Network Working Group
INTERNET DRAFT
<draft-syam-ipv6-state-model-00.txt>
Expires: April 2004
Category:Informational

S. Madanaplli
S. Kumar
O.L.N. Rao
S. Park
SAMSUNG

October 2003

State Model for IPv6 Interfaces

Status of this Memo

Abstract

This document specifies a generic flexible state model for IPv6 Interfaces.

Table of Contents

1. Introduction

This document defines a state model for IPv6 Interfaces. This state model facilitates the administrator to know the current status of the IPv6 interface at any instant and provides information about what actions the administrator may need to take to bring the interface UP, if it is currently unavailable for performing the provisioned services.

Any entity in any layered architecture can be DOWN (non-functional) because of the following three reasons:

- The management (administrator) explicitly prevented in performing the assigned services.
- The lower layer is not providing its assigned services.
- There is an internal fault in the entity itself.

At any instant, there can be multiple reasons (the combination of the above) because of which the entity may be non-functional. This document captures all the states an IPv6 interface may under go because of the above mentioned reasons.

The State Model defined in this document is flexible in the sense that one can define their own reasons/fault conditions for the IPv6 interfaces depending on their needs.

The State Model described here is based on the Control State Machine that has been implemented in Samsung's IPv6 Protocol Stack.

2. Terminology

Primary State (PST)

Indicates the current overall service condition of an entity.

Primary State Qualifier (PSTQ)

This gives further information about why the entity is in a particular PST.

Secondary State (SST)

Provides additional information relevant to state management.

3. State Model

The State of an entity consists of Operational State and Administrative State. The Operational State indicates whether the entity is capable of providing its provisioned functions. The Administrative State indicates whether it is administratively inhibited from providing its provisioned functions. The Primary State provides the overall service condition of the entity which will be qualified by the Primary State Qualifier. The secondary State and its Qualifiers provide further information why the entity is not able to provide its assigned services.

3.1. Interface States

3.1.1. Primary State

Primary State indicates the overall service condition of the entity, whether it is UP (In-Service), or DOWN (Out-of-Service).

UP
The entity is partially or fully operable to provide some or all of its assigned services to the users. The entity is operationally capable and at the same time administratively allowed to provide its services. That is, both the operational and administrative states are UP.

DOWN
The entity is totally inoperable and unable to provide any of its assigned services to the users. The PSTQ value will qualify the unavailability of the entity. For example, whether it is operationally incapable or administratively inhibited from providing its services.

3.1.2. Primary State Qualifier

The following values of PSTQ qualify the PST value DOWN.

AU (Autonomous)
Operational State is DOWN.

MA (Management)
Administrative State is DOWN.

AUMA (Autonomous-and-Management)
Both Operational and Administrative States are DOWN.

Autonomous (AU)

The entity is incapable of providing any of its services, and there is no external administrative restriction inhibiting the entity from providing these services. In general, the cause of incapability is an unsolicited event occurrence on the Interface. Examples of such events include, but not limited to a defect developed in the entity, its Lower Layer (Supporting Entity) is DOWN or the Interface ID is duplicate incase of IPv6 Interface etc.

Management (MA)

The entity is intentionally suspended by the external management command from providing all of its services. In this state the entity itself is still operationally capable of, even though it is currently being suspended from providing service. While resident in this state, updates of providing service, data, and testing and maintenance activities are permitted. Fault detection

shall be continued in this state, however no reports will be generated to the management.

AUMA (Autonomous-and-Management)

The entity is incapable of providing services, and at the same time it has been intentionally suspended from providing all of its services. While resident in this state, updates of provisioning data and Testing and maintenance activities are permitted. Fault detection shall be continued to determine if an operational problem has been corrected or an additional operational problem has occurred.

3.1.3. Secondary State

The following are the SST values that a stack entity can have:

UAS (Unassigned)
The IPv6 interface has not been assigned with the necessary provisioning data. That is the IPv6 Interface does not exist. No SSTQs have been defined for this SST.

LLD (Lower Layer Down)
The associated lower layer entity (Layer 2) is DOWN. No SSTQs have been defined for this SST.

LLD (Lower Layer Association Down)
The associated lower layer entity (Layer 2) Association is DOWN. No SSTQs have been defined for this SST.

FLT (Internal Fault)
The stack entity itself has got some fault that inhibited it from providing services. NORS and DIID have been defined as SSTQs for this SST.

3.1.4. Secondary State Qualifier

Currently the following SSTQs have been defined. Implementers can define their own SSTQs based on their requirements.

NORS
Stack entity is out of resources.

DIID
The interface identifier is Duplicate.

3.2. Events

3.2.1. Management Events

ADMIN-LOCK
Management inhibited the interface from providing services.

ADMIN_UNLOCK
Management permitted interface to provide services.

CREATE
Create an IPv6 Interface.

DELETE
Remove an IPv6 Interface.

3.2.2. Lower Layer Events

LLD
The Lower Layer is DOWN.

LLU
The Lower Layer is UP.

LLAD
The Lower Layer Association is DOWN.

LLAU
The Lower Layer Association is UP.

3.2.3. Autonomous Events

RESOURCE REQUEST FAILED
The request for a particular of resource that is required for the interface to be functional is FAILED.

DAD FAILED
Duplicate IID Detection FAILED.

DAD FAIL RECOVER
Duplicate IID Detection for the new IID is SUCCEEDED after Management intervention or by some other mechanism.

3.3. Dependencies among states

The following are the possible combination of Operational and Administrative State values.

DOWN and Locked (DOWN, AUMA)
The resource is totally inoperable, and it is also administratively prohibited from providing service. To make it available for use, both management permission (an unlock operation) and some corrective action are necessary.

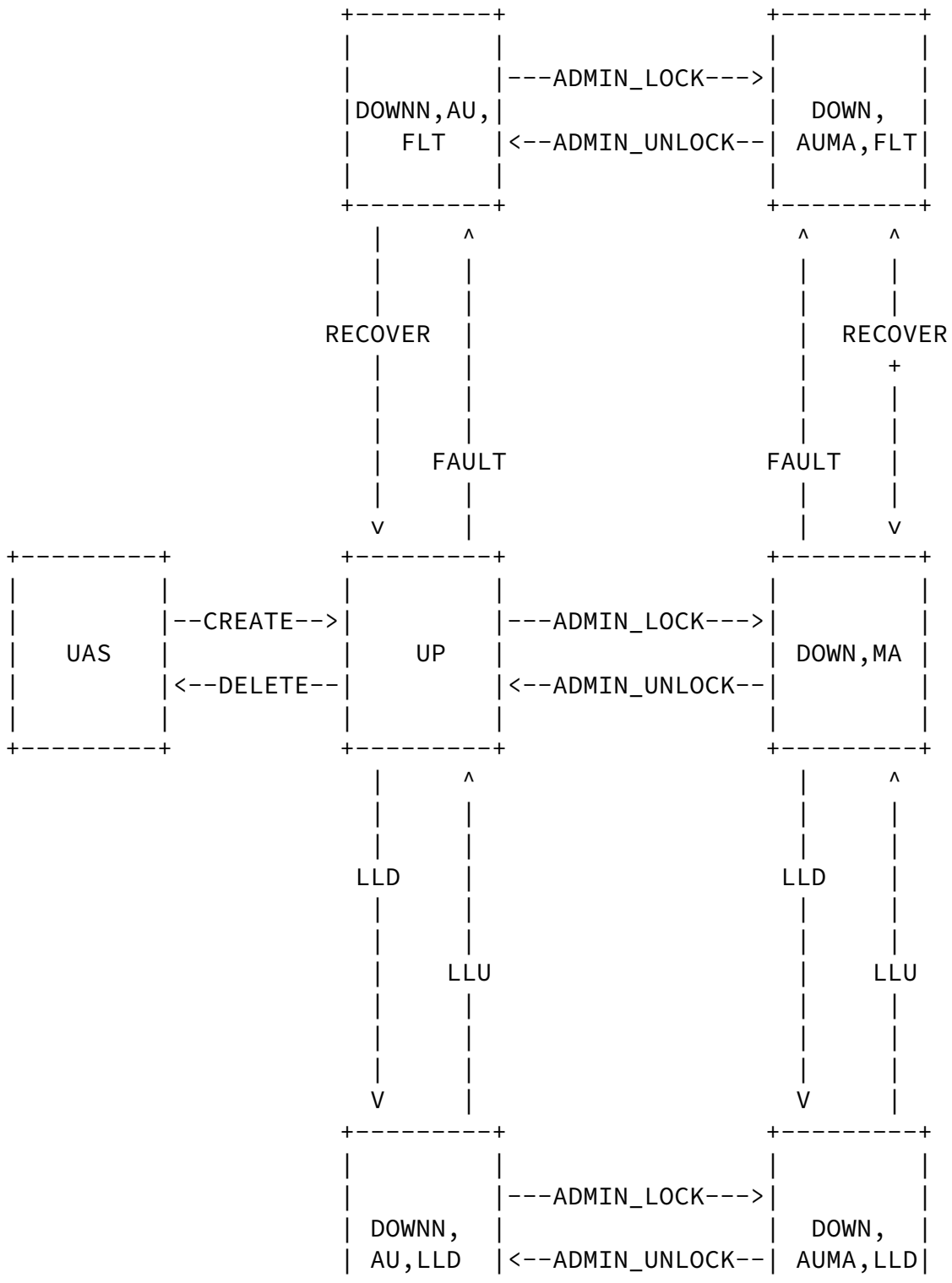
UP and Locked (DOWN, MA)
The resource is partially or fully operable, but is administratively prohibited from providing service. To make it available for use, only management permission (an unlock operation) is required.

DOWN and Unlocked (DOWN, AU)
The resource is totally inoperable, but it is not administratively prohibited from providing service. To make it available for use, some corrective action is required.

UP and Unlocked (UP)
The resource is partially or fully operable, and is not administratively prohibited from providing service.

3.4. State Transition Diagram

The following is the simplified view of the state machine for IPv6 Interfaces. The diagram does not take care of all possible state transitions from different states.



3.5. State Transition Table

Current State	Event	Next State	Actions to be taken
UAS	CREATE	UP	Create Interface and Make it UP
UP	ADMIN_LOCK	DOWN,MA	Set Admin Flag
UP	LLD	DOWN,AU,LLD	Clear Lower Layer flag
UP	LLAD	DOWN,AU,LLAD	Clear Association flag
UP	FAULT	DOWN,AU,FLT	Set Fault flag
DOWN,MA	ADMIN_UNLOCK	UP	Clear Admin Flag
DOWN,MA	LLD	DOWN,AUMA,LLD	Clear Lower Layer flag
DOWN,MA	LLAD	DOWN,AUMA,LLAD	Clear Association flag
DOWN,MA	FAULT	DOWN,AUMA,FLT	Set Fault flag
DOWN,AU,LLD	ADMIN_LOCK	DOWN,AUMA,LLD	Set Admin Flag
DOWN,AU,LLD	LLU	UP	Set Lower Layer Flag
DOWN,AUMA,LLD	ADMIN_UNLOCK	DOWN,AU,LLD	Clear Admin Flag
DOWN,AUMA,LLD	LLU	DOWN,MA	Set Lower Layer Flag
DOWN,AU,LLAD	ADMIN_LOCK	DOWN,AUMA,LLAD	Set Admin Flag
DOWN,AU,LLAD	LLAU	UP	Set Association Flag
DOWN,AUMA,LLAD	ADMIN_UNLOCK	DOWN,AU,LLAD	Clear Admin Flag

DOWN,AUMA,LLAD	LLAU	DOWN,MA	Set Association Flag
DOWN,AU,FLT	ADMIN_LOCK	DOWN,AUMA,FLT	Set Admin Flag
DOWN,AU,FLT	RECOVER(LLU)	UP	Set Lower Layer Flag
DOWN,AU,FLT	RECOVER(LLD)	DOWN,AU,LLD	Clear Lower Layer Flag

DOWN,AU,FLT	RECOVER(LLAU)	UP	Set Lower Layer Flag
DOWN,AU,FLT	RECOVER(LLAD)	DOWN,AU,LLAD	Clear Association Flag
DOWN,AUMA,FLT	ADMIN_UNLOCK	DOWN,AU,FLT	Clear Admin Flag
DOWN,AUMA,FLT	RECOVER(LLU)	DOWN,MA	Set Lower Layer Flag
DOWN,AUMA,FLT	RECOVER(LLD)	DOWN,AUMA,LLD	Clear Lower Layer Flag
DOWN,AUMA,FLT	RECOVER(LLAU)	DOWN,MA	Set Lower Layer Flag
DOWN,AUMA,FLT	RECOVER(LLAD)	DOWN,AUMA,LLAD	Clear Association Flag
<AnyState>	DELETE	UAS	Lock and then Shutdown the Interface

4. Security Considerations

CREATE/DELETE and ADMIN_LOCK/ADMIN_UNLOCK operations on an IPv6 Interface may be considered sensitive or vulnerable in some network environments. The support for such operations in a non-secure environment without proper protection can have a negative effect on network operations.

SNMPv1 by itself is not a secure environment. 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 state attributes defined in this document.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework when giving access to remote entity using SNMP. Specifically, the use of the User-based Security Model RFC 2574 and the View-based Access Control Model RFC 2575 is recommended.

It is then a customer/user responsibility to ensure that the SNMP entity giving access to the state attributes defined in this document, is properly configured to give access to the attributes only to those principals (users) that have legitimate rights to

indeed GET or SET (change/create/delete) them.

5. References

[1] Chisholm, S. and Perkins, D., "Entity State MIB", draft-ietf-entmib-state-00.txt, January 2003.

[2] McCloghrie, K. and F. Kastenholz, "The Interface Group MIB", RFC 2863, June 2000.

[3] ITU Recommendation X.731, "Information Technology - Open Systems Interconnection - System Management: State Management Function", 1992

6. Acknowledgement

The authors would like to thank Margaret Wasserman and Andy Bierman for their comments on this draft.

7. Authors' Addresses

Syam Madanapalli
Network Systems Division, SAMSUNG India Software Operations, INDIA
Phone: +91-80-51197777
Email:syam@samsung.com

O.L.N. Rao
Network Systems Division, SAMSUNG India Software Operations, INDIA
Phone: +91-80-51197777
Email:olnrao@samsung.com

Suraj Kumar
Network Systems Division, SAMSUNG India Software Operations, INDIA
Phone: +91-80-51197777
Email:suraj@samsung.com

Soohong Daniel Park

Mobile Platform Laboratory, SAMSUNG Electronics
Phone: +82-31-200-4508
Email:soohong.park@samsung.com

8. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

9. Full Copyright Statement