



CHAPTER 3

AclApp Service

This chapter describes the DCNM web services' API methods for the AclApp service.

Information About AclApp Service

An access control list (ACLs) allows you to perform packet classification and filtering. An ACL is an ordered set of access control rules. An access control rule is commonly referred to as an access control entry (ACE). Each ACE specifies a packet matching criteria and an action.

Matching criteria can be defined based on packet parameters such as the source address, and the destination address and protocols. An action permits or denies packets that match the specified criteria. A packet may match multiple ACEs in an ACL, but only the first matching ACE is considered. If a packet does not match any of the ACEs, then the packet is dropped.

An ACL must be attached to a target for the target to be activated. The target can be a Layer 3 interface, a VLAN, or a Layer 2 interface.

The API categories are as follows:

- IPv4 ACL—An IPv4 ACL is used to refer the following:
 - Standard IP access lists—Classify or filter traffic using a source address (IPv4 addresses).
 - Extended IP access lists—Classify or filter traffic using a source and destination address (IPv4 addresses) and optional protocol type information.
- MAC ACL— Classify or filter traffic using source and destination MAC addresses and optional protocol type information.
- IPv6 ACL— Classify or filter IPv6 traffic using source and destination addresses and optional protocol type information.
- VLAN Access Map—Provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN.
- Role-based access control lists (RBACL)—Provide access control within a Cisco TrustSec (CTS) domain.

ACL service APIs are defined for the following categories:

- Query/Get APIs—Query data from the persistent database.
- Create APIs—Create new ACLs.
- Modify APIs—Modify existing ACLs.
- Delete APIs—Delete existing ACLs.

Send document comments to nexus7k-docfeedback@cisco.com

- Bind and Unbind APIs—Bind and unbind an association between ACLs and other features.

addRedirectNetworkInterfacesToVlanAccessMapEntry

Assigns one or more network interfaces as redirect interfaces of a VACE. If there are already some interfaces used as redirect interfaces in that VACE, then these interfaces will be added to the existing list of redirected interfaces.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceId is not a valid VlanAccessMapEntry InstanceNameId.
- If the networkInterfaceInstanceIdCol collection is null or the collection is empty.
- If the networkInterfaceInstanceIdCol collection contains any null element, or the collection contains an invalid NetworkInterface InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceId—InstanceId of VlanAccessMapEntry object.

networkInterfaceInstanceIdCol—a collection of InstanceNameId of NetworkInterface objects to which the classified/filtered traffic needs to be redirected.

Return Value

void

bindIpv4AclToNetworkInterfaces

Assigns an IPv4 ACL to one or more network interfaces in a specified direction.

ParameterException is thrown if any of the following situations occurs:

- If ipv4AclInstanceId is null or it is empty.
- If ipv4AclInstanceId is not a valid StandardAccessControlList or ExtendedAccessControlList InstanceNameId.
- If the networkInterfaceInstanceIdCol collection is null or the collection is empty.
- If the networkInterfaceInstanceIdCol collection contains any null element, or the collection contains an invalid InstanceNameId of a NetworkInterface.
- If the direction is null.

Parameters

opContext—Operational context. operational context.

networkInterfaceInstanceIdCol—a collection that contains one or more InstanceNameId of NetworkInterface object.

ipv4AclInstanceId—InstanceId of a StandardAccessControlList or ExtendedAccessControlList object.

Send document comments to nexus7k-docfeedback@cisco.com

direction—direction of the network interface traffic, on which the IPv4 ACL needs to be applied. Direction can be either "IN" or "OUT".

Return Value

A list of newly created AclAppliesToNetworkInterface objects.

bindIpv4AclsToVlanAccessMapEntry

Applies one or more IPv4 ACLs to a VACE to filter/classify traffic. If there are already some IPv4 ACLs assigned to that VACE, then these IPv4 ACLs will be added to the existing list.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceNameId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceNameId is not a valid VlanAccessMapEntry InstanceNameId.
- If the ipv4AclInstanceNameIdCol collection is null or the collection is empty.
- If the ipv4AclInstanceNameIdCol collection contains any null element, or the collection contains an invalid StandardAccessControlEntry or ExtendedAccessControlList InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceNameId—InstanceNameId of VlanAccessMapEntry object.

ipv4AclInstanceNameIdCol—a collection of InstanceNameId of one or more StandardAccessControlList or ExtendedAccessControlList objects.

Return Value

void

bindIpv6AclToNetworkInterfaces

Assigns an IPv6 ACL to one or more network interfaces in a specified direction.

ValidationException is thrown if any of the following situations occurs:

- If ipv6AclInstanceNameId is null or it is not of type Ipv6AccessControlList InstanceNameId.
- If ipv6AclInstanceNameId is not a valid Ipv6AccessControlList InstanceNameId.
- If the networkInterfaceInstanceNameIdCol collection is null or the collection is empty.
- If the networkInterfaceInstanceNameIdCol collection contains any null element, or the collection contains an invalid NetworkInterface InstanceNameId.
- If the direction is null.

Parameters

opContext—Operational context.

networkInterfaceInstanceNameIdCol—a collection that contains one or more InstanceNameId of NetworkInterface object.

ipv6AclInstanceNameId—InstanceNameId of a Ipv6AccessControlList object.

Send document comments to nexus7k-docfeedback@cisco.com

direction—direction of the network interface traffic, on which the IPv6 ACL needs to be applied. Direction can be "IN" or "OUT".

Return Value

A list of newly created AclAppliesToNetworkInterface objects.

bindIpv6AclsToVlanAccessMapEntry

Applies one or more IPv6 ACLs to a VACE to filter/classify traffic. If there are already some IPv6 ACLs assigned to that VACE, then these IPv6 ACLs will be added to the existing list.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceNameId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceNameId is not a valid VlanAccessMapEntry InstanceNameId.
- If the ipv6AclInstanceNameIdCol collection is null or the collection is empty.
- If the ipv6AclInstanceNameIdCol collection contains any null element, or the collection contains an invalid Ipv6AccessControlList InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceNameId—InstanceNameId of VlanAccessMapEntry object.

ipv6AclInstanceNameIdCol—a collection of InstanceNameId of one or more Ipv6AccessControlList objects.

Return Value

void

bindMacAclToNetworkInterfaces

Assigns an MAC ACL to one or more network interfaces in a specified direction.

ValidationException is thrown if any of the following situations occurs:

- If macAclInstanceNameId is null or it is not of type MacAccessControlList InstanceNameId.
- If macAclInstanceNameId is not a valid MacAccessControlList InstanceNameId.
- If the networkInterfaceInstanceNameIdCol collection is null or the collection is empty.
- If the networkInterfaceInstanceNameIdCol collection contains any null element, or the collection contains an invalid NetworkInterface InstanceNameId.
- If the direction is null.

Parameters

opContext—Operational context.

networkInterfaceInstanceNameIdCol—a collection that contains one or more InstanceNameId of NetworkInterface object.

macAclInstanceNameId—InstanceNameId of a MacAccessControlList object.

Send document comments to nexus7k-docfeedback@cisco.com

direction—direction of the network interface traffic, on which the MAC ACL needs to be applied.

Return Value

A list of newly created AclAppliesToNetworkInterface objects.

bindMacAclsToVlanAccessMapEntry

Applies one or more MAC ACLs to a VACE to filter/classify traffic. If there are already some MAC ACLs assigned to that VACE, then these MAC ACLs will be added to the existing list.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceId is not a valid VlanAccessMapEntry InstanceNameId.
- If the macAclInstanceIdCol collection is null or the collection is empty.
- If the macAclInstanceIdCol collection contains any null element, or the collection contains an invalid MacAccessControlList InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceId—InstanceId of VlanAccessMapEntry object.

macAclInstanceIdCol—a collection of InstanceNameId of one or more MacAccessControlList objects.

Return Value

void

bindTimeRangeToAces

Assigns a time range to one or more ACEs.

ValidationException is thrown if any of the following situations occurs:

- If timerangeInstanceId is null or it is not of type TimeRange InstanceNameId.
- If timerangeInstanceId is not a valid TimeRange InstanceNameId.
- If the aceInstanceIdCol collection is null or the collection is empty.
- If the aceInstanceIdCol collection contains any null element, or the collection contains an invalid ExtendedAccessControlList, Ipv6AccessControlList or RoleBasedAccessControlList InstanceNameId.
- If the direction is null.

Parameters

opContext—Operational context.

aceInstanceIdCol—List of Extended ACEs, IPv6 ACEs or Role Based ACEs on which time range need to be applied.

timerangeInstanceId—Instance name ID of a timerange object.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

void

bindVlanAccessMapToVlans

Assigns an VACL to one or more VLANs.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapEntryInstanceId is null or it is not of type VlanAccessMap InstanceNameId.
- If vlanAccessMapEntryInstanceId is not a valid VlanAccessMap InstanceNameId.
- If the vlanIds is null.

Parameters

opContext—Operational context.

vlanAccessMapInstanceId—InstanceId of a VlanAccessMap object.

vlanIds—One or more VLAN ID, that uniquely identifies a VLAN.

Return Value

void

createExtendedIpAcls

Creates one or more Extended IP ACL objects in a network element. Given the InstanceNameId of a network element and a list of Extended IP ACL objects, creates the objects in the server and returns its instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceId is null.
- If neInstanceId is not a valid network element InstanceNameId.
- If the extendedIpAclCol is null or the collection is empty.
- If the extendedIpAclCol contains one or more null element, or the collection contains objects that are not of type ExtendedAccessControlList.
- If the ExtendedAccessControlEntry, inside the ExtendedAccessControlList does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the extendedIpAclCol collection, if any of the ExtendedAccessControlList attribute is not valid or the ExtendedAccessControlEntry inside a Extended ACL is not valid.

Example:

- name of an ACL starts with a number. Because, an ACL name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the extendedIpAclCol contains a ExtendedAccessControlList that already exist in the database.

Send document comments to nexus7k-docfeedback@cisco.com

- If a ExtendedAccessControlList in the extendedIpAclCol contains duplicate ExtendedAccessControlEntry objects.

This API will not consider the interface association. If a Extended ACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the Extended ACL to an interface.

Parameters

opContext—Operational context. operational context.

neInstanceId—InstanceId of a network element.

extendedIpAclCol—a collection (one or more) of Extended ACL objects that needs to be created.

Return Value

Instance name IDs of the newly created Extended ACL objects.

createIpv6Acls

Creates one or more IPv6 ACL objects in a network element. Given the InstanceNameId of a network element and a list of IPv6 ACL objects, creates the objects in the server and returns it's instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceId is null.
- If neInstanceId is not a valid network element InstanceNameId.
- If the ipv6AclCol is null or the collection is empty.
- If the ipv6AclCol contains one or more null element, or the collection contains objects that are not of type Ipv6AccessControlList.
- If the Ipv6AccessControlEntry, inside the Ipv6AccessControlList does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the ipv6AclCol collection, if any of the Ipv6AccessControlList attribute is not valid or the Ipv6AccessControlEntry inside a IPv6 ACL is not valid.

Example:

- name of an ACL starts with a number. Because, an ACL name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the ipv6AclCol contains a Ipv6AccessControlList that already exist in the database.
- If a Ipv6AccessControlList in the ipv6AclCol contains duplicate Ipv6AccessControlEntry objects.

This API will not consider the interface association. If a IPv6 ACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the IPv6 ACL to an interface.

Parameters

opContext—Operational context.

Send document comments to nexus7k-docfeedback@cisco.com

neInstanceNameId—InstanceNameId of a network element.

ipv6AclCol—a collection (one or more) of IPv6 ACL objects that needs to be created.

Return Value

Instance name IDs of the newly created IPv6 ACL objects.

createMacAcls

Creates one or more MAC ACL objects in a network element. Given the InstanceNameId of a network element and a list of MAC ACL objects, creates the objects in the server and returns its instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceNameId is null.
- If neInstanceNameId is not a valid network element InstanceNameId.
- If the macAclCol is null or the collection is empty.
- If the macAclCol contains one or more null element, or the collection contains objects that are not of type MacAccessControlList.
- If the MacAccessControlEntry, inside the MacAccessControlList does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the macAclCol collection, if any of the MacAccessControlList attribute is not valid or the MacAccessControlEntry inside a MAC ACL is not valid.

Example:

- name of an ACL starts with a number. Because, an ACL name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the macAclCol contains a MacAccessControlList that already exist in the database.
- If a MacAccessControlList in the macAclCol contains duplicate MacAccessControlEntry objects.

This API will not consider the interface association. If a MAC ACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the MAC ACL to an interface.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of a network element.

macAclCol—a collection (one or more) of MAC ACL objects that needs to be created.

Return Value

Instance name IDs of the newly created MAC ACL objects.

Send document comments to nexus7k-docfeedback@cisco.com

createRbaclPolicies

Creates one or more Role Based ACL Policy objects in a network element. Given the InstanceNameId of a network element and a list of Role Based ACL Policy objects, creates the objects in the server and returns its instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceNameId is null.
- If neInstanceNameId is not a valid network element InstanceNameId.
- If the rbaclPolicyCol is null or the collection is empty.
- If the rbaclPolicyCol contains one or more null element, or the collection contains objects that are not of type RoleBasedAccessControlPolicy.

PropertiesException is thrown if any of the following situations occurs:

- In the rbaclPolicyCol collection, if any of the RoleBasedAccessControlPolicy attribute is not valid or the RoleBasedAccessControlEntry inside a Role Based ACL Policy is not valid.

IntegrityException is thrown if any of the following situations occurs:

- If the rbaclPolicyCol contains a RoleBasedAccessControlPolicy that already exist in the database.
- If a RoleBasedAccessControlPolicy in the rbaclPolicyCol contains duplicate elements.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of a network element.

rbaclPolicyCol—a collection (one or more) of RoleBasedAccessControlPolicy objects that needs to be created.

Return Value

Instance name IDs of the newly created RoleBasedAccessControlPolicy objects.

createRbacls

Creates one or more RBACL objects in a network element. Given the InstanceNameId of a network element and a list of RBACL objects, creates the objects in the server and returns its instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceNameId is null.
- If neInstanceNameId is not a valid network element InstanceNameId.
- If the rbaclCol is null or the collection is empty.
- If the rbaclCol contains one or more null element, or the collection contains objects that are not of type RoleBasedAccessControlList.
- If the RoleBasedAccessControlEntry, inside the RoleBasedAccessControlList does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the rbaclCol collection, if any of the RoleBasedAccessControlList attribute is not valid or the RoleBasedAccessControlEntry inside a RBACL is not valid.

Send document comments to nexus7k-docfeedback@cisco.com

Example:

- name of an ACL starts with a number. Because, an ACL name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the rbaclCol contains a RoleBasedAccessControlList that already exist in the database.
- If a RoleBasedAccessControlList in the rbaclCol contains duplicate RoleBasedAccessControlEntry objects.

This API will not consider the interface association. If a RBACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the RBACL to an interface.

Parameters

opContext—Operational context.

neInstanceId—InstanceId of a network element.

rbaclCol—a collection (one or more) of RBACL objects that needs to be created.

Return Value

Instance name IDs of the newly created RBACL objects.

createStandardIpAcls

Creates one or more standard IP ACL objects in a network element. Given the InstanceNameId of a network element and a list of StandardAccessControlList objects, creates the objects in the server and returns the created StandardAccessControlList objects.

InstanceException is thrown if any of the following situations occurs:

- If neInstanceId is null.
- If neInstanceId is not a valid InstanceNameId of a network element.

ParameterException is thrown if any of the following situations occurs:

- If the standardIpAclCol is null or the collection is empty.
- If the standardIpAclCol contains one or more null element, or the collection contains objects that are not of type StandardAccessControlList.
- If the StandardAccessControlEntry, inside the StandardAccessControlList does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the standardIpAclCol collection, if any of the StandardAccessControlList attribute is not valid or the StandardAccessControlEntry inside a StandardAccessControlList is not valid.

Example:

- name of an ACL starts with a number. Because, an ACL name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
- Remark description value of an ACL has more than 100 characters.

FeatureException is thrown if any of the following situations occurs:

Send document comments to nexus7k-docfeedback@cisco.com

- If the standardIpAclCol contains a StandardAccessControlList that already exist in the database.
- If a StandardAccessControlList in the standardIpAclCol contains duplicate StandardAccessControlEntry objects.

This API will not consider the interface association. If a StandardAccessControlList is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the StandardAccessControlList to an interface.

Parameters

opContext—Operational context. operational context.

neInstanceId—InstanceId of a network element.

standardIpAclCol—a collection (one or more) of StandardAccessControlList objects that will be created in the database.

Return Value

StandardAccessControlList objects that are newly created.

createTimeRanges

Creates one or more TimeRange objects in a network element. Given the InstanceNameId of a network element and a list of TimeRange objects, creates the objects in the server and returns it's instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceId is null.
- If neInstanceId is not a valid network element InstanceNameId.
- If the timerangeCol is null or the collection is empty.
- If the timerangeCol contains one or more null element, or the collection contains objects that are not of type TimeRange.

PropertiesException is thrown if any of the following situations occurs:

- In the timerangeCol collection, if any of the TimeRange attribute is not valid or the PeriodicTimeRange inside a TimeRange is not valid.

Example:

- name of a TimeRange starts with a number. Because, an TimeRange name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

IntegrityException is thrown if any of the following situations occurs:

- If the timerangeCol contains a TimeRange that already exist in the database.
- If a TimeRange in the timerangeCol contains duplicate PeriodicTimeRange objects.

This API will not consider the ACE association. If a TimeRange is passed with the ACE association, that will not be considered by this API. User needs to call separate API to bind the TimeRange to an ACE.

Parameters

opContext—Operational context.

neInstanceId—InstanceId of a network element.

Send document comments to nexus7k-docfeedback@cisco.com

timerangeCol—a collection (one or more) of TimeRange objects that needs to be created.

Return Value

Instance name IDs of the newly created TimeRange objects.

createVlanAccessMaps

Creates one or more VACL objects in a network element. Given the InstanceNameId of a network element and a list of VACL objects, creates the objects in the server and returns its instance name IDs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceNameId is null.
- If neInstanceNameId is not a valid network element InstanceNameId.
- If the vlanAccessMapEntryCol is null or the collection is empty.
- If the vlanAccessMapEntryCol contains one or more null element, or the collection contains objects that are not of type VlanAccessMap.
- If the VlanAccessMapEntry, inside the VlanAccessMap does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the vlanAccessMapEntryCol collection, if any of the VlanAccessMap attribute is not valid or the VlanAccessMapEntry inside a VACL is not valid.

Example:

- name of an ACL starts with a number. Because, an ACL name, cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the vlanAccessMapEntryCol contains a VlanAccessMap that already exist in the database.
- If a VlanAccessMap in the vlanAccessMapEntryCol contains duplicate VlanAccessMapEntry objects.

This API will not consider the interface association. If a VACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the VACL to an interface.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of a network element.

vlanAccessMapCol—a collection (one or more) of VACL objects that needs to be created.

Return Value

Instance name IDs of the newly created VACL objects.

deleteExtendedIpAcls

Deletes one or more Extended IP ACL objects. Given the InstanceNameId of the ExtendedAccessControlList objects, those objects will be deleted from the server.

Send document comments to nexus7k-docfeedback@cisco.com

ValidationException is thrown if any of the following situations occurs:

- If extendedIpAclInstanceNameIdCol collection is null or it is empty.
- If extendedIpAclInstanceNameIdCol collection contains an element that is not of type ExtendedAccessControlList InstanceNameId.
- If extendedIpAclInstanceNameIdCol collection contains a ExtendedAccessControlList that does not exist in the database.

Parameters

opContext—Operational context.

extendedIpAclInstanceNameIdCol—a collection that contains InstanceNameId of one or more ExtendedAccessControlList objects that needs to be deleted.

Return Value

void

deletelpv6Acls

Deletes one or more IPv6 ACL objects. Given the InstanceNameId of the Ipv6AccessControlList objects, those objects will be deleted from the server.

ValidationException is thrown if any of the following situations occurs:

- If ipv6AclInstanceNameIdCol collection is null or it is empty.
- If ipv6AclInstanceNameIdCol collection contains an element that is not of type Ipv6AccessControlList InstanceNameId.
- If ipv6AclInstanceNameIdCol collection contains a Ipv6AccessControlList that does not exist in the database.

Parameters

opContext—Operational context.

ipv6AclInstanceNameIdCol—a collection that contains InstanceNameId of one or more Ipv6AccessControlList objects that needs to be deleted.

Return Value

void

deleteMacAcls

Deletes one or more MAC ACL objects. Given the InstanceNameId of the MacAccessControlList objects, those objects will be deleted from the server.

ValidationException is thrown if any of the following situations occurs:

- If macAclInstanceNameIdCol collection is null or it is empty.
- If macAclInstanceNameIdCol collection contains an element that is not of type MacAccessControlList InstanceNameId.

Send document comments to nexus7k-docfeedback@cisco.com

- If macAclInstanceNameIdCol collection contains a MacAccessControlList that does not exist in the database.

Parameters

opContext—Operational context.

macAclInstanceNameIdCol—a collection that contains InstanceNameId of one or more MacAccessControlList objects that needs to be deleted.

Return Value

void

deleteRbacPolicies

Deletes one or more Role based ACL Policy objects. Given the InstanceNameId of the RoleBasedAccessControlPolicy objects, those objects will be deleted from the server.

ValidationException is thrown if any of the following situations occurs:

- If rbacPolicyInstanceNameIdCol collection is null or it is empty.
- If rbacPolicyInstanceNameIdCol collection contains an element that is not of type RoleBasedAccessControlPolicy InstanceNameId.
- If rbacPolicyInstanceNameIdCol collection contains a RoleBasedAccessControlPolicy that does not exist in the database.

Parameters

opContext—Operational context.

rbacPolicyInstanceNameIdCol—a collection that contains InstanceNameId of one or more RoleBasedAccessControlPolicy objects that needs to be deleted.

Return Value

void

deleteRbacIs

Deletes one or more Role based ACL objects. Given the InstanceNameId of the RoleBasedAccessControlList objects, those objects will be deleted from the server.

ValidationException is thrown if any of the following situations occurs:

- If rbacInstanceNameIdCol collection is null or it is empty.
- If rbacInstanceNameIdCol collection contains an element that is not of type RoleBasedAccessControlList InstanceNameId.
- If rbacInstanceNameIdCol collection contains a RoleBasedAccessControlList that does not exist in the database.

Parameters

opContext—Operational context.

Send document comments to nexus7k-docfeedback@cisco.com

rbaclInstanceNameIdCol—a collection that contains InstanceNameId of one or more RoleBasedAccessControlList objects that needs to be deleted.

Return Value

void

deleteStandardIpAcls

Deletes one or more standard IP ACL objects. Given the InstanceNameId of the StandardAccessControlList objects, those objects will be deleted from the server.

ParameterException is thrown if any of the following situations occurs:

- If standardIpAclInstanceNameIdCol collection is null or it is empty.
- If standardIpAclInstanceNameIdCol collection contains an element that is not of type StandardAccessControlList InstanceNameId.
- If standardIpAclInstanceNameIdCol collection contains a StandardAccessControlList that does not exist in the database.

Parameters

opContext—Operational context. operational context.

standardIpAclInstanceNameIdCol—a collection that contains InstanceNameId of one or more StandardAccessControlList objects that needs to be deleted.

Return Value

void

deleteTimeRanges

Deletes one or more TimeRange objects. Given the InstanceNameId of the TimeRange objects, those objects will be deleted from the server.

ValidationException is thrown if any of the following situations occurs:

- If timerangeInstanceNameIdCol collection is null or it is empty.
- If timerangeInstanceNameIdCol collection contains an element that is not of type TimeRange InstanceNameId.
- If timerangeInstanceNameIdCol collection contains a TimeRange that does not exist in the database.

Parameters

opContext—Operational context.

timerangeInstanceNameIdCol—a collection that contains InstanceNameId of one or more TimeRange objects that needs to be deleted.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com

deleteVlanAccessMaps

Deletes one or more VACL objects. Given the InstanceNameId of the VlanAccessMap objects, those objects will be deleted from the server.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapEntryInstanceNameIdCol collection is null or it is empty.
- If vlanAccessMapEntryInstanceNameIdCol collection contains an element that is not of type VlanAccessMap InstanceNameId.
- If vlanAccessMapEntryInstanceNameIdCol collection contains a VlanAccessMap that does not exist in the database.

Parameters

opContext—Operational context.

vlanAccessMapInstanceNameIdCol—a collection that contains InstanceNameId of one or more VlanAccessMap objects that needs to be deleted.

Return Value

void

getAssociatedVlanAccessMap

Returns VlanAccessMap associated to a VLAN. Given a network element InstanceNameId and a VLAN ID in the network element, returns VlanAccessMap object associated to that VLAN.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of a network element.

vlanId—ID of a VLAN.

Return Value

VlanAccessMap object associated to the VLAN with given VLAN ID. In the returned VlanAccessMap object, only the following associations will be present, and all other associations will be cleared.

- All associated VlanAccessMapEntry in the returned VlanAccessMap object.
- IP ACL/MAC ACL/IPv6 ACL objects associated with each VlanAccessMapEntry (as these ACLs are used as match conditions in VlanAccessMapEntry), if any, in VlanAccessMap. In IP/MAC/IPv6 ACLs all associations will be cleared, except that of VlanAccessMapEntry.
- NetworkInterface objects associated with each VlanAccessMapEntry, if any, as redirect interfaces. In the network interfaces all associations will be cleared, except that of VlanAccessMapEntry.

Returns null if no VlanAccessMap is associated to that VLAN.

Send document comments to nexus7k-docfeedback@cisco.com

getExtendedIpAclToNetworkInterfaceAssociationsInNetwork Element

Returns all ExtendedAccessControlList objects to NetworkInterface associations configured in a network element. Given the InstanceNameId of the network element, returns a collection of ExtendedAccessControlList to NetworkInterface association objects.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of AclAppliesToNetworkInterface objects, that represents the association between ExtendedAccessControlList and NetworkInterface. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- ExtendedAccessControlList object. In the ACL object all the associations will be cleared, except AclAppliesToNetworkInterface association.
- NetworkInterface object. In the NetworkInterface object all the associations will be cleared, except AclAppliesToNetworkInterface association.

getExtendedIpAcls

Returns ExtendedAccessControlList objects from its InstanceNameIds. Given a collection of InstanceNameId of ExtendedAccessControlList, returns corresponding ExtendedAccessControlList objects.

ValidationException is thrown if any of the following situations occurs:

- If extendedIpAclInstanceNameIdCol is null or it is empty.
- If extendedIpAclInstanceNameIdCol contains invalid InstanceNameId of a ExtendedAccessControlList.
- If extendedIpAclInstanceNameIdCol contains a null value.
- If there is no equivalent ExtendedAccessControlList object with the given InstanceNameId in the extendedIpAclInstanceNameIdCol.

Parameters

opContext—Operational context.

extendedIpAclInstanceNameIdCol—a collection of InstanceNameId of ExtendedAccessControlList.

Return Value

List of ExtendedAccessControlList objects corresponding to given collection of InstanceNameId. In the returned list of ExtendedAccessControlList objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.

Send document comments to nexus7k-docfeedback@cisco.com

- TimeRange association for every ACEs, if any, in ExtendedAccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getExtendedIpAclsInNetworkElement

Returns all ExtendedAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of ExtendedAccessControlList objects in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of ExtendedAccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRangeassociation for every ACEs, if any, in ExtendedAccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getExtendedNamedIpAclsInNetworkElement

Returns all named ExtendedAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of ExtendedAccessControlList objects in the network element, that are uniquely identified by it's name.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of named ExtendedAccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList. If that TimeRangehas other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

Send document comments to nexus7k-docfeedback@cisco.com

getExtendedNumberedIpAclsInNetworkElement

Returns all numbered ExtendedAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of ExtendedAccessControlList objects in the network element, that are uniquely identified by its number.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of numbered ExtendedAccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getIpAclToNetworkInterfaceAssociationsInNetworkElement

Returns all IP ACLs (IPv4 ACLs and IPv6 ACLs) to network interface associations configured in a network element. Given the instance name ID of the network element, returns a collection of IP ACL to network interface association objects.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of AclAppliesToNetworkInterface objects, that represents the association between Standard/Extended/IPv6 ACL and NetworkInterface. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- StandardAccessControlList, ExtendedAccessControlList or Ipv6AccessControlList object. In the ACL object all the associations will be cleared, except AclAppliesToNetworkInterface association.
- NetworkInterface object. In the NetworkInterface object all the associations will be cleared, except AclAppliesToNetworkInterface association.

getIpAclsInNetworkElement

Returns all IP ACLs (IPv4 ACLs and IPv6 ACLs) configured in a network element. Given the InstanceNameId of the network element, returns a collection of IP ACL objects.

Send document comments to nexus7k-docfeedback@cisco.com

InstanceException is thrown if the argument passed neInstanceId is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context. operational context.

neInstanceId—InstanceNameId of the network element.

Return Value

List of StandardAccessControlList, ExtendedAccessControlList and Ipv6AccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- All associated remarks of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList and Ipv6AccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

Returned ACLs will be ordered by the name or number of the ACL.

getIpv4AclToNetworkInterfaceAssociationsInNetworkElement

Returns all IPv4 ACLs both StandardAccessControlList and ExtendedAccessControlList objects) to NetworkInterface associations configured in a network element. Given the InstanceNameId of the network element, returns a collection of IPv4 ACL to NetworkInterface association objects.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceId—InstanceNameId of the network element.

Return Value

List of AclAppliesToNetworkInterface objects, that represents the association between Standard/Extended ACL and NetworkInterface. NetworkInterface. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- StandardAccessControlList or ExtendedAccessControlList object. In the ACL object all the associations will be cleared, except AclAppliesToNetworkInterface association.
- NetworkInterface object. In the NetworkInterface object all the associations will be cleared, except AclAppliesToNetworkInterface association.

getIpv4Acls

Returns IPv4 ACLs (both StandardAccessControlList and ExtendedAccessControlList objects) from it's InstanceNameIds. Given a collection of InstanceNameId of StandardAccessControlList and ExtendedAccessControlList, returns corresponding StandardAccessControlList and ExtendedAccessControlList objects.

Send document comments to nexus7k-docfeedback@cisco.com

ValidationException is thrown if any of the following situations occurs:

- If ipv4AclInstanceNameIdCol is null or it is empty.
- If ipv4AclInstanceNameIdCol contains invalid InstanceNameId of a StandardAccessControlList or ExtendedAccessControlList.
 - null value.
- If there is no equivalent IPv4 ACL object with the given InstanceNameId in the ipv4AclInstanceNameIdCol.

Parameters

opContext—Operational context.

ipv4AclInstanceNameIdCol—a collection of InstanceNameId of StandardAccessControlList and ExtendedAccessControlList.

Return Value

List of StandardAccessControlList and ExtendedAccessControlList objects corresponding to given collection of InstanceNameId. In the returned list of IPv4 ACL objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getIpv4AclsInNetworkElement

Returns all IPv4 ACLs (Standard ACLs and Extended ACLs) configured in a network element. Given the InstanceNameId of the network element, returns a collection of IP ACL objects.

InstanceException is thrown if the argument passed neInstanceNameId is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context. operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of StandardAccessControlList, ExtendedAccessControlList and Ipv6AccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- All associated remarks of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList and Ipv6AccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

Returned ACLs will be ordered by the name or number of the ACL.

Send document comments to nexus7k-docfeedback@cisco.com

getIpv4AclsWithoutAcesInNetworkElement

Returns all IPv4 ACLs (Standard ACLs and Extended ACLs) configured in a network element. Given the InstanceNameId of the network element, returns a collection of IP ACL objects.

InstanceException is thrown if the argument passed neInstanceNameId is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context. operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of StandardAccessControlList, ExtendedAccessControlList and Ipv6AccessControlList objects. In the returned list of objects, all associations will be cleared. Returned ACLs will be ordered by the name or number of the ACL.

getIpv6AclToNetworkInterfaceAssociationsInNetworkElement

Returns all Ipv6AccessControlList objects to NetworkInterface associations configured in a network element. Given the InstanceNameId of the network element, returns a collection of Ipv6AccessControlList to NetworkInterface association objects.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of AclAppliesToNetworkInterface objects, that represents the association between Ipv6AccessControlList and NetworkInterface. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- Ipv6AccessControlList object. In the ACL object all the associations will be cleared, except AclAppliesToNetworkInterface association.
- NetworkInterface object. In the NetworkInterface object all the associations will be cleared, except AclAppliesToNetworkInterface association.

getIpv6Acls

Returns Ipv6AccessControlList objects from it's InstanceNameIds. Given a collection of InstanceNameId of Ipv6AccessControlList}, returns corresponding Ipv6AccessControlList objects.

ValidationException is thrown if any of the following situations occurs:

- If ipv6AclInstanceNameIdCol is null or it is empty.
- If ipv6AclInstanceNameIdCol contains invalid InstanceNameId of a Ipv6AccessControlList.

Send document comments to nexus7k-docfeedback@cisco.com

- If ipv6AclInstanceNameIdCol contains a null value.
- If there is no equivalent Ipv6AccessControlList object with the given InstanceNameId in the ipv6AclInstanceNameIdCol.

Parameters

opContext—Operational context.

ipv6AclInstanceNameIdCol—a collection of InstanceNameId of Ipv6AccessControlList.

Return Value

List of Ipv6AccessControlList objects corresponding to given collection of InstanceNameId. In the returned list of Ipv6AccessControlList objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in Ipv6AccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getIpv6AclsInNetworkElement

Returns all IPv6 ACLs in a network element. Given the InstanceNameId of a network element, returns a collection of IPv6 ACLs in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of Ipv6AccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in Ipv6AccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getIpv6AclsWithoutAcesInNetworkElement

Returns all IPv6 ACLs in a network element. Given the InstanceNameId of a network element, returns a collection of IPv6 ACLs in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

List of Ipv6AccessControlList objects. In the returned list of objects, all associations will be cleared.

getMacAcIToNetworkInterfaceAssociationsInNetwork Element

Returns all MAC ACLs to network interface associations configured in a network element. Given the instance name ID of the network element, returns a collection of MAC ACL to network interface association objects.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of AclAppliesToNetworkInterface objects, that represents the association between MAC ACL and network interface. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- MacAccessControlList object. In the ACL object all the associations will be cleared, except AclAppliesToNetworkInterface association.
- NetworkInterface object. In the network interface object all the associations will be cleared, except AclAppliesToNetworkInterface association.

getMacAcls

Returns MacAccessControlList objects from it's InstanceNameIds. Given a collection of InstanceNameId of MacAccessControlList, returns corresponding MacAccessControlList objects.

ValidationException is thrown if any of the following situations occurs:

- If macAcIInstanceNameIdCol is null or it is empty.
- If macAcIInstanceNameIdCol contains invalid InstanceNameId of a MacAccessControlList.
- If macAcIInstanceNameIdCol contains null values.
- If there is no equivalent MacAccessControlList object with the given InstanceNameId in the macAcIInstanceNameIdCol.

Parameters

opContext—Operational context.

macAcIInstanceNameIdCol—a collection of InstanceNameId of MacAccessControlList.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

List of MacAccessControlList objects corresponding to given collection of InstanceNameId. In the returned list of MacAccessControlList objects, only the MacAccessControlEntry associated with returned MacAccessControlList objects will be present, and all other associations will be cleared.

getMacAclsInNetworkElement

Returns all MacAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of MacAccessControlList in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of MacAccessControlList objects. In the returned list of MacAccessControlList objects, only the MAC ACEs associated with returned MacAccessControlList objects will be present, and all other associations will be cleared.

getMacAclsWithoutAcesInNetworkElement

Returns all MacAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of MacAccessControlList in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of MacAccessControlList objects. In the returned list of MacAccessControlList objects, all associations will be cleared.

getNamedIpv4AclsInNetworkElement

Returns all named IPv4 ACLs (both StandardAccessControlList and ExtendedAccessControlList objects) in a network element. Given the InstanceNameId of a network element, returns a collection of IPv4 ACLs in the network element, that are uniquely identified by its name.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Send document comments to nexus7k-docfeedback@cisco.com

Parameters

opContext—Operational context.

neInstanceId—InstanceId of the network element.

Return Value

List of named StandardAccessControlList and ExtendedAccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getNumberedIpv4AclsInNetworkElement

Returns all numbered IPv4 ACLs (both StandardAccessControlList and ExtendedAccessControlList) objects in a network element. Given the InstanceNameId of a network element, returns a collection of IPv4 ACLs in the network element, that are uniquely identified by it's number.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceId—InstanceId of the network element.

Return Value

List of numbered StandardAccessControlList and ExtendedAccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- TimeRange association for every ACEs, if any, in ExtendedAccessControlList. If that TimeRange has other associations like PeriodicTimeRange entries and so on, those associations will be cleared.

getRbacPolicies

Returns RBACL policies from it's InstanceNameIds. Given a collection of InstanceNameId of RoleBasedAccessControlPolicy, returns corresponding RBACL policies objects.

ValidationException is thrown if any of the following situations occurs:

- If rbacPolicyInstanceIdCol is null or it is empty.
- If rbacPolicyInstanceIdCol contains invalid Role Based ACL InstanceNameId or null value.
- If there is no equivalent RBACL Policy object with the given InstanceNameId in the rbacPolicyInstanceIdCol.

Parameters

opContext—Operational context.

rbacPolicyInstanceIdCol—a collection of InstanceNameId of RoleBasedAccessControlPolicy.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

List of RoleBasedAccessControlPolicy objects corresponding to given collection of InstanceNameId. In the returned list of RBACL Policy objects, only the following associations will be present, and all other associations will be cleared.

- All associated RoleBasedAccessControlList objects. In the RBACL objects all the associations will be cleared, except that of RBACL Policies.

getRbacIPoliciesInNetworkElement

Returns all Role Based ACL policies in a network element. Given the InstanceNameId of a network element, returns a collection of Role Based ACL policies in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of RoleBasedAccessControlPolicy objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated RoleBasedAccessControlList objects. In the RBACL objects all the associations will be cleared, except that of RBACL Policies.

getRbacls

Returns Role Based ACLs from it's InstanceNameIds. Given a collection of InstanceNameId of RoleBasedAccessControlList, returns corresponding Role Based ACL objects.

ValidationException is thrown if any of the following situations occurs:

- If rbacInstanceNameIdCol is null or it is empty.
- If rbacInstanceNameIdCol contains invalid Role Based ACL InstanceNameId or null value.
- If there is no equivalent Role Based ACL object with the given InstanceNameId in the rbacInstanceNameIdCol.

Parameters

opContext—Operational context.

rbacInstanceNameIdCol—a collection of InstanceNameId of RoleBasedAccessControlList.

Return Value

List of RoleBasedAccessControlList objects corresponding to given collection of InstanceNameId. In the returned list of Role Based ACL objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.

Send document comments to nexus7k-docfeedback@cisco.com

- Timerange association for every ACEs, if any, in RoleBasedAccessControlList. If that TimeRange has other associations like periodic TimeRange entries and so on, those associations will be cleared.

getRbacIsInNetworkElement

Returns all Role Based ACLs in a network element. Given the InstanceNameId of a network element, returns a collection of Role Based ACLs in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of RoleBasedAccessControlList objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated ACEs of the returned ACL object.
- Timerange association for every ACEs, if any, in RoleBasedAccessControlList. If that TimeRange has other associations like periodic TimeRange entries and so on, those associations will be cleared.

getStandardIpAclToNetworkInterfaceAssociationsInNetworkElement

Returns all StandardAccessControlList objects to NetworkInterface associations configured in a network element. Given the InstanceNameId of the network element, returns a collection of StandardAccessControlList to NetworkInterface association objects.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of AclAppliesToNetworkInterface objects, that represents the association between StandardAccessControlList and NetworkInterface. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- StandardAccessControlList object. In the ACL object all the associations will be cleared, except AclAppliesToNetworkInterface association.
- NetworkInterface object. In the network interface object all the associations will be cleared, except AclAppliesToNetworkInterface association.

Send document comments to nexus7k-docfeedback@cisco.com

getStandardIpAcls

Returns StandardAccessControlList objects from it's InstanceNameIds. Given a collection of InstanceNameId of StandardAccessControlList, returns corresponding StandardAccessControlList objects.

ValidationException is thrown if any of the following situations occurs:

- If standardIpAclInstanceNameIdCol is null or it is empty.
- If standardIpAclInstanceNameIdCol contains invalid InstanceNameId of a StandardAccessControlList.
- If standardIpAclInstanceNameIdCol collection contains a null value.
- If there is no equivalent StandardAccessControlList object with the given InstanceNameId in the standardIpAclInstanceNameIdCol.

Parameters

opContext—Operational context.

standardIpAclInstanceNameIdCol—a collection of InstanceNameId of StandardAccessControlList.

Return Value

List of StandardAccessControlList objects corresponding to given collection of InstanceNameId. In the returned list of StandardAccessControlList objects, only the StandardAccessControlEntry objects associated with returned StandardAccessControlList objects will be present, and all other associations will be cleared.

getStandardIpAclsInNetworkElement

Returns all StandardAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of StandardAccessControlList objects in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of StandardAccessControlList objects. In the returned list of StandardAccessControlList objects, only the Standard ACEs associated with returned StandardAccessControlList objects will be present, and all other associations will be cleared.

getStandardNamedIpAclsInNetworkElement

Returns all named StandardAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of StandardAccessControlList objects in the network element, that are uniquely identified by it's name.

Send document comments to nexus7k-docfeedback@cisco.com

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of named StandardAccessControlList objects. In the returned list of named StandardAccessControlList objects, only the Standard ACEs associated with returned StandardAccessControlList objects will be present, and all other associations will be cleared.

getStandardNumberedIpAclsInNetworkElement

Returns all numbered StandardAccessControlList objects in a network element. Given the InstanceNameId of a network element, returns a collection of StandardAccessControlList objects in the network element, that are uniquely identified by it's number.

ValidationException is thrown if the argument passed is null or it is not a valid InstanceNameId of an AbstractNetworkElement.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of numbered StandardAccessControlList objects. In the returned list of numbered StandardAccessControlList objects, only the StandardAccessControlEntry objects associated with returned StandardAccessControlList objects will be present, and all other associations will be cleared.

getTimeRanges

Returns TimeRanges from it's InstanceNameIds. Given a collection of InstanceNameId of TimeRange, returns corresponding TimeRange objects.

ValidationException is thrown if any of the following situations occurs:

- If timerangeInstanceNameIdCol is null or it is empty.
- If timerangeInstanceNameIdCol contains invalid Extended ACL InstanceNameId or null value.
- If there is no equivalent TimeRange object with the given InstanceNameId in the timerangeInstanceNameIdCol.

Parameters

opContext—Operational context.

timerangeInstanceNameIdCol—a collection of InstanceNameId of TimeRange.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

List of TimeRange objects corresponding to given collection of InstanceNameId. In the returned list of TimeRange objects, only the following associations will be present, and all other associations will be cleared.

- All associated periodic TimeRange entries.
- Absolute TimeRange entry.

getTimeRangesInNetworkElement

Returns all TimeRanges in a network element. Given the InstanceNameId of a network element, returns a collection of TimeRanges in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of TimeRange objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated periodic TimeRange entries.
- Absolute TimeRange entry.

getTimeRangesWithoutEntriesInNetworkElement

Returns all TimeRanges in a network element. Given the InstanceNameId of a network element, returns a collection of TimeRanges in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of the network element.

Return Value

List of TimeRange objects. In the returned list of objects, all associations will be cleared.

getVlanAccessLogSettingInNetworkElements

Returns VACL log settings applied on the network elements. Given a collection of InstanceNameId of a network element, returns the VACL log settings applied on those network elements.

ValidationException is thrown if any of the following situations occurs:

Send document comments to nexus7k-docfeedback@cisco.com

- If neInstanceIdCol is null or it is empty.
- If neInstanceIdCol contains invalid network element InstanceNameId or null value.
- If there is no equivalent network element object with the given InstanceNameId in the neInstanceIdCol.

Parameters

opContext—Operational context.

neInstanceIdCol—a collection of InstanceNameId of the network element.

Return Value

List of VlanAccessLog objects corresponding to the InstanceNameId of the network element.

getVlanAccessMaps

Returns VACLs from the InstanceNameIds. Given a collection of InstanceNameId of VlanAccessMap, returns corresponding VACL objects.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapEntryInstanceNameIdCol is null or it is empty.
- If vlanAccessMapEntryInstanceNameIdCol contains invalid VACL InstanceNameId or null value.
- If there is no equivalent VACL object with the given InstanceNameId in the vlanAccessMapEntryInstanceNameIdCol.

Parameters

opContext—Operational context.

vlanAccessMapInstanceNameIdCol—a collection of InstanceNameId of VlanAccessMap.

Return Value

List of VlanAccessMap objects corresponding to given collection of InstanceNameId. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated VACEs in the returned VACL object.
- IP ACL/MAC ACL/IPv6 ACL objects associated with each VACE (as these ACLs are used as match conditions in VACE), if any, in VlanAccessMap. In IP/MAC/IPv6 ACLs all associations will be cleared, except that of VACE.
- NetworkInterface objects associated with each VACE, if any, as redirect interfaces. In the network interfaces all associations will be cleared, except that of VACE.

getVlanAccessMapsInNetworkElement

Returns all VLAN ACLs in a network element. Given the InstanceNameId of a network element, returns a collection of VLAN ACLs in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Send document comments to nexus7k-docfeedback@cisco.com

Parameters

opContext—Operational context.

neInstanceId—InstanceId of the network element.

Return Value

List of VlanAccessMap objects. In the returned list of objects, only the following associations will be present, and all other associations will be cleared.

- All associated VACEs in the returned VACL object.
- IP ACL/MAC ACL/IPv6 ACL objects associated with each VACE (as these ACLs are used as match conditions in VACE), if any, in VlanAccessMap. In IP/MAC/IPv6 ACLs all associations will be cleared, except that of VACE.
- NetworkInterface objects associated with each VACE, if any, as redirect interfaces. In the network interfaces all associations will be cleared, except that of VACE.

getVlanAccessMapsWithoutVlanAccessMapEntriesInNetworkElement

Returns all VLAN ACLs in a network element. Given the InstanceNameId of a network element, returns a collection of VLAN ACLs in the network element.

ValidationException is thrown if the argument passed is null or it is not a valid network element InstanceNameId.

Parameters

opContext—Operational context.

neInstanceId—InstanceId of the network element.

Return Value

List of VlanAccessMap objects. In the returned list of objects, all associations will be cleared.

modifyAclSequence

Modifies the sequence number of the ACEs in an ACL, based on the starting sequence number and the step to increment the sequence numbers.

Parameters

opContext—Operational context.

aclInstanceIdCol—InstanceId of one or more ACLs.

If the platform type is Nexus 7000 series switch, then the ACLs can be of any of the following types:

- StandardAccessControlList
- ExtendedAccessControlList
- MacAccessControlList
- Ipv6AccessControlList

Send document comments to nexus7k-docfeedback@cisco.com

- RoleBasedAccessControlList

If the platform type is Catalyst 6500 series switches, then the ACLs can be of any of the following types:

- StandardAccessControlList
- ExtendedAccessControlList

startSeqNo—Access list entries will be resequenced using this initial value.

increment—number by which the sequence numbers change. For example, if the increment value is 5 and the start sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.

Return Value

void

modifyExtendedIpAcls

Modifies one or more existing Extended IP ACL objects.

ValidationException is thrown if any of the following situations occurs:

- If extendedIpAclCol collection is null or it is empty.
- If extendedIpAclCol collection contains an object that is not of type ExtendedAccessControlList.
- If any of the ExtendedAccessControlEntry, in the ExtendedAccessControlList, does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the extendedIpAclCol collection, if any attribute in the ExtendedAccessControlList is not valid or if any ExtendedAccessControlEntry inside a Extended ACL is not valid.

Example:

- seqNo of an ACE is out of range.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the extendedIpAclCol collection contains a ExtendedAccessControlList that does not exist in the database.
- If a ExtendedAccessControlList in the extendedIpAclCol contains duplicate ExtendedAccessControlEntry objects.

This API will not consider the interface association. If a Extended ACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the Extended ACL to an interface.

Parameters

opContext—Operational context. operational context.

extendedIpAclCol—a collection (one or more) of ExtendedAccessControlList objects that will replace the existing ExtendedAccessControlList objects in the database.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com

modifyIpv6Acls

Modifies one or more existing IPv6 ACL objects.

ValidationException is thrown if any of the following situations occurs:

- If ipv6AclCol collection is null or it is empty.
- If ipv6AclCol collection contains an object that is not of type Ipv6AccessControlList.
- If any of the Ipv6AccessControlEntry, in the Ipv6AccessControlList, does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the ipv6AclCol collection, if any attribute in the Ipv6AccessControlList is not valid or if any Ipv6AccessControlEntry inside a IPv6 ACL is not valid.

Example:

- seqNo of an ACE is out of range.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the ipv6AclCol collection contains a Ipv6AccessControlList that does not exist in the database.
- If a Ipv6AccessControlList in the ipv6AclCol contains duplicate Ipv6AccessControlEntry objects.

This API will not consider the interface association. If a IPv6 ACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the IPv6 ACL to an interface.

Parameters

opContext—Operational context.

ipv6AclCol—a collection (one or more) of Ipv6AccessControlList objects that will replace the existing Ipv6AccessControlList objects in the database.

Return Value

void

modifyMacAcls

Modifies one or more existing MAC ACL objects.

ValidationException is thrown if any of the following situations occurs:

- If macAclCol collection is null or it is empty.
- If macAclCol collection contains an object that is not of type MacAccessControlList.
- If any of the MacAccessControlEntry, in the MacAccessControlList, does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the macAclCol collection, if any attribute in the MacAccessControlList is not valid or if any MacAccessControlEntry inside a MAC ACL is not valid.

Example:

Send document comments to nexus7k-docfeedback@cisco.com

- seqNo of an ACE is out of range.
- number attribute is set for a MAC ACL, as all MAC ACLs are identified by it's name.

IntegrityException is thrown if any of the following situations occurs:

- If the macAclCol collection contains a MacAccessControlList that does not exist in the database.
- If a MacAccessControlList in the macAclCol contains duplicate MacAccessControlEntry objects.

This API will not consider the interface association. If a MAC ACL is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the MAC ACL to an interface.

Parameters

opContext—Operational context.

macAclCol—a collection (one or more) of MacAccessControlList objects that will replace the existing MacAccessControlList objects in the database.

Return Value

void

modifyRbacPolicies

Modifies one or more existing RBACL Policy objects.

ValidationException is thrown if any of the following situations occurs:

- If rbacPolicyCol collection is null or it is empty.
- If rbacPolicyCol collection contains an object that is not of type RoleBasedAccessControlPolicy.

PropertiesException is thrown if any of the following situations occurs:

- In the rbacPolicyCol collection, if any attribute in the RoleBasedAccessControlPolicy is not valid.

Example:

- srcTagType is not specified in RoleBasedAccessControlPolicy.
- sgt is not specified in RoleBasedAccessControlPolicy.

IntegrityException is thrown if any of the following situations occurs:

- If the rbacPolicyCol collection contains a RoleBasedAccessControlPolicy that does not exist in the database.
- If the rbacPolicyCol collection contains duplicate RoleBasedAccessControlPolicy objects.

Parameters

opContext—Operational context.

rbacPolicyCol—a collection (one or more) of RoleBasedAccessControlPolicy objects that will replace the existing RoleBasedAccessControlPolicy objects in the database.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com

modifyRbacls

Modifies one or more existing Role Based ACL objects.

ValidationException is thrown if any of the following situations occurs:

- If rbaclCol collection is null or it is empty.
- If rbaclCol collection contains an object that is not of type RoleBasedAccessControlList.
- If any of the RoleBasedAccessControlEntry, in the RoleBasedAccessControlList, does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the rbaclCol collection, if any attribute in the RoleBasedAccessControlList is not valid or if any RoleBasedAccessControlEntry inside a Role Based ACL is not valid.

Example:

- seqNo of an ACE is out of range.
- remark attribute value of an ACL contains more than 100 characters.

IntegrityException is thrown if any of the following situations occurs:

- If the rbaclCol collection contains a RoleBasedAccessControlList that does not exist in the database.
- If a RoleBasedAccessControlList in the rbaclCol contains duplicate RoleBasedAccessControlEntry objects.

Parameters

opContext—Operational context.

rbaclCol—a collection (one or more) of RoleBasedAccessControlList objects that will replace the existing RoleBasedAccessControlList objects in the database.

Return Value

void

modifyStandardIpAcls

Modifies one or more existing StandardAccessControlList objects.

ParameterException is thrown if any of the following situations occurs:

- If standardIpAclCol collection is null or it is empty.
- If standardIpAclCol collection contains an object that is not of type StandardAccessControlList.
- If any of the StandardAccessControlEntry, in the StandardAccessControlList, does not contain sequence number.
- If the standardIpAclCol collection contains a StandardAccessControlList that does not exist in the database.

PropertiesException is thrown if any of the following situations occurs:

- In the standardIpAclCol collection, if any attribute in the StandardAccessControlList is not valid or if any StandardAccessControlEntry inside a Standard ACL is not valid.

Example:

Send document comments to nexus7k-docfeedback@cisco.com

- seqNo of an ACE is out of range.
- Remark description value of an ACL contains more than 100 characters.

FeatureCompoundException is thrown if any of the following situations occurs:

- If a StandardAccessControlList in the standardIpAclCol contains duplicate StandardAccessControlEntry objects.

This API will not consider the interface association. If a StandardAccessControlList is passed with the interface association, that will not be considered by this API. User needs to call separate API to bind the StandardAccessControlList to an interface.

Parameters

opContext—Operational context. operational context.

standardIpAclCol—a collection (one or more) of StandardAccessControlList objects that will replace the existing StandardAccessControlList objects in the database.

Return Value

void

modifyTimeRanges

Modifies one or more existing TimeRange objects.

ValidationException is thrown if any of the following situations occurs:

- If timerangeCol collection is null or it is empty.
- If timerangeCol collection contains an object that is not of type TimeRange.

PropertiesException is thrown if any of the following situations occurs:

- In the timerangeCol collection, if any attribute in the TimeRange is not valid or if any PeriodicTimeRange inside a TimeRange is not valid or if any AbsoluteTimeRange inside a TimeRange is not valid.

Example:

- Both startTime and endTime is not set in AbsoluteTimeRange.
- endTime is not greater than startTime in AbsoluteTimeRange or PeriodicTimeRange.

IntegrityException is thrown if any of the following situations occurs:

- If the timerangeCol collection contains a TimeRange that does not exist in the database.
- If a TimeRange in the timerangeCol contains duplicate PeriodicTimeRange objects.

This API will not consider the ACE association. If a TimeRange is passed with ACE association, that will not be considered by this API. User needs to call separate API to bind the TimeRange to an ACE.

Parameters

opContext—Operational context.

timerangeCol—a collection (one or more) of TimeRange objects that will replace the existing TimeRange objects in the database.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com

modifyVlanAccessLogSetting

Modifies VACL log object in a network element.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceId is null.
- If neInstanceId is not a valid network element InstanceNameId.
- If the vlanAccessMapEntryLog is null.

PropertiesException is thrown if any of the following situations occurs:

- In the vlanAccessMapEntryLog, if any attribute is invalid.

Example:

- maxFlow of a VlanAccessLog is out of range.
- rateLimit of a VlanAccessLog is out of range.

Parameters

opContext—Operational context.

neInstanceId—InstanceNameId of a network element.

vlanAccessLog—VlanAccessLog object that will replace the existing VlanAccessLog object in the database.

Return Value

void

modifyVlanAccessMaps

Modifies one or more existing VACL objects.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapEntryCol collection is null or it is empty.
- If vlanAccessMapEntryCol collection contains an object that is not of type VlanAccessMap.
- If any of the VlanAccessMapEntry, in the VlanAccessMap, does not contain a sequence number.

PropertiesException is thrown if any of the following situations occurs:

- In the vlanAccessMapEntryCol collection, if any attribute in the VlanAccessMap is not valid or if any VlanAccessMapEntry inside a VACL is not valid.

Example:

- seqNo of a VlanAccessMapEntry is out of range.
- No IP ACL or MAC ACL or IPv6 ACL is specified in the match condition of any of the VlanAccessMapEntry.

IntegrityException is thrown if any of the following situations occurs:

- If the vlanAccessMapEntryCol collection contains a VlanAccessMap that does not exist in the database.
- If a VlanAccessMap in the vlanAccessMapEntryCol contains duplicate VlanAccessMapEntry objects.

Send document comments to nexus7k-docfeedback@cisco.com

Parameters

opContext—Operational context.

vlanAccessMapCol—a collection (one or more) of VlanAccessMap objects that will replace the existing VlanAccessMap objects in the database.

Return Value

void

unbindIpv4AclFromNetworkInterface

Clears the IPv4 ACL association from a network interface on a specific direction.

ParameterException is thrown if any of the following situations occurs:

- If networkInterfaceInstanceId is null or it is not a valid InstanceNameId of a NetworkInterface object.
- If the direction is null.

Parameters

opContext—Operational context.

networkInterfaceInstanceId—InstanceNameId of a NetworkInterface object from which ACL needs to be removed.

direction—direction from which StandardAccessControlList or ExtendedAccessControlList object needs to be removed.

Return Value

void

unbindIpv4AclsFromVlanAccessMapEntry

Clears the given list of IPv4 ACLs from the VACE.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceId is not a valid VlanAccessMapEntry InstanceNameId.
- If the ipv4AclInstanceIdCol collection is null or the collection is empty.
- If the ipv4AclInstanceIdCol collection contains any null element, or the collection contains an invalid StandardAccessControlList or ExtendedAccessControlList InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceId—InstanceNameId of VlanAccessMapEntry object.

ipv4AclInstanceIdCol—a collection of InstanceNameId of one or more StandardAccessControlList or ExtendedAccessControlList objects.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

void

unbindIpv6AclFromNetworkInterface

Clears the IPv6 ACL association from a network interface on a specific direction.

ValidationException is thrown if any of the following situations occurs:

- If networkInterfaceInstanceId is null or it is not a valid NetworkInterface object InstanceNameId.
- If the direction is null.

Parameters

opContext—Operational context.

networkInterfaceInstanceId—InstanceNameId of a NetworkInterface object from which ACL needs to be removed.

direction—direction from which Ipv6AccessControlList object needs to be removed.

Return Value

void

unbindIpv6AclsFromVlanAccessMapEntry

Clears the given list of IPv6 ACLs from the VACE.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceId is not a valid VlanAccessMapEntry InstanceNameId.
- If the ipv6AclInstanceIdCol collection is null or the collection is empty.
- If the ipv6AclInstanceIdCol collection contains any null element, or the collection contains an invalid Ipv6AccessControlList InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceId—InstanceNameId of VlanAccessMapEntry object.

ipv6AclInstanceIdCol—a collection of InstanceNameId of one or more Ipv6AccessControlList objects.

Return Value

void

unbindMacAclFromNetworkInterface

Clears the MAC ACL association from a network interface on a specific direction.

Send document comments to nexus7k-docfeedback@cisco.com

ValidationException is thrown if any of the following situations occurs:

- If networkInterfaceInstanceId is null or it is not a valid NetworkInterface object InstanceNameId.
- If the direction is null.

Parameters

opContext—Operational context.

networkInterfaceInstanceId—InstanceNameId of a NetworkInterface object from which ACL needs to be removed.

direction—direction from which MacAccessControlList object needs to be removed.

Return Value

void

unbindMacAclsFromVlanAccessMapEntry

Clears the given list of MAC ACLs from the VACE.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceId is not a valid VlanAccessMapEntry InstanceNameId.
- If the macAcInstanceIdCol collection is null or the collection is empty.
- If the macAcInstanceIdCol collection contains any null element, or the collection contains an invalid MacAccessControlList InstanceNameId.

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceId—InstanceNameId of VlanAccessMapEntry object.

macAcInstanceIdCol—a collection of InstanceNameId of one or more MacAccessControlList objects.

Return Value

void

unbindNetworkInterfacesFromVlanAccessMapEntry

Clears the given list of network interfaces that are assigned as redirect interfaces, from the VACE.

ValidationException is thrown if any of the following situations occurs:

- If vlanAccessMapInstanceId is null or it is not of type VlanAccessMapEntry InstanceNameId.
- If vlanAccessMapInstanceId is not a valid VlanAccessMapEntry InstanceNameId.
- If the networkInterfaceInstanceIdCol collection is null or the collection is empty.
- If the networkInterfaceInstanceIdCol collection contains any null element, or the collection contains an invalid NetworkInterface InstanceNameId.

Send document comments to nexus7k-docfeedback@cisco.com

Parameters

opContext—Operational context.

vlanAccessMapEntryInstanceNameId—InstanceNameId of VlanAccessMapEntry object.

networkInterfaceInstanceNameIdCol—a collection of InstanceNameId of one or more NetworkInterface objects that needs to be removed from redirection.

Return Value

void

unbindTimeRangeFromAces

Clears timerange from one or more ACEs.

ValidationException is thrown if any of the following situations occurs:

- If the aceInstanceNameIdCol collection is null or the collection is empty.
- If the aceInstanceNameIdCol collection contains any null element, or the collection contains an invalid ExtendedAccessControlEntry, Ipv6AccessControlEntry or RoleBasedAccessControlEntry InstanceNameId.

Parameters

opContext—Operational context.

aceInstanceNameIdCol—a collection of InstanceNameId of one or more ACEs. ACEs can be ExtendedAccessControlEntry, Ipv6AccessControlEntry or RoleBasedAccessControlEntry.

Return Value

void

unbindVlanAccessMapFromVlans

Clears VACL from one or more VLANs.

ValidationException is thrown if any of the following situations occurs:

- If neInstanceNameId is null or it is not of type NetworkElement InstanceNameId.
- If neInstanceNameId is not a valid NetworkElement InstanceNameId.
- If the vlanIds value is null.

Parameters

opContext—Operational context.

neInstanceNameId—InstanceNameId of a NetworkElement.

vlanIds—One or more VLAN IDs, that uniquely identifies a VLAN.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com