMP will negotiate include:

- ❖ **Encryption Algorithm** - DES, 3DES, or in the future AES
- ❖ **Hashing Algorithm** - MD5 or SHA
- ❖ **Authentication** - Signatures, Encrypted nonces (random numbers), or pre-shared keys
- ❖ **Lifetime** – The lifetime of the SA, stated in seconds.

There are three methods of configuring ISAKMP:

- ❖ **Pre-shared keys** – Easy to setup
- ❖ **Certificate Authority** – Scalable solution
- ❖ **DNS Secure (DNSSec)** - Not commonly supported

IPSec Glossary

- ❖ **Certification Authority (CA)** - A third-party entity that is responsible for issuing and revoking certificates. Each device that has its own certificate and the public key of the CA can authenticate every other device within that CA's domain. Remember that CA is not just the abbreviation for the state of California.
- ❖ **Certificate** - A cryptographically signed object that contains an identity and a public key associated with an identity.
- ❖ **Certificate Revocation List (CRL)** - A digitally signed message that lists all the current but revoked certificates listed by a given CA. This is similar to a list of stolen credit card numbers that allows banks and merchants to reject bad credit cards.
- ❖ **Authentication Header (AH)** - A security protocol that provides authentication and optional replay detection. AH is embedded in the data to be protected. AH can be used either by itself or with an Encryption Service. AH is IP Protocol 51 and RFC 2402.
- ❖ **Encapsulating Security Payload (ESP)** - A security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. ESP completely encapsulates user data. ESP may be used either by itself or in conjunction with AH. Refer to RFC 2406: IP Encapsulating Security Payload (ESP). ESP is IP Protocol 50.
- ❖ **Hash** - A one-way function that takes an input message of arbitrary length and produces a fixed-length digest. Most IPSec implementations support both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes.
- ❖ **Message Digest 5 (MD5)** - MD5 is a one-way hashing algorithm that produces a 128-bit hash. MD5 is a variation on MD4 designed to strengthen the security of the MD4 hashing algorithm.
- ❖ **Secure Hash Algorithm (SHA)** - SHA is a one-way hash put forth by NIST. SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to brute-force attacks than 128-bit hashes, like MD5.
- ❖ **HMAC** - A mechanism for message authentication using cryptographic hashes such as SHA and MD5. Refer to RFC 2104 for more information.
- ❖ **Diffie-Hellman** - A method of establishing a shared key over an insecure medium. Oakley and IKE use Diffie-Hellman as their key exchange mechanism. I like to describe this as two parents having a conversation in front of their kids, without the kids knowing what the parents are talking about.

- ❖ **Oakley** - A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm. You can find the standard in RFC 2412: The OAKLEY Key Determination Protocol.
- ❖ **Internet Key Exchange (IKE)** - A hybrid protocol that uses part Oakley and part of another protocol suite called SKEME inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each VPN device must be able to verify the identity of its peer. Refer to RFC 2409: The Internet Key Exchange (IKE).
- ❖ **Internet Security Association and Key Management Protocol (ISAKMP)** - A protocol framework that defines the mechanics of implementing a key exchange protocol and negotiation of a security policy.
- ❖ **Perfect Forward Secrecy (PFS)** - PFS ensures that a given IPSec SA's key was not derived from any other secret key. In other words, if someone were to crack a key, PFS ensures that the attacker would not be able to derive any other key. If PFS is not enabled, someone could hypothetically break the IKE SA secret key and copy all the IPSec protected data. With PFS, breaking IKE would not give an attacker immediate access to IPSec. The attacker would have to break each IPSec SA individually.
- ❖ **Security Association (SA)** - An instance of security policy and keys applied to a data flow. Both IKE and IPSec use SAs, although the SAs are independent of one another. IPSec SAs are unidirectional, and they are unique in each security protocol. A set of SAs is needed for a protected data pipe, one per direction per protocol. IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually. An IKE SA is used by IKE only and, unlike the IPSec SA, is bi-directional.
- ❖ **Transform** - A transform describes a security protocol (AH or ESP) with its corresponding algorithms. For example, ESP with the DES cipher algorithm and HMAC-SHA for authentication.
- ❖ **Transport Mode** - An encapsulation mode for AH/ESP. Transport Mode encapsulates the upper layer payload (TCP or UDP) of the original IP datagram. This mode can only be used when the peers are the endpoints of the communication; i.e., Client-to-Client VPNs.
- ❖ **Tunnel Mode** - Encapsulation of the complete IP datagram for IPSec. Tunnel Mode is used to protect datagrams that are not sourced from the IPSec devices themselves. This is the mode used in Server-to-Server and Client-to-Server VPNs. Tunnel mode is ideal for hosts with private IP addresses (RFC 1918 addresses) to connect through a VPN over the public Internet.
- ❖ As mentioned above, IPSec combines IKE, ESP, and AH to get the job done. ESP and IKE are, most typically, used together with AH being more of an option.
- ❖ IPSec uses the MD5 or SHA-1 hash algorithms. MD5 is 128 bit and SH is 160 bits. SHA-1 takes longer to calculate but its considered being more secure.
- ❖ Diffie-Hellman has two groups, group 1 and group 2. Group 1 is 768bits and Group 2 is 1024bits.
- ❖ Cipher Text is data that has been encrypted. To unencrypt cipher text, the receiver must have the appropriate key.
- ❖ Can IPSec be applied to broadcast or multicast packets? No- IPSec only works with unicast packets.

Configuration of IPSec in Cisco IOS


As IPSec & IKE are quite complex, it can be complex to configure them.

Note the following:

- ❖ IKE must either be configured, as part of configuring IPSec, or it must be disabled.
- ❖ Note that IKE uses UDP/500 and IPSec uses protocols 50 and 51. (500,50,51)
- ❖ The default lifetime of an IPSec Security Association (SA) is 3600 seconds (one hour).
- ❖ Access-lists between two peers should, typically, be a mirror of each other (mirrored). In other words, they should be opposite, or, for example:
 - Host A- permit host A traffic X to host B traffic Y
 - Host B- permit host B traffic Y to host A traffic X
- ❖ A packet must be defined as interesting (match an access-list) to be included in the IPSec tunnel.
- ❖ The access-list is defined in the crypto-map.
- ❖ Cisco does not recommend ever using the “any” keyword in a crypto access-list. You should know exactly what traffic is being encrypted and what traffic is not.
- ❖ Four basic steps to configure IPSec include:
 - Define an access list:


```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```
 - Define a transform set:


```
crypto ipsec transform-set theset esp-des esp-sha
```



Are You Ready to Take the Exam?

Comprehensive Exam Preparation:

- Progress tracking
- Detailed answers and explanations
- Packed with quality practice questions
- Customizable learning features

[Try a Demo Now](#)

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified

Get this **Study Guide** and many more for **FREE** at

CramSession
www.cramsession.com

Use the crypto map to join the access-list and transform-set

```
crypto map mymap 10 ipsec-isakmp
```

```
match address 101
```

```
set transform-set theset
```

```
set peer 192.168.2.12
```

- Apply the crypto map to an interface

```
interface Serial 0/0.1
```

```
ip address 192.168.1.1
```

```
crypto map mymap
```

Learn more about [Cisco IOS IPsec Configuration at this link](#).

Here is a [link to Cisco IPsec sample configuration documentations](#).

Checkout this Cramsession.com article on "[Understanding IPsec](#)".

Internet Key Exchange (IKE)

IKE (Internet Key Exchange) negotiates the IPsec tunnel settings between two IPsec peers. Cisco says this about IKE:

- ❖ IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

There is always confusion between the purposes of IKE vs. ISAKMP. One of the reasons is that many people use IKE and ISAKMP synonymously. The following text is taken from [this link](#):

"The ISAKMP protocol [3] is a key management framework for transferring key and authentication data independent of the key generation process. IKE builds on this generic ISAKMP protocol framework to precisely define a set of protocol exchanges that set up a secure channel for key management, as well as the exchange of key and authentication data.

Generalized payloads for exchanging key generation and authentication data are defined by ISAKMP [3]. IKE [4] specifies a precise usage of these generic payloads for setting up a secure channel (phase 1 SA). This channel can then be used to securely achieve key management for a specific security protocol (so-called a Domain of Interpretation - DOI) such as IPsec (IPsec DOI). The combination of IKE/ISAKMP with a Domain of Interpretation (DOI) defines the specifics of key exchange in the context of a specific security protocol such as IPsec."

Hopefully this clears up some of the confusion between IKE and ISAKMP. In general, IKE and ISAKMP are very similar. As you can see from the above text, if you look at the definitions, they are certainly different. However, when you are talking, in general, about IPSec, if you know that IKE/ISAKMP are basically the same thing, you will be fine.

IKE characteristics:

- ❖ IKE has two phases:
 - Phase One- Main or Aggressive Mode
 - Phase Two- Quick Mode
- ❖ The same things are accomplished in Phase One if you use Main or Aggressive modes. The difference is that, with aggressive mode, the IKE communications are not encrypted, as with Main mode.
- ❖ In Phase One, the two peers agree on parameters, authenticate, and generate keys.
- ❖ In Phase Two, Quick Mode, the peers agree on attributes used to create encrypted IPSec security associations (for ESP).
- ❖ Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.
- ❖ Also in Phase Two, if using PFS, the Diffie-Hellman exchange is renegotiated.
- ❖ IKE has three authentication mechanisms. They are:
 - Preshared Keys – Long and difficult to use as your network grows, don't require a CA.
 - Digital Signatures (RSA Signatures) – Provide non-repudiation (you can prove to a third party that you did perform IKE negotiation with the IKE peer, definition below). This type uses Certification Authorities (CAs) to certify that the IKE device is “who it says it is”.
 - Encrypted Nonces (RSA Encrypted Nonces) – Provide repudiation (you CANNOT prove to a third party that you did perform IKE negotiation with the IKE peer, definition below). In other words, no one can prove that the communication ever took place. (Protects against man-in-the-middle attacks).
- ❖ Okay, so what are “nonces”? According to the Cisco Press Book, “Network Security Principles and Practices”, Nonces are “pseudo-random numbers exchanged between the peers and used in the generation of the SKEYS”. Nonces can protect against “man in the middle attacks”.
- ❖ What does the CA provide?
 - Its certificate

- The requested device's name, IP address, and organization
- A record that the transaction occurred
- ❖ Both peers must trust the same Certificate Authority for the association to form.
- ❖ Public & Private Keys are very important when it comes to IKE and IPSec.
 - Public keys and private keys do two things.
 - Provide Confidentiality – What is encrypted with the private key can only be decrypted with the public key. What is encrypted with the private key can only be decrypted with the public key.
 - Provide Authentication – A device can send data that was encrypted with the private key to another device who can then, encrypt it with the public key. Thus, the remote device knows that the original device must be authentic, as it must have had the private key.
 - The public key is owned by whatever device wishes to communicate securely with a host.
 - The private key is only owned by its host.
- ❖ The Merriam-Webster Dictionary offers the following definition for repudiation:
 - Main Entry: **re-pu-di-a-tion**
Pronunciation: ri-"pyü-dE-'A-sh&n
Function: *noun*
: the act of [repudiating](#) : the state of being [repudiated](#); *especially* : the refusal of public authorities to acknowledge or pay a debt
- ❖ So, remember the different between:
 - Repudiation – A third-party **cannot** prove something for you.
 - Non-Repudiation – A third party **can** prove something for you (that you did perform IKE negotiation with the IKE peer, in this case).

You can learn more about [IKE at this link](#).

Certificate Enrollment Protocol (CEP) (aka SCEP)

CEP is now also known as (aka) SCEP (Simple Certificate Enrollment Protocol). This is the protocol is used between a device wishing to use a certificate (in our case, probably a router or a PIX) and the certificate server.

Cisco's site has this definition of CEP:

“Certificate Enrollment Protocol (CEP) - A certificate management protocol jointly developed by Cisco Systems and VeriSign, Inc. CEP is an early implementation of Certificate Request Syntax (CRS), a standard proposed to the Internet Engineering Task Force (IETF). CEP specifies how a device communicates with a CA, including how to retrieve the CA's public key, how to enroll a device with the CA, and how to retrieve a Certificate revocation list (CRL). CEP uses RSA's PKCS (public key cryptography standards) 7 and 10 as key component technologies. The IETF's public key infrastructure working group (PKIX) is working to standardize a protocol for these functions, either CRS or an equivalent. When an IETF standard is stable, Cisco will add support for it.”

To use digital certificates for IPSec purposes, you must have a Certificate Authority (CA) available on your network. This CA must support Cisco's SCEP protocol.

While IPSec can be implemented without certificates, certificates will provide the following benefits:

- ❖ Ease of management and configuration as the network grows and changes.
- ❖ Centralized management of certificates.
- ❖ Authenticity of the peer that you are communicating with on the other side of the IPSec connection.

To use IPSec without a CA, a router must use either encrypted nonces or preshared keys.

Each router may check the certificate revocation list (CRL), on the CA, before accepting a certificate.

You must assign a hostname and a domain name to your router as this is used with IPSec negotiation and the CA.

To generate keys on your router, type:

- ❖ **crypto key generate rsa**

The two required commands to define your CA are:

- ❖ **crypto ca identity** *name*
- ❖ **enrollment url** *url*

The router must, then, authenticate the CA:

- ❖ **crypto ca authenticate** *name*

And then, you must request your certificates:

- ❖ **crypto ca enroll *name***

To show your router's public keys run:

- ❖ **show crypto key mypubkey rsa**

To show your router's certificates type:

- ❖ **show crypto ca certificates**

Learn more about [IOS Configuration of Certificate Authorities at this Cisco link](#).

Learn more about [CEP at this Cisco link](#).

Learn more about [SCEP \(Simple Certificate Enrollment Protocol\) at this link](#).

Point to Point Tunneling Protocol (PPTP)

PPTP is used to tunnel one network's traffic over another network. Thus, this is a VPN technology. PPTP is one of the three possible VPN protocols that can be used on Cisco equipment (the others are L2F and L2TP, discussed below).

The PPTP protocol was created with the help of Microsoft and a number of other networking vendors. Cisco came up with their own, L2F (Layer 2 Forwarding). PPTP is an extension of PPP.

- ❖ PPTP supports multiple protocols: IP, NetBEUI, and IPX.
- ❖ PPTP uses MS-CHAP and MD4 for encrypted authentication. The session key, from that encrypted authentication, is used to encrypt the payload of the packet.
- ❖ PPTP does not require certificates or a CA.
- ❖ Cisco support PPTP.
- ❖ An IOS access-list that allows PPTP in looks like this:

```
access-list 100 permit tcp any gt 1023 host 13.161.251.7 eq 1723
```

```
access-list 100 permit gre any host 13.161.251.7
```

- ❖ Microsoft Windows PC's come with PPTP clients in the operating system.
- ❖ PPTP would primarily be configured on a router using VPDN. There is an example of this configuration in the VPDN section of this document.

Learn more about [Cisco's PPTP at this link](#).

Learn more about [Microsoft's PPTP at this link](#).

Layer 2 Tunneling Protocol (L2TP)

L2TP (Layer 2 Tunneling Protocol) is a VPN technology used to tunnel PPP packets from one network, over a public network, to the Internet.

L2TP is an IETF standard that, according to Cisco, "combines the best features of the two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's PPTP (Point to Point Tunneling Protocol).

- ❖ An interesting chart, taken from the following Cisco link, shows the comparison between the various VPN protocol terminology:

VPN Hardware Terminology Generic Term	L2F Term	L2TP Term	PPTP Term
Tunnel Server	Home Gateway	L2TP Network Server (LNS)	PPTP Network Server (PNS)
Network Access Server (NAS)	NAS	L2TP Access Concentrator (LAC)	PPTP Access Concentrator (PAC)

([Taken from this link](#).)

- ❖ L2TP can tunnel any layer 3 protocols. The L3 protocol is unaware of L2TP, as L2TP operates at layer 2.
- ❖ L2TP does not provide for Encryption but relies on IPSec for encryption.
- ❖ L2TP is based on [RFC2661](#). The side that initiates the L2TP protocol chooses an available source port and L2TP always uses the destination UDP port 1701.
- ❖ This port 1701 is also used for Cisco's L2F, also known as [RFC2341](#).
- ❖ Configuring L2TP is complex and would also require the configuration of AAA and VPDN, among other things.

You can learn more about [configuring L2TP at this Cisco link](#).

Also, check out this [Cisco link to a "L2TP Technology Brief"](#).

Operating Systems

UNIX

You should be knowledgeable of basic Unix security practices and terminology.

- ❖ The “all powerful”, “super-user” account, in Unix, is the “root” account. The root account has a user ID (also known as a GID) of 0 (zero). If another user in the `/etc/passwd` or `/etc/shadow` files has a user ID of zero, then they are a root equivalent user. This would be of great security concern.
- ❖ In some versions of Unix, usernames and passwords are stored in the `/etc/passwd` file. That file must be readable by everyone. As the passwords are in a simple encryption algorithm, this is a security risk. It is recommended, and standard today in many Unix systems, that the passwords be stored in the `/etc/shadow` file, accessible only by root.
- ❖ When a user attempts to login to a Unix server, the login program validates the user, checks his username, password, and other security checks. These include checking to see if they are allowed to login on that particular device. If the login is successful, the login program initiates the user’s environment, makes an entry in the `/etc/utmp` file, tracks the login to perform entries in the `/var/adm/wtmp` file (used for accounting purposes), and does things like display the message of the day. If the login is unsuccessful, the login program makes an entry in a “failed login” file. (In AIX, for instance, this is called `/etc/security/failedlogin`. In Sun Solaris, this is called `/var/adm/loginlog`.)
- ❖ In Sun Unix (Solaris), every successful, or unsuccessful attempt to change from a regular user to the super user (root), using the `su` command, is logged in `/var/adm/sulog`. A good Unix security administrator should check this file regularly.

File Permissions

In Unix, only the owner of the file or root can modify file permissions.

Files have an owner and a group setting. For example, the following file is owned by “bob” and has group permissions for the “ops” group

```
-rw-rwx-w- 3 bob ops 104580 Sep 16 12:02 myfile
```

You can change the owner with the `chown` command, and the group with the `chgrp` command.

File permissions are set by being “r”, read, “w”, write, “x”, execute “-”, none, or other special permissions. These are assigned for three areas for each



The PrepLogic Mega Guide

PrepLogic took the CramSession Study Guide and made it better!

- Over 100 pages
- More in-depth content
- Expanded resources
- Includes review practice questions

Get \$10 Off
Get it Now

Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Cautious. Get Certified.

Get this **Study Guide and many more** for **FREE** at

CramSession
www.cramsession.com

file, for the owner of the file, the group the file belongs to, and everyone else, or “other”. Here is an example:

```
-rwxrwxr-x 3 bob ops 104580 Sep 16 12:02 /usr/bin/passwd
```

In the above example, the first “-“ tells you that this is a file and not a “special file”. Then, the next “rwx” says that it is readable, write able, and executable by the owner, “bob”. The next “rwx” says the same thing for the group the file belongs to, “ops”. Finally, the last set “r-x” says that the file is readable and executable by everyone else but not write able by everyone else.

An example of special permissions is the SETUID bit. This says that anyone who executes the file gets the permissions of the user who owns the file. Obviously, this could be a security risk, especially if the root user owns the file. The following file is marked with the SETUID bit:

```
-r-sr-sr-x 3 root sys 104580 Sep 16 12:02 /usr/bin/passwd
```

When we talk about file permissions, in Unix, we are also talking about directories, or any other special files. This is because, in Unix, “everything is a file”, meaning, that things like directories, links, or devices are all represented by files and each has its own permissions.

There are two ways to set file permissions, absolute and symbolic.

Both are done with the **chmod** command. Its usage is:

- ❖ Absolute – Using the octal (numeric) values to set permissions where each of the numbers, of the three octal numbers used, represent User, Group, and then other. Absolute changes the permissions to what you specify, regardless of the existing permissions. The existing permissions are lost and the new permissions are put in place.

Usage- **chmod ### filename**

- Example- **chmod 662 myfile**
- Reference the Absolute chart, below, and you'll see that 662 will set the following permissions:

```
-rw-rw--w- 3 bob ops 104580 Sep 16 12:02 myfile
```

- Most of the time, you will be using chmod just as it is above. However, you can also use chmod like this:
- Usage- **chmod ##### filename**
- Yes, with FOUR possible numbers. The first one, on the left, has been added on. This is the “special permission” column. The possibilities for this column are below in the “special permission” chart.
- Thus, an example would be to set the SETUID bit.

- Example- **chmod 4770 myfile**

```
-rwsrwx--- 3 bob ops 104580 Sep 16 12:02 myfile
```

- ❖ Symbolic – Using letters and operators to get the same thing done. In symbolic, you specify “who” gets the permissions, the “operator”, and the permissions. Symbolic does this by leaving what are already the permissions and only appending to them, or removing from them, the settings you request. Reference the Symbolic chart, below, to see your choices.

- Usage- **chmod who operator permission filename**

- Example- **chmod g+x myfile**

- Reference the chart below and you’ll see that 662 will set the following permissions (you know the previous permissions were what is below with the addition of the group executable permission):

- **-rw-rwx-w-** 3 bob ops 104580 Sep 16 12:02 myfile

- Thus, an example would be to set the SETGID bit.

Example- **chmod g+s myfile**

```
-rwxrws--- 3 bob ops 104580 Sep 16 12:02 myfile
```

The following three tables on file permissions are taken from the Solaris 9 Documentation link, referenced below.

Setting File Permissions in Absolute Mode:

Octal Value	File Permissions Set	Permissions Description
0	---	No permissions
1	--x	Execute permission only
2	-w-	Write permission only
3	-wx	Write and execute permissions

Octal Value	File Permissions Set	Permissions Description
4	r--	Read permission only
5	r-x	Read and execute permissions
6	rw-	Read and write permissions
7	rwX	Read, write, and execute permissions

Setting Special Permissions in Absolute Mode:

Octal Value	Special Permissions Set
1	Sticky bit
2	Setguid
4	Setuid

Setting File Permissions in Symbolic Mode:

Symbol	Function	Description
u	Who	User (owner)
G	Who	Group
O	Who	Others

Symbol	Function	Description
A	Who	All
=	Operator	Assign
+	Operator	Add
-	Operator	Remove
R	Permission	Read
W	Permission	Write
X	Permission	Execute
I	Permission	Mandatory locking, setgid bit is on, group execution bit is off
S	Permission	setuid or setgid bit is on
S	Permission	suid bit is on, user execution bit is off
T	Permission	Sticky bit is on, execution bit for others is on
T	Permission	Sticky bit is on, execution bit for others is off

A useful and important Unix command to display network status and open ports is **netstat**. Take a look at its [usage and example output at this link](#).

The [Solaris 9 Documentation on "Managing System Security"](#) can be found at this link.

This [link has a list of Unix Security Recommendations from CERT](#).

Windows (NT/95/98/2000)

You should be knowledgeable of basic Windows security practices and terminology.

- ❖ The equivalent account, in Windows, to the Unix root account is the “administrator” account.
- ❖ You should be cautious about anyone being a member of the “administrator group” as they have administrator equivalent privileges.
- ❖ Windows 95 and 98 use the FAT or FAT32 file systems. These do not have any sort of user, group, or file permissions.
- ❖ Windows NT, 2000, and XP use the NTFS file system. NTFS has user, group, and file permissions. It also offers EFS, or encrypted file system.
- ❖ Windows 2000/XP file permissions are typically set from a GUI interface. A file can have the following permissions:
 - Full control
 - Modify
 - Read
 - Read & Execute
 - Write

Learn more about [setting Windows File Permissions at this link](#).



Who Do You Trust for Your Certification Training?

PrepLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

PrepLogic Comprehensive Training Tools:
CBT • Practice Exams • Audio Training • Mega Guides • Discount Exam Vouchers

For Free Product Demos, [Click Here](#).

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide and many more** for **FREE** at

CramSession
www.cramsession.com

Windows NT/2000 Groups:

- ❖ Global groups - Stored on domain controllers. Available to any computer within a domain. Contain users from anywhere in the domain. **Cannot contain other groups**. Only Windows NT servers can host global groups.
- ❖ Local groups - Usually local to a single computer. Local groups can contain domain accounts or global groups, but cannot contain other Local groups.
- ❖ Users should be added to global groups, which should be added to Local Groups. Local groups are then assigned permissions to access resources.

In the Windows environment, there are Share (network shared folders/directories) and NTFS permissions. Above, we were talking about NTFS permissions. When you take a NTFS folder (directory) and share it, there are share permissions assigned. In most versions of Windows, the default share permission is EVERYONE. This is definitely a security concern.

Shares are referenced by their UNC (Universal Naming Convention) name. An example is \\FILESERVER\SHARED-FOLDER. On the other hand, files & folders are referenced by their drive letter, folder, and filename. An example is C:\FOLDER\MY-FILE.TXT

Share permissions are **first** checked and must be met before NTFS permissions are met. That means that, say, you had a folder called C:\XYZ. It has NTFS permissions Full Control assigned to the “HR Group” and “General Manager”. You share that folder and assign Read permissions to the “General Manager” Group. Who can access that SHARED folder? The answer is, only the “General Manager” Group can READ the folder, NO OTHER ACCESS IS PERMITTED (yes, even though the GM group and HR group both have FULL CONTROL in NTFS).

Also, remember that DENIED permissions override all other permissions. So, if Bob is a member of the HR group and the Bob has FULL CONTROL to a directory but HR is DENIED access then, so is Bob.

A FAT or FAT32 file system only has shared access and it is limited to Read, Modify, or Full Control.

A useful and important Windows command to display network status and open ports is **netstat** – its options look like this:

```
C:\>netstat -h
```

Displays protocol statistics and current TCP/IP network connections.

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

-a Displays all connections and listening ports.

-e Displays Ethernet statistics. This may be combined with the –s option.

-n Displays addresses and port numbers in numerical form.

-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.

Interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

Checkout this [great article on shared vs. NTFS permissions](#), from Cramsession.com.

Application Protocols

The RFC that specifies the named (assigned) TCP/IP port numbers for all well-known applications is [RFC1700](#).

Domain Name System (DNS)

DNS is the Domain Name System. It resolves IP addresses to domain names. It does this in a hierarchical (treed) method. The root domain is "." (or dot). From there, the tree goes down to the next level (branch) of sub-domains. For instance, ".com", then down to the next level, like "Cramsession.com", then to, perhaps, [www.Cramsession.com](#).

- ❖ When you type in a domain name to surf with your web browser, run a telnet session, or just ping an Internet host, a DNS resolution is done. Without DNS, the resolutions would fail and you would have to use IP addresses.
- ❖ DNS uses TCP and UDP port 53.
- ❖ There are 30+ RFC's that cover DNS, but a couple of the primary ones are [RFC1035](#) and [RFC2181](#).
- ❖ The PIX firewall offers a feature to help prevent DNS-based DoS attacks. A DNS Dos attack occurs when the attacker falsely says that it is a DNS server that has received a request from a client and then floods the client with responses. The PIX attempts to prevent this by:
 - Only allowing one DNS response from a DNS server
 - Closing DNS translations as soon as the first DNS server responds to requests
- ❖ To configure DNS lookup on an IOS router, do the following:
 - **ip name-server** *server-address1 server-address2 ...*
 - **ip domain-lookup**

- ❖ An access-list example that permits DNS lookups is:

```
access-list 100 permit tcp any host 163.161.251.4 eq domain
```

```
access-list 100 permit udp any eq domain host 163.161.251.4 gt 1023
```

Checkout this Cramsession.com article on "[How DNS Queries Work](#)".

Read more about [configuring the Cisco IOS for DNS at this link](#).

Trivial File Transfer Protocol (TFTP)

TFTP is a basic file-transfer protocol. It uses UDP and offers very limited features. It is typically used to transfer BOOTP images, upgrade routers, or transfer configuration files.

- ❖ TFTP is based on [RFC1350](#).
- ❖ TFTP has no user authentication and cannot list remote files. Its only ability is to read or write files from one system to another.
- ❖ TFTP uses port 69.
- ❖ TFTP is frequently used to copy images or configurations to Cisco routers. Example:

```
copy tftp: [///location/]directory/filename] flash-filesystem:[filename]
```

- ❖ As TFTP has no authentication it is very unsecure. FTP is preferred over TFTP for security and reliability reasons.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a protocol that transfers files between one host and another. FTP has a number of features and is much preferred over TFTP.

- ❖ FTP uses a username and password but it is not encrypted and thus still not a secure protocol.
- ❖ FTP uses TCP/UDP port 20 for data and TCP/UDP port 21 for connection setup and control.
- ❖ An IOS access-list to permit FTP request out would look like this:

```
access-list 100 permit tcp host 162.161.251.10 eq ftp any gt 1023
```

```
access-list 100 permit tcp host 162.161.251.10 eq ftp-data any gt 1023
```

- ❖ The RFC for FTP is [RFC959](#).
- ❖ Take a look at the [Cisco IOS documentation on configuring FTP](#).

Hypertext Transfer Protocol (HTTP)

HTTP is the protocol that web pages are requested for and supplied in. HTTP is very likely the protocol that you used to retrieve this information from the Internet.

- ❖ HTTP uses port 80
- ❖ HTTP Version 1.1 is based on [RFC2068](#).
- ❖ An IOS access-list that permits HTTP looks like this:

```
access-list 100 permit tcp any host 63.161.251.2 eq www
```

- ❖ Cisco supports web based (HTTP) management of routers. It is not enabled by default on most routers. To enable http management, run:
 - **ip http server**
- ❖ If you must use this, you should set authentication and only permit it from specific IP addresses. To do these things, run:
 - **ip http authentication { aaa | enable | local | tacacs }**
 - **ip http access-class { access-list # | access-list name }**
- ❖ If you are going to pass any sensitive information, using HTTP, you should use HTTPS or HTTP with SSL. (See below.)

Secure Socket Layer (SSL)

HTTP over TLS, HTTP/TLS, or HTTPS, is based on [RFC2818](#) and uses port 443.

An IOS access list to allow SSL is:

```
access-list 100 permit tcp any host 13.161.251.2 eq 443
```

Other facts about SSL:

- ❖ Netscape originally developed SSL.

- ❖ The IETF standard for SSL is called TLS. The TLS RFC is [RFC2246](#). The RFC on layering HTTP over TLS (SSL) is [RFC2818](#).
- ❖ SSL authenticates server and client as well as providing encryption between the two (confidentiality).
- ❖ SSL can prevent a man-in-the-middle attack by the client verifying the server domain name matches the domain name in the certificate from that server.

Netscape offers a good [introduction to SSL at this link](#).

The [Netscape SSL 3.0 draft is available at this link](#).

Simple Mail Transfer Protocol (SMTP)

SMTP is the standard protocol for sending mail. This is the protocol that a server uses to send mail from one server to another or for a client to use to send mail to the server.

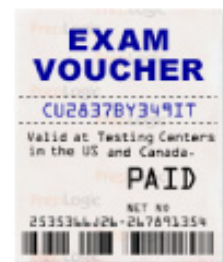
- ❖ SMTP is not used by a client to receive mail. That would be, typically, either POP3 or IMAP.
- ❖ SMTP uses port 25.
- ❖ An access-list to allow SMTP in and out, for a mail server, would be:

```
access-list 100 permit tcp any eq smtp host 63.161.251.2 gt 1023
```

```
access-list 100 permit tcp any host 63.161.251.2 eq smtp
```

- ❖ The RFC for SMTP is [RFC2821](#).
- ❖ Cisco routers do not use SMTP other than to either allow it or not allow it in an access-list.
- ❖ A PIX firewall feature is MailGuard. MailGuard will protect a SMTP server by only allowing seven commands in, through the firewall, to the mail server. This helps to prevent an attack on the mail server. You can enable this feature by doing **fixup protocol smtp 25**. However, this feature does not work well with Microsoft Exchange, as it uses ESMTP.

Take Your Exam for Less!



Discount Exam Vouchers from PrepLogic

Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

Buy Your Voucher Now

PrepLogic

Be Prepared. Be Confident. Get Certified.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is used to synchronize the time between devices on a network.

NTP is based on [RFC1305](#), uses port 123 and is disabled, by default, on IOS routers.

To enable NTP in IOS do the following:

- ❖ Use the **ntp server** command if this will be a NTP server.
- ❖ Use the **ntp peer** command if this will be a NTP client.
- ❖ NTP supports MD5 authentication so you should use it. To configure NTP authentication do:
 - **ntp authenticate**
 - **ntp authentication-key *number* md5 *value***
- ❖ NTP also supports access-groups where you can define the IP addresses of hosts and their functions. Use the **ntp access-group** command to do this.

Checkout the [Cisco link for Configuring NTP](#).

Secure Shell (SSH)

Secure Shell is a protocol and application that provides secure replacement to the Unix-based rsh, rcp, and rlogin commands.

- ❖ There are two types of SSH, version 1 and 2. Cisco only supports version 1.
- ❖ SSH is highly recommended over using telnet as the username/password (as well as the commands) are all encrypted and secured.
- ❖ Before configuring SSH, you must first have an image that supports either DES or 3DES. You must also configure the following:
 - **hostname *hostname***
 - **ip domain-name *domainname***
 - **crypto key generate rsa**
 - At this point, SSH is enabled. You can further configure it using the **ip ssh** commands.

The [Cisco documentation on Configuring SSH is located here](#).

Lightweight Directory Access Protocol (LDAP)

The lightweight directory access protocol (LDAP) is simply used to query a X.500 directory. This directory could be the Windows Active Directory (AD) containing usernames and groups (among other things), it could be a directory of certificates revocations on a certificate server (CA), or it could be a directory containing other information.

- ❖ LDAP is based on [RFC1777](#).
- ❖ LDAP uses TCP port number 389.
- ❖ Cisco primarily uses LDAP in routers to query a CA for a certificate revocation list or CRL.
- ❖ A Cisco router can be configured to query a CA for a CRL with either LDAP or the SCEP.

Active Directory

Active directory is a directory service used by Windows 2000 domain controllers.

Active directory is a “hierarchical namespace of objects that is tightly integrated with DNS”. From this, hopefully, you realize that DNS is required for AD.

There is a long list of ports required for AD to function as well as other services like LDAP. AD communications should be done on a secured network, so typically you won't ever be opening ports for AD services through a firewall to a public network.

Active Directory holds information in domains, trees, and forests.

Windows AD data can be used for Cisco network securing through Windows server features, such as, LDAP, RADIUS, and certificate services.

The NSA offers a [guide to securing Active Directory](#).

General Networking

Networking Basics

General Networking Theory

OSI Models

Most people who attempt the CCIE Written have either gone through the CCNA and CCNP exams, or already have a solid background in networking. In either case, I'm sure you have a solid grasp on the OSI model; but, it's on the blueprint and therefore deserves at least a quick review.

The OSI model is a common tool for conceptualizing how network traffic is handled. For the CCIE track, the bulk of your focus will be on the three lower levels. Just a reminder, you can use the old mnemonic “**All People Seem To Need Data Processing**” as a way to help remember the sequence. The seven layers of the OSI model are:

- ❖ **Application** – Provides services directly to applications.

- ❖ **Presentation** – Provides a variety of coding and conversion functions that ensure information sent from the application layer of one system will be readable by the application layer of another.
- ❖ **Session** – Establishes, manages, maintains, and terminates communication sessions between applications.
- ❖ **Transport** – Segments and reassembles data into data streams, and provides for both reliable and unreliable end-to-end data transmission.
 - **Network** – Applies logical addressing to provide routing and related functions to allow multiple data links to be combined into an internetwork. Network layer protocols include routing and routed protocols (make sure you know the difference between these).
- ❖ **Data Link** – The data link layer provides for reliable transmission of data across physical media. The Data link layer is commonly subdivided into two sub-layers, known as the Media Access Control (MAC) Layer and the Logical Link Control (LLC) layer.
 - **LLC** – The LLC sub-layer manages communications between devices over a single link of a network. It provides error control, flow control, framing, and MAC sub-layer addressing.
 - **MAC** – The MAC layer manages addressing and access to the physical layer.
- ❖ **Physical** – The electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems.

Note: Remember that **routing** is handled at Layer-3 of the OSI model, while **bridging** is handled at Layer-2 of the OSI model.

MAC Addressing

Media Access Control (MAC) is the lower of the two sub-layers of the Data Link Layer defined in the OSI model, which provides access to the shared media. MAC addresses are the standard, unique address that every networked device must have; it is the true burned-in physical address of the Network Interface Card (NIC) in a host, server, router interface or other device on a network. They are 6 bytes (48 bits) long and are controlled by the IEEE. They can be broken down into two sub-fields:

- ❖ The first three bytes (24 bits) are called the Organization Unique Identifier (OUI) field and are issued in series to manufacturers.
- ❖ The second part of the MAC address, the last three bytes (24 bits), is a unique identifier burned into the device by the manufacturer from the series issued to it.

General Routing Concepts

- ❖ **Autonomous Systems (ASs)** - A group of routers sharing a single routing policy; run under a single technical administration; and commonly, with a single Interior Gateway Protocol (IGP). Each AS has a unique identifying number between 1 and 65,535 (64,512 through 65,535 are set aside for private use) usually assigned by an outside authority.
- ❖ **Convergence** – The process of bringing the routing tables on all the routers in the network to a consistent state.
- ❖ **Load Balancing** – Load balancing allows the transmission of packets to a specific destination over two or more paths.

- ❖ **Metrics** – All routing protocols use metrics to calculate the best path. Some protocols use simple metrics, such as RIP, which uses hop count. Others, such as EIGRP, use more meaningful information.
- ❖ **Passive-Interface** – Prevents interfaces from sending routing updates. They will, however, continue to listen for updates. This command is applied in the router configuration, and specifies a physical interface.
- ❖ **Redistribution** - The process of sharing routes learned from different sources (usually routing protocols). For instance, you might redistribute the routes learned through OSPF to a RIP domain, in which case you might have problems with VLSM; or you might redistribute routes learned through static entries into EIGRP. Redistribution is just the sharing of information learned from different sources, and it must be manually configured.
- ❖ **Route Flapping** – The frequent changing of preferred routes as an interface or router goes into and out of operation (error condition). This process can create problems in a network, especially in complex OSPF networks, as this information will cause the routers to constantly recalculate their OSPF database and flood the network with LSAs (Link State Advertisements).
- ❖ **Static Routing** –Static routes can point to a specific host, a network, a subnet, or a super-net. You can also have floating static routes: routes that have an Administrative Distance (AD) set higher than the dynamic routing protocol in use.

Standards

There are several organizations that have taken responsibility for developing and documenting network standards, including:

- ❖ **The Institute of Electrical and Electronics Engineers (IEEE)** – A professional organization that develops communications and network standards. For example, details of all the 802.x protocols can be found on their excellent website at www.ieee.org.
- ❖ **The Internet Engineering Task Force (IETF)** – An international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. You will find a list of the current and developing Requests for Comment (RFCs) at the [IETF website](#).

Protocol Mechanics

Transmission Control Protocol (TCP)

TCP is a connection-oriented Layer-4 (transport layer) protocol designed to provide reliable end-to-end transmission of data in an IP environment. It groups bytes into sequenced segments, and then passes them to IP for delivery.

These sequenced bytes have forward acknowledgment numbers that indicate to the destination host what next byte it should see. Bytes not acknowledged to the source host within a specified time period are retransmitted, which allows devices to deal with lost, delayed, duplicate, or misread packets.

TCP hosts establish a connection-oriented session with one another through a "three-way handshake" mechanism, which synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. Each host first randomly chooses a sequence number to use in tracking bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner:


1. The initiating host (Host-A) initiates a connection by sending a packet with the initial sequence number ("X") and SYN bit (or flag) set to make a connection request of the destination host (Host-B).
2. Host-B receives the SYN bit, records the sequence number of "X", and replies by acknowledging the SYN (with an ACK = X + 1).
3. Host-B includes its own initial sequence number ("Y"). As an example: An ACK of "20" means that Host-b has received bytes 0 through 19, and expects byte 20 next. This technique is called forward acknowledgment.
4. Host-A then acknowledges all bytes Host-B sent, with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1).
5. Data transfer can now begin.

You will find an excellent write up on this process by one of the best authors in networking, Laura Chappell, at:

http://www.nwconnection.com/2000_03/pdf30/hand30.pdf

There is an acknowledgment process associated with TCP. Here is a sample sequence to show how this works:

1. The sender (Host-A) has a sequence of ten bytes ready to send (numbered 1 to 10) to a recipient (Host-B) who has a defined window size of five.
2. Host-A will place a window around the first five bytes and transmit them together, then wait for an acknowledgment.
3. Host-B will respond with an "ACK = 6", indicating that it has received bytes 1 to 5, and is expecting byte 6 next.
4. Host-A then moves the sliding window five bytes to the right and transmits bytes 6 to 10.
5. Host-B will respond with an "ACK = 11", indicating that it is expecting sequenced byte 11 next. In this packet, the receiver might indicate that its window size is 0 (because, for example, its internal buffers are full). Host-A won't send any more bytes until Host-B sends a subsequent packet with a window size greater than 0.



The PrepLogic Mega Guide

PrepLogic took the CramSession Study Guide and made it better!

- Over 100 pages
- Expanded resources
- More in-depth content
- Includes review practice questions

Get \$10 Off
Get it Now

Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide** and many more for **FREE** at

CramSession
www.cramsession.com

TCP also has a mechanism called "slow start" that is designed to expand and contract the window size based on flow control needs, starting with small window sizes and increasing over time as the link proves to be reliable. When TCP sees that packets have been dropped (ACKS are not received for packets sent), it tries to determine the rate at which it can send traffic through the network without dropping packets. Once data starts to flow again, it slowly begins the process again. This may create oscillating window sizes if the main problem has not been resolved, so the window size is slowly expanded after each successful ACK is received.

TCP/IP

IP Addressing

IP is the routed protocol of the Internet, and is the default protocol in most networks today. Addresses are 32 bits long, with the most significant bits specifying the network, as determined by a subnet mask. This subnet is either derived from the first few bits of the address, or specified directly, depending on if you are using classful (confirming to major address boundaries) or classless (further subnetting classful addresses) addressing. IP addresses are written in dotted-decimal format, with each set of eight bits separated by a period. The minimum and maximum packet headers for IP are 20 and 24 bytes, respectively.

Though a long discussion on the nature of Subnet Masks is possible, for the purposes at hand, let us just discuss the major classes: A, B, C, D, and E. Only the first three are available for commercial use; the others are special purpose address ranges. The left-most (high-order) bits indicate the network class. Here are the basic facts about the different classes of IP addresses:

IP Address Class	Purpose	High-Order Bit(s)	Default Subnet Mask	Address Range
A	Few large organizations	0	255.0.0.0	1.0.0.0 to 126.0.0.0
B	Medium-size organizations	10	255.255.0.0	128.1.0.0 to 191.254.0.0
C	Relatively small organizations	110	255.255.255.0	192.0.1.0 to 223.255.254.0
D	Multicast groups (RFC 1112)	1110	N/A	224.0.0.0 to 239.255.255.255
E	Experimental	1111	N/A	240.0.0.0 to 254.255.255.255

Remember that the default Subnet Mask is just that, a default; it can be adjusted as necessary (depending on the routing protocol) by the network designer.

Subnetting

IP addresses are made up of two pieces of information, the network that the host can be found on, and the unique address of the host. The network segment is on the left, the host portion on the right, but where the delineation occurs depends on the definition of the subnet mask. The subnet mask provides the ability to have an extended network prefix by taking bits from the host portion of the address, and adding them to the network prefix. For example, a classful Class C network prefix consists of the first 24 bits of the IP address (three octets); but the network prefix can be extended into the fourth octet to provide more granularity to the configuration.

It is also common to designate the subnet mask in the */bits* ("slash bits") format. This is simply the number of bits dedicated to the network part of the IP address. In the two examples above, the */bits* designations would be */27* and */21*.

Subnetting Tricks

I have found the following chart to be helpful for quick subnet mask calculations. If you take a few seconds at the beginning of the test session and write this out from memory on a piece of scratch paper, it can be a useful timesaver during any exam that requires subnetting and binary conversion.

Line 1	Bits	1	2	3	4	5	6	7	8
Line 2	Binaries	128	64	32	16	8	4	2	1
Line 3	Subnet	128	192	224	240	248	252	254	255
Line 4	Hosts	126	62	30	14	6	2	0	0
Line 5	Nets	2	4	8	16	32	64	128	256

How to create the chart:

- ❖ Line #1 - Write the numbers one through eight from left-to-right. Besides being a handy column header, this provides the number of bits in a subnet.
 - Line #2 - Starting with 1 and working from right-to-left, double each number. This gives you the column values for hex-to-binary conversion.
- ❖ Line #3 - Write out your subnets. You can derive these values by adding the number above to the number on the left (example: $64+128=192$).
- ❖ Line #4 - The number of hosts per subnet can be derived by subtracting two from the values in row #2 (if the value is <0 , round up to 0).
- ❖ Line #5 - Start with two in the left most column, and double each number going across. This will give you the number of networks for each subnet.

Route Summarization

Route summarization condenses routing information by consolidating like routes, and collapsing multiple subnet routes into a single network route. Where summarization is not applied, each router in a network must retain a route to every subnet in the network. This means as the network grows, the routing table becomes larger and larger. Routers that have had their routes summarized can reduce some sets of routes to a single advertisement, which reduces the load on the router and simplifies the network design.

Some important reasons to take advantage of summarization:

- ❖ The larger the routing table, the more memory is required because every entry takes up some of the available memory.
- ❖ The routing decision process may take longer to complete as the number of entries in the table are increased.
- ❖ An added benefit of reducing the IP routing table size is that it requires less bandwidth and time to advertise the network to remote locations, thereby increasing network performance.

Depending on the size of the network, the reduction in route propagation and routing information overhead can be significant. Route summarization is of minor concern in production networks until their size gets considerable. However, if summarization has not been taken into account during the initial design phase, it is very difficult to implement later.

Some routing protocols, EIGRP for example, summarize automatically. Other routing protocols, such as OSPF, require manual configuration to support route summarization.

Remember that when redistributing routes from a routing protocol that supports VLSM (such as EIGRP or OSPF) into a routing protocol that does not (such as RIPv1 or IGRP), you might lose some routing information.

Some important requirements exist for summarization:

- ❖ Multiple IP addresses must share the same high-order bits. Since the summarization takes place on the low-order bits, the high-order bits must have commonality.
- ❖ Routing tables and protocols must use classless addressing to make their routing decisions; in other words, they are not restricted by the Class A, B and C designations to indicate the boundaries for networks.
- ❖ Routing protocols must carry the prefix length (subnet mask) with the IP address.

Switching and Bridging (including: VLANs, Spanning Tree, etc.)

Bridging and LAN Switching

Transparent Bridging (TB)

Found predominantly in Ethernet environments, the operation of a Transparent Bridge is transparent to the network end-devices concerned; the hosts are completely unaware that they are not local to one another when they communicate.

A TB learns the network's topology by reading the source address of incoming frames from all attached networks, and caches that information in a forwarding table. TB's never change the make-up of a frame. The fully intact frame is either forwarded or filtered based on its destination MAC address. No RIF is present, or required.

There is a problem inherent with this type of layer-2 technology - loops. The Spanning Tree Protocol (STP), based on the Spanning Tree Algorithm (STA), provides the bridge-to-bridge communication necessary to have the desired redundancy, while not causing bridges to fail.

Bridge Protocol Data Units (BPDUs) are passed between the bridges at fixed intervals, usually every one to four seconds. If a bridge fails, or a topology change occurs, the lack of BPDUs will be detected and the STA calculation will be re-run. Since topology decisions are made locally as the BPDUs are exchanged between neighboring bridges, there is no central control on the network topology. The tools for fine-tuning an STP domain include adjusting the bridge priority, port priority and path cost parameters.

There are two major disadvantages to TB:

- ❖ The forwarding tables must be cleared each time STP reconfigures, which can trigger a broadcast storm as the tables are being reconstructed.
- ❖ The volume of broadcasts can overwhelm low-speed serial interfaces when the network is flooded with unknown frames.

Cisco supports Transparent Bridging over DDR (Dial-on-Demand Routing), as well as both Frame Relay and X.25 networks.

LAN Switching

Layer-2 switches are sometimes called micro-segmentation devices because you can think of them as bridges with dozens of ports, sometimes having as few as one host per collision domain. Because switches facilitated the move away from shared media for end-devices, they had the affect of increasing available bandwidth without increasing complexity. They have the following features:

- ❖ Each port on a switch is a separate collision domain.
- ❖ Each port can be assigned a VLAN (Virtual Local Area Network) membership, which creates controllable broadcast domains.
- ❖ While switch ports are more expensive than shared media, they are generally much cheaper than Router ports.

Switching Technique Types

- ❖ **Store-and-forward** – Receives the complete frame before forwarding. Copies the entire frame into the buffer and then checks for CRC errors. Higher latency than other techniques. This technique is used on Cat5000s.
- ❖ **Cut-through** – Checks the destination address as soon as the header is received and immediately forwards it out, lowering the latency level.
- ❖ **Fast switching** - The default switching type. It can be configured manually through use of the “ip route-cache” command. The first packet is copied into packet memory, while the destination network or host information is stored in the fast-switching cache.
- ❖ **Process Switching** - This technique doesn't use route caching, so it runs slow; however, slow usually means SAFE. To enable, use the command “no protocol route-cache”.
- ❖ **Optimum Switching** – From its name you can understand what it is – high performance! This is the default on 7500's.

Trunking

Trunks transport the packets of multiple VLANs over a single network link using either IEEE 802.1Q or Cisco's proprietary Inter-Switch Link (ISL). IEEE has become common in Cisco networks because it gives you the flexibility to include other vendor's equipment, and because of the reduced overhead when compared to ISL, which is encapsulated with a 26-byte header that transports VLAN IDs between switches and routers.

Note that not all Cisco switches support all encapsulation methods; for instance the Cat2948G and Cat4000 series switches support only 802.1Q encapsulation. In order to determine whether a switch supports trunking, and what trunking encapsulations are supported, look to the hardware documentation or use the "show port capabilities" command.

Trunks are configured for a single Fast-Ethernet, Gigabit Ethernet, or Fast- or Gigabit EtherChannel bundle and another network device, such as a router or second switch. Notice that I specifically excluded 10Mb Ethernet ports, which cannot be used for trunking. For trunking to be enabled on EtherChannel bundles, the speed and duplex settings must be configured the same on all links. For trunking to be auto-negotiated on Fast Ethernet and Gigabit Ethernet ports, the ports must be in the same VTP domain.

To help understand how trunks negotiate, this chart tells where they will form, based on the settings of the ports:

Trunk Negotiation:

Ports	On	Off	Auto	Desirable	Non-Negotiate
On	Yes	No	Yes	Yes	Yes
Off	No	No	No	No	No
Auto	Yes	No	No	Yes	No
Desirable	Yes	No	Yes	Yes	Yes
Non-Negotiate	Yes	No	No	Yes	Yes

Virtual LAN (VLAN)

A VLAN is an extended logical network that is configured independent of the physical network layout. Each port on a switch can be defined to join whatever VLAN suits the Network Architect's plans.

VLAN Trunk Protocol (VTP)

VTP is a layer-2 messaging protocol that centralizes the management of VLANs on a network-wide basis, simplifying the management of large switched networks with many VLANs.

Switches defined as part of a VTP domain can be configured to operate in any of three VTP modes:

- ❖ **Server** – Advertise VLAN configuration to other switches in the same VTP domain and synchronize with other server switches in the domain. You can create, modify, and delete VLANs, as well as modify VLAN configuration parameters, such as VTP version and VTP pruning for the entire domain. This is the default mode for a switch.

- ❖ **Client** – Advertise VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links; however, they are unable to create, change, or delete VLAN configurations.
- ❖ **Transparent** – Does not advertise its VLAN configuration and does not synchronize its VLAN configuration with other switches. If the switch is running VTP version 2, it does forward VTP advertisements, while still not acting on them.

Switches can only belong to one VTP domain, but if you have more than one group of switches, and each group has a different set of VLANs that it has to recognize, you could use a separate domain for each group of switches.

There is a second version of VTP that has features not supported in version one, including Token Ring LAN Switching and VLANs, unrecognized Type Length Value, Version Dependent Transparent Mode and Consistency Checks.

Please note that all switches in the VTP domain must run the same VTP version. In general, don't enable VTP version 2 in the VTP domain unless you are ready to migrate all the switches to that version. However, if the network is Token Ring, you will need VTP version 2.

Spanning-Tree Protocol (STP)

The Spanning-Tree Protocol (STP) is a Layer 2 link management protocol designed to run on bridges and switches to provide path redundancy and prevent undesirable loops from forming in the network. It uses the Spanning Tree Algorithm (STA) to calculate the best loop-free path through a switched network.

Root Bridges and Switches

The key to STP is the election of a root bridge, which becomes the focal point in the network. All other decisions in the network, such as which ports are blocked and which ports are put in forwarding mode, are made from the perspective of this root bridge.

When implemented in a switched network, the root bridge is usually referred to as the "root switch." Depending on the type of spanning-tree enabled, each VLAN may have its own root bridge/switch. In this case, the root for the different VLANs may all reside in a single switch, or it can reside in varying switches, depending on the estimates of the Network Architect.

You should remember that selection of the root switch for a particular VLAN is extremely important. You can allow the network to decide the root based on arbitrary criteria, or you can define it yourself.

Bridge Protocol Data Units (BPDUs)

All switches exchange information to use in the selection of the root switch, as well as for subsequent configuration of the network. This information is carried in Bridge Protocol Data Units (BPDU).

The primary functions of BPDUs are to:

- ❖ Propagate bridge IDs in order for the selection of the root switch.
- ❖ Find loops in the network.
- ❖ Provide notification of network topology changes.
- ❖ Remove loops by placing redundant switch ports in a backup state.

How STP Works

When the switches first come up, they start the root switch selection process with each switch transmitting BPDU to its directly connected switch neighbors on a per-VLAN basis.

As the BPDUs go through the network, each switch compares the BPDU it sent out to the ones it has received from its neighbors. From this comparison, the switches determine the root switch. The switch with the lowest priority in the network wins this election process. (Remember, there may be one root switch identified per VLAN, depending on the type of STP selected.)

STP Timers

- ❖ **Hello timer** - How often the switch broadcasts Hello messages to other switches.
- ❖ **Forward delay timer** - Amount of time a port will remain in the listening and learning states before going into the forwarding state.
- ❖ **Maximum age timer** – How long protocol information received on a port is stored by the switch.

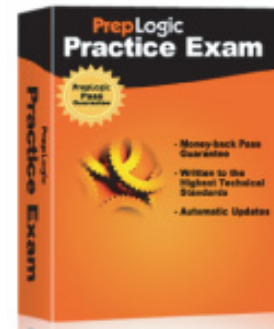
Ports in an STP domain will progress through the following states:

- ❖ **Blocking** – Listens for BPDUs from other bridges, but does not forward them or any traffic.
- ❖ **Listening** – An interim state while moving from blocking to learning. Listens for frames and detects available paths to the root bridge, but will not collect host MAC addresses for its address table.
- ❖ **Learning** – Examines the data frames for source MAC addresses to populate its address table, but no user data is passed.
- ❖ **Forwarding** – Once the learning state is complete, the port will begin its normal function of gathering MAC addresses and passing user data.
- ❖ **Disabled** – Either there has been an equipment failure, a security issue or the port has been disabled by the Network Administrator.

Notes about STP Port States:

- ❖ A port in blocking state does not participate in frame forwarding. The switch always goes into blocking state immediately following switch initialization.

Are You Ready to Take the Exam?



PrepLogic Practice Exams

Comprehensive Exam Preparation:

- Progress tracking
- Detailed answers and explanations
- Packed with quality practice questions
- Customizable learning features

Try a Demo Now

A+, MCSE, CCNA, CEH, CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified.

- ❖ When a port changes from the listening state to the learning state, it is preparing to participate in frame forwarding.
- ❖ Port in the forwarding state actually forwards frames (User data, BPDUs, etc.).

STP Enhancements:

There are three major enhancements available for Spanning Tree, as it is applied on Cisco devices:

- ❖ **PortFast** - By default, all ports on a switch are assumed to have the potential to have bridges or switches attached to them. Since each of these ports must be included in the STP calculations, they must go through the four different states whenever the STP algorithm runs (when a change occurs to the network). Enabling PortFast on the user access ports is basically a commitment between the Network Architect and the switch, agreeing that the specific port does not have a switch or bridge connected, and therefore this port can be placed directly into the Forwarding state; this allows the port to avoid being unavailable for 50 seconds while it cycles through the different bridge states, simplifies the STP recalculation, and reduces the time to convergence.
- ❖ **UplinkFast** - Convergence time on STP is 50 seconds. Part of this is the need to determine alternative paths when a link between switches is broken. This is unacceptable on networks where real-time or bandwidth-intensive applications are deployed (basically any network). If the UplinkFast feature is enabled (it is not by default) AND there is at least one alternative path whose port is in a blocking state AND the failure occurs on the root port of the actual switch, not an indirect link; then UplinkFast will allow switchover to the alternative link without recalculating STP, usually within 2 to 4 seconds. This allows STP to skip the listening and learning states before unblocking the alternative port.
- ❖ **BackboneFast** - BackboneFast is used at the Distribution and Core layers, where multiple switches connect together, and is only useful where multiple paths to the root bridge are available. This is a Cisco proprietary feature that speeds recovery when there is a failure with an active link in the STP. Usually when an indirect link fails, the switch must wait until the maximum aging time (max-age) has expired, before looking for an alternative link. This delays convergence in the event of a failure by 20 seconds (the max-age value). When BackboneFast is enabled on all switches, and an inferior BPDU arrives at the root port - indicating an indirect link failure - the switch rolls over to a blocked port that has been previously calculated.

The primary difference between UplinkFast and BackboneFast is that BackboneFast can detect indirect link failures, and is used at the Distribution and Core layers, while UplinkFast is aware of only directly connected links, and is used primarily on Access layer switches. If UplinkFast is turned on for the root switch, it will automatically disable it. Since BackboneFast is an enhancement strictly for Core and Distribution layer devices, and these are all Set-based switches, there is no command to enable it for IOS based switches.

The Cisco Press book "**Cisco LAN Switching**" by Clark and Hamilton is an excellent resource for leaning about switching.

Routed Protocols

Routing Protocol Concepts

Routing protocols provide dynamic network information to the routers that are part of the domain, and represent one of the most important areas for a Network Engineer to master.

Distance-Vector Routing Protocols

These are protocols that are designed to periodically pass the full contents of their routing tables to all of their immediate neighbors (usually every 30 to 90 seconds). Each recipient then increments the values and updates its routing table to send out in the next update. Once this information has made the rounds, each router will have built a routing table with information about the "distances" to networked resources without learning anything specific about the other routers, or about the network's actual topology.

The primary benefits of these protocols are how easy they are to configure and maintain. The problems associated with them include slow convergence, routing loops, counting to infinity problems, and excessive bandwidth utilization from the size and repetition of the updates.

The two common Distance Vector protocols are the **Routing Information Protocol (RIP)**, and Cisco's proprietary **Interior Gateway Routing Protocol (IGRP)**, which uses bandwidth and delay.

Link State Routing Protocols

Link State Routing Protocols develop and maintain a full knowledge of the network's routers, as well as how they connect to one another. This information is gathered through the exchange of link-state advertisements (LSAs) between routers, which develop a topological database that is used by the Shortest Path Algorithm to compute reachability to networked destinations. This process allows quick discovery of changes in the network topology.

The chief advantages of Link State protocols is that the transmission of LSAs takes less bandwidth than the full updates provided by Distance Vector routing protocols; it has faster convergence; and it has greater scalability.

The concerns with Link-State protocols include flooding that is done during the initial discovery process, and that they can be both memory and processor intensive.

Open Shortest Path First (OSPF) and **Intermediate System-to-Intermediate System (IS-IS)** are the primary examples of Link State protocols.

Hybrid Routing Protocols

Hybrid Routing Protocols combine characteristics of both Distance Vector and Link State protocols. They converge more rapidly than distance-vector protocols, while avoiding the processing overhead associated with link-state updates. Also, they are event driven rather than using a timer to decide when to send updates; this conserves bandwidth for the transmission of user data.

Cisco's proprietary **Enhanced Interior Gateway Routing Protocol (EIGRP)** is the most common Hybridized routing protocol (and the only one I've ever heard of). It was designed to combine the best aspects of distance-vector and link-state routing protocols without incurring any of the performance limitations specific to either. Remember that one of the major limitations to EIGRP is that it only runs on Cisco equipment.

Distribution Lists

Distribution lists are used to filter the contents of inbound or outbound distance vector routing protocol updates (RIP and IGRP). Standard IP access lists are used to define a list against which the contents of the routing updates are matched. Remember that the access list is applied to the contents of the update, not to the source or destination of the routing update packets themselves.

The "distribute-list" command is entered at the global or router configuration levels, and there is an option to apply the list to specific interfaces. For any given routing protocol, it is possible to define one interface-specific distribute-list per interface, and one protocol-specific distribute-list for each process/autonomous-system pair.

Example:

```
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 2 permit 172.16.3.0 0.0.0.255
router rip
  distribute-list 1 in ethernet 0
  distribute-list 2 out
```

Routing Loops

Routing loops occur when the routing tables of some or all of the routers in a given domain route a packet back and forth without ever reaching its final destination. Routing loops often occur during route redistribution, especially in networks with multiple redistribution points.

There are several commonly used methods for preventing routing loops, including:

- ❖ **Holddowns** – Routes are held for a specified period of time to prevent updates advertising networks that are possibly down. The period of time varies between routing protocols, and is configurable. Holddown timers should be set very carefully - if they are too short, they are ineffective; too long and convergence will be delayed.
- ❖ **Triggered updates** – Also known as flash updates, these are sent immediately when a router detects that a metric has changed or a network is no longer available. This helps speed convergence. Instead of waiting for a certain time interval to elapse to update the routing tables, the new information is sent as soon as it is learned.
- ❖ **Split horizon** – If a router has received a route advertisement from another router, it will not re-advertise it back out the interface from which it was learned.
- ❖ **Poison reverse** – Once you learn of a route through an interface, advertise it as unreachable, back through that same interface.

Administrative Distance

When a route is advertised by more than one routing protocol, the router must decide which protocol's routes to use. The predefined Administrative Distances of routing protocols allow the router to make that decision, more or less telling the router the relative trustworthiness of the different protocols. Here is a list of the common ADs:

Directly Connected	0
Static	1
EBGP	20
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140

EIGRP (External)	170
IBGP	200
BGP Local	200
Unknown	255

Policy Routing

Policy routing is a means of managing routes and the paths used with manually configured rules. It makes routing decisions based on a variety of parameters such as source address or source and destination address rather than just destination address alone. Policy routing can be used to manipulate traffic inside an AS or between ASs. Policy routing has many of the same drawbacks as static routing.

Route Dampening

A network that has a router with flapping routes (routes that go up and down) can often cause problems, as the BGP routers must continuously update their routing tables. Route dampening is used to control this route instability. Dampening classifies routes as "well-behaved" or "ill-behaved" based on their past reliability and penalties are assigned each time a route flaps. When a set penalty is reached, BGP suppresses the route until it is well behaved and trusted again. There is no penalty limit at which a route is permanently barred from joining the domain. Route dampening is not enabled by default.

The Cisco Press books "**Internet Routing Architectures, 2nd edition**" by Sam Halabi, "**Routing TCP/IP, volume 2**" by Jeff Doyle and the "**Cisco BGP-4 Command and Configuration Handbook**" by William Parkhurst are excellent resources for BGP.

Routing Protocols (including: RIP, EIGRP, OSPF, BGP)

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) has been around for many years. RIP is a distance vector routing protocol (Bellman-Ford).

RIP has these features:

- ❖ RIP V1 uses UDP port 520 to send routing updates every 30 seconds.
- ❖ RIP V2 uses multicast 224.0.0.9 to send updates but can be configured for unicast with the **neighbor** command.
- ❖ The RIP defaults are: hello=30sec, dead=180, holddown=240
- ❖ RIP chooses the best route by hop count (the number of router hops between the RIP router and the destination network).
- ❖ RIP ignores the speed of the links on the network and thus doesn't take this into consideration when choosing the best route.

- ❖ RIP, version 1, is based on [RFC1058](#). RIP, Version 2, is based on [RFC2453](#).

RIP V2 provides the following enhancements over V1:

- Subnetting, as the subnet mask is carried in the RIP updates
 - MD5 & clear-text authentication
 - Multicast updates
 -
 - Route tagging
- ❖ To enable RIPv2 authentication, you must:
 - In Global Configuration mode, configure a key-chain with the commands:
 - o **key chain** *name-of-chain*
 - On the interface, run:
 - o **ip rip authentication key-chain** *name-of-chain*
 - o **ip rip authentication mode** { **text** | **md5** }
 - ❖ Cisco PIX firewalls have limited support for RIP

Check out the [Cisco IOS documentation on configuring RIP](#).

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco proprietary protocol that is considered a 'hybrid' because it combines attributes of both Link State and Distance Vector routing protocols. It was released as an enhancement to Cisco's other proprietary routing protocol, IGRP. It also supports automatic route summarization, VLSM addressing, multicast updates, non-periodic updates, unequal-cost load balancing, and independent support for IPX and AppleTalk.

EIGRP has a number of added features to overcome the limitations of IGRP:

- ❖ **DUAL (Diffusing Update Algorithm)** - Tracks all the routes advertised by all neighbors. DUAL will use various metrics to select the most efficient path. It selects routes to be inserted into the routing table based on feasible successors.
- ❖ **Protocol Dependent Modules** - These are individually responsible for IP, IPX, and Appletalk. The IPX EIGRP module is responsible for sending and receiving EIGRP packets that are encapsulated in IPX. The Apple EIGRP module is responsible for AppleTalk packets. The IP EIGRP module is responsible for IP packets. They route like strangers in the night, except they don't even exchange glances.


- ❖ **Neighbor Discovery/Recovery** - Routers learn of the other routers on their directly attached networks dynamically, by sending Hello Packets. A router is assumed to be present by its neighbor through the hello packets it sends.
- ❖ Performs incremental updates instead of periodic updates; meaning changes are only sent out when changes occur.
- ❖ Does classless routing.
- ❖ Results in more efficient summarization of networks.
- ❖ Is efficient in the use of link bandwidth for routing updates.
- ❖ Provides authentication.

EIGRP sends hello packets every 5 seconds on high bandwidth links, like PPP and HDLC leased lines, Ethernet, TR, FDDI and Frame Relay point-to-point and ATM. It sends hellos every 60 seconds on low bandwidth multipoint links, like FR multipoint and ATM multipoint links.

An important point to remember with EIGRP is that very old routes are to be expected in a healthy network. Since updates only occur when there is a change, change is bad. Like fine wines, EIGRP routes should be seasoned by time.

- ❖ EIGRP Support MD5 authentication of routing updates. To configure this, you must do the following:
 - In Global Configuration mode, configure a key-chain with the commands:
 - **key chain** *name-of-chain*
 - On the interface, run:
 - **ip authentication key-chain eigrp** *AS# name-of-chain*
 - **ip authentication mode eigrp** *AS# md5*

Take Your Exam for Less!



EXAM VOUCHER
EXAM VOUCHER
PAID

Discount Exam Vouchers from PrepLogic

Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

Buy Your Voucher Now

PrepLogic
Be Prepared. Be Confident. Get Certified.

Tables

- ❖ **Neighbor table** – The current configuration of all the router's immediately adjacent neighbors.
- ❖ **Topology table** - This table is maintained by the protocol dependent modules and is used by DUAL. It has all the destination networks advertised by the other neighbor routers.
- ❖ **Routing table** - EIGRP chooses the best routes to a destination network from the topology table and places these routes in the routing table. The routing table contains:
 - How the route was discovered
 - Destination network address and the subnet mask
 - Metric Distance: This is the cost of the metric from the router
 - Next hop address
 - Route age
 - Outbound interface

Choosing Routes

DUAL selects primary and backup routes based on the composite metric and guarantees that the selected routes are loop free. The primary routes are then moved to a routing table. The rest (up to 6) are stored in the topology table as feasible successors.

EIGRP uses the same composite metric as IGRP to determine the best path*. The default criteria used are:

- ❖ **Bandwidth** - The smallest bandwidth cost between source and destination.
- ❖ **Delay** – The cumulative interface delay along the path.
- ❖ **Reliability** – The worst reliability between source and destination based on keepalives.
- ❖ **Load** – The utilization on a link between source and destination based on bits per second on its worst link.
- ❖ **MTU** - The smallest Maximum Transmission Unit.

* Only Bandwidth and Delay are used by default.

** To help you remember these, think of “**B**ob **D**oesn't **R**eally **L**ike **M**e” (for **B**andwidth, **D**elay, **R**eliability, **L**oad and **M**TU).

The command to disable EIGRP's default summarization of addresses at network boundaries is “no auto-summary”.

The Cisco Press book “**EIGRP Network Design Solutions**”, by Ivan Pepelnjak, is an excellent resource for learning EIGRP.

For more information on configuring EIGRP, check out the [Cisco EIGRP Configuration link](#).

Open Shortest Path First (OSPF)

OSPF is an open standard Link State routing protocol that uses Dijkstra's Shortest Path First (SPF) algorithm. Several of OSPF's advantages include fast convergence, classless routing, VLSM support, authentication support, support for much larger inter-networks, the use of areas to minimize routing protocol traffic, and a hierarchical design.

All OSPF routers must have a unique router ID. The router ID is the highest IP address on any of its loopback interfaces. If the router doesn't have any loopback interfaces, then it chooses the highest IP address on any of its enable interfaces. The interface doesn't have to have OSPF enabled on it. Loopback interfaces are often used because they are always active and there is usually more leeway in its address assignment.

OSPF contains these network types:

- ❖ Point-to-point
- ❖ Broadcast
- ❖ Non-broadcast multi-access (NBMA)
- ❖ Point-to-multipoint, and virtual-links

OSPF supports clear-text and MD5 authentication.

To configure OSPF authentication, do the following:

- ❖ In router configuration mode, run:
 - **area X authentication**
 - **area X authentication message-digest** --- If you want MD5
- ❖ In Interface configuration mode, run:
 - **ip ospf authentication-key** *key* – (for plain-text)
 - **ip ospf message-digest-key** *key-id md5 key*
 - **ip ospf authentication message-digest**

To find more information on configuring OSPF, take a look at this: [Cisco OSPF Configuration link](#).

Area 0

This is the core area for OSPF. One of the basic rules of OSPF is that all areas must connect to area 0 (just as all roads lead to Rome). If there is an area that is not contiguous with area "0", your only option is to use a virtual-link. This will provide a tunnel through another area in order to make it appear that the area is directly connected to area 0.

Area Border Routers (ABRs) are responsible for maintaining the routing information between areas. Internal routers receive all routes from the ABR except for those routes that are contained within the internal area.

Traffic destined for networks outside of the AS must traverse Area 0 to an Autonomous System Border Router (ASBR). The ASBR is responsible for handling the routing between OSPF and another AS using another routing protocol such as EIGRP.

OSPF Area Types:

- ❖ **Standard** - Accepts internal, external and summary LSA's.
- ❖ **Backbone (transit area)** - In multi-area OSPF networks all other areas must connect directly to this area in order to exchange route information. It must be labeled area "0", and it accepts all LSA types. This behaves like a normal *Standard* area, except it happens to reside in the middle of the network.
- ❖ **Stub** - Refers to an area that does not accept Type-5 LSAs to learn of external ASs. If routers need to route to networks outside the autonomous system, they must use a default route.
- ❖ **Not-so-stubby** – Also known as NSSA. It is the same as a stub area, except it accepts LSA Type 7. This is useful if you want to accept redistributed routes from another routing protocol. Once these redistributed routes leave the NSSA they are converted to Type 5. Type 7 LSAs can only exist in an NSSA.
- ❖ **Totally Stubby** – All LSAs, except Type 1 and 2, are blocked. Intra-area routes and the default route are the only routes passed within a totally stubby area. This is Cisco proprietary.

Stub and Totally Stubby Area Similarities

- ❖ There can only be a single ABR and single exit point from the area.
- ❖ All routers within the stub area must be configured as stub routers. If not, they cannot form adjacencies with the other stub routers.
- ❖ A stub area cannot be used as a transit area for virtual links.
- ❖ An ASBR cannot be internal to a stub area.
- ❖ Inter-area routing is based on a default route.
- ❖ Neither will accept Type-5 LSAs (autonomous system entries).
- ❖ There are typically used in a hub and spoke topology with the spokes being remote sites configured as stub or totally stubby areas.

Stub and Totally Stubby Area Differences

- ❖ Totally stubby areas have smaller routing tables, since the only routes they accept are from area 0, which is the default route.
- ❖ Totally stubby will not accept Summary LSA's (Type-3 and Type-4).
- ❖ Totally stubby is Cisco proprietary, while Stub is an OSPF standard.

Router Types

- ❖ **Internal Router (LSA Type 1 or 2)** – Routers that have all their interfaces in the same area. They have identical link-state databases and run single copies of the routing algorithm.
- ❖ **Area Border Router (LSA Type 3 or 4)** – Routers that have interfaces attached to multiple areas. They maintain separate link-state databases for each area. This may require the router to have more memory and CPU power. These routers act as gateways for inter-area traffic. They must have at least one interface in the backbone area, unless a virtual link is configured. These routers will often summarize routes from other areas into the backbone area.
- ❖ **Autonomous System Boundary Router (LSA Type 5 or 7)** – These routers that have at least one interface into an external network, such as a non-OSPF network. These routers can redistribute non-OSPF network information to and from an OSPF network. Redistribution into an NSSA area creates a special type of link-state advertisement (LSA) known as type 7. This router will be running another routing protocol besides OSPF, such as EIGRP, IGRP, RIP, IS-IS, etc.

Traffic Types

- ❖ **Intra-area** - Traffic passed between routers within a single area.
- ❖ **Inter-area** - Traffic passed between routers in different areas.
- ❖ **External** - Traffic passed between an OSPF router and a router in another autonomous system.

NMBA Networks

Designated Routers (DRs) and Backup Designated Routers (BDRs) are elected on Broadcast and Nonbroadcast Multi-access networks such as Ethernet broadcast domains. You can control the selection of DRs through the use of the "IP OSPF Priority" command; the highest priority wins, and a setting of "0" makes the router ineligible to become DR.

If a router joins the network with a priority somewhere between the existing DR and BDR, the network does not recalculate until the DR fails, then the BDR becomes the DR, and the new router will become BDR.

LSA Types:

- ❖ **Router link entry** - Type 1 LSA. Broadcasts only in a specific area. Contains all the default Link State information. Generated by each router for each area to which it belongs. It describes the state of the router's link to the area. The link status and cost are two of the descriptors provided.
- ❖ **Network entry** - Type 2 LSA. Multicast to all area routers in a multi-access network by the DR. They describe the set of routers attached to a particular network and are flooded only within the area that contains the network.
- ❖ **Summary entry** - Type 3 and 4 LSA's. Type 3 LSA's have route information for the internal networks and are sent to the backbone routers. Type 4 LSA's have information about the ASBRs. This information is broadcast by the ABR, and it will reach all the backbone routers.
- ❖ **Autonomous system entry** - This is a Type 5 or 7 LSA. It comes from the ASBR and has information relating to the external networks. Type 7 LSA's are only found in NSSA areas.

Border Gateway Protocol (BGP)

BGP version 4 is a path vector routing protocol used to exchange routing information between Autonomous Systems, and can be considered the routing protocol of the Internet. It carries information as a sequence of AS numbers, which indicate the autonomous systems that must be used to get to a destination network.

Specific neighbor commands must be entered to create BGP neighbors because neighbors are defined in the configuration, not by their physical location in the network. Even if two routers are physically connected, they are not necessarily neighbors unless they form a TCP connection, which is configured by the Network Engineer.

When BGP talkers (routers) communicate for the first time, they exchange their entire routing tables. The protocol maintains a table version number to track the current instance of the BGP routing table, and uses keepalives to make sure their neighbors are up. BGP uses TCP (port 179) as its transport protocol to ensure reliable delivery.

There are both internal and external flavors of BGP (IBGP and EBGP) configurations.

- ❖ **Internal BGP (IBGP)** - Used inside a specific BGP Autonomous System. Neighbors don't need to be directly connected, but they do need IP connectivity via an IP Internal Gateway Protocol (IGP), such as OSPF.
- ❖ **External BGP (EBGP)** - Used between different BGP Autonomous Systems. Neighbors normally need direct connectivity; however, Cisco provides the "ebgp-multihop" router configuration command to override this behavior.

Any time you make changes to the BGP configuration on a router, your BGP neighbor connection must be reset. Use the Cisco IOS command "clear ip bgp *" to perform this task. Use the command "show ip bgp" command to view your BGP table.

BGP's effective use of Classless Inter-domain Routing (CIDR) has been a major factor in slowing the explosive growth of the Internet routing table. CIDR doesn't rely on classes of IP networks such as Class A, B, and C. In CIDR, a prefix and a mask, such as 197.32.0.0/14, represent a network. This would normally be considered an illegal Class C network, but CIDR handles it just fine. A network is called a super-net when the prefix boundary contains fewer bits than the network's natural mask.

Situations that may require BGP:

- ❖ Extremely large networks
- ❖ A network that is connected to more than one AS
- ❖ Networks that are connected to two or more Internet Service Providers
- ❖ When you're preparing for, or taking the CCIE Lab exam

Synchronization/Full Mesh

IBGP must either maintain a full mesh within an AS, or use route reflectors to simulate the mesh. This is necessary because BGP doesn't advertise to internal BGP (IBGP) peer routes that were learned via other IBGP peers.

BGP routing information must be in sync with the IGP before advertising transit routes to other ASs. This can be turned off using the Cisco IOS command "no sync"; but this isn't recommended unless all the routers in your BGP AS are running BGP and are fully meshed, or the AS in question isn't a transit AS. The careless use of the "no sync" command could cause non-BGP routers within an autonomous system to receive traffic for destinations that they don't have a route for. With synchronization enabled, BGP waits until the IGP has propagated routing information across the autonomous system before advertising transit routes to other ASs.

Next-Hop-Self Command

In a non-meshed environment where you know that a path exists from the current router to a specific address, the BGP router command “neighbor {ip-address | peer-group-name} next-hop-self” can be used to disable next-hop processing. This will cause the current router to advertise itself as the next hop for the specified neighbor, simplifying the network. Other BGP neighbors will then forward packets for that destination to the current router. This would not be useful in a fully meshed environment, since it will result in unnecessary extra hops where there may be a more direct path.

BGP Path Selection

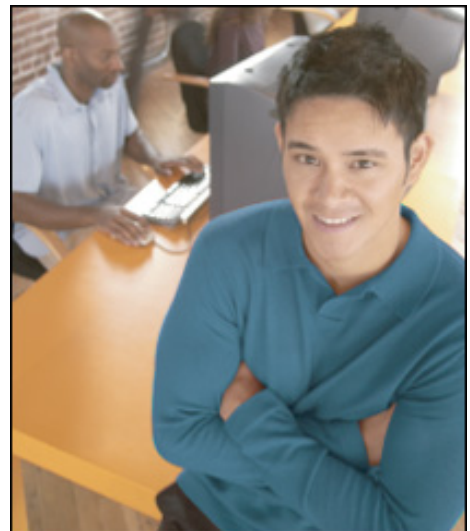
BGP will select what it considers the one best path, which is then put into the BGP routing table and then propagated to its neighbors. The criteria for selecting the path for a destination are:

- ❖ If the path specifies a next hop that is not accessible, the update is dropped.
- ❖ The path with the **largest weight** is preferred.
- ❖ If the weights are the same, the path with the **larger local preference** is preferred.
- ❖ If the local preference is the same, then prefer the path that originated on this router.
- ❖ If no route originated on this router, then prefer the one with the **shortest AS-path**.
- ❖ If they have the same AS_path, then prefer the path with the **lowest origin path**.
- ❖ If the origin codes are the same, then prefer the path with the **lowest MED**.
- ❖ If the MED is the same, then **prefer an external path to an internal path**.
- ❖ If these are the same, then prefer a path through the **closest IGP neighbor**.
- ❖ Lastly, prefer the path with the **lowest IP address**, as specified by the BGP router ID. If a loopback is configured, this will be used as the router ID.

Scalability Problems (and Solutions) with IBGP

Autonomous systems consisting of hundreds of routers can create management problems for network administrators. Remember that IBGP must be fully meshed unless you use one of the techniques listed below, which requires BGP neighbor statements to and from every IBGP router in a given AS.

- ❖ **Peer Groups** - Several BGP routers that share the same update policies can be grouped into a peer group to simplify configuration and to make updating more efficient. The power of this function will be



Who Do You Trust for Your Certification Training?

PreLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

PreLogic Comprehensive Training Tools:

- CBT • Practice Exams • Audio Training
- Mega Guides • Discount Exam Vouchers

For Free Product Demos,
[Click Here.](#)

PreLogic

Be Prepared. Be Confident. Get Certified.

obvious the first time you need to configure hundreds of routers and type the same commands over, and over, and over again. The members of a peer group will inherit changes made to the peer group, simplifying updates.

- ❖ **Confederations** - Confederations eliminate the need to fully mesh BGP communications in a given AS by splitting a single AS into sub-AS's and using EBGP between them. The sub-ASs will usually use private AS numbers. In most BGP environments it is too cumbersome to have all the BGP routers peered to each other. ASs external to the confederation group look like a single AS to the routers inside.
- ❖ **Route Reflectors** - Route reflectors can also reduce the number of BGP peering statements by configuring some of the IBGP routers as route reflectors. The route reflector clients only peer with the route reflectors, and not each other. This setup can greatly reduce the number of BGP peering configurations required in an AS. You can cluster BGP Route Reflectors to provide redundancy. This prevents the failure of a single router from bringing down your IBGP domain.

BGP Security

As this is a security exam, always look at protocols and features from a security perspective.

BGP supports MD5 for authentication. As this is a security-focused exam, BGP authentication is always recommended. To configure BGP authentication, do the following:

- ❖ In router configuration mode, run:

```
neighbor { IP-Address | peer-group ) password string
```

- ❖ An access-list that would permit BGP traffic in and out looks like:

```
access-list 100 remark Begin -- Allow BGP In and Out
```

```
access-list 100 permit tcp host 204.250.74.129 host 216.250.9.94 eq bgp
```

```
access-list 100 permit tcp host 144.250.250.137 host 63.250.250.4 eq bgp
```

```
access-list 100 permit udp any host 63.250.250.4 gt 33000
```

For more information on configuring BGP, take a look at this [Cisco BGP Configuration link](#).

Point to Point Protocol (PPP)

PPP is a standard encapsulation method for transporting multi-protocol datagrams over point-to-point links. Under ISDN, PPP only runs over the B Channels, where it provides:

- ❖ A means of encapsulating multi-protocol datagrams.
- ❖ A Link Control Protocol (LCP) for establishing, configuring and testing the data-link connection.
- ❖ A set of Network Control Protocols (NCPs) for establishing and configuring network layer protocols.

PPP provides three methods of authentication, PAP, CHAP, and MS-CHAP. CHAP is preferred because PAP transmits passwords in clear text over the network. MS-CHAP, Microsoft's version of CHAP, is used by Windows clients.

Other PPP characteristics:

- ❖ PPP Security is controlled by the following command:

```
ppp authentication { pap | chap | ms-chap }
```
- ❖ PPP is based on [RFC1661](#). PPP authentication is based on [RFC1334](#).
- ❖ PPP is a Layer 2 protocol encapsulation protocol, like Frame-Relay or HDLC. In fact, PPP actually uses HDLC as its underlying protocol.
- ❖ PPP can be used on Synchronous, Asynchronous, ISDN, or DSL lines. There is also Multi-link PPP that can bundle multiple lines, like the two B channels of an ISDN circuit.
- ❖ CHAP and PAP identify the router by its hostname. Usernames (the hostname of the router, by default) and passwords are exchanged under PAP and CHAP.
- ❖ You could also configure PPP to use RADIUS or TACACS+ for authentication parameters.
- ❖ CHAP uses MD5 to form its 128-bit hash. CHAP never sends the clear-text password over the line.
- ❖ You can use DDR (dial on demand routing) with PPP and dialup interfaces to route traffic over dialup lines, using PPP and routing protocols (or static routes).
- ❖ There are two kinds of DDR, Legacy DDR and Dialer Profiles.
- ❖ Features like callback, data compression, and Link Quality Management (LQM) are also available.
- ❖ At this link you will find the Cisco documentation on configuring [asynchronous PPP](#).

IP Multicast

IP Multicasting allows a device on the network to send a stream of information to a limited and defined group of hosts. These hosts generally add and remove themselves to and from the data stream. By this time you should be comfortable with the concepts behind Unicasts and Broadcasts, but just to reiterate:

- ❖ **Unicast** – A packet that has a specific destination address of a unique host in the IP network. The packet is passed through the routed or switched network to its destination, or dropped if it is unreachable.
- ❖ **Broadcast** - Packet that a single host sends to all IP hosts on the broadcast domain (usually a network segment). Keep in mind that every host that receives the broadcast interrupts its other work to process the packet. Under normal circumstances, routers do not forward broadcasts.

Multicast traffic is a different beast. It's based on the concept of a group; a collection of recipient hosts which have "asked" to join a particular data stream; the group does not necessarily have any physical or geographical boundaries

(depending on the network design), and potentially, group members can be located anywhere on the Internet. Analogously, think of it as a newspaper subscription, or a cable TV drop; they don't normally "just happen", the recipient must make an effort, you know - express an interest.

Hosts interested in receiving a particular data flow join the IP Multicast Group using Internet Group Management Protocol (IGMP). Hosts must be a member of the group to receive the data stream. Hosts join the group – they receive the traffic; if they don't – they don't.

The source then sends IP packets to an IP Multicast Group Address, then IP multicast routers forward out packets to interfaces that lead to members of the group. This means one flow of traffic leaves the source, and the routers in between know how to process the packets to get them to a series of destinations that have either chosen or been defined as part of a multicast group.

The same information could be sent through broadcasts, but then every destination would be affected; or it could be sent through unicasts, but then each communication would require a separate data-stream, consuming valuable bandwidth. With thousands of potential receivers, even low-bandwidth applications benefit from using IP Multicast. High-bandwidth applications can often require a large portion of the available network bandwidth for just one single stream; the thought of multiple monster streams is what keeps a good Network Architect from spending time with their family.

As you can see, we have been describing a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to any number of destinations, without forwarding the traffic to disinterested destinations. It delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers, while using less network bandwidth than might otherwise be the case.

Popular IP Multicast applications include:

- ❖ **Multimedia Conferencing** – Geographically dispersed group meetings using audio/visual or audio-only communication, and often including electronic whiteboard applications.
- ❖ **Data Distribution** – Reliably replicating data files from a central site to a number of remote locations, such as distributing price and product information from a central corporate headquarters to a number of remote sales locations.
- ❖ **Real-Time Data Multicasts** – Pushing out real-time data to a number of subscribing hosts, such as stock or news ticker updates.

The benefits of IP Multicasting include significant savings in both bandwidth and server overhead because the source device only sends the material once. Because of the reduced bandwidth utilization, there may also be a reduction of router CPU utilization, although the added load of handling multicast traffic may negate that under some circumstances.

Multicast packets are replicated in the network by Cisco routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols. Configuration is fairly simple, and should be part of your knowledge arsenal if you intend to take the CCIE path later.

Because IP Multicasting is a one-to-many proposition, UDP is the layer-4 protocol of choice. Problems related to unreliable packet delivery - such as lost packets, duplicate packets and lack of control over network congestion - do exist, but can be reduced by proper network design.

Addressing

Normal Unicast traffic is defined with a specific destination IP address that corresponds to a specific physical device. This is not true of Multicast traffic, which forwards to a set of destinations, none of which has the specific IP address designated in the packet. Remember when you first learned IP addressing, and you used A, B and C-class addresses? Well, the instructor didn't mention it to you - but there was also a D-class set of addresses, and that's what is used for multicast addressing.

Multicast IP addresses (D-class addresses) are in the range of 224.0.0.0 to 239.255.255.255, meaning the first four bits of the address are 0x1110. These addresses are administered by the Internet Assigned Number Authority (IANA), and tightly controlled they are. Don't count on grabbing a few addresses in case you ever need them; with that limited range of addresses available, they are very stingy about assigning them. One interesting outcropping of this is that there is now a DHCP-like service running that allows the entire Internet community to share the remaining unassigned range of IP multicast addresses dynamically (please notice I said DHCP-like, not actual DHCP).

The IANA has put aside 239.0.0.0 through 239.255.255.255 for private multicast domains, much like the reserved IP unicast ranges (192.168.x.x, 172.16.x.x and 10.x.x.x). When you are developing an internal application that will remain within the boundaries of your network, these should be the addresses you choose to implement.

The addresses in the range of 224.0.0.0 to 224.0.0.255 have been put aside by the IANA for use by routing protocols on the local network segment, meaning routers have been programmed not to forward them, regardless of what the TTL value is. Reserved addresses in this range include:

Address	Usage
224.0.0.1	All Hosts
224.0.0.2	All Multicast Routers
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF Routers
224.0.0.6	OSFP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10	IGRP Routers
224.0.0.12	DHCP Server/Relay Agent
224.0.0.13	All PIM Routers

Translate Multicast Addresses into Ethernet MAC Addresses

IANA maintains a block of Ethernet MAC addresses from 0100.5e00.0000 through 0100.5e7f.ffff as the range of available Ethernet MAC address destinations for IP Multicast. This allocation allows 23 bits in the Ethernet Address to correspond to the IP Multicast group address.

As we've already discussed, Multicast IP addresses are Class-D addresses which are in the range 224.0.0.0 to 239.255.255.255 (first octet equal to binary 11100000 through 11101111). They are also referred to as Group Destination Addresses (GDA). For each GDA there is an associated MAC address. This MAC address is formed by

appending 01-00-5e to the last 23 bits of the GDA, translated into hex. Remember that since only the last 23 bits of the GDA address is used, the second octet of the address can have either of two values and still be correct.

For example:

A GDA of 229.119.213.55 translates to a MAC of 01-00-5e-77-d5-37

Here's why...

Decimal IP address = 229.119.213.55

Binary equivalent = 11100101.01110111. 11010101.00110111

Last 23 bits = 1110111. 11010101.00110111

Hex equivalent of last 23 bits = 77-d5-37

Append with 01-00-5e = 01-00-5e-77-d5-37

Internet Group Management Protocol (IGMP) and Cisco Group Management Protocol (CGMP)

In order to manage IP multicasting, allow directed switching of multicast traffic, and dynamically configure switch ports so that IP multicast traffic is forwarded only to the appropriate ports, Cisco switches use:

- ❖ **Internet Group Management Protocol (IGMP)** - A standard protocol designed to manage the multicast transmissions passed to routed ports by dynamically registering individual hosts in a multicast group. Hosts identify group memberships by sending IGMP messages to their local multicast routers. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet. One of the problems with this protocol is if a VLAN on a switch is set to receive, all the workstations on that VLAN will get the multicast stream.
- ❖ **Cisco Group Management Protocol (CGMP)** - A Cisco proprietary protocol designed to control the flow of multicast streams to individual VLAN port members while limiting the impact on the switch. CGMP requires IGMP to be running on the router.

IGMP

There are two versions of IGMP. Version 1 is defined in RFC 1112 and provides just two different types of IGMP messages:

- ❖ **Membership Reports** - Hosts send out IGMP Membership Reports corresponding to a particular multicast group to indicate they are interested in joining that group.
- ❖ **Membership Queries** - The router periodically sends out an IGMP Membership Query to verify that at least one host on the subnet is still interested in receiving traffic directed to that group. When there is no reply to three consecutive IGMP Membership Queries, the router will stop forwarding traffic directed toward that group.

IGMP Version 2 is defined in RFC 2236. The primary difference is the inclusion of a *Leave Group* message, which allows hosts to take the initiative and actively communicate to the local multicast router that they no longer wish to be part of the multicast group. The router then sends out a group specific query and determines if there are any remaining hosts interested in receiving the traffic. If there are no replies, the router will time out the group and stop forwarding the traffic. This can greatly reduce the leave latency found with IGMP Version 1.

The default behavior for a Layer 2 switch would be to forward all multicast traffic to every port that belongs to the destination LAN on the switch. Basically, if one host on a VLAN wants to see the multicast, everybody on the VLAN gets it. Since the purpose of a switch is to limit traffic to just the ports that need to see it, this is not a desirable behavior. There are two methods to deal the problem - Cisco Group Management Protocol (CGMP) and IGMP Snooping.

CGMP

CGMP and IGMP software components run on both the Cisco routers and Cisco Catalyst switches. Together they allow these switches to leverage IGMP information on Cisco routers to make layer-2 (switching) forwarding decisions. With CGMP, IP Multicast traffic is delivered only to those Catalyst switch ports that are interested in the traffic; ports that have not explicitly requested the traffic will not receive it.

When the CGMP/IGMP-capable router receives an IGMP control packet, it processes it as it would any other IGMP request, and then creates a CGMP message, which it then forwards to the switch. These can either be “join” or “leave” messages, depending on what the host is asking for.

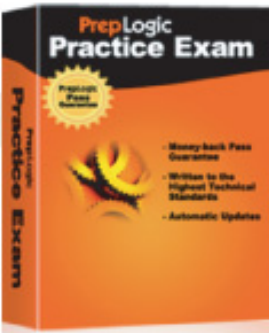
The switch receives the CGMP message and then modifies the port status in its CAM (Content Addressable Memory) table for that multicast group. All subsequent traffic directed to this multicast group will be forwarded to the port. The router port is also added to the entry for the multicast group.

It's important to note that Multicast routers are required to monitor all multicast traffic for every group, since the IGMP control messages look just like regular multicast traffic. With CGMP, the switch only has to listen to CGMP “Join” and “Leave” messages from the router. The rest of the multicast traffic is forwarded using its CAM table as normal. The router carries the load.

Please note that if there is a spanning-tree topology change, the CGMP/IGMP-learned multicast groups on the VLAN are purged and the CGMP/IGMP-capable router must generate new multicast group information. If a CGMP/IGMP-learned port link is disabled, the corresponding port is removed from any multicast group.

CGMP/IGMP-capable routers send out periodic multicast group queries, so if a host wants to remain in a multicast group, it must respond to the query. If, after a number of queries, the router receives no reports from any host in a multicast group, the router sends a CGMP/IGMP command to the switch to remove the group from the forwarding tables. CGMP's fast-leave-processing allows the switch to detect IGMP version-2 leave messages sent to the all-routers multicast address by hosts on any of the supervisor engine module ports.

Remember that CGMP must be configured on both the multicast routers and the layer-2 switches and that CGMP is Cisco proprietary.



Are You Ready to Take the Exam?

Comprehensive Exam Preparation:

- Progress tracking
- Detailed answers and explanations
- Packed with quality practice questions
- Customizable learning features

[Try a Demo Now](#)

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified.

Integrated Services Digital Network (ISDN)

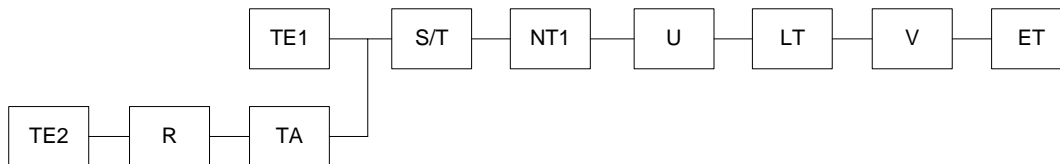
ISDN is offered by regional telephone carriers to provide digital telephony and data-transport services over existing telephone wires. When it was released, it represented an effort to standardize subscriber services, user/network interfaces, and network and internetwork capabilities. ISDN can be used to provide a PVC (Permanent Virtual Circuit) for data passing, or an on-demand circuit for backing up other WAN technologies, or for a cost-effective way of linking remote sites that have limited requirements.

ISDN circuits will often require service profile identifiers (SPIDs), which are similar to telephone numbers in that they are unique line identifiers provided by the LEC (Local Exchange Carrier). A common question people have is when is an SPID required, and when is it not. Well, the simple answer is – when the carrier requires it... Since the type of carrier switch or how the switch is configured determines the need for a SPID, you as an end-user will have no control of this element of the configuration.

Encapsulation for ISDN can be PPP, HDLC or LAPD, with the default encapsulation method being HDLC. CHAP and PAP authentication techniques are associated with PPP.

Many Cisco routers with built-in ISDN interfaces (such as the 2503) have an ST interface. In order to convert the U interface circuit from the carrier to an ST interface circuit that the router can handle, an external Network Terminating Unit (NT1) is required. There might be two of these units sitting between the BRI ports on the ISDN simulator and the routers. These units usually do not need to be configured, but the ports must be accurate: U goes to the simulator, S/T to the router.

ISDN Specifics



* Note: U is two wire, S/T is four wire. The NT1 provides this conversion.

If you have completed the CCNP path, the diagram above should look familiar. It shows the relationship between the ISDN equipment, protocol standards and reference points, which are of course:

Equipment	Reference Points	Protocol Standards
Terminal adapter (TA) – Converts RS-232, V.35, and other signals into BRI.	R - Defines the hand-off from non-ISDN equipment and the TA.	E - Specifies ISDN on existing telephone technology.

Terminal equipment (TE1 2): TE1 - An interface that complies with the ISDN user-network interface recommendations, which means it has an integrated TA. TE2 – Complies with interface recommendations other than the ISDN, which means it requires a TA to connect and work with ISDN.	S – Defines the hand-off from user terminals to an NT2.	I - Specifies concepts, terminology and services.
Network termination type 1 (NT1) - Equipment that connects the subscription 4 wires to the 2 wire local loop.	T – Defines the hand-off between the NT1 and NT2.	Q - Specifies switching and signaling.
Network termination type 2 (NT2) – Equipment that performs protocol functions of the data link and network layers.	U - Define the hand-off between the NT1 and line-termination equipment in a carrier network.	
Local Termination (LT) – Portion of the local exchange that terminates the local loop.		
Exchange Termination (ET) – Portion of the exchange that communicates with the ISDN components.		

Channels

Data on an ISDN line is channelized, with the two types of channels being:

- ❖ **B**(earer) channel: Used for transporting user data (voice or data).
- ❖ **D**(ata) channel: Used for control/signaling information using LAPD. Q.931, the network layer protocol that provides messages for ISDN call setup and tear down, runs over the D Channel. It uses Q.921, a derivative of HDLC, as its data-link layer transport.

Flavors of ISDN

There are three types of ISDN circuit, only two of which are found in the United States:

- ❖ **BRI** – 2B /1D (B=64kb / D = 16kb)
- ❖ **PRI** – 23B / 1D (B=64kb / D = 64kb)
- ❖ **E1** (Europe) – 30B / 1D (B=64kb / D = 64kb)

Async

Async ports can be configured as command-line ports (like the console and aux ports) or network ports doing encapsulation like PPP. PPP is typically used today on asynchronous links for network connectivity.

Some important Async commands are:

- ❖ **async mode { dedicated | interactive }** – async mode is off, by default
- ❖ **autoselect { ppp | slip | during-login | arap }**
- ❖ **transport input { all | lat | map | nasi | none | pad | rlogin | telnet | v120 }**
- ❖ **encapsulation ppp**

Take a look at this example on [Cisco IOS configuring PPP Async dialup](#).

Access Devices (for example: Cisco AS 5300 series)

- ❖ Cisco specifically mentions the AS5300 in their list of suggested Access Devices a CCIE Security candidate should be familiar with. The [link to information on the AS5300 is located here](#). In particular, the [AS5300 data sheet is at this link](#).
- ❖ The AS5300 has been announced as an end-of-life product and will not be available for sale after December 31, 2002.
- ❖ Other models of access devices are the 2500 and 6700 model lines.
- ❖ In general, access devices, like the AS5300, have a high-density of asynchronous ports and/or modems built into them. They allow multiple connections to the device and function as a NAS (Network access server).
- ❖ On the small end, these devices could be used as a dialup modem pool at a small business. On the large end, these devices could be used by telephone carriers or Internet Service Providers (ISP) for hundreds or thousands of customers to connect to a network.

Security Technologies

Concepts

The book “Network Security Principles and Practices” states, “Network Security is the process through which a network is secured against internal and external threats of various forms”. The part about “various forms” is what makes it a challenge.

The book “Control and Security of Computer Information Systems”, by M. Fites states the following approach to implementing network security

- ❖ Identify what you are trying to protect.
- ❖ Determine what you are trying to protect it from.
- ❖ Determine how likely the threats are.
- ❖ Implement measures that protect your assets in a cost-effective manner.
- ❖ Review the process continuously, and make improvements each time you find a weakness.

You should always have a Network Security Policy. That is included in the first step of the process just mentioned.

[RFC2196 is the Site Security Handbook](#). This handbook makes many excellent recommendations for security your network, both physically, through policy, and through technology.

You should also review the [Cisco SAFE whitepapers and blueprint](#). This is Cisco's security methodology.

You should be familiar with the security concept of IOS privilege levels. Cisco IOS provides for 16 (0-15) privilege levels. Level 0 has almost no access, while Level 15 has full router access.

- ❖ You can set certain commands to be available at certain privilege levels. Use this command to do this:

privilege mode level *level command*

- ❖ You can set passwords assigned to specific privilege levels using this command:

enable password level *level password*

- ❖ You can configure lines to have a certain privilege level, by default.
- ❖ Use the **enable level** and **disable level** commands to move from one level to another.
- ❖ With local authentication, you can configure a user to have a specific privilege level with the command:

username name [*privilege level*]

Packet Filtering

Access Control Lists (ACL)

An Access List is an ordered set of statements that permit or deny the flow of packets through an interface. They are used for security purposes, to provide QoS, or to define types of traffic for purposes of filtering, queuing or prioritizing.

They define the criteria on which decisions are made based on information contained inside the packets. Decisions are based on the source and/or destination network/subnet/host address(es) of the packets.

The basic concept of the access list wildcard mask is that any "0" in the wildcard mask means the corresponding bit in the address has to match, and any "1" in the wildcard mask means the value isn't checked.

You can only append to an access list, you cannot add lines to the middle of it. To make changes, copy your access list to notepad, and make your changes there; then from the Cisco router console type "no access-list" and the number, then paste the updated access list into the configuration.

Things to know about ACLs:

- ❖ The wildcard mask, which looks like a reversed subnet mask, defines which bits of the address are used for the access list decision-making process.
- ❖ Lists are processed top-down. In other words, the first matching rule preempts further processing.
- ❖ Only one access list is allowed per port/per direction/per protocol.
- ❖ Remember that there is an implicit deny at the end of all access lists (so the last configured line should always be a permit statement).
- ❖ If you apply an access number that does not exist, all traffic will be passed.
- ❖ An *Access Class* limits VTY (telnet) access.
- ❖ A *Distribution List* filters incoming or outgoing routing updates.

Access list types are designated by the list Numbers:

1-99	IP standard
100-199	Extended IP
200-299	Protocol type-code
300-399	DECNet
400-499	XNS standard
500-599	XNS extended
600-699	AppleTalk
700-799	48-bit Mac Address
800-899	IPX standard
900-999	IPX extended
1000-1099	IPX Sap
1100-1199	Extended 48-bit Mac Address
1200-1299	IPX Summary Address

O'Reilly & Associates' "**Cisco IOS Access Lists**" by Jeff Sedayao, and McGraw-Hill's "**Cisco Access Lists: Field Guide**" by Held and Hundley are excellent resources for this topic.

IP Extended Access-Lists are what is most important in Internet security today. You should be familiar with the configuration of IP Extended access-lists, more so than the others.

In many of the technologies mentioned in this document, there are access-lists included that match that particular protocol or application. Use the information in this Access-List section to understand those access-lists.

Proxies

A proxy server is an application that receives a request for a network service (like a web page, or ftp file) and goes to retrieve what is requested, on the requestor's behalf. Typically, a proxy server is used to retrieve web pages for a company, group, or even a home network.

- ❖ The benefits of a proxy server are:
 - Greater performance through caching frequently requested pages
 - Filtering, authorization, and logging
- ❖ Many people confuse proxy servers with NAT and/or PAT, however, they are quite different.
- ❖ Proxy servers are an application that works at Layer 4, or above. Proxy servers do not hide the fact that they are the ones retrieving the information for the requestor. Both the client requesting the information and the site that it is requested from can tell, to some degree (the client more so than the site that finally receives the request) that the proxy server is acting as the middle-man.
- ❖ On the other hand, with NAT, neither the source nor destination knows that the traffic has been through a router, or device, performing NAT. NAT acts at Layer 3.
- ❖ The Cisco IOS firewall feature set (talked about later in this Cramsession), offers a feature called "authentication-proxy" (auth-proxy). This feature will authenticate HTTP requests, from clients, using an AAA server and open ports based on what the AAA server specifies for that user (access-lists on a per-user basis).

Learn more about [Configuring IOS auth-proxy at this link](#).



The PrepLogic Mega Guide

PrepLogic took the CramSession Study Guide and made it better!

- Over 100 pages
- More in-depth content
- Expanded resources
- Includes review practice questions

Get \$10 Off
Get it Now

Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide and many more** for **FREE** at

CramSession
www.cramsession.com

Port Address Translation (PAT)

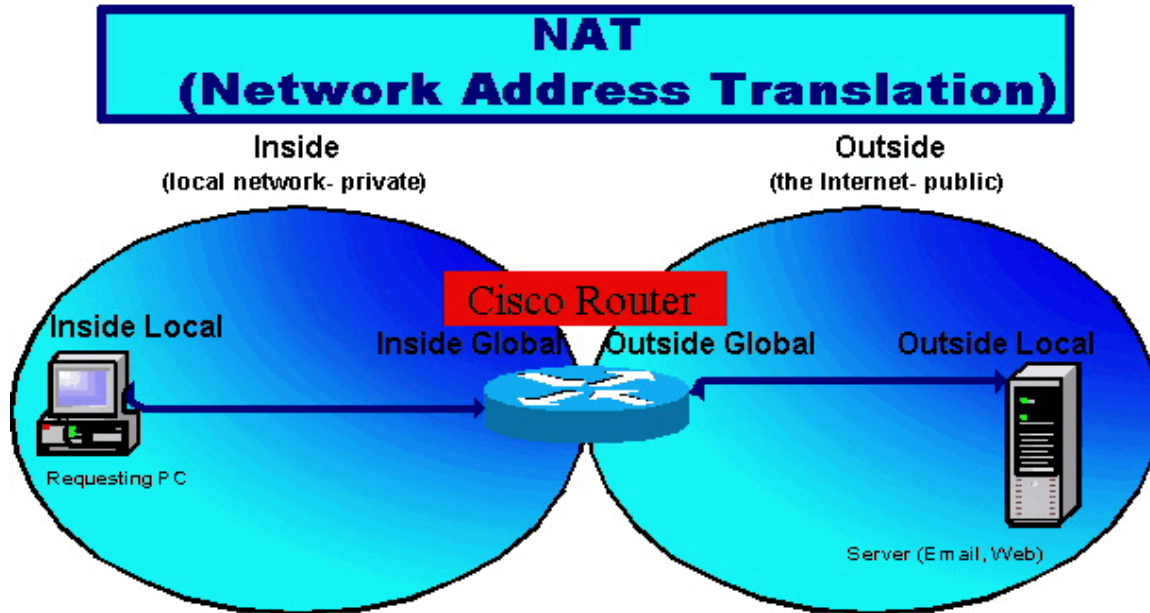
PAT is the same as NAT (covered in the next section) but it keeps track of port numbers. PAT is a function of NAT. With Cisco, PAT is called "NAT overload". There really is no configuration of PAT, only NAT or NAT overload.

- ❖ PAT does "one-to-many" translation of network addresses. Thus, multiple hosts may be going through the PAT device and appear as they are all coming from the same IP address on the other side of the PAT device. PAT keeps track of these ports and translates the data back to the requestors without the hosts ever knowing what happened to their data.
- ❖ NAT, mentioned in the next section, is a one-to-one translation.
- ❖ Both PAT and NAT are configured with the Global Configuration mode command- **ip nat ...**
- ❖ I wrote an article on how to "[Setup Port Address Translation in the Cisco IOS](#)" for TechRepublic that may help to visually understand PAT vs. NAT.
- ❖ Learn more about configuring PAT and NAT at the [Cisco IOS Configuring IP Addressing link, for NAT](#).
- ❖ Take a look at the diagram in the Nat section to help you better visualize NAT terminology.

Network Address Translation (NAT)

Network Address Translation (NAT) translates private ([RFC1918](#)) IP addresses into public Internet IP Addresses. This is the typical use of NAT. Also, it can be used to join two networks with the same IP address scheme.

- ❖ Other functions of NAT are "NAT overload", also known as PAT (mentioned in the previous section).
- ❖ Both PAT and NAT can provide security benefits, as the host on the public Internet that receives the request never knows the real IP address of the host that requested the data. Thus, the IP addresses on the internal network are kept private. This is ideal for networks that use non-routable, [RFC1918](#), IP Addresses.
- ❖ Both PAT and NAT are configured with the Global Configuration mode command- **ip nat ...**
- ❖ Learn more about configuring PAT and NAT at the [Cisco IOS Configuring IP Addressing link, for NAT](#).
- ❖ I wrote an article on how to "[Setup NAT using the Cisco IOS](#)" for TechRepublic that may help to visually understand NAT and how to configure it.
- ❖ Here is a diagram that may help you to visualize NAT terminology. (This diagram is based on diagrams from the TechRepublic article, mentioned above):



Firewalls

Webopedia.com offers the following definition of a firewall:

“A system designed to prevent unauthorized [access](#) to or from a private [network](#). Firewalls can be implemented in both [hardware](#) and [software](#), or a combination of both. Firewalls are frequently used to prevent unauthorized [Internet](#) users from accessing private networks connected to the Internet, especially [intranets](#). All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified [security](#) criteria.”

In general, a firewall protects a network that you want to secure from some outside network. Most frequently, it is protecting a network from the public Internet. However, a firewall can also be used to protect one Intranet from another Intranet, like between two companies that have their networks interconnected or between, say, the Human Resources department and the rest of a company.

[Network Security Principles and Practices](#) defines the five types of firewalls. They are:

- ❖ Circuit-level – Act as relays for TCP connections.
- ❖ Proxy Server – Examine packets at the application layer.
- ❖ Nonstateful Packet Filters – Allow some packets but block other packets.
- ❖ Stateful Packet Filters – Allow some packets and block others but also keep a record of packet flow and only allow inbound packets that have been requested (that is the connection state).
- ❖ Personal – Installed on personal computers.

Other firewall facts:

- ❖ DMZ – Demilitarized zone. In firewall terminology, this is the area between the inside network and the outside network. This is the area where you would locate your servers that must be accessed by the Internet zone but also need some level of protection (examples would be public email servers or web servers).
- ❖ The Cisco PIX firewalls use something called the Adaptive Security Algorithm (ASA) to define how the PIX examines traffic as it passes between network zones with different security levels (such as the inside network, the DMZ, and the outside network). ASA defines the least secure network with a number of 0 (zero) and the most secure network with a level of 100. If the router has a DMZ interface, by default, this is set at a level of 50. Also, by default, packets are not allowed to traverse from a less secure network to a more secure network without some specific configuration.
- ❖ The PIX firewall ASA has a feature to protect networks from TCP SYN Flooding.
- ❖ The PIX line of firewalls offers stateful packet inspection, a wide variety of logging features, access-lists to only allow certain IP addresses and ports in or out, basic routing, NAT, fail over and redundancy, and VPN features.

The [product homepage for Cisco PIX firewalls is at this link](#).

The [datasheet for the Cisco PIX Version 6.0 software](#) lists the features of the PIX firewall series.

Active Audit

Active Audit is Cisco's process of **proactively** looking for security issues. This is in comparison to putting a security infrastructure in place and passively waiting for something to happen. Most people would not know if their security was working or not.

- ❖ Cisco's Active Audit recommends using NetSonar and NetRanger to actively search out suspicious network activity or attacks and take action. NetRanger (now called Cisco Secure Intrusion Detection System) and NetSonar (now called Cisco Secure Scanner) are covered later in this Cramsession.
- ❖ With NetRanger, packets, at some point on the network, are scanned to look for intrusions. When an intrusion is detected, NetRanger immediately notifies the router, PIX firewall, or switch that can thwart the attack or intrusion, instructing that device to be blocked (shunned).

For more on Active Audit, take a look at this [Cisco Networkers Presentation covering Active Audit](#).

Content Filters

Content-Based Application Recognition (CBAC)

CBAC is used to “intelligently filter TCP and UDP packets”. That means that CBAC is, basically, a firewall but it can automatically recognize applications (like FTP, HTTP, Sql*Net, and more) and permit or deny them. It also offers logging of its activities and SMTP intrusion detection (it monitors and stops SMTP attacks).

- ❖ CBAC commands all start with the **ip inspect ...** command.
- ❖ CBAC supports the following protocols: cuseeme, ftp, h323, netshow, rcmd, realaudio, smtp, sqlnet, streamworks, tftp, and vdolive.
- ❖ CBAC is stateful for TCP and approximates states for UDP packets (as UDP is a connection-less protocol, that is the best you can do).
- ❖ CBAC can protect against DoS attacks by maintaining three different thresholds for half-open sessions and then, when a threshold is met, either send a reset packet or just drop all SYN packets.

For more information on [configuring Cisco IOS CBAC, take a look at this link](#).

Committed Access Rate (CAR)

CAR is used on interfaces to rate-limit traffic based on IP addresses or by protocol. The first step to using CAR is setting your rate policy, which determines what is to be done with traffic that exceeds a set bandwidth threshold. For example, you can configure an interface to drop all Telnet traffic that exceeds 64Kbps.

The rate limit consists of 3 values: average rate (bits per second), normal burst size (bytes per second), and excess burst size (bytes per second). Note that average rate is specified at bits per second, and the other two values are bytes per second. If the bandwidth being utilized is below the average rate, it is said to conform to the rate policies. Once the traffic exceeds this defined threshold, it is said to exceed the rate policy. Once traffic exceeds the average rate, it is allowed to continue to be sent only if the policy allows for a burst.

This is all dependent on the values you choose. Normal burst size is the amount of traffic that can be sent before it gets to another exceeded value. Once traffic exceeds the normal burst value, it is subject to RED. RED only drops some of the packets in order to get the traffic rate below the limit. If the traffic is not slowed enough by RED, and exceeds the excess burst size, then all traffic is dropped or subject to whatever rate policy you decide.

To configure CAR, you first define the access-list necessary for the traffic you want to limit, then create a rate-limit and apply it to an interface.

CAR is important for security purposes to limit attack traffic that can saturate links. An example would be limiting ICMP (ping) traffic to a small percentage of your link so that an attacker cannot perform a DoS attack.

Network-Based Application Recognition (NBAR)

Network-Based Application Recognition (NBAR) classifies application-level protocols so that QoS policies can be applied to the classified traffic. This intelligent classification includes a wide variety of applications, including web-based and other difficult-to-classify protocols that use dynamic TCP/UDP port assignments. NBAR is also capable of determining which protocols and applications are currently running on a network so that an appropriate QoS policy can be instituted. It can also perform subport classification of HTTP traffic by HOST name in addition to classification by MIME-type or URL. This enables users to classify HTTP traffic by web server names.

NBAR provides a special Protocol Discovery feature that determines which application protocols are traversing a network at any given time. The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

NBAR can also classify static port protocols. Although Access Control Lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACLs.

Once an application is recognized and classified by NBAR, a network can invoke services specific to that application. In this way, NBAR ensures that network bandwidth is used efficiently by working with QoS features to provide:

- ❖ Guaranteed bandwidth
- ❖ Bandwidth limits
- ❖ Traffic shaping
- ❖ Packet coloring

NBAR introduces several new classification features:

- ❖ Classification of applications that dynamically assign TCP/UDP port numbers.
- ❖ NBAR can classify application traffic by looking beyond the TCP/UDP port numbers of a packet into the TCP/UDP payload itself and classifies packets on content within the payload such as transaction identifier, message type, or other similar data. This is called subport classification, an example of which would be classification of HTTP by URL, HOST, or Multipurpose Internet Mail Extension (MIME) type.
- ❖ NBAR can classify Citrix Independent Computing Architecture (ICA) traffic and perform subport classification of that traffic based on Citrix published applications.

NBAR is capable of classifying the following three types of protocols:

- ❖ Non-UDP and non-TCP IP protocols
- ❖ TCP and UDP protocols that use statically assigned port numbers
- ❖ TCP and UDP protocols that dynamically assign port numbers and therefore require stateful inspection

NBAR is especially important for security purposes. It helps to recognize unwanted or harmful applications and stops them from being delivered to your internal network. An example is [being able to stop the Code Red Worm with NBAR](#).

Configuring NBAR

Cisco Express Forwarding (CEF) must be enabled before NBAR can be configured. NBAR is configured by using the following commands to configure traffic classes of policies that will be applied to those traffic classes, and the attaching of policies to interfaces:

- ❖ NBAR Terminology:
 - **Class-map** - Defines one or more traffic classes by specifying the criteria by which traffic is classified.
 - **Policy-map** - Define one or more QoS policies (such as shaping, policing, and so on) to apply to traffic defined by a class map.
 - **Service-policy** - Attaches a policy map to an interface on the router.

For more information on configuring NBAR, check out the [Cisco IOS Configuring NBAR link](#).

Public Key Infrastructure (PKI)

Cisco's definition of PKI is:

“Public-Key Infrastructure (PKI) is a system of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.”

Netscape offers this page on [Understanding PKI](#). On that page, they offer this definition of PKI:

“Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

PKIs integrate [digital certificates](#), public-key cryptography, and [certificate authorities](#) into a total, enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.”

Basically, PKI is the “whole ball of wax” when it comes to certificates, the certificate authorities, the digital signatures, directories, revocations, rules about it, how it all works, etc. Know these topics and you'll know all you need to know.

A good resource to learn about PKI is the [PKI Page](#).

Authentication Technologies

You should be aware of the variety of authentication technologies available today. Some of these are:

- ❖ Tokens
- ❖ Digital certificates
- ❖ Usernames & passwords
- ❖ Smart cards
- ❖ USB devices
- ❖ Biometrics

Virtual Private Networks (VPN)

Cisco offers the following definition for a VPN:

“Any network built upon a public network and partitioned for use by individual customers.”

VPNs can be either encrypted or unencrypted. Many people believe that a VPN must be encrypted but that is not the case.

[Network Security Principles and Practices](#) states that VPNs can be categorized three ways:

- ❖ Data Link Layer VPN – Frame-relay & ATM
- ❖ Network Layer VPN – GRE, L2TP, L2F, PPTP
- ❖ Application Layer VPN – SSL, SSH



Who Do You Trust for Your Certification Training?

PrepLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

PrepLogic Comprehensive Training Tools:
CBT • Practice Exams • Audio Training • Mega Guides • Discount Exam Vouchers

For Free Product Demos, [Click Here.](#)

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide and many more** for **FREE** at

CramSession
www.cramsession.com

Cisco Security Applications

Cisco Secure UNIX

Cisco Secure ACS for Unix is an Access Control Server (ACS). This **software** package is designed to provide all the AAA (authentication, authorization, and accounting) features you would want with an Enterprise-level network. Obviously, it runs on Unix, more specifically, Sun Solaris.

Some of the features that Secure ACS for Unix supports are:

- ❖ TACACS+
- ❖ RADIUS
- ❖ VPDN support for L2F tunnels
- ❖ Relational database support
- ❖ Easy administration of users and groups

The [Product Support page for Cisco Secure ACS for Unix is located at this link](#).

Cisco Secure NT

The Cisco Secure ACS for Windows (and NT) is an Access Control Server (ACS) **software** package. This software is designed to provide all the AAA (authentication, authorization, and accounting) features you would want with an Enterprise-level network. This version runs on Window NT or 2000.

- ❖ This package is, essentially, the same as Cisco Secure Unix that was mentioned in the previous section.

Learn more about the [Cisco Secure ACS server at this Cisco link](#).

Cisco Secure PIX Firewall

The Cisco Secure PIX Firewall is a **hardware** firewall device. Learn more about firewalls in the Firewall section of this document.

- ❖ The PIX line of firewalls offers stateful packet inspection, a wide variety of logging features, access-lists to only allow certain IP addresses and ports in or out, basic routing, NAT, fail over and redundancy, and VPN features.

The [product homepage for Cisco PIX firewalls is at this link](#).

The [datasheet for the Cisco PIX Version 6.0 software](#) tells the features of the PIX firewall series.

Learn more about the [Cisco Secure PIX Firewall at this link](#).

Cisco Secure Policy Manager (formerly Cisco Security Manager)

CSPM, as it is called, is a centralized policy manager for Cisco PIX firewalls and VPN devices. This **software** package eases the management of multiple devices in an enterprise by allowing the administrator to manage, distribute, audit, and control the firewall policies from a central workstation.

Learn more about [Cisco Secure Policy Manger at this link](#).

Cisco Secure Intrusion Detection System (formerly NetRanger)

There are two types of IDS systems, host-based and network based. Host-based systems run on the host that could be attacked. Network-based run on a device, on the network, that monitors for attacks.

- ❖ Cisco makes the IDS4200 hardware device. On this IDS hardware sensor is the software that monitors the network for intrusions. Based on the configuration on that device, it can notify routers, PIX firewalls, and switches to deny (block or shun) the traffic source of the attack. It can also log network traffic and alert (email or pager, for example) when attacks occur.
- ❖ There is also a Catalyst 6000 Switch blade module that performs IDS.

Here is a good [Cisco Q&A on the Cisco Secure Intrusion Detection System](#).

The [data sheet for the Cisco secure Intrusion Detection System software for the 4200 series IDS appliances is located here](#).

Cisco Secure Scanner (formerly NetSonar)

Cisco Secure Scanner (NetSonar) has been discontinued. Secure Scanner is a network vulnerability scanner that checks IP addresses on your network (hosts) for weaknesses or security holes. [Cisco Secure Scanner's web page is located here](#).

IOS® Firewall Feature Set

The IOS Firewall is a version of the IOS that can be loaded on a Cisco IOS router.

This version contains the following features:

- ❖ Intrusion Detection
- ❖ Stateful filtering
- ❖ Application recognition
- ❖ Dynamic authentication, authorization, and filtering

- ❖ URL filtering
- ❖ Java application blocking

IOS Firewall offers a feature called “authentication-proxy” (auth-proxy). This feature will authenticate HTTP requests, from clients, using an AAA server and open ports based on what the AAA server specifies for that user (access-lists on a per-user basis). Learn more about [Configuring IOS auth-proxy at this link](#).

Learn about configuring [Cisco IOS Firewall IDS at this link](#)

The [IOS Firewall data sheet is located at this link](#).

The [IOS Firewall feature set description is located at this link](#).

The [IOS Firewall Application Overview is located at this link](#).

Security General

Policies

The following are guidelines taken from the NSA (National Security Agency) guidelines on Securing Cisco Router (reference- <http://www.nsa.gov/snac/cisco/guides/cis-1.pdf>):

- ❖ Maintain a security policy
- ❖ Keep a copy of all router configurations stored offline
- ❖ Test security of router regularly
- ❖ Shutdown unneeded router services:
 - Small services (echo, discard, chargen) with **no service tcp-small-servers**
 - BOOTP with **no ip bootp server**
 - Finger with **no service finger**
 - HTTP with **no ip http server**
 - SNMP with **no snmp server**
 - CDP with **no cdp run**
 - Remote config with **no service config**

- Source routing with **no ip source-route**
- Classless routing with **no ip classless**

- ❖ Interfaces should be secured with:
 - **shutdown** (if unused)
 - **no ip directed broadcasts** (prevent smurf attacks)
 - **no ip proxy-arp** (prevent unplanned routes)

- ❖ Set an exec-timeout and proper transports on your console, aux line, and vty ports.
 - **exec-timeout 5 0**
 - **transport input telnet** (or none and **no exec**, if not being used)

- ❖ Configure passwords on all lines and make sure that passwords are complex (like My\$Router1).

- ❖ Configure an **enable secret password** , which will be encrypted with MD5 encryption.

- ❖ Configure **service password-encryption** to encrypt all other passwords (like routing protocol passwords).

- ❖ Configure an access list for the virtual terminal lines to control telnet access. Use the **access-class** commands to do this. If you must use SNMP, then select and configure hard-to-guess SNMP community string like this- **snmp community MyStr+ing!**.

The Cisco SAFE blueprint says this about the need for a security policy:

“It is important to understand that network security is an evolutionary process. No one product can make an organization “secure”. True network security comes from a combination of products and services, combined with a comprehensive security policy and a commitment to adhere to that policy from the top of the organization down. In fact, a properly implemented security policy without dedicated security hardware can be more effective at mitigating the threat to enterprise resources than a comprehensive security product implementation without an associated policy.”

Review the [Cisco SAFE whitepapers and blueprint](#). This is Cisco’s security methodology.

Standards Bodies

- ❖ [IETF – Internet Engineering Task Force](#)
- ❖ [IANA – Internet Assigned Numbers Authority](#)
- ❖ [ARIN – American Registry for Internet Numbers](#)

Incident Response Teams

- ❖ [CERT/CC – Computer Emergency Response Team / Coordination Center](#)
- ❖ [FedCIRC – Federal Computer Incident Response Center](#)
- ❖ [SANS Institute – SysAdmin, Audit, Network, Security](#)
- ❖ [NSA – National Security Agency](#)

Vulnerability discussions

Vulnerability is defined as being “susceptible to attack”. You can use a network vulnerability scanner (like NetSonar / Cisco Secure Scanner or others on the market) to see if and where your network is susceptible to attack.

In the next section, I will cover common vulnerabilities.

Attacks and Common Exploits

Common Attacks and Exploits

The [Cisco SAFE Blueprint](#) states these common attacks:

- ❖ IP Spoofing – Where the attacker pretends to be another host than it really is. You can prevent this with Unicast RPF, talked about below, and access control lists.
- ❖ DoS attacks – Can be prevented with CAR, CBAC, and stateful firewalls. Some common versions are listed below:
 - TCP SYN Flood
 - Ping of Death
 - Tribe Flood Network – to prevent TFN, use Unicast RFP
 - Trinoo
 - Stacheldraht

- Trinity
 - Shaft
 - Land.c - To prevent a land attack, block incoming packets that have the same source and destination address.
 - Smurf
- ❖ Password attacks – Can be prevented with strong passwords and password policies.
 - ❖ Man-in-the-Middle attacks – Can be prevented through cryptography, like SSL and encrypted nonces.
 - ❖ Application layer attacks – Exploiting weaknesses in configurations of network services, like http, ftp, or telnet. These can be prevented by proper configuration, as is discussed in other areas of this document.
 - ❖ Virus and Trojan Horse Applications – Malicious code that can infect servers and workstations. This can be prevented with NBAR.

Refer to the Cisco document on [“Improving Security on Cisco Routers”](#) for more information.

Unicast Reverse Path Forwarding

Cisco IOS offers this feature to help prevent IP Spoofing. Cisco describes the feature as:

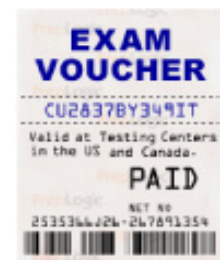
“Helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribe Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.”

Intrusion Detection

Intrusion Detection is a practice of monitoring a network for unauthorized access, attempts at unauthorized access, or attempts to damage network performance or services.

- ❖ Cisco offers IDS features in routers (with IOS Firewall Feature Set), PIX Firewalls, IDS hardware sensors, and IDS host-based sensor software.

Take Your Exam for Less!



Discount Exam Vouchers from PrepLogic

Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

Buy Your Voucher Now

PrepLogic

Be Prepared. Be Confident. Get Certified.

- ❖ IDS devices monitor the network, can recognize the attacks, log the attacks, notify appropriate personnel, and, if configured to do so, stop the attack by instructing a network device (firewall, router, or switch) to block (shun) access for the attacker. This is an example of a countermeasure that can be taken to ward off the network attack.
- ❖ Without logging, you have no record of packets that are denied by access-lists. While these logs aren't usually constantly reviewed, they can be extremely helpful in record keeping of "normal" vs. "abnormal" network activity. To turn on logging on a IOS router, do the following:
 - **logging on**
 - **logging buffered**
 - **logging X.X.X.X** (to the syslog host)
 - To configure the router to include time information in the logging run, **service timestamps log datetime**
 - You should also configure NTP to make sure that time on routers are synchronized.

Learn about configuring [Cisco IOS Firewall IDS at this link](#).

The [data sheet for the Cisco secure Intrusion Detection System software for the 4200 series IDS appliances is located here](#).

Cisco General

IOS Specifics

Command-Line Interface (CLI)

One of the nicest things about working on Cisco routers is the transparency of IOS. Because a similar command set has been developed for each family of routers, the knowledge gained from working on one router is applicable to others.

This nicety does not carryover into the world of Cisco switches. Because there are several families of switches that were acquired from disparate places, the Command Line Interface (CLI) differs significantly between the families of switches.

- ❖ **Menu Configurable** - Found primarily on older low-end switches, there are several different menu based systems, such as those found on the 1900 or 3900 series switches. These are meant to be intuitive, but have their own configuration problems awaiting the uninitiated, not the least of which is figuring out what keys the menu expects you to use to select between options.
- ❖ **IOS-Like** - Another common CLI is the IOS-like version found on many Access-layer switches, like the 2950 and 3550 series. Those who have worked on Cisco routers in the past will find that the command nomenclature is familiar and, other than a few new commands, the same rules generally apply.

- ❖ **Set-based** - The most common CLI is that which was brought into the Cisco family with the acquisition of Crescendo Communications in 1993. It is found on the Catalyst 4000/5000/6000 series of switches, and is often called XDI, CatOS, or the Set-based CLI. This is what you will find on most of the Core and Distribution layer switches, and most new products use this CLI. XDI is based on the Unix csh or c-shell prompt, and the reason it is commonly called the Set-based CLI is that "Set" is one of the three primary commands used. Most commands start with one of the following keywords:
 - *Set* – Implements configuration changes.
 - *Show* – Verifies and provides information on the configuration.
 - *Clear* – Removes configuration elements.