CHAPTER 31

Access Control Lists

This chapter describes the level of support that Cisco ANA provides for Access Control Lists (ACLs), as follows:

Technology Description

ACLs

An ACL is a group of statements. Each defines a pattern of data that can be found in an IP packet. As each packet comes through an interface with an associated ACL, the ACL is scanned from top to bottom, in the exact order in which it was entered, for a pattern that matches the incoming packet. A permit or deny rule associated with each pattern determines that packet's fate. A mask (similar to a wild card) can also be used to determine how much of an IP source or destination address to use when matching against the pattern. The pattern statement can also include a TCP or UDP port.

Note that Cisco ANA currently supports IP ACLs only. MAC ACLs are not supported.

Information Model Objects (IMOs)

This section describes the following IMOs:

- Access List Traffic Descriptor (IAccessList)
- Access List Entry (IAccessListEntry)

Access List Traffic Descriptor

The Access List Traffic Descriptor, with its Access List Entry objects, describes an access list of a single type (*Unknown, Standard, Extended,* or *Rate Limit*). It is aggregated by a Traffic Descriptor Container object (see Common Components).

Table 31-1 Access List Traffic Descriptor (IAccessList)

Attribute Name	Attribute Description	Scheme	Polling Interval
Type	Access list type (*Unknown, Standard, Extended, Rate Limit*)	Any	Configuration
Access List Entries Table	Array of instances of Access List Entry	Any	Configuration
Name or ID	Traffic descriptor name or identifier	Any	Configuration
Index	Traffic descriptor index	Any	Configuration

Access List Entry

Table 31-2 Access List Entry (IAccessListEntry)

Attribute Name	Attribute Description	Scheme	Polling Interval
Entry Identification	Entry identifier.	Any	Configuration
Action Logic	Action logic (*Unknown, Permit, Deny*).	Any	Configuration
Source and Destination Address	Source and destination IP address.	Any	Configuration
Source and Destination Wildcard	Source and destination IP wildcard.	Any	Configuration
Protocol Type	Internet Assigned Numbers Authority (IANA) type of the protocol (*HOPORT, ICMP, IGMP, GGP, IP in IP, ST, TCP, CBT, EGP, IGP*, and so on).	Any	Configuration
Source and Destination Ports Ranges	Source and destination TCP/UDP port ranges.	Any	Configuration
Source and Destination Port Action	Source and destination port action (*Null, Equal, Not Equal, Greater Than, Less Than, Range*).	Any	Configuration
Protocol Specific Info	Protocol specific information.	Any	Configuration
Differential Services Code Points	Differential Services Code Points (DSCP).	Any	Configuration

Table 31-2 Access List Entry (IAccessListEntry) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Type of Service	Type of Service (ToS) (*Normal [0], Min Cost [1], Max Reliability [2], 3, Max Throughput [4], 5, 6, 7, Min Delay [8], 9, 10, 11, 12, 13, 14, 15*).	Any	Configuration
Precedence	Precedence (*Routine [0], Priority [1], Immediate [2], Flash [3], Flash Override [4], Critical [5], Internet [6], Network [7]*).	Any	Configuration
Matches	The number of matches made.	Any	Configuration

Vendor-Specific Inventory and IMOs

In this chapter, Information Model Objects (IMOs), page 31-2, currently describes Cisco's QoS objects. However, these are generic QoS objects that can be used by other vendors.

Network Topology

There is no specific network topology associated with this technology.

Service Alarms

There are no faults or alarms associated with this technology.

For detailed information about alarms and correlation, see the *Cisco Active Network Abstraction 3.7 User Guide*.