Access Node Control Protocol (ANCP) MIB module for Access Nodes
draft-ietf-ancp-mib-an-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 11, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols. In particular it defines objects for managing access nodes that are using the Access Node Control Protocol (ANCP).
Table of Contents

1. Introduction .................................................. 3
2. The Internet-Standard Management Framework ................. 3
3. Conventions .................................................. 3
4. Overview ....................................................... 3
5. Structure of the MIB Module ................................ 3
   5.1. Textual Conventions .................................. 5
   5.2. The ANCP Subtree for the Access Node ............... 5
   5.3. The Notifications Subtree ............................. 5
   5.4. Relationship to Other MIB Modules ................... 5
6. ANCP MIB Definitions for the Access Node ................ 6
7. Security Considerations ..................................... 24
8. IANA considerations ......................................... 28
9. Acknowledgements ............................................ 28
10. References .................................................. 29
   10.1. Normative References ................................. 29
   10.2. Informative References ............................... 30
Authors’ Addresses ............................................. 30
Intellectual Property and Copyright Statements ............... 31
1. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols. In particular it defines objects for managing access nodes as described in [ANCPF] that are using the Access Node Control Protocol defined in [ANCPP].

2. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIV2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

3. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

4. Overview

In [ANCPF], the framework for the Access Node Control Protocol (ANCP) is described. It defines 2 network entities, the Access Node (AN) and the Network Access Server (NAS), between which ANCP sessions are established. The detailed protocol specification of ANCP is described in [ANCPP]. This document specifies a MIB module for an AN that supports ANCP.

Note: the current MIB definition is specific for [ANCPP]. If [ANCPP] gets updated later, then the MIB definition in this document will also follow these changes.

5. Structure of the MIB Module

The ANCP MIB module for the AN has 3 tables. The tables are the
following:

- **ancpAnSessionConfigTable**
  
  This table is used to configure ANCP sessions at the AN towards a specific NAS. The NAS is identified by a number of attributes in this table (ancpAnSessionConfigNasIpAddressType and ancpAnSessionConfigNasIpAddress). The other attributes in this table can be used to configure properties that are specific for that particular ANCP session.

- **ancpAnCurrentSessionTable**
  
  This table shows the operational state of a particular ANCP session. Each session configured in ancpAnSessionConfigTable has a corresponding row in ancpAnCurrentSessionTable. When a session is configured or deleted in the ancpAnSessionConfigTable, then the corresponding row of that session in the ancpAnCurrentSessionTable is, respectively, automatically created or deleted.

- **ancpAnInterfaceConfigTable**
  
  This table is used to assign interfaces to particular partitions if partitions are being used as indicated by the scalar ancpAnPartitionsUsed. When partitions are used, a row in this table is created automatically when an interface is created in the ifTable of the IF-MIB [RFC2863] for which the system supports ANCP.

Four groups are defined:

- **ancpAnConfigGroup**
  
  This group contains all objects of the ancpAnSessionConfigTable in which the ANCP sessions are configured in the access node.

- **ancpAnCurrentGroup**
  
  This group contains all objects of the ancpAnCurrentSessionTable where the operational state and other information of the ANCP sessions are shown.

- **ancpAnInterfaceGroup**
  
  This group contains all objects to configure interfaces to be used by ANCP. Assigning interfaces to particular partitions is part of this group in case partitions are used.
o  ancpAnNotificationsGroup

   This group contains the notifications that indicate state changes of ANCP sessions.

5.1.  Textual Conventions

Two new textual convention, GsmpSubVersion and AncpAnSessionCapabilities, are defined in this MIB module. The ANCP specification in [ANCPPR] is re-using the GSMP specification in [RFC3292] where the GSMP subversion is introduced. These textual convention complement the textual conventions defined in [RFC3295], GsmpVersion, GsmpNameType, and GsmpPartitionIdType, which are also used in this MIB module. These textual conventions are used for the convenience of humans reading the MIB.

5.2.  The ANCP Subtree for the Access Node

TBD

5.3.  The Notifications Subtree

Notifications are defined to inform the management station about state changes of ANCP sessions, whenever an ANCP session changes state. Two notifications are defined for this purpose. The notification ancpAnSessionUp is to inform the management station when the session comes up, and the notification ancpAnSessionDown is to inform when the ANCP session is down again after it was up before.

Attributes are introduced to enable and disable the generation of these notifications per ANCP session. No other special measures for congestion avoidance for the notifications are needed because the number of ANCP sessions in an access node is typically small. In addition, establishing an ANCP session and tearing down it again, takes some time such that for a particular ANCP session, not many notifications in a short time period can be generated.

5.4.  Relationship to Other MIB Modules

There is a dependency with the Interfaces Group MIB (IF-MIB) defined in [RFC2863]. The ifIndex defined in the ifTable of IF-MIB is used as the index of the ancpAnInterfaceConfigTable defined in the ANCP MIB module for access nodes. Each time that an entry is created in the ifTable for which the system supports ANCP (e.g., in a DSLAM this is typically for each DSL line), a row is created automatically in the ancpAnInterfaceConfigTable if partitions are being used.
6. ANCP MIB Definitions for the Access Node

ANCP-AN-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE,
    Unsigned32, mib-2, TimeTicks,
    NOTIFICATION-TYPE
    FROM SNMPv2-SMI                            -- [RFC2578]
    ZeroBasedCounter32
    FROM RMON2-MIB                             -- [RFC4502]
    ifIndex        FROM IF-MIB                        -- [RFC2863]
    InetAddressType, InetAddress, InetPortNumber
    FROM INET-ADDRESS-MIB                      -- [RFC4001]
    MODULE-COMPLIANCE, OBJECT-GROUP,
    NOTIFICATION-GROUP
    FROM SNMPv2-CONF                           -- [RFC2580]
    GsmpVersion, GsmpNameType, GsmpPartitionIdType
    FROM GSMP-MIB                              -- [RFC3295]
    RowStatus, TEXTUAL-CONVENTION, TruthValue
    FROM SNMPv2-TC;                            -- [RFC2579]

ancpAnMIB MODULE-IDENTITY
LAST-UPDATED "200711080000Z" -- 8 November 2007
ORGANIZATION "IETF ANCP Working Group"
CONTACT-INFO
  " Editors:
    Stefaan De Cnodder
    Alcatel-Lucent
    Postal: Copernicuslaan 50
    B-2018 Antwerp
    Belgium
    EMail: stefaan.de_cnodder@alcatel-lucent.be
    Phone: +32 3 240 85 15
    Moti Morgenstern
    ECI Telecom Ltd.
    Postal: 30 Hasivim St.
    Petach Tikva 49517,
    Israel.
    Email: moti.morgenstern@ecitele.com
    Phone: +972 3 926 6258
  "
DESCRIPTION
  "The MIB module for entities implementing the access node side of the Access Node Control Protocol (ANCP)."
Copyright (C) The IETF Trust (2007). The initial version of this MIB module was published in RFC yyyy; for full legal notices see the RFC itself.

-- RFC Ed.: replace yyyy with actual RFC number & remove this note
REVISION "200711080000Z" -- 8 November 2007
DESCRIPTION "Initial version as published in RFC yyyy."

-- RFC Ed.: replace yyyy with actual RFC number & remove this note
::= { mib-2 xxx }
-- The value xxx to be assigned by IANA.

ancpAnNotifications OBJECT IDENTIFIER ::= { ancpAnMIB 0 }
ancpAnObjects OBJECT IDENTIFIER ::= { ancpAnMIB 1 }
ancpAnConformance OBJECT IDENTIFIER ::= { ancpAnMIB 2 }

GsmpSubVersion ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
"The subversion numbers defined for the GSMP protocol."
SYNTAX Unsigned32

AncpAnSessionCapabilities ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
"ANCP capabilities supported by the AN.
The following capabilities are available:
topologyDiscovery (0) - Access Topology Discovery
lineConfig (1) - Line Configuration
multicast (2) - Multicast
120am (3) - Layer 2 OAM
A bit set means the associated capability is supported."
SYNTAX BITS {
  topologyDiscovery (0),
  lineConfig (1),
  multicast (2),
  120am (3)
}

--
-- Global ANCP Control Parameters
--
-- The following scalar parameters globally control the behavior
-- of the ANCP implementation
--

ancpAnPartitionsUsed OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-write
This object allows the manager to specify whether or not to use the ‘Partition ID’ field in the GSMP message header. When set to ‘false’ the application does not use partitions and the ancpAnSessionConfigPartitionId object MUST be zero for all sessions. In addition, rows SHOULD not be created in the ancpAnInterfaceConfigTable. When set to ‘true’ the application uses partitions and the ancpAnSessionConfigPartitionId object MUST be set, for every session, to a nonzero value. In such a case, rows are created in ancpAnInterfaceConfigTable. The default value zero in ancpAnInterfaceConfigPartitionId object means that the operator did not associate the interface with a particular partition. Note that modifying the value of this object is restricted. E.g., prior to setting it from ‘true’ to ‘false’ ancpAnSessionConfigRowStatus objects for all sessions should be set to notInService and the partition ID value MUST be set to zero.

The value of this object is persistent.

DEFVAL { false }
::= { ancpAnObjects 1 }
Internet-Draft                  ANCP MIB                   November 2007

ancpAnSessionConfigTable OBJECT-TYPE
SYNTAX  SEQUENCE OF AncpAnSessionConfigEntry
MAX-ACCESS not-accessible
STATUS   current
DESCRIPTION
"This table represents the ANCP sessions in the access
node. An entry in this table needs to be configured
(created) before an ANCP session might be started."
::= { ancpAnObjects 3 }

ancpAnSessionConfigEntry OBJECT-TYPE
SYNTAX AncpAnSessionConfigEntry
MAX-ACCESS not-accessible
STATUS   current
DESCRIPTION
"An entry in the table showing the data for a
specific actual or yet to be established session.
If partitions are used, one session corresponds to
one specific access node partition."
INDEX { ancpAnSessionConfigSessionId }
::= { ancpAnSessionConfigTable 1 }

AncpAnSessionConfigEntry ::= SEQUENCE {
ancpAnSessionConfigSessionId           Unsigned32,
ancpAnSessionConfigRowStatus           RowStatus,
ancpAnSessionConfigGsmpVersion         GsmpVersion,
ancpAnSessionConfigGsmpSubVersion      GsmpSubVersion,
ancpAnSessionConfigEncapsulationType   INTEGER,
ancpAnSessionConfigCapabilities        AncpAnSessionCapabilities,
ancpAnSessionConfigAliveTimer          Unsigned32,
ancpAnSessionConfigPortReportShaper    Unsigned32,
ancpAnSessionConfigAggregateReportShaper Unsigned32,
ancpAnSessionConfigTransportRetryTimer Unsigned32,
ancpAnSessionConfigAncpRetryTimer      Unsigned32,
ancpAnSessionConfigAnName              GsmpNameType,
ancpAnSessionConfigPartitionId         GsmpPartitionIdType,
ancpAnSessionConfigWindowSize          Unsigned32,
ancpAnSessionConfigNasIpAddressType    InetAddressType,
ancpAnSessionConfigNasIpAddress        InetAddress,
ancpAnSessionConfigEncapPortNumber     InetPortNumber,
ancpAnSessionConfigNotifyDnEnable      TruthValue,
ancpAnSessionConfigNotifyUpEnable      TruthValue
}

ancpAnSessionConfigSessionId OBJECT-TYPE
SYNTAX  Unsigned32 (1..255)
MAX-ACCESS not-accessible
STATUS   current
DESCRIPTION
"An index of a session referred by this row. The index
is unique across all partitions.
The referred session may be actually established or
just potential.
Prior to creating a row in the table it is advised to
check the ancpAnNextSessionId for an available index."
::= { ancpAnSessionConfigEntry 1 }

ancpAnSessionConfigRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"An object that allows entries in this table to
be created, modified and deleted using the RowStatus
convention.
A SET operation to any other attribute in this row, when
this object is set to 'active' (1), MUST be rejected with
an SNMP error (e.g., inconsistentValue).
In order to perform a SET operation to any other attribute
in this table the manager MUST set this object to
notInService (2). After setting the object back to
'active' the implementation MAY tear down the session and
recreate it, depending on what session attributes have
been modified."
::= { ancpAnSessionConfigEntry 2 }

ancpAnSessionConfigGsmpVersion OBJECT-TYPE
SYNTAX GsmpVersion
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The maximum version number of the GSMP protocol that
may be used in this session. The value of this object
is persistent."
DEFVAL { 3 }
::= { ancpAnSessionConfigEntry 3 }

ancpAnSessionConfigGsmpSubVersion OBJECT-TYPE
SYNTAX GsmpSubVersion
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The maximum subversion number of the GSMP protocol that
may be used in this session. The value of this object
is persistent."
DEFVAL { 1 }


```plaintext
::= { ancpAnSessionConfigEntry 4 }

ancpAnSessionConfigEncapsulationType OBJECT-TYPE
SYNTAX INTEGER {
    tcp(1)
} MAX-ACCESS read-create
STATUS current
DESCRIPTION "Required encapsulation for this session. The value of
this object is persistent."
DEFVAL { tcp }
::= { ancpAnSessionConfigEntry 5 }

ancpAnSessionConfigCapabilities OBJECT-TYPE
SYNTAX AncpAnSessionCapabilities
MAX-ACCESS read-create
STATUS current
DESCRIPTION "ANCP capabilities supported by the AN in this session.
When all bits are set to zero then this means that no
capabilities are supported. The value of this object
is persistent."
DEFVAL { { topologyDiscovery, l2Oam } }
::= { ancpAnSessionConfigEntry 6 }

ancpAnSessionConfigAliveTimer OBJECT-TYPE
SYNTAX Unsigned32(1..255)
UNITS "deciseconds"
MAX-ACCESS read-create
STATUS current
DESCRIPTION "The timer specifies the nominal time between periodic
adjacency protocol messages generated by the access node.
It is a constant for the duration of an ANCP session. The
timer is specified in units of 100ms. The value of this
object is persistent."
DEFVAL { 100 }
::= { ancpAnSessionConfigEntry 7 }

ancpAnSessionConfigPortReportShaper OBJECT-TYPE
SYNTAX Unsigned32(1..255)
UNITS "deciseconds"
MAX-ACCESS read-create
STATUS current
DESCRIPTION "The timer specifies the nominal time between
2 EventReport messages related to the same port.
```
It is a constant for the duration of a GSMP session. The timer is specified in units of 100ms. The value of this object is persistent.

DEFVAL { 10 }
 ::= { ancpAnSessionConfigEntry 8 }

ancpAnSessionConfigAggregateReportShaper OBJECT-TYPE
SYNTAX     Unsigned32(1..2550)
UNITS      "centiseconds"
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The timer specifies the nominal time between 2 EventReport messages related to any port. It is a constant for the duration of a GSMP session. The timer is specified in units of 10ms. The value of this object is persistent."
DEFVAL { 10 }
 ::= { ancpAnSessionConfigEntry 9 }

ancpAnSessionConfigTransportRetryTimer OBJECT-TYPE
SYNTAX     Unsigned32(0..255)
UNITS      "deciseconds"
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The timer specifies the nominal time between 2 transport connection setup attempts done by the access node. The transport protocol is specified in ancpAnSessionConfigEncapsulationType. The timer is specified in units of 100ms. A value 0 means that the access node will NOT initiate nor setup the transport connection. The value of this object is persistent."
DEFVAL { 10 }
 ::= { ancpAnSessionConfigEntry 10 }

ancpAnSessionConfigAncpRetryTimer OBJECT-TYPE
SYNTAX     Unsigned32(0..255)
UNITS      "deciseconds"
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The timer specifies the nominal time between 2 ANCP connection setup attempts. The timer is specified in units of 100ms. A value 0 means that the access node will NOT spontaneously trigger an ANCP session."
Whatever the setting of this timer, the access node shall always listen for ANCP session setup. The value of this object is persistent.

DEFVAL { 10 }
::= { ancpAnSessionConfigEntry 11 }

ancpAnSessionConfigAnName OBJECT-TYPE
SYNTAX     GsmpNameType
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The name of the access node. The first three octets must be an Organizationally Unique Identifier (OU1) that identifies the manufacturer of the access node. This can be (one of) the MAC address(es) of the access node on the network side.
When set to zero, the access node shall autonomously decide on using the most appropriate MAC address of the access node. Then the actually used access node name can be read from ancpAnCurrentSessionAnName.
The value of this object is persistent."
DEFVAL { '000000000000'H }
::= { ancpAnSessionConfigEntry 12 }

ancpAnSessionConfigPartitionId OBJECT-TYPE
SYNTAX     GsmpPartitionIdType
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The Id for this session’s specific access node partition. This object has a meaning only if partitions are used (ancpAnPartitionsUsed='true’) and is ignored otherwise.
The value of this object is persistent."
DEFVAL { '00'H }
::= { ancpAnSessionConfigEntry 13 }

ancpAnSessionConfigWindowSize OBJECT-TYPE
SYNTAX     Unsigned32(1..65535)
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The maximum number of unacknowledged request messages that may be transmitted by the controller without the possibility of loss. This field is used to prevent request messages from being lost in the access node because of overflow in the receive buffer. The field is a hint to the controller. The value of this object is
ancpAnSessionConfigNasIpAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The type of address in ancpAnSessionConfigNasIpAddress.
The value of this object is persistent."
::= { ancpAnSessionConfigEntry 14 }

ancpAnSessionConfigNasIpAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The IP address used for the ANCP session peer (NAS).
The type of this IP address attribute is determined
by the value of ancpAnSessionConfigNasIpAddressType.
The value of this object is persistent."
::= { ancpAnSessionConfigEntry 15 }

ancpAnSessionConfigEncapPortNumber OBJECT-TYPE
SYNTAX InetPortNumber (1..65535)
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The port number used for the transport protocol
establishment to the ANCP peer. The transport
protocol type is specified by ancpAnSessionConfigEncapsulationType and as
it is set by default to 'tcp' then the default
port number is set to 6068 (see details in
http://www.iana.org/). Other port numbers may
be relevant if other transport protocols are used.
The value of this object is persistent."
DEFVAL { 6068 }
::= { ancpAnSessionConfigEntry 16 }

ancpAnSessionConfigNotifyDnEnable OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies if ancpAnSessionDown
notification should be generated when this session
leaves the ‘estab’ state as given by
ancpAnCurrentSessionState in the corresponding row
in ancpAnCurrentSessionTable.
The value of this object is persistent."
DEFVAL { false }
::= { ancpAnSessionConfigEntry 18 }

ancpAnSessionConfigNotifyUpEnable OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies if ancpAnSessionUp
notification should be generated when this session
goes to ‘estab’ state as given by
ancpAnCurrentSessionState in the corresponding row
in ancpAnCurrentSessionTable.
The value of this object is persistent."
DEFVAL { false }
::= { ancpAnSessionConfigEntry 19 }

--
-- Operational Information of ANCP Sessions
--

ancpAnCurrentSessionTable OBJECT-TYPE
SYNTAX SEQUENCE OF AncpAnCurrentSessionEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This table gives actual information of the sessions
in the access node.
A row in this table is created when the corresponding row
in the ancpAnSessionConfigTable is created.
A row in this table is deleted when the corresponding row
in the ancpAnSessionConfigTable is deleted."
::= { ancpAnObjects 4 }

ancpAnCurrentSessionEntry OBJECT-TYPE
SYNTAX AncpAnCurrentSessionEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry in the table showing the data for a
specific actual session."
INDEX { ancpAnSessionConfigSessionId }
::= { ancpAnCurrentSessionTable 1 }
AncpAnCurrentSessionEntry ::= SEQUENCE {
    ancpAnCurrentSessionState              INTEGER,
    ancpAnCurrentSessionGsmpVersion        GsmpVersion,
    ancpAnCurrentSessionGsmpSubVersion     GsmpSubVersion,
    ancpAnCurrentSessionAnName             GsmpNameType,
    ancpAnCurrentSessionNasName            GsmpNameType,
    ancpAnCurrentSessionAnIpAddressType    InetAddressType,
    ancpAnCurrentSessionAnIpAddress        InetAddress,
    ancpAnCurrentSessionAnInstance         Unsigned32,
    ancpAnCurrentSessionNasInstance        Unsigned32,
    ancpAnCurrentSessionCapabilities       AncpAnSessionCapabilities,
    ancpAnCurrentSessionStartUptime        TimeTicks,
    ancpAnCurrentSessionDiscontinuityTime  TimeTicks,
    ancpAnCurrentSessionStatSentMessages   ZeroBasedCounter32,
    ancpAnCurrentSessionStatReceivedValidMessages ZeroBasedCounter32,
    ancpAnCurrentSessionStatDiscardedMessages     ZeroBasedCounter32
}

ancpAnCurrentSessionState OBJECT-TYPE
SYNTAX  INTEGER {
    null(1),
    synsent(2),
    synrcvd(3),
    estab(4)
}
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The state of this session. The null (1) state is returned if the proper encapsulation data is not yet configured, if the row is not in active status or if the session is in NULL state as defined in the GSMP specification."
::= { ancpAnCurrentSessionEntry 1 }

ancpAnCurrentSessionGsmpVersion OBJECT-TYPE
SYNTAX  GsmpVersion
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The actual version number of the GSMP protocol that is used in this session. This object has value 0 if ancpAnCurrentSessionState is not estab(4)."
::= { ancpAnCurrentSessionEntry 2 }

ancpAnCurrentSessionGsmpSubVersion OBJECT-TYPE
SYNTAX  GsmpSubVersion
ancpAnCurrentSessionAnName OBJECT-TYPE
SYNTAX      GsmpNameType
MAX-ACCESS read-only
STATUS      current
DESCRIPTION
  "The name of the access node used in this session.
   It should be the same as ancpAnSessionConfigAnName if that
   object is not set to zero. If ancpAnSessionConfigAnName
   is set to zero, then this object will contain the MAC
   address selected by the access node as described in the
   description of ancpAnSessionConfigAnName.
   The value of this object is used as value for the
   'Sender Name' field in the header of the ANCP messages
   generated for this session by the AN."
 ::= { ancpAnCurrentSessionEntry 4 }

ancpAnCurrentSessionNasName OBJECT-TYPE
SYNTAX      GsmpNameType
MAX-ACCESS read-only
STATUS      current
DESCRIPTION
  "The name of the NAS as advertised in the adjacency
  message.
  The value of this object is set to the value of the
  'Sender Name' field in the header of the ANCP messages
  received on this session. This object has value 0 if
  ancpAnCurrentSessionState is not estab(4)."
 ::= { ancpAnCurrentSessionEntry 5 }

ancpAnCurrentSessionAnIpAddressType OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS read-only
STATUS      current
DESCRIPTION
  "The type of address in ancpAnCurrentSessionAnIpAddress."
 ::= { ancpAnCurrentSessionEntry 6 }

ancpAnCurrentSessionAnIpAddress OBJECT-TYPE
SYNTAX      InetAddress

MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The IP address used for the access node.
The type of this IP address attribute is determined
by the value of ancpAnCurrentSessionAnIpAddressType."
::= { ancpAnCurrentSessionEntry 7 }

ancpAnCurrentSessionAnInstance OBJECT-TYPE
SYNTAX Unsigned32(0..16777215)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The instance number used by the access node during this
session. The Instance number is a 24-bit number
that should be guaranteed to be unique within
the recent past and to change when the link
or node comes back up after going down. Zero is
not a valid instance number.
This object has value 0 if ancpAnCurrentSessionState is
not estab(4)."
::= { ancpAnCurrentSessionEntry 8 }

ancpAnCurrentSessionNasInstance OBJECT-TYPE
SYNTAX Unsigned32(0..16777215)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The instance number used by the NAS during this
session. The Instance number is a 24-bit number
that should be guaranteed to be unique within
the recent past and to change when the link
or node comes back up after going down.
This object has value 0 if ancpAnCurrentSessionState is
not estab(4)."
::= { ancpAnCurrentSessionEntry 9 }

ancpAnCurrentSessionCapabilities OBJECT-TYPE
SYNTAX AncpAnSessionCapabilities
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The common ANCP capabilities supported by the AN and
NAS in this session.
The object has the value 0 if no capabilities are
supported
or if ancpAnCurrentSessionState is not estab(4)."
::= { ancpAnCurrentSessionEntry 10 }
ancpAnCurrentSessionStartUptime OBJECT-TYPE
SYNTAX     TimeTicks
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The value of sysUpTime when the session came to
established state.
This object has value 0 if ancpAnCurrentSessionState is
not estab(4)."
::= { ancpAnCurrentSessionEntry 11 }

ancpAnCurrentSessionDiscontinuityTime OBJECT-TYPE
SYNTAX     TimeTicks
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The value of sysUpTime on the most recent occasion at
which session’s counters suffered a discontinuity.
If no such discontinuities have occurred since then,
this object contains the same value as
ancpAnCurrentSessionStartUptime."
::= { ancpAnCurrentSessionEntry 12 }

ancpAnCurrentSessionStatSentMessages OBJECT-TYPE
SYNTAX     ZeroBasedCounter32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of messages that have been sent in this session
by the access node.
All ANCP messages pertaining to this session after
the session came to established state shall
be counted, also including adjacency protocol messages
and failure response messages.
Discontinuities of this counter are indicated by
ancpAnCurrentSessionDiscontinuityTime."
::= { ancpAnCurrentSessionEntry 13 }

ancpAnCurrentSessionStatReceivedValidMessages OBJECT-TYPE
SYNTAX     ZeroBasedCounter32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of messages that have been received and
processed in this session by the access node.
All ANCP messages pertaining to this session after
the session came to established state shall
be counted, also including adjacency protocol messages
Discontinuities of this counter are indicated by ancpAnCurrentSessionDiscontinuityTime.

::= { ancpAnCurrentSessionEntry 14 }

ancpAnCurrentSessionStatDiscardedMessages OBJECT-TYPE
SYNTAX     ZeroBasedCounter32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of messages that in this session have been received and discarded for whatever reason by the access node. All ANCP messages pertaining to this session after the session came to established state shall be counted, also including adjacency protocol messages and failure response messages. Discontinuities of this counter are indicated by ancpAnCurrentSessionDiscontinuityTime."

::= { ancpAnCurrentSessionEntry 15 }

--
-- Partitions
--

ancpAnInterfaceConfigTable OBJECT-TYPE
SYNTAX SEQUENCE OF AncpAnInterfaceConfigEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"This table configures the association of user facing interfaces to ANCP partitions in the access node. An entry in this table needs to be added by the agent for each relevant user facing interface with the value of ancpAnInterfaceConfigPartitionId set to zero at the time of the creation of the row. A relevant user facing interface is created whenever a row is created in the ifTable of the IF-MIB that can be controlled by ANCP. When such an interface is deleted from the ifTable, the corresponding row in this table has to be removed by the agent. Rows should only be created by the agent when ancpAnPartitionsUsed is set to ‘true’. If no partitions are used, then no rows should be created in this table."

::= { ancpAnObjects 5 }

ancpAnInterfaceConfigEntry OBJECT-TYPE
SYNTAX AncpAnInterfaceConfigEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "An entry in the table showing the partition id for a
specific user facing interface"
INDEX { ifIndex }
 ::= { ancpAnInterfaceConfigTable 1 }

AncpAnInterfaceConfigEntry ::= SEQUENCE {
   ancpAnInterfaceConfigPartitionId GsmpPartitionIdType
}

ancpAnInterfaceConfigPartitionId OBJECT-TYPE
SYNTAX GsmpPartitionIdType
MAX-ACCESS read-write
STATUS current
DESCRIPTION "A partition Id associated with the related ifIndex.
Upon creation of the row, the value is set to '00' H.
The value of this object is persistent."
DEFVAL { '00' H }
 ::= { ancpAnInterfaceConfigEntry 1 }

--
-- Notifications
--

ancpAnSessionDown NOTIFICATION-TYPE
OBJECTS {
   ancpAnCurrentSessionAnIpAddressType,
   ancpAnCurrentSessionAnIpAddress,
   ancpAnSessionConfigNasIpAddressType,
   ancpAnSessionConfigNasIpAddress,
   ancpAnCurrentSessionAnInstance,
   ancpAnCurrentSessionNasInstance,
   ancpAnCurrentSessionStartUptime,
   ancpAnCurrentSessionStatSentMessages,
   ancpAnCurrentSessionStatReceivedValidMessages,
   ancpAnCurrentSessionStatDiscardedMessages
}
STATUS current
DESCRIPTION "This notification is generated whenever an ANCP session
goes down. A session can go down for several reasons:
1) The ANCP session can be deleted by a manager from the
ancpAnSessionConfigTable, and hence it will also be
removed from the ancpAnCurrentSessionTable."
2) The session can go operational down due to some malfunction in the network, the AN, or the NAS. In this case, the ANCP session will be still in the ancpAnSessionConfigTable and ancpAnCurrentSessionTable, but the ancpAnCurrentSessionState moves from the estab state to another state.

::= { ancpAnNotifications 1 }

ancpAnSessionUp NOTIFICATION-TYPE
OBJECTS {
  ancpAnCurrentSessionAnInstance
}
STATUS current
DESCRIPTION
"This notification is generated when an ANCP session enters the estab state as given by ancpAnCurrentSessionState. Since ancpAnCurrentSessionAnInstance identifies the ANCP session uniquely the other attributes can be derived from this attribute."

::= { ancpAnNotifications 2 }

-- ANCP AN Compliance

ancpAnGroups OBJECT IDENTIFIER ::= { ancpAnConformance 1 }
ancpAnCompliances OBJECT IDENTIFIER ::= { ancpAnConformance 2 }

ancpAnModuleCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The compliance statement for agents that support the ANCP MIB module for access nodes."
MODULE -- this module
MANDATORY-GROUPS {
  ancpAnConfigGroup,
  ancpAnCurrentGroup,
  ancpAnInterfaceGroup,
  ancpAnNotificationsGroup
}
::= { ancpAnCompliances 1 }

-- units of conformance

ancpAnConfigGroup OBJECT-GROUP
OBJECTS {
  ancpAnNextSessionId,
  ancpAnSessionConfigRowStatus,
ancpAnSessionConfigGsmpVersion,
ancpAnSessionConfigGsmpSubVersion,
ancpAnSessionConfigEncapsulationType,
ancpAnSessionConfigCapabilities,
ancpAnSessionConfigAliveTimer,
ancpAnSessionConfigPortReportShaper,
ancpAnSessionConfigAggregateReportShaper,
ancpAnSessionConfigTransportRetryTimer,
ancpAnSessionConfigAncpRetryTimer,
ancpAnSessionConfigAnName,
ancpAnSessionConfigPartitionId,
ancpAnSessionConfigWindowSize,
ancpAnSessionConfigNasIpAddressType,
ancpAnSessionConfigNasIpAddress,
ancpAnSessionConfigEncapPortNumber
}
STATUS current
DESCRIPTION
"These objects apply to the configuration of ANCP
sessions in access nodes."
::= { ancpAnGroups 1 }

ancpAnCurrentGroup OBJECT-GROUP
OBJECTS {
   ancpAnCurrentSessionState,
   ancpAnCurrentSessionGsmpVersion,
   ancpAnCurrentSessionGsmpSubVersion,
   ancpAnCurrentSessionAnName,
   ancpAnCurrentSessionNasName,
   ancpAnCurrentSessionAnIpAddressType,
   ancpAnCurrentSessionAnIpAddress,
   ancpAnCurrentSessionAnInstance,
   ancpAnCurrentSessionNasInstance,
   ancpAnCurrentSessionCapabilities,
   ancpAnCurrentSessionStartUptime,
   ancpAnCurrentSessionDiscontinuityTime,
   ancpAnCurrentSessionStatSentMessages,
   ancpAnCurrentSessionStatReceivedValidMessages,
   ancpAnCurrentSessionStatDiscardedMessages,
   ancpAnSessionConfigNotifyDnEnable,
   ancpAnSessionConfigNotifyUpEnable
}
STATUS current
DESCRIPTION
"These objects show the operational state of all ANCP
sessions configured in the access node."
::= { ancpAnGroups 2 }
ancpAnInterfaceGroup OBJECT-GROUP

OBJECTS {
    ancpAnPartitionsUsed,
    ancpAnInterfaceConfigPartitionId
}

STATUS current

DESCRIPTION
"These objects are used to assign user facing interface to partitions."

::= { ancpAnGroups 3 }

ancpAnNotificationsGroup NOTIFICATION-GROUP

NOTIFICATIONS {
    ancpAnSessionDown,
    ancpAnSessionUp
}

STATUS current

DESCRIPTION
"These notifications inform management stations about changes in the state of ANCP sessions."

::= { ancpAnGroups 4 }

END

7. Security Considerations

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/vulnerability:

- ancpAnPartitionsUsed
  
  This scalar object supports SET operations. Unauthorized changes to this object could result in a wrong interpretation of ancpAnSessionConfigPartitionId attribute of all sessions, as if all sessions use partition id zero, or to actually disabling the use of partitions in the system.

- ancpAnSessionConfigTable

  The table consists of the following objects that support SET operations:
Unauthorized changes to ancpAnSessionConfigRowStatus could result in session being created or brought into service prematurely; or could result in session being inadvertently deleted or taken out of service.

Unauthorized changes to ancpAnSessionConfigGsmpVersion or ancpAnSessionConfigGsmpSubVersion could have an adverse operational effect by limiting the GSMP version to be used in the context of this session or enabling a GSMP version number that is actually unsupported by the access node.

Unauthorized changes to ancpAnSessionConfigEncapsulationType could have an adverse operational effect by configuring the session to use an undesired or even unsupported protocol.

Unauthorized changes to ancpAnSessionConfigCapabilities could have an adverse operational effect by disabling certain ANCP capabilities that the operator assumed that are enabled, or enable a capability that the operator would not like to activate.

Unauthorized changes to ancpAnSessionConfigAliveTimer could have an adverse operational effect by increasing the frequency of adjacency protocol messages generated by the access node and leading to an overload of such messages. Decreasing the frequency of such messages may harm the synchronization between the access node and the NAS.

Unauthorized changes to ancpAnSessionConfigPortReportShaper or ancpAnSessionConfigAggregateReportShaper could have an adverse
operational effect by increasing the frequency of Event Report messages generated by the access node and leading to an overload of such messages. Decreasing the frequency of such messages may delay the responsiveness of the system to events associated with one or more ports.

Unauthorized changes to ancpAnSessionConfigTransportRetryTimer could have an adverse operational effect by increasing the frequency of transport connection setup attempts initiated by the access node or even unexpectedly enabling the access node to initiate the transport connection setup when that supposed to be disabled. Alternatively, when the operator basically planned transport connection setup attempts by the access node unauthorized changes to the attribute may cause unexpected low frequency of such attempts or unexpectedly disable those attempts.

Unauthorized changes to ancpAnSessionConfigAncpRetryTimer could have an adverse operational effect by increasing the frequency of ANCP connection setup attempts initiated by the access node or even unexpectedly enabling the access node to initiate the ANCP connection setup when that supposed to be disabled. Alternatively, when the operator basically planned ANCP connection setup attempts by the access node unauthorized changes to the attribute may cause unexpected low frequency of such attempts or unexpectedly disable those attempts.

Unauthorized changes to ancpAnSessionConfigAnName could confuse the NAS, e.g., by detecting the same name from multiple access nodes. This may also override the operator’s will to allow/avoid the access node to autonomously determine its name.

Unauthorized changes to ancpAnSessionConfigPartitionId could mean that partitions are used when actually they are not, or vice versa. It could also at least specify a different partition ID than the one actually associated with the session.

Unauthorized changes to ancpAnSessionConfigWindowSize are not directly harmful. However, if the controller adopts the suggested wrong window size it may either cause the controller to send too many messages in a window or unnecessarily limit itself and that could reduce the system performance.

Unauthorized changes to ancpAnSessionConfigNasIpAddressType and/or ancpAnSessionConfigNasIpAddress and/or ancpAnSessionConfigEncapPortNumber could produce a wrong address type (interpretation) and/or IP address for the NAS and/or specify a wrong transport protocol port number for the session, respectively.
Unauthorized changes to ancpAnSessionConfigNotifyDnEnable could lead (if the change was setting the attribute to ‘enable’) to overload of notification messages at the SNMP manager in case multiple sessions leave the ‘estab’ state simultaneously. If the change was setting the attribute to ‘disable’ it could lead to hiding the actual session state from the SNMP manager.

Unauthorized changes to ancpAnSessionConfigNotifyUpEnable could lead (if the change was setting the attribute to ‘enable’) to overload of notification messages at the SNMP manager in case multiple sessions enter the ‘estab’ state simultaneously. If the change was setting the attribute to ‘disable’ it could lead to hiding the actual session state from the SNMP manager.

- ancpAnInterfaceConfigTable

The table consists of the following objects that support SET operations:

* ancpAnInterfaceConfigPartitionId

Unauthorized changes to ancpAnInterfaceConfigPartitionId could result in a wrong association between the interface and a partition. It could result in not being able to manage the interface from the correct session and/or to exposing the interface to a wrong NAS.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. This is the table and these are the objects and their sensitivity/vulnerability:

- ancpAnCurrentSessionTable

Access to these objects would allow an intruder to obtain information about which vendor’s equipment is in use on the network. Further, such information is considered sensitive in many environments for competitive reasons.

* ancpAnCurrentSessionState
* ancpAnCurrentSessionGsmpVersion
* ancpAnCurrentSessionGsmpSubVersion
SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], Section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

8. IANA considerations

IANA is requested to assign an OID xxx under mib-2.

9. Acknowledgements

The authors would like to thank Paul Reynders and Bert Wijnen for their feedback.

10. References
10.1. Normative References


10.2. Informative References


Authors' Addresses

Stefaan De Cnodder
Alcatel-Lucent
Copernicuslaan 50
B-2018 Antwerp
Belgium

Phone: +32 3 240 85 15
Email: stefaan.de_cnodder@alcatel-lucent.be

Moti Morgenstern
ECI Telecom Ltd.
30 Hasivim St.
Petach Tikva 49517
Israel

Phone: +972 3 926 6258
Fax: +972 3 928 7342
Email: moti.Morgenstern@ecitele.com
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).