



CHAPTER 6

DaiApp Service

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

Information About DaiApp Service

Dynamic Address Resolution Protocol (ARP) inspection (DAI) is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings, which allows you to protect the network from man-in-the-middle attacks, where an attacker could send forged ARP packets (for example, gratuitous ARPs) carrying a bogus IP/MAC binding in the payload to a host or to the default gateway.

bindArpAclOnVlans

Applies the ARP ACL on to a collection of VLANs. API to validate whether the VLANs already has an ARP ACL. API shall also validate whether DAI is enabled on the VLAN. If DAI is enabled on the VLAN, then API shall throw a warning message stating that ARP inspection based on ARP ACL will take precedence over validation done by DAI. That is, if a packet has to be denied based on ARP ACL, it will be denied even though the packet is valid as per DAI.

ValidationException is thrown if any of the following situations occurs:

- If arpAclInstanceId is null or it is not of type ARP ACL InstanceNameId.
- If the vlanInstanceNameIdCol is null or empty.
- If the vlanInstanceNameIdCol collection contains one null element, or the collection contains an invalid VLAN InstanceNameId.

Parameters

opContext— Operational context.

arpAclInstanceId— InstanceNameId of ARP ACL object.

vlanInstanceNameIdCol— A collection of InstanceNameId of VLAN.

explicitDenyEnable—Indicates whether the ARP ACL has to be configured as a static ACL.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com

bindArpAclOnVlansByArpAclName

Binds pre-provisioned ARP ACL to a collection of VLANs. For ARP ACL to be bound to a collection of VLANs, ARP ACL need not be physically configured in the device. We can bind ARP ACL to a collection just by using the name of ARP ACL. This API addresses this pre-provisioning configuration.

ValidationException is thrown if any of the following situations occurs:

- If the passed argument arpAclName is null.
- If the vlanInstanceIds collection is null or empty.
- If the vlanInstanceIds collection one null element, or the collection contains an invalid VLAN instance name Id.
- If the vlanInstanceIds collection contains an instance ID of a VLAN that does not exist in the database.

PropertiesException is thrown if any of the following situations occurs.

- If arpAclName contains an invalid ARP ACL name string.

Example:

- If the ARP ACL name does not start with an alphabet like "2acl_test".
- If the ARP ACL name contains a space or question mark character or quotation mark character like "acl test2" or "acl?test2" or "acl'test".

Parameters

opContext— Operational context.

arpAclName— Name of the ARP ACL. This ACL need not be configured in the device.

vlanInstanceIds— A collection of InstanceNameId of VLANs in a network element that are configured in the device.

explicitDenyEnable— Indicates whether the ARP ACL has to be configured as a static ACL.

Return Value

void

bindArpAclOnVlansForRange

Binds pre-provisioned ARP ACL to a collection of pre-provisioned VLANs. For ARP ACL to be bound to a collection of VLANs, both ARP ACL and VLAN need not have been configured in the device. Users can bind ARP ACL name to a collection of VLANs and then create both ARP ACLs and the bound VLANs at a latter stage. This API addresses this pre-provisioning configuration.

ValidationException is thrown if any of the following situations occurs:

- If the passed argument arpAclName is null.
- If the passed argument vlanRange is null.
- If the networkElementId is null or not of type network element InstanceNameId.
- If the network element with the InstanceNameId given by networkElementId does not exist in the database.

PropertiesException is thrown if any of the following situations occurs:

Send document comments to nexus7k-docfeedback@cisco.com

- If the ARP ACL name given as the argument arpAclName is not a valid ARP ACL name string.

Example:

- If the ARP ACL name does not start with an alphabet like "2acl_test".
- If the ARP ACL name contains a space or question mark character or quotation mark character like "acl test2" or "acl?test2" or "acl'test".

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

arpAclName— Name of the ARP ACL. This ACL need not have been configured in the device.

vlanRange— A String representing the range of VLANs. The string holds comma separated / hyphenated list of VLANs. For example, vlanRange could be 4,6,9,15-20,25.

explicitDenyEnable— Indicates whether the ARP ACL has to be configured as a static ACL.

Return Value

void

clearArpRateLimitingConfigurationInInterfaces

Clears the ARP rate limiting and burst interval configurations done in a collection of interfaces. This API also restores the rate limiting and burst interval values to default values.

ValidationException is thrown if any of the following situations occurs:

- If the argument interfaceNameIds is null or it is not of type interface InstanceNameId.
- If the interface specified by any of the InstanceNameId in the collection interfaceNameIds does not exist in the database.

Parameters

opContext— Operational context.

interfaceNameIds— A collection of InstanceNameId of the interfaces.

Return Value

void

createArpAcls

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

ValidationException is thrown if any of the following situations occurs:

- If neInstanceNameId is null or it is not of type network element InstanceNameId.
- If neInstanceNameId is not a valid network element InstanceNameId.
- If the ARP ACLs objects in the arpAclCol do not have their name attribute set.

Send document comments to nexus7k-docfeedback@cisco.com

- If the arpAclCol contains duplicate entries of the ARP ACLs.

javax.xml.bind.PropertyException is thrown if any of the following situations occurs:

- If name of an ARP ACL does not start with alphabets.
- If name of an ARP ACL contains space or quotation mark character.
- If name of an ARP ACL contains more than 234 characters.

IntegrityException is thrown if any of the following situation occurs:

- If the arpAclCol contains an ARP ACL that already exists in the database.
- If an ARP ACL in the arpAclCol contains duplicate ARP ACL entry objects.

VlanExternal associations with the ARP ACLs will not be considered by this API. User has to call separate API to bind the ARP ACL to a VLAN.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

arpAclCol— A collection of ARP ACL objects to be created.

Return Value

A collection of newly created ARP ACL objects.

deleteArpAcls

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

ValidationException is thrown if any of the following situations occurs:

- If the arpAcls collection is null or empty.
- If the arpAcls collection contains an element that is not of type ARP ACL.
- If the arpAcls collection contains an ARP ACL that does not exist in the database.

Parameters

opContext— Operational context.

arpAclInstanceNameIds— A collection that contains InstanceNameId of ARP ACLs to be deleted

Return Value

void

disableDaiOnVlans

Disables DAI for a given collection of VLANs in a network element.

ValidationException is thrown if the argument passed is null or it is not of type VLAN InstanceNameId.

Send document comments to nexus7k-docfeedback@cisco.com

Parameters

opContext— Operational context.

vlanIds— InstanceNameId of the VLANs.

Return Value

void

enableDaiOnVlans

Enables DAI for a given collection of VLANs in a network element. API to validate whether DHCP Snooping is enabled on the VLAN. If not, API to throw an Exception stating that DHCP Snooping has to be enabled for DAI to function.

ValidationException is thrown if the argument passed is null or it is not of type VLAN InstanceNameId.

Parameters

opContext— Operational context.

vlanIds— InstanceNameId of the VLANs.

Return Value

A list of InstanceNameId of DaiSetting objects that are associated with the VLANs corresponding to the given list of vlanIds.

enableDaiOnVlansByRange

Enables Dynamic ARP Inspection in a pre-provisioned VLAN. It is possible to enable Dynamic ARP Inspection just by using VLAN IDs. The VLANs in which Dynamic ARP Inspection has to be enabled need not actually exist in the device. This API addresses this pre-provisioning configuration.

ValidationException is thrown if any of the following situations occurs.

- If the passed argument networkElementId is null or not of type network element InstanceNameId.
- If the passed argument vlanRange is null.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

vlanRange— A String representing the range of VLANs. The string holds comma separated / hyphenated list of VLANs. For example, vlanRange could be 4,6,9,15-20,25

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com

getArpAclsInNetworkElement

Returns a collection of all ARP ACLs configured in a given network element, given the InstanceNameId of the network element.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId the network element.

Return Value

List of all ARP ACL objects present in the network element. In the returned list of objects, only the following associations will be present and other associations will be cleared.

- All associated ACEs of the returned ARP ACL object.
- The VLANs which are referring the returned ARP ACL object.
- The network element in which the returned ARP ACLs are configured.

getArpAclsInVlans

Given a collection of VLAN InstanceNameIds, this API returns the ARP ACLs associated to it, if any.

Parameters

opContext—

vlanInstanceNameIdCol—

Return Value

List of ARP ACLs associated to VLAN. If no ARP ACL is associated to a VLAN in the parameter collection, then the list will contain null element in the corresponding position.

getArpAclsWithoutAcesInNetworkElement

Returns a collection of all ARP ACLs configured in a given network element, given the InstanceNameId of the network element.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId the network element.

Return Value

List of all ARP ACL objects present in the network element. In the returned list of objects, all associations will be cleared.

Send document comments to nexus7k-docfeedback@cisco.com

getDaiDisabledVlansInNetworkElement

Returns all the DAI Disabled VLANs in the given network element.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

Return Value

A list of DAI disabled VlanExternal objects. In the returned list of objects, only the following associations will be present and other associations will be cleared.

- DaiSetting association.
- ARP ACL association. If that ARP ACL has ARP ACL entries, those associations will be cleared.

getDaiEnabledVlansInNetworkElement

Returns all the DAI Enabled VLANs in the given network element.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

Return Value

A list of DAI enabled VlanExternal objects. In the returned list of objects, only the following associations will be present and other associations will be cleared.

- DaiSetting association.
- ARP ACL association. If that ARP ACL has ARP ACL entries, those associations will be cleared.

getDaiGlobalSettingsInNetworkElements

Gets the DAI global settings for a given list of network elements. Given the InstanceNameId of the network element, returns a collection of DAI global settings.

ValidationException is thrown if the passed argument is null or not of type network element InstanceNameId.

Parameters

opContext— Operational context.

neInstanceNameIds— InstanceNameId of the network elements.

Send document comments to nexus7k-docfeedback@cisco.com

Return Value

A list of DaiGlobalSetting objects. The returned List will contain DaiGlobalSetting objects pertaining to a given list of network elements.

getDaiSettingOnVlans

Returns the list of DAI settings pertaining to the given list of VLANs.

ValidationException is thrown if the argument passed is null or it is not of type VLAN InstanceNameId.

Parameters

opContext— Operational context.

vlanIds— InstanceNameId of the VLANs.

Return Value

A list of DaiSetting objects. In the returned list of objects, only the following associations will be present and other associations will be cleared.

- VLAN association.
- ARP ACL associated with the VLAN, that is associated with the DAI Setting. If that ARP ACL has ARP ACL entries, those associations will be cleared.

getInterfacesWithArpRateLimitingInNetworkElement

Returns all the interfaces in the given network element having ARP rate and burst interval configured. These interfaces have configured values for ARP rate limiting and burst interval.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

Return Value

A collection of interface objects having ARP rate limiting and burst interval configured.

getTrustStateSettingInInterfaces

Returns the collection of trust state setting objects. Given the collection of interface InstanceNameId, returns a collection of trust state setting objects.

ValidationException is thrown if the argument passed is null or it is not of type interlace InstanceNameId.

Parameters

opContext— Operational context.

Send document comments to nexus7k-docfeedback@cisco.com

interfaceInstanceIds— InstanceNameId of interfaces.

Return Value

A collection of TrustStateSetting objects.

getUntrustedInterfacesWithDefaultRateInNetworkElement

Returns all the untrusted interfaces in the given network element having default ARP rate and burst interval values, given the InstanceNameId of the network element.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

Return Value

A collection of untrusted interface objects having default rate limiting and burst interval.

getVlansWithDaiSettingNetworkElement

Returns all the VLANs with DaiSetting object, in the given network element.

ValidationException is thrown if the argument passed is null or it is not of type network element InstanceNameId.

Parameters

opContext— Operational context.

networkElementId— InstanceNameId of the network element.

Return Value

A list of VLANs with DaiSetting object. In the returned list of objects, only the following associations will be present and other associations will be cleared.

- DaiSetting association.
- ARP ACL association. If that ARP ACL has ARP ACL entries, those 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.

aclInstanceNameIdCol— InstanceNameId of one or more ACLs.

Send document comments to nexus7k-docfeedback@cisco.com

Resequencing is supported only if the platform type is Nexus 7000 series switch.

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

modifyArpAcls

Modifies one or more existing ARP ACL objects.

ValidationException is thrown if any of the following situations occurs:

- If arpAcls collection is null or empty.
- If arpAcls collection contains an object that is not of type ARP ACL.

PropertiesException is thrown if any of the following situations occurs:

- If the name of the ARP ACL in the arpAcls collection is modified.

IntegrityException is thrown if any of the following situation occurs:

- If the arpAcls collection contains an ARP ACL object that does not exist in the database.
- If the ARP ACL in the arpAcls collection contains a duplicate ARP ACL entry objects.

This API will not consider VLAN association of the ARP ACL objects. User needs to call separate API to bind an ARP ACL to a VLAN.

Parameters

opContext— Operational context.

arpAcls— a collection of modified ARP ACL objects that will replace the existing ARP ACL objects in the database.

Return Value

Void.

modifyDaiGlobalSettingsInNetworkElements

Modifies one or more existing DAI global setting objects in a given collection of network elements.

ValidationException is thrown if any of the following situations occurs:

- If the networkElementIds collection is null or empty.
- If the networkElementIds collection contains one null element, or the collection contains an invalid network element InstanceNameId.

PropertiesException is thrown if any of the following situations occurs:

- In the daiGlobalSettings collection, if any one of the daiGlobalSetting attribute is not valid.

Example:

- If logBufferSize attribute does not contains a value between 0—1024.

Send document comments to nexus7k-docfeedback@cisco.com

- If the logInterval attribute does not contain a value between 0—86400.

IntegrityException is thrown if any of the following situations occurs:

- If the size of the collections networkElementIds and the daiGlobalSettings are not equal.

Parameters

opContext— Operational context.

networkElementIds— InstanceNameId of network elements in which the DAI Global parameters have to be modified.

daiGlobalSettings— Modified DAI global setting objects

Return Value

void

modifyDaiOnVlans

Modifies one or more existing DAI setting objects.

ValidationException is thrown if any of the following situations occurs:

- If modifiedDaiSettings collection is null or empty.
- If modifiedDaiSettings collection contains an object that is not of type DaiSetting.

PropertiesException is thrown if any of the following situations occurs:

- If the reference to a VLAN in the modified DAI setting object is changed.

Parameters

opContext— Operational context.

modifiedDaiSettings— A collection of modified DaiSetting objects that will replace the existing DAI setting objects in the database.

Return Value

void

modifyDaiSettingsAndArpAclBindingsOnVlans

Modifies DAI settings and ARP ACL bindings in a given collection of VLANs. VLAN objects passed shall have modified DAI settings and modified ARP ACL bindings.

Modification of ARP ACL Entry is not supported in this API. use modifyArpAcls(List arpAcls) API to modify ARP ACL Entry of an ARP ACL.

ValidationException is thrown if any of the following situations occurs:

- If modifiedVlanObjects collection is null or empty.
- If the modifiedVlanObjects contains a VLAN that does not exist in the database.
- If the VLAN in the database, corresponding to the elements in modifiedVlanObjects collection does not contain DAI setting.

Send document comments to nexus7k-docfeedback@cisco.com

PropertiesException is thrown if any of the DAI setting's attribute or attributes of ARP ACLs associated to the VLAN in modifiedVlanObjects, is not valid.

Parameters

opContext— Operational context.

modifiedVlanObjects— A collection of modified VLAN objects with DAI settings and ARP ACL references.

Return Value

void

modifyTrustStateSettings

Modifies one or more existing trust state setting objects in a given collection of network interfaces.

ValidationException is thrown if any of the following situations occurs:

- If interfaceInstanceIds collection is null or empty.
- If interfaceInstanceIds collection contains one null element, or the collection contains an invalid interface InstanceNameId.
- If the trustStateSettings collection is null or empty.
- If the trustStateSettings collection contains an element that is not of type TrustStateSetting.

PropertiesException is thrown if any of the following situations occurs:

- In the trustStateSettings collection, if any of the trustStateSetting attribute is not valid.

Example:

- If the arpRate attribute does not contain a value between 0—2048.
- If the burstInterval attribute does not contain a value between 0—15.

IntegrityException is thrown if any of the following situations occurs:

- If the interfaceInstanceIds and trustStateSettings collections size are not equal.
- If the trustStateSettings collection contains an interface which is not of type TrustStateSetting.

Parameters

opContext— Operational context.

interfaceInstanceIds—InstanceNameIds of interfaces.

trustStateSettings—Modified TrustStateSetting objects.

Return Value

void

unbindArpAclFromVlans

Removes the association with ARP ACLs in a collection of VLANs

ValidationException is thrown if any of the following situations occurs:

Send document comments to nexus7k-docfeedback@cisco.com

- If the vlanInstanceNameIds collection is null or empty.
- If the vlanInstanceNameIdCol collection contains one null element, or the collection contains an invalid VLAN instance name ID.

Parameters

opContext— Operational context.

vlanInstanceNameIds— InstanceNameId of VLANs in which the ARP ACL association has to be removed.

Return Value

void

Send document comments to nexus7k-docfeedback@cisco.com