CCIE Security Version 5 Advanced Technologies Class

Access-Lists Logging

What is ACL logging?

What are the ACL logging options?

Access-List Logging Overview

- Whenever an ACL entry is matched, it might be useful for the router to generate a log message
  - Troubleshooting
  - Monitoring and tracking user traffic
- With ACL logging, the router can log information about
  - Only layer3/layer 4 headers of the packet
  - Layer2/layer3/layer4 headers of the packet, including the ingress interface

Access-List Logging Overview

- Each time the router needs to log a message
  - CPU is affected as it needs to generate the log
- In order to protect the CPU, by default:
  - The router generates a message only for each first packet (unique layer2/layer3/layer4) of a session
  - All matches are counted for a 5 minute interval and reported afterwards (this timer is not configurable)

Access-List Logging Enhancements

- ▷To further protect the CPU
  - A global interval affecting all ACL's may be configured to control how many packets can be processed-switched per-interval, regardless of how many ACE's are configured for logging
  - This only works for IPv4 ACL's
- ▷If you need logging to happen more often than 5 minutes
  - A global threshold can be configured which specifies after how many hits a new log should be generated

Access-List Syslog Enhancements

- For easier identification and monitoring of ACL log messages from a remote syslog server
  - Each ACL entry can include a unique router-generated MD5 hash
  - Each ACL entry can include a user-defined cookie

Access-List Syslog Enhancements

▷Implementation Steps

- Configure ACL logging
- Verify its functionality

▷Optional Implementation Steps

- Configure ACL logging enhancements
- Verify its functionality

Knowledge is Power!