# Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Error Type | Location | NSI State | Impact | Recovery Actions | Comments/Open questions |
| Resources change from available to not available (topology changes) | Transport Plane | Between Reservation and Provisioning | Some reservations may be able to be provisioned. | * Find impacted reservations * Examine SLA (optional) * Reserve alternative resources within domain, if not, across domains | * How much into the future do you search for impacted reservations? * What is the settling time for the error? Is it a concern of NSI? |
| Provisioning in progress | Provisioning will fail causing a service error | * If the call has protection capabilities reserved, initiate provisioning of the protection path * If the service request calls for restoration, try to restore the path * Else, Notify the RA and children PA’s of a provisioning error   + Children PA and parent RA clear the call with appropriate error code | * Are there any expectations of “time” when provisioning is expected to be done within a certain domain? |
| Call in service | Connectivity/Call will fail | * Exercise multi-domain Protection/Restoration options if capabilities were requested and provisioned earlier. * Notify the RA and children PA’s of call in service error   + Children PA and parent RA clear the call with appropriate error code |  |
| RA becomes unavailable | Service Plane | Reservation Phase (before reservation complete) | Reservation confirmation cannot be sent to RA | * Complete reserving the local resources * Send reservation request down the service tree * Send reservation complete messages to RA. If no response after N number of tries, OR provisioning time reached, then generate error * Send cancel messages down the service tree | There is no way for the PA to verify if the entire reservation is complete. If it cannot reach the RA that made the request, it has to assume that either:   * It is disconnected from the RA and RA will find alternate resources * RA is unavailable and there is no guarantee when it will come back – so there is no point holding on to resources |
|  | Provisioning Phase (before provisioning complete) | Provisioning confirmation cannot be send to RA | * Complete provisioning the local resources * Send provisioning request down the service tree * Send provisioning complete messages to RA. If no response after N number of tries, then teardown call * Send cancel messages down the service tree | There is no way for the PA to verify if the entire provisioning is complete. If it cannot reach the RA that made the request, it has to assume that either:   * It is disconnected from the RA and RA will not be able to confirm up the service chain if the provisioning is complete * If the provisioning is “auto provisioned” – it is not clear if the RA domain provisioned their circuit. So rather than take chances of stranded resources, clear the resources for someone else. |
|  | Teardown Phase (before teardown complete) | Teardown confirmation cannot be sent to the RA | * Complete teardown of the local resources * Send teardwon request down the service tree * Send teardown complete messages to RA. If no response after N number of tries, clear state machine and call information * Release resources |  |
| PA becomes  unavailable | Service Plane | Reservation Phase | Reservation Confirmation cannot be received | * If no reservation confirmation received in a certain time (TIMEOUT) then cancel the reservation * Send cancel messages down all the service tree |  |
| Provisioning Phase |  | * If no provisioning confirmation received in a certain time (TIMEOUT) then cancel the reservation * Send cancel messages down all the service tree |  |
| Teardown Phase |  | * If no teardown confirmation received in a certain time (TIMEOUT) then release the resources and remove the state machine * Send release messages down all the service tree |  |

NSI Error Handling

Failures can occur at any state within the NSI state machine. The following sections focus mainly on failures signalled to NSI from the transport plane and service plane.

The following table summarizes the various error conditions described below:

# Transport Plane Error Handling

Failures in the transport plane can occur at anytime, however within the framework of the NSI architecture, there are two time windows in which a transport plane failure is significant;

1. The time between the service reservation phase and provisioning phase, and
2. The time between the service provisioning phase and teardown phase.

Of course, the errors only need to be handled by the NSA if the transport resource errors affect the user service.

Figure 1. Transport Plane Failure Sensitive Sections

## Error Handling of Transport Plane Between Reservation and Provisioning

When a failure in the Transport plane occurs after resources have been committed and before they are provisioned, actions need to be taken to recover from this. The action taken can depend on the characteristics of the requested service, negotiated SLA or user-profile. Below are some of the actions that can be taken:

* Abort the reservation (DEFAULT action)
  + Notify RA
  + Send cancel messages down the service tree
* Find alternative local resources aka intra-domain recovery. The alternate resources in case of intra-domain should honor the inter-domain STP’s and service parameters requested in the original service request. A better service can be provided as well.
  + If available
    - Reserve alternative local resources
    - Notify RA(?)
  + Unavailable
    - Notify RA
    - Send cancel messages down the service tree
* Find alternative global (external) resources aka inter-domain recovery. The recovery resources can span multiple domains, and construct a new path through additional domains as long as the A to Z STPs for the original user service request is honored along with the service parameters.
  + Available
    - Send cancel/create messages to NSAs in service tree (and create a new one accordingly)
    - Notify RA
  + Unavailable
    - Notify RA
    - Send cancel messages down the service tree

[seems like just waiting to see if failure is repaired is a possibility]

In case the advanced reservation start time (in-service) start time is reached during the recovery process, the negotiated SLA will be honored. For example, if the SLA instructs the call be torn down if it does not meet the start time, cancel messages will be sent down the tree.

[This raises the question of whether an alternative path might be reserved for some class of service]

## Error Handling of Transport Plane Between Provisioning and Teardown

When a failure in the Transport plane occurs while the transport resources are in use, several actions can be taken to address this. The action taken can depend on the characteristics of the requested service, negotiated SLA or user-profile. Below are some of the actions that can be taken:

* Cancel the reservation
  + Notify RA
  + Send cancel messages down the service tree
* Local protection
  + Available
    - Switch to backup
* Local restoration with alternative resources
  + Available
    - Notify RA
    - Reserve and provision
    - Notify RA that alternate path is available
* Global protection
  + Available
    - Notify RA
    - Send protection switch messages down the service tree (?)
* Global restoration with alternative resources
  + Available
    - (?)
* Unrecoverable
  + Notify RA
  + Send cancel messages down the service tree

# Service Plane Error Handling

Failures in the service plane can result in inconsistent states across the various NSAs that may lead to service disruptions until these states can be synchronized. In the event of an NSA failure, the following assumptions must hold true;

1. A failure in the service plane (i.e NSA) should not affect connections that are provisioned and active in the transport plane.
2. An NSA recovering from a failed condition cannot depend solely on it’s peer NSAs to reconstruct it’s state.
3. An NSA must be able recover the state of the local transport plane from it’s NRM(s).
4. The start of a service action should be recorded to facilitate rewind and replay if a failure occurred prior to the completion of the service action.
5. The completion of a service action should result in a persistent or stable state whereby an NSA could recover to (i.e. checkpoint).

Unlike failures in the transport plane, service plane failures that interrupt an NSA workflow (i.e. service action) can be problematic. This is especially true during the following service actions; i. Reservation, ii. Provisioning, iii. Teardown, and iv. Release .

Figure 2. Service Plane Failure Sensitive Sections

The failure of the NSA during a service action can be classified into two main categories; i. local or remote, and ii. RA or PA.

Since reliable transport is assumed for NSA interactions, failure in communication with a PA or RA can be assumed to be a remote NSA failure.

Figure 3. RA/PA Local/Remote Failures

## Error Handling During Reservation Phase

If the local PA fails during the reservation service action (i.e. TReservationStart < TFailure > TReservationCoimpleted), the time at which it recovers will dictate the subsequent actions it will execute. The main decider of recovery actions to be taken is based on whether the in-service start time can be met.

* TRecovery <= TProvisionStart + ReservationLeadTime (where ReservationLeadTime is the amount of time needed to make a reservation)
  + In-service start time is not compromised
  + Rewind and replay reservation service request
* TRecovery > TProvisionStart + ReservationLeadTime
  + In-service start time is compromised
  + Notify failure
  + Send cancel up/down service tree

## Error Handling During Provisioning Phase

If the local PA fails during the provisioning service action (i.e. TProvisioningStart < TFailure > TProvisioningCoimpleted), it would result in the in-service start time being compromised, as such, the recovery action would be to notify the failure, and send cancel messages up and down the service tree.

## Error Handling During Teardown Phase

If the local PA fails during the teardown service action (i.e. TTeardownStart < TFailure > TTeardownCoimpleted), it would not affect the service that has already been provided to the RA. As such, the recovery action in this case would be to determine the state of the transport plane from the NRM, and rewind and replay the teardown service action if applicable.

## Error Handling During Release Phase

If the local PA fails during the release service action (i.e. TReleaseStart < TFailure > TReleaseCoimpleted), it would not affect the service that has already been provided to the RA. As such, the recovery action in this case would be to and rewind and replay the release service action to clean up it’s state.