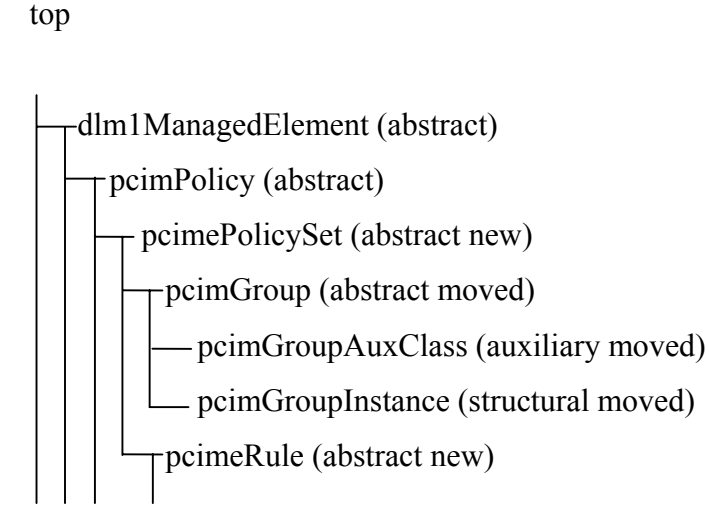
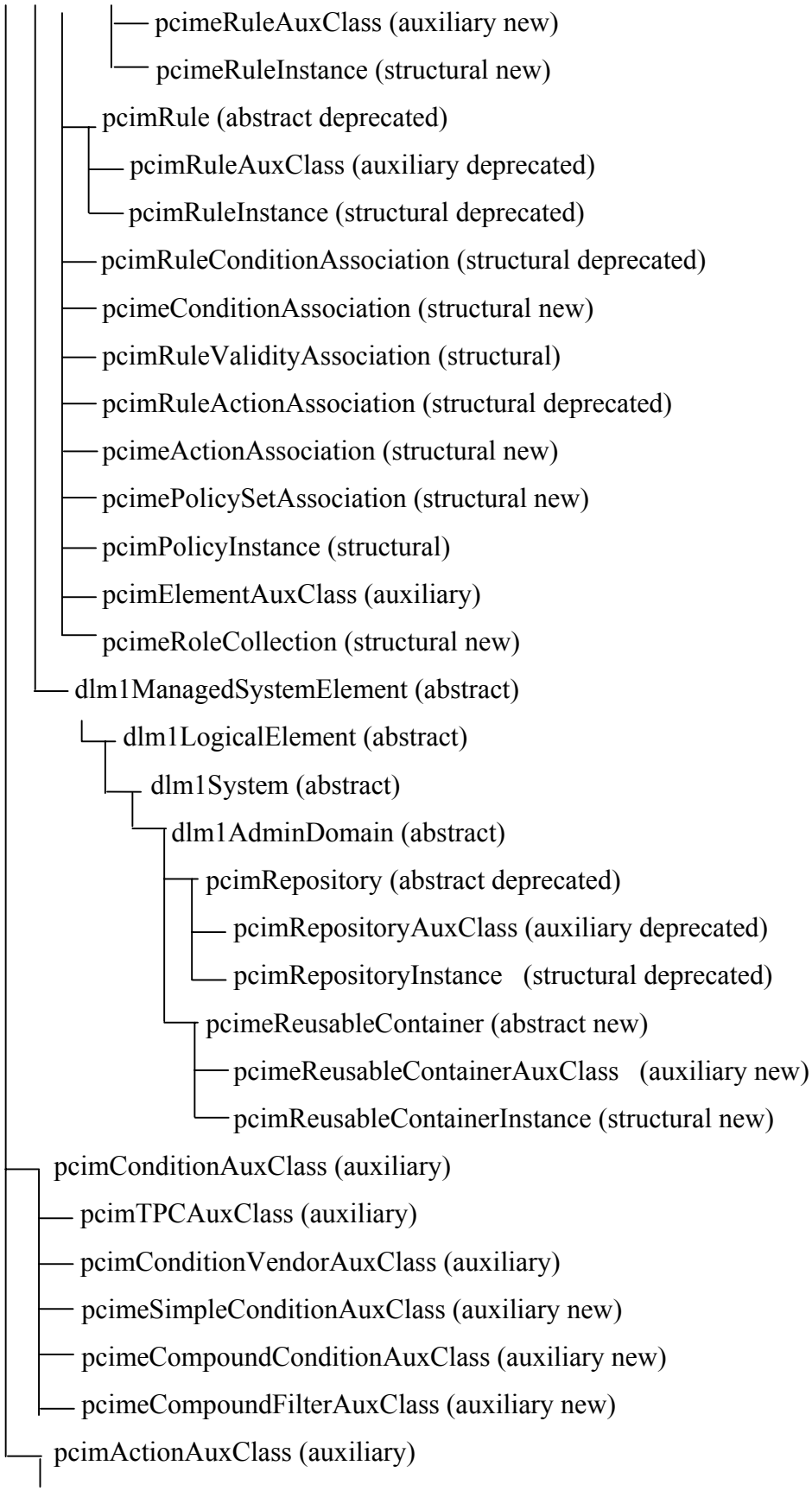
Appendix I

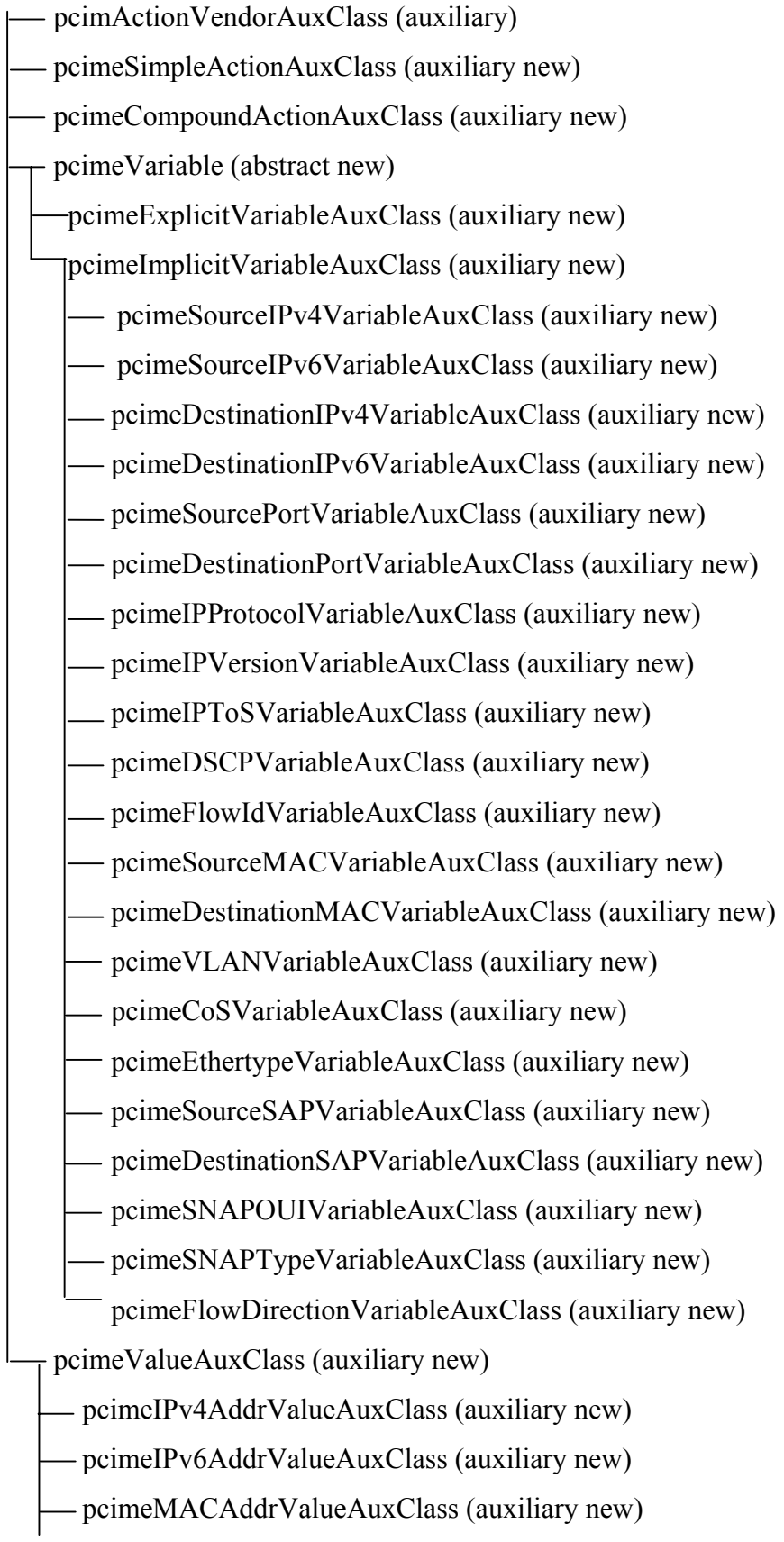
Policy Core Extension LDAP Schema (PCELS)

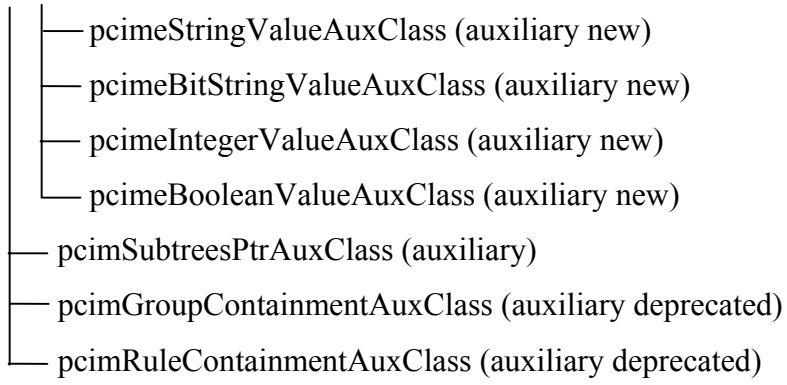
I.1 Inheritance Hierarchy for PCELS

The following diagram illustrates the class hierarchy for the LDAP Classes defined in [Strassner02] and the new LDAP classes that we defined [Reyes03].




pcimeRuleAuxClass (auxiliary new)
pcimeRuleInstance (structural new)
pcimRule (abstract deprecated)
pcimRuleAuxClass (auxiliary deprecated)
pcimRuleInstance (structural deprecated)
pcimRuleConditionAssociation (structural deprecated)
pcimeConditionAssociation (structural new)
pcimRuleValidityAssociation (structural)
pcimRuleActionAssociation (structural deprecated)
pcimeActionAssociation (structural new)
pcimePolicySetAssociation (structural new)
pcimPolicyInstance (structural)
pcimElementAuxClass (auxiliary)
pcimeRoleCollection (structural new)
dlm1ManagedSystemElement (abstract)
dlm1LogicalElement (abstract)
dlm1System (abstract)
dlm1AdminDomain (abstract)
pcimRepository (abstract deprecated)
pcimRepositoryAuxClass (auxiliary deprecated)
pcimRepositoryInstance (structural deprecated)
pcimeReusableContainer (abstract new)
pcimeReusableContainerAuxClass (auxiliary new)
pcimReusableContainerInstance (structural new)
pcimConditionAuxClass (auxiliary)
pcimTPCAuxClass (auxiliary)
pcimConditionVendorAuxClass (auxiliary)
pcimeSimpleConditionAuxClass (auxiliary new)
pcimeCompoundConditionAuxClass (auxiliary new)
pcimeCompoundFilterAuxClass (auxiliary new)
pcimActionAuxClass (auxiliary)


pcimActionVendorAuxClass (auxiliary)
pcimeSimpleActionAuxClass (auxiliary new)
pcimeCompoundActionAuxClass (auxiliary new)
pcimeVariable (abstract new)
pcimeExplicitVariableAuxClass (auxiliary new)
pcimeImplicitVariableAuxClass (auxiliary new)
pcimeSourceIPv4VariableAuxClass (auxiliary new)
pcimeSourceIPv6VariableAuxClass (auxiliary new)
pcimeDestinationIPv4VariableAuxClass (auxiliary new)
pcimeDestinationIPv6VariableAuxClass (auxiliary new)
pcimeSourcePortVariableAuxClass (auxiliary new)
pcimeDestinationPortVariableAuxClass (auxiliary new)
pcimeIPProtocolVariableAuxClass (auxiliary new)
pcimeIPVersionVariableAuxClass (auxiliary new)
pcimeIPToSVariableAuxClass (auxiliary new)
pcimeDSCPVariableAuxClass (auxiliary new)
pcimeFlowIdVariableAuxClass (auxiliary new)
pcimeSourceMACVariableAuxClass (auxiliary new)
pcimeDestinationMACVariableAuxClass (auxiliary new)
pcimeVLANVariableAuxClass (auxiliary new)
pcimeCoSVariableAuxClass (auxiliary new)
pcimeEthertypeVariableAuxClass (auxiliary new)
pcimeSourceSAPVariableAuxClass (auxiliary new)
pcimeDestinationSAPVariableAuxClass (auxiliary new)
pcimeSNAPOUIVariableAuxClass (auxiliary new)
pcimeSNAPTypeVariableAuxClass (auxiliary new)
pcimeFlowDirectionVariableAuxClass (auxiliary new)
pcimeValueAuxClass (auxiliary new)
pcimeIPv4AddrValueAuxClass (auxiliary new)
pcimeIPv6AddrValueAuxClass (auxiliary new)
pcimeMACAddrValueAuxClass (auxiliary new)



I.1.1 Class Definitions

This sections details all the new classes previously mentioned.

The pcimePolicySet Class.

This abstract class PolicySet in the [PCIM_EXT] is introduced to provide an abstraction for a set of rules. The class value 'pcimePolicySet' is used as the mechanism for identifying group and rule- related instances in the DIT.

In [PCIM_EXT], the classes PolicyGroup and PolicyRule are moved, so that they are now derived from PolicySet class. A pcimePolicySet object refers to instances of pcimGroup and pcimeRule via the attribute pcimePolicySetList and the attribute pcimePolicySetDN in the pcimePolicySetAssociation object class.

The definition of the abstract class pcimePolicySet:

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimePolicySet'
  DESC 'Abstract class that represents a collection of policies that form a coherent set.'
  SUP pcimPolicy
  ABSTRACT
  MAY ( pcimePolicySetName   $ pcimeDecisionStrategy  $ pcimRoles
          $ pcimePolicySetList )
)
```

One of the attributes of the pcimePolicySet class, the pcimRoles is already defined in [PCLS]. The other three attributes are defined below. The attribute pcimePolicySetName may be used as naming attribute for pcimePolicySet entries:

```
 ( IANA-ASSIGNED-OID.2.x
  NAME 'pcimePolicySetName'
  DESC 'The user-friendly name of a policy set.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The attribute pcimeDecisionStrategy is used to define the evaluation method among the rules in the policy set and is mapped directly from the PolicyDecisionStrategy property defined in [PCIM_EXT].

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeDecisionStrategy'
  DESC 'The evaluation method used for the components of a in the pcimePolicySet.
        Valid values: 1 [FirstMatching], 2 [AllMatching]'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)
```

The attibute pcimePolicySetList is used to realize the PolicySetComponent aggregation.

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimePolicySetList'
  DESC 'List of DN references to the pcimePolicySetAssociation entries used to aggregate policy sets.'
  EQUALITY distinguishedNameMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
```

The subclasses pcimGroup and pcimeRule are now derived from pcimePolicySet.

The Structural Class pcimePolicySetAssociation

The pcimePolicySetAssociation class is used to aggregate components into pcimePolicySet entries. Instances of this class are always subordinated to the aggregating pcimePolicySet. The aggregation of reusable instances of (subclasses of) pcimePolicySet are referenced via the pcimePolicySetDN attribute. Non-reusable instances of (subclasses of) pcimePolicySet are attached as auxiliary classes directly to the pcimePolicySetAssociation entries.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimePolicySetAssociation'
  DESC 'Structural class that contains attributes characterizing the relationship between a policy set and one of

        its components.'
  SUP pcimPolicy
  STRUCTURAL
  MUST ( pcimePriority )
  MAY ( pcimePolicySetName $ pcimePolicySetDN )
)
```

The Attribute pcimePriority:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimePriority'
  DESC 'Policy priority.'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)
```

The Attribute pcimePolicySetDN:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimePolicySetDN'
  DESC 'DN reference to a pcimePolicySet entry.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE
)
```

The moved pcimGroup class

The pcimGroup is defined in [PCLS]. Its superclass is changed here so that the pcimGroup can take advantage of the pcimePolicySet and its aggregation method.

```
( IANA-ASSIGNED-OID.1.2
  NAME 'pcimGroup'
  DESC  'A container for a set of related pcimeRules and/or a set of related pcimGroups.'
  SUP     pcimePolicySet
  ABSTRACT
   MAY    (pcimGroupName)
)
```

The Deprecated Class pcimGroupContainmentAuxClass

The policy group aggregation is replaced by the more comprehensive policy set aggregation. Therefore this class is deprecated:

```
( IANA-ASSIGNED-OID.1.22
  NAME 'pcimGroupContainmentAuxClass'
  DESC 'An auxiliary class used to bind pcimGroups to an appropriate container object.'
  OBSOLETE
  SUP top
  AUXILIARY
  MAY ( pcimGroupsAuxContainedSet )
)
```

The attribute pcimGroupsAuxContainedSet is also deprecated:

```
( IANA-ASSIGNED-OID.2.38
  NAME 'pcimGroupsAuxContainedSet'
  DESC 'DNs of pcimGroups associated in some way with the instance to which this attribute has been
        appended.'
  OBSOLETE
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
```

The Deprecated Class pcimRuleContainmentAuxClass

The policy rule aggregation is replaced by the more comprehensive policy set aggregation. Therefore this class is deprecated.

```
( IANA-ASSIGNED-OID.1.23
```

```
  NAME 'pcimRuleContainmentAuxClass'
  DESC 'An auxiliary class used to bind pcimRules to an appropriate container object.'
  OBSOLETE
  SUP top
  AUXILIARY
  MAY ( pcimRulesAuxContainedSet )
)
```

The attribute pcimRulesAuxContainedSet is also deprecated:

```
( IANA-ASSIGNED-OID.2.39
  NAME 'pcimRulesAuxContainedSet'
  DESC 'DNs of pcimRules associated in some way with the instance to which this attribute has been
        appended.'
  OBSOLETE
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
```

The three new pcimeRule classes

The base class representing policy rules is redefined without a priority attribute. In addition, this class uses the Condition and Action aggregation methods as the CompoundCondition and the CompoundAction.

```
    (IANA-ASSIGNED-OID.1.x
     NAME 'pcimeRule'
     DESC   'The base class for representing the "If Condition then Action" semantics
             associated with a Policy Rule'
     SUP    pcimePolicySet
     ABSTRACT
     MAY    (pcimRuleName $ pcimRuleEnabled $ pcimeConditionListType $
             pcimeConditionList $pcimeActionList $ pcimRuleValidityPeriodList $
             pcimRuleUsage $ pcimRuleMandatory $pcimeSequencedActions
             $ pcimeExecutionStrategy)
    )

    ( IANA-ASSIGNED-OID.1.x
      NAME 'pcimeRuleAuxClass'
      DESC 'An auxiliary class for representing the "If Condition then Action" semantics
             associated with a policy rule.'
      SUP pcimeRule
      AUXILIARY
    )

    ( IANA-ASSIGNED-OID.1.x
      NAME 'pcimeRuleInstance'
      DESC 'A structural class for representing the "If Condition then Action" semantics associated with a
```

```
            policy rule.'
    SUP pcimeRule
    STRUCTURAL
  )
```

The attributes pcimRuleCoditionListType, pcimRuleConditionList and pcimRuleActionList defined in [PCLS] are replaced in PCELS in order to reuse them in pcimeCompoundConditionAuxClass and pcimeCompoundActionAuxClass object classes. The definitions are as follows:

```
( IANA-ASSIGNED-OID.2.x
    NAME 'pcimeConditionListType'
    DESC 'a value of 1 means that this policy rule is in disjunctive normal form; a value of 2 means that this
          policy rule is in conjunctive normal form.'
    EQUALITY integerMatch
    ORDERING integerOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
    SINGLE-VALUE
)

( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeConditionList'
  DESC 'unordered set of Dns to the pcimeConditionAssociation entries used to
        aggregate policy conditions.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)

 ( IANA-ASSIGNED-OID.2.x
    NAME 'pcimeActionList'
    DESC 'Unordered set of DNs to the pcimeActionAssociation entries used to aggregate policy actions.'
    EQUALITY distinguishedNameMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
   )

( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeSequencedActions'
  DESC 'Indicates whether the ordered execution of actions in an aggregate is mandatory, recommended, or
        dontCare.'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)
```

The new attribute pcimeExecutionStrategy is a direct mapping of the ExecutionStrategy property in the [PCIM_EXT]'s PolicyRule class.

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeExecutionStrategy'
  DESC 'Indicates the execution strategy to be used upon an action aggregate.
  VALUES: 1 [Do until success]; 2 [Do all]; 3 [do until failure]. Default value  = 2.'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)
```

The Structural Class pcimeConditionAssociation

This class is used to aggregate policy conditions in compound policy conditions or policy rules.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeConditionAssociation'
  DESC 'This class contains attributes characterizing the relationship between a policy condition and one of
        its ggregators: pcimeRule or pcimeCompoundConditionAuxClass). It is used in the realization of a

        policy condition structure.'
  SUP pcimPolicy
  STRUCTURAL
  MUST ( pcimConditionGroupNumber   $ pcimConditionNegated )
  MAY ( pcimConditionName  $ pcimConditionDN )
  )
```

Its attributes are defined in the section 5.4 of the [PCLS].

The Structural Class pcimeActionAssociation

This class is used to aggregate policy actions in compound policy actions or policy rules. It implements the PolicyActionInPolicyRule and PolicyActionInPolicyAction aggregations. The class definition follows:

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeActionAssociation'
  DESC 'This class contains attributes characterizing the relationship between a policy action and one of its
        aggregators. It is used in the realization of a policy action  structure.'
```

```
  SUP pcimPolicy
  STRUCTURAL
  MUST ( pcimActionOrder )
  MAY ( pcimActionName   $ pcimActionDN )
)
```

Its attributes are defined in [PCLS].

The Three Deprecated pcimRule classes

The class pcimRule and its subclasses are replaced by pcimeRule and its subclasses. Therefore pcimeRule and its subclasses are deprecated.

```
( IANA-ASSIGNED-OID.1.5
  NAME 'pcimRule'
  DESC 'The base class for representing the "If Condition then Action" semantics
        associated with a policy rule.'
  OBSOLETE
  SUP pcimPolicy
  ABSTRACT
  MAY ( pcimRuleName     $ pcimRuleEnabled      $ pcimRuleConditionListType
        $ pcimRuleConditionList      $ pcimRuleActionList
        $ pcimRuleValidityPeriodList      $ pcimRuleUsage      $ pcimRulePriority
        $ pcimRuleMandatory      $ pcimRuleSequencedActions      $ pcimRoles )
)

( IANA-ASSIGNED-OID.1.6
  NAME 'pcimRuleAuxClass'
  DESC 'An auxiliary class for representing the "If Condition then Action" semantics associated with a policy
        rule.'
  OBSOLETE
  SUP pcimRule
  AUXILIARY
)

 ( IANA-ASSIGNED-OID.1.7
  NAME 'pcimRuleInstance'
  DESC 'A structural class for representing the "If Condition then Action" semantics associated with a
        policy rule.'
  OBSOLETE
  SUP pcimRule
  STRUCTURAL
)
```

The following attributes are also deprecated since with the deprecation of pcimRule, no other classes use them:

```
( IANA-ASSIGNED-OID.2.7
  NAME 'pcimRuleConditionListType'
  DESC 'A value of 1 means that this policy rule is in  disjunctive normal form; a value  of 2 means that this
        policy rule is in conjunctive normal form.'
  OBSOLETE
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)

( IANA-ASSIGNED-OID.2.8
  NAME 'pcimRuleConditionList'
  OBSOLETE
  DESC 'Unordered set of DNs of pcimRuleConditionAssociation entries representing
        associations between this policy rule and its conditions.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)

( IANA-ASSIGNED-OID.2.9
  NAME 'pcimRuleActionList'
  OBSOLETE
  DESC 'Unordered set of DNs of pcimRuleActionAssociation entries representing associations between this
        policy  rule and its actions.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)

 ( IANA-ASSIGNED-OID.2.12
  NAME 'pcimRulePriority'
  DESC 'A non-negative integer for prioritizing this pcimRule relative to other pcimRules. A larger value
        indicates a higher priority.'
  OBSOLETE
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)

( IANA-ASSIGNED-OID.2.14
  NAME 'pcimRuleSequencedActions'
  DESC 'An integer enumeration indicating that the ordering of actions defined by the
        pcimActionOrder attribute is mandatory(1), recommended(2), or dontCare(3).'
  OBSOLETE
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE
)
```

The Deprecated Class pcimRuleConditionAssociation.

This class is replaced by the more flexible pcimeConditionAssociation.

```
( IANA-ASSIGNED-OID.1.8
  NAME 'pcimRuleConditionAssociation'
  DESC 'This class contains attributes characterizing the relationship between a policy
        rule and one of its policy conditions.'
  OBSOLETE
  SUP pcimPolicy
  STRUCTURAL
  MUST ( pcimConditionGroupNumber  $ pcimConditionNegated )
  MAY ( pcimConditionName  $ pcimConditionDN )
)
```

The Deprecated Class pcimeRuleActionAssociation.

This class is replaced by the more flexible pcimeActionAssociation.

```
 ( IANA-ASSIGNED-OID.1.10
  NAME 'pcimRuleActionAssociation'
  DESC 'This class contains attributes characterizing the  relationship between a policy
        rule and one of its policy actions.'
  OBSOLETE
  SUP pcimPolicy
  STRUCTURAL
  MUST ( pcimActionOrder )
  MAY ( pcimActionName    $ pcimActionDN )
)
```

The Auxiliary Class pcimeSimpleConditionAuxClass.

This class indicates if a specific <variable> match with a specific <value>. The "match" relationship is to be interpreted by analyzing the variable and value instances associated with the simple condition.

There is an attribute to realize pcimePolicyValueinSimplePolicyCondition and pcimePolicyVariableinSimplePolicyCondition associations. The class definition is as follows:

```
(  IANA-ASSIGNED-OID.1.x
   NAME 'pcimeSimpleConditionAuxClass'
   DESC   'An auxiliary class that evaluate the matching between a
          value and a variable'.
   SUP     pcimConditionAuxClass
   AUXILIARY
   MAY (pcimeVariableDN $ pcimeValueDN)
)
```

There are two attributes that may be in the pcimeSimpleConditionAuxClass class: the attribute pcimeVariableDN and pcimeValueDN. The pcimeVariableDN attribute definition is:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeVariableDN'
  DESC 'DN reference to a pcimeVariable entry.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE
)
```

The pcimeValueDN attribute definition is:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeValueDN'
  DESC 'DN reference to a pcimeValue entry.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE
)
```

The Auxiliary Class pcimeCompoundConditionAuxClass.

This class represents a compound policy condition, formed by aggregation of simple policy conditions. There is an attribute representing a boolean combination of simpler conditions. The class definition is as follows:

```
(  IANA-ASSIGNED-OID.1.x
   NAME "pcimeCompoundConditionAuxClass"
   DESC   "An auxiliary class that represents a boolean combination of simpler
           conditions".
   SUP     pcimConditionAuxClass
   AUXILIARY
   MAY   (pcimeConditionListType $ pcimeConditionList)
```

)

The attribute pcimeConditionListType is used to specify whether the list of policy conditions associated with this compound policy condition is in disjunctive normal form (DNF) or conjunctive normal form (CNF). The attribute pcimeConditionList is an unordered set of DNs to conditions aggregated in the compound condition. The attributes are previously defined.

The Auxiliary Class pcimeCompoundFilterAuxClass.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeCompoundFilterAuxClass'
  DESC 'A compound condition with mirroring capabilities for traffic
          caracterization.'
  SUP pcimeCompoundConditionAuxClass
  AUXILIARY
  MAY ( pcimeIsMirrored )
)
```

The Attribute pcimeIsMirrored:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeIsMirrored'
  DESC 'Indicates whether traffic that mirrors the specified filter is to be treated as
        matching the filter.'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE
)
```

The Auxiliary Class pcimeSimpleActionAuxClass.

This class overwrites an old value of the <variable> and set the new <value>. There is an attribute to realize pcimePolicyValueInSimplePolicyAction, pcimeValueDN, and pcimePolciyVariableInSimplePolicyAction associations, pcimeVariableDN. The first attribute is used to attach a variable to a SimplePolicyAction and the second one is used to attach a value to a SimplePolicyAction.

The class definition is as follows:

```
(  IANA-ASSIGNED-OID.1.x
   NAME 'pcimeSimpleActionAuxClass'
```

```
    DESC   'This class contains attributes characterizing the relationship between a
           Simple PolicyAction and one variable and one value.'
    SUP pcimActionAuxClass
    AUXILIARY
    MAY (pcimeVariableDN $ pcimeValueDN)
  )
```

The attributes are previously defined.

The Auxiliary Class pcimeCompoundActionAuxClass.

This class maps the CompoundPolicyAction class of the [PCIM_EXT]. The class definition is as follows:

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeCompoundActionAuxClass'
  DESC 'A class that aggregates simpler actions in a sequence with specific execution strategy.'
  SUP pcimActionAuxClass
  AUXILIARY
  MAY ( pcimeActionList   $ pcimeSequencedActions   $ pcimeExecutionStrategy )
)
```

The attributes pcimeSequencedActions, pcimeExecutionStrategy and pcimeActionList are previously defined.

The Abstract Class pcimeVariable.

Variables specify the property of a flow or an event that should be matched when evaluating the condition. A given variable selects the set of matchable value types through the ExpectedPolicyValuesForVariable association.
The classes definitions are as follows. First, the definition of the abstract class pcimePolicyVariable:

```
  ( IANA-ASSIGNED-OID.1.x
    NAME 'pcimeVariable'
    DESC 'Base class for representing a variable whose actual value can be matched against or set to a specific

          value.'
    SUP top
    ABSTRACT
```

```
  MAY ( pcimeVariableName $ pcimeExpectedValueList )
)
```

The attribute pcimeVariableName is an user-friendly name for the variable.

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeVariableName'
  DESC 'The user-friendly name of a variable.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The attribute pcimeExpectedValueList is an unordered set of DNs to subclasses of pcimeValueAuxClass. It maps the PCIM_EXT's ExpectedPolicyValuesForVariable association:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeExpectedValueList'
  DESC 'List of DN references to the pcimeValueAuxClass entries that represent the
        acceptable values.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
```

The auxiliary Class pcimeExplicitVariableAuxClass

The subclass pcimeExplicitVariableAuxClass is defined as follows:

```
(  IANA-ASSIGNED-OID.1.x
   NAME 'pcimeExplicitVariableAuxClass'
   DESC 'Explicitly defined policy variable evaluated within the context of the CIM
         Schema.'
   SUP pcimeVariable
   AUXILIARY
   MUST ( pcimeVariableModelClass $ pcimeVariableModelProperty )
)
```

The attribute pcimeVariableModelClass is a string specifying the class name whose property is evaluated or set as a variable:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeVariableModelClass'
  DESC 'Specifies a CIM class name or oid.'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The attribute pcimeVariableModelProperty is a string specifying the attribute, within the pcimeVariableModelClass, which is evaluated or set as a variable:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeVariableModelProperty'
  DESC 'Specifies a CIM property name or oid.'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The Auxiliary Class pcimeImplicitVariableAuxClass

The subclass pcimeImplicitVariableAuxClass is defined as follows:

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeImplicitVariableAuxClass'
  DESC 'Implicitly defined policy variables whose evaluation depends on the usage
        context. Subclasses specify the data type and semantics of the variables.'
  SUP pcimeVariable
  AUXILIARY
  MUST ( pcimeExpectedValueTypes )
)
```

The attribute pcimeExpectedValueTypes is the direct mapping from the valueTypes property in the PCIM_EXT's PolicyImplicitVariable class. This attribute representes a set of allowed value types to be used with this variable.

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeExpectedValueTypes'
  DESC 'List of object class names or oids of subclasses of pcimeValueAuxClass that
       define acceptable value types.'
  EQUALITY caseIgnoreMatch
```

```
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  )
```

Subclasses of pcimeImplicitVariableAuxClass

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSourceIPv4VariableAuxClass'
  DESC 'Source IP v4 address'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSourceIPv6VariableAuxClass'
  DESC 'Source IP v6 address'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeDestinationIPv4VariableAuxClass'
  DESC 'Destination IP v4 address'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeDestinationIPv6VariableAuxClass'
  DESC 'Destination IP v6 address'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSourcePortVariableAuxClass'
  DESC 'Source port'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeDestinationPortVariableAuxClass'
  DESC 'Destination port'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeIPProtocolVariableAuxClass'
  DESC 'IP protocol number'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
```

```
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeIPVersionVariableAuxClass'
  DESC 'IP version nulmer'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeIPToSVariableAuxClass'
  DESC 'IP ToS'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeDSCPVariableAuxClass'
  DESC 'DiffServ code point'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)


( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeFlowIdVariableAuxClass'
  DESC 'Flow Identifier'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSourceMACVariableAuxClass'
  DESC 'Source MAC address'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeDestinationMACVariableAuxClass'
  DESC 'Destination MAC address'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeVLANVariableAuxClass'
  DESC 'VLAN'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeCoSVariableAuxClass'
  DESC 'Class of service'
  SUP pcimeImplicitVariableAuxClass
```

```
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeEthertypeVariableAuxClass'
  DESC 'Ethertype'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSourceSAPVariableAuxClass'
  DESC 'Source SAP'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeDestinationSAPVariableAuxClass'
  DESC 'Destination SAP'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSNAPOUIVariableAuxClass'
  DESC 'SNAP OUI'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeSNAPTypeVariableAuxClass'
  DESC 'SNAP type'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeFlowDirectionVariableAuxClass'
  DESC 'Flow direction'
  SUP pcimeImplicitVariableAuxClass
  AUXILIARY
)
```

The Auxiliary Class pcimeValueAuxClass.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeValueAuxClass'
  DESC 'Base class for representing a value that can be matched against or set for a specific variable.'
  SUP top
  AUXILIARY
```

```
  MAY ( pcimeValueName )
)
```

The Attribute pcimeValueName:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeValueName'
  DESC 'The user-friendly name of a value.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

Subclasses of pcimeValueAuxClass.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeIPv4AddrValueAuxClass'
  DESC 'IP v4 address value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeIPv4AddrList )
)
```

The Attribute pcimeIPv4AddrList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeIPv4AddrList'
  DESC 'List of IPv4 address values, ranges or hosts.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeIPv6AddrValueAuxClass'
  DESC 'IP v6 address value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeIPv6AddrList )
)
```

The Attribute pcimeIPv6AddrList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeIPv6AddrList'
  DESC 'List of IPv6 address values, ranges or hosts.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeMACAddrValueAuxClass'
  DESC 'MAC address value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeMACAddrList )
)
```

The Attribute pcimeMACAddrList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeMACAddrList'
  DESC 'List of MAC address values or ranges.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeStringValueAuxClass'
  DESC 'String value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeStringList )
)
```

The Attribute pcimeStringList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeStringList'
  DESC 'List of strings or wildcarded strings.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeBitStringValueAuxClass'
  DESC 'Bit string value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeBitStringList )
)
```

The Attribute pcimeBitStringList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeBitStringList'
  DESC 'List of bit strings or masked bit strings.'
  EQUALITY caseIgnoreMatch
```

```
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeIntegerValueAuxClass'
  DESC 'Integer value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeIntegerList )
)
```

The Attribute pcimeIntegerList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeIntegerList'
  DESC 'List of integers or integer ramges.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeBooleanValueAuxClass'
  DESC 'Boolean value.'
  SUP pcimeValueAuxClass
  AUXILIARY
  MUST ( pcimeBoolean )
)
```

The Attribute pcimeBoolean:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeBoolean'
  DESC 'A boolean value.'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE
)
```

The three new Reusable Container classes.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeReusableContainer'
  DESC 'A container for reusable policy information.'
  SUP dlm1AdminDomain
  ABSTRACT
  MAY ( pcimeReusableContainerName $ pcimeReusableContainerList )
)

( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeReusableContainerAuxClass '
  DESC 'An auxiliary class that can be used to aggregate reusable policy information.'
  SUP pcimeReusableContainer
  AUXILIARY
)
```

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeReusableContainerInstance'
  DESC 'A structural class that can be used to aggregate reusable policy information.'
  SUP pcimeReusableContainer
  STRUCTURAL
)
```

The Attribute pcimeReusableContainerName:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeReusableContainerName'
  DESC 'The user-friendly name of a reusable policy container.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The Attribute pcimeReusableContainerList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeReusableContainerList'
  DESC 'List of DN references to the pcimeReusableContainer entries.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
```

The three deprecated Repository classes.

The pcimRepository and its subclasses are replaced by the pcimeReusableContainer and its subclasses.

```
( IANA-ASSIGNED-OID.1.18
  NAME 'pcimRepository'
  DESC 'A container for reusable policy information.'
  OBSOLETE
  SUP dlm1AdminDomain
  ABSTRACT
  MAY ( pcimRepositoryName )
)

( IANA-ASSIGNED-OID.1.19
  NAME 'pcimRepositoryAuxClass'
  DESC 'An auxiliary class that can be used to aggregate reusable policy information.'
  OBSOLETE
  SUP pcimRepository
  AUXILIARY
)

( IANA-ASSIGNED-OID.1.20
  NAME 'pcimRepositoryInstance'
```

```
  DESC 'A structural class that can be used to aggregate reusable policy information.'
  OBSOLETE
  SUP pcimRepository
  STRUCTURAL
)
```

The following attribute is also deprecated:

```
( IANA-ASSIGNED-OID.2.36
  NAME 'pcimRepositoryName'
  DESC 'The user-friendly name of this policy repository.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The new class pcimeRoleCollection.

```
( IANA-ASSIGNED-OID.1.x
  NAME 'pcimeRoleCollection'
  DESC 'This class is used to group together entries that share a same role.'
  SUP pcimPolicy
  STRUCTURAL
  MUST ( pcimeRole )
  MAY ( pcimeRoleCollectionName   $ pcimeElementList )
)
```

The Attribute pcimeRole:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeRole'
  DESC 'String representing a role.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The Attribute pcimeRoleCollectionName:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeRoleCollectionName'
  DESC 'The user-friendly name of a role collection.'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
)
```

The Attribute pcimeElementList:

```
( IANA-ASSIGNED-OID.2.x
  NAME 'pcimeElementList'
  DESC 'List of DN references to the entries representing managed elements.'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
)
```

I.2 Security Considerations

This topic is based on requirements from previous documents [Strassner02], [Moore01] and [Moore03] and also takes into account other RFCs about different aspects, for example [Hodges02]. These RFC documents provide a general framework for security architecture of the system. However some comments have to be provided as a consequence of the inclusion of extensions in this own document and its relation with PCLS doc.

Due to the new considered scenarios, with reusability and information containers located in other DITs etc, these conditions are expressed in chapter 4.4 of the [Strassner02] document. As a consequence, new types of threats in the system have to be considered. In fact, it is necessary to define new security services in order to protect against these new aspects. As a result of this, the following new security services are defined:

1) Athentication between entities of the network
2) Mutual authentication between network operator and network entities (p.e. DITs)
3) Integrity and confidentiality of links between network entities and also in the LDAP directories.

Several definitions and security mechanisms related about DITs can also obtained from the following ITU specification: X.509 The Directory Authentication framework. Furthermore, the obtention of the OIDs and values of the attributes from the DITs in a distributed scenario has as a consequence the interaction between diverse network entities with changes of security domain and/or administrative domain.

In this directory scenario, with migration of data, the use of DSP (Directory Service Protocol) protocol with types of queries like referral, chaining and multicasting with different key management and authentication among network entities would have to be considered.

I.3 IANA Considerations

Object Identifiers

It is requested that IANA register an LDAP Object Identifer for use in this technical specification according to the following template:

Subject: Request for LDAP OID Registration Person & email address to contact for further information:XXX
Specification: RFC XXXX
Author/Change Controller: IESG
Comments: The assigned OID will be used as a base for identifying a number of schema elements defined in this document.

Object Identifier Descriptors

It is requested that IANA register the LDAP Descriptors used in this technical specification as detailed in the following template:

Subject: Request for LDAP Descriptor Registration Update
Descriptor (short name): see comment
Object Identifier: see comment
Person & email address to contact for further information: Bob Moore (remoore@us.ibm.com)

Usage: see comment

Specification: RFC XXXX

Author/Change Controller: IESG

Comments:

The following descriptors should be added:

NAME	Type	OID
pcimeXXX	O	IANA-ASSIGNED-OID.1.1

I.4 Open Issues

1. To define classes to search errors and classes to detect failures in the system
2. Because of the policy server is centralized and the LDAP is distributed hierarchically could be necessary to add classes in order to find duplicates in the information. It can occur, for example when updating is excessively often.
3. Mapping between Network domains and the updating of information.
4. Servers via resource management programs could manage some of these topics, even though it is necessary to add specific classes.
5. Considerations about the relation between performances related to retrieval of information and storage capacity of DITs.
6. The following PCIM EXT classes and aggregations need to be addressed: FilterEntryBase, IpHeadersFilter, 8021Filter, FilterList and EntriesInFilterList.

References

[CIM] Distributed Management Task Force, Inc., *Common Information Model (CIM) Schema,* version 2.3, March 2000. The components of the CIM schema are available via links on the following DMTF web page: http://www.dmtf.org/spec/cims.html

[Hodges02] J. Hodges, R. Morgan. *Lightweight Directory Access Protocol (v3): Technical Specification.* September IETF Request For Comments (RFC) 3377. 2002.

[Moore01] B. Moore, E. Ellesson, J. Strassner, *Policy Core Information Model -- Version 1 Specification,* IETF Request For Comments (RFC) 3060. May, 2000.

[Moore03] B. Moore at el., *Policy Core Information Model (PCIM) Extensions*, IETF Request For Comments (RFC) 3460, January 2003.

[Reyes03] Reyes, A., Barba A., Moron, D., Brunner, M., Pana M. *Policy Core Extension LDAP Schema (PCELS)*, Internet Draft. February 2003.

[Strassner02] J. Strassner, E. Ellesson, B. Moore, R. Moats, *Policy Core LDAP Schema*, IETF Internet Draft, draft-ietf-policy-core-schema-16.txt. October 2002

[Zeilenga02] Zeilenga, K., *Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP),* BCP 64, IETF Request For Comments (RFC) 3383, September 2002.