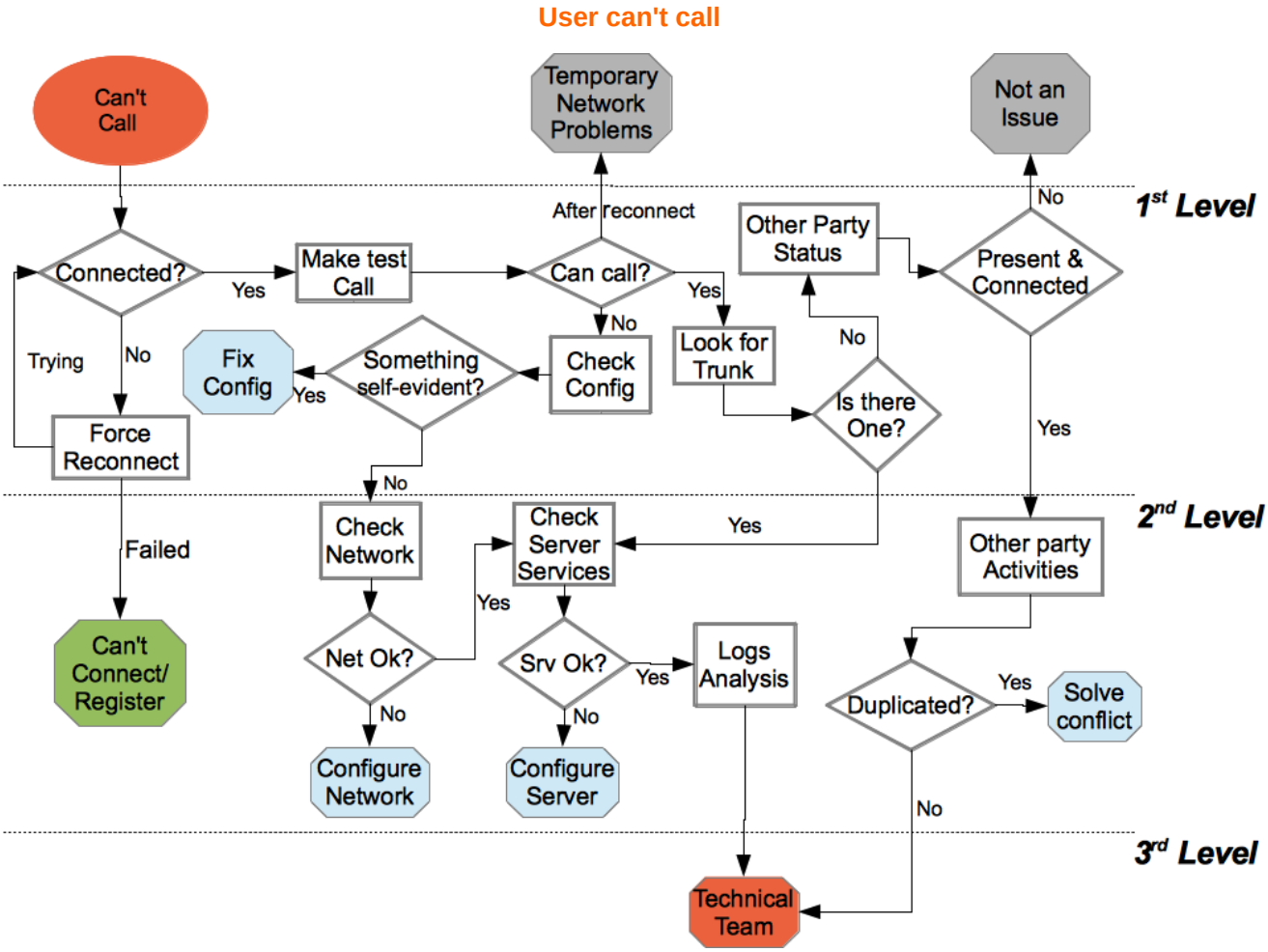
User can't call - enterprise

Introduction

This is one of the most claimed incidents to occur. This Incident troubleshooting must be confronted only if the incident definition and description hasn't pointed out any operational requirements violation. "User can't call" cause is equally divided into client/server **misconfigurations** and **connection** issues.

> Please note that this troubleshooting workflow only applies if no specific error messages are written by the PrivateGSM (e.g. License problems, user offline or doesn't exist, etc...).



First Level

We check the connection on the PrivateGSM side is fine: check the connection status declared by the application. After we record the connection status, we perform a App - Force Manual Reconnection to make sure that the connection action is correctly triggered and thus we can collect answer by the client. If the connection has some problem, then we move to the Connection Issues troubleshooting. If the connection proceeds fine or was declared all right then is possible that the User experienced a Temporary Network Problem which could be over.

To test the actual Incident status first of all we ask the User to make a test call.

If the call fails, first check that the PrivateGSM configurations are correct and if not, fix them and close the Incident. If they are fine, let's escalate to the second level

If PrivateGSM reconnects to perform the test call, then most probably we had a Temporary Network Problem issue. If the test call goes fine, check if the PrivateServer is configured with one or more Outgoing trunks. If almost one trunk is present, then you need to escalate.

On the other hand, if no trunks are configured, let's check if the User can call other party now, if he (she) can then close the incident.

If the User still can't call then check that the other device is connected and registered and if it doesn't, close the incident as "Not an issue". If the other party is connected and registered then escalate to the second level.

Second Level

We can receive an escalation request for three reasons: a User's remote party configuration needs to be checked, we have to check wether one or more trunk are configured, a general network status check.

In the first case we have to check the User's remote party activities on the server in order to discover some conflict, such as a virtual number duplication and eventually try to solve the conflicts.

In the second case we need to check if the User is using such trunk to route the call and so check trunk(s) status and configuration, by performing the checks described in PSAM 3.3 Check Server Services section.

In the latter case, no issues have been found in User client configuration, so we need to perform some tests on the Network status to understand if some communication issue are causing the Incident.

If all of the above are fine, the final possibility of a bug in the client become feasible, thus we check the client logs and then we escalate to the third level.