1 ATN Message Decoder Design Document

1.1 High-level Overview

This document proposes a design for the implementation of the following functionalities:

- Capture network traffic on the external network interface of the MAIN server in an ATN Router cluster (Pacemaker/Corosync).
- Execute the following processing steps at regular intervals (e.g., 1 minute):
  - Filter the relevant Aeronautical Telecommunication Network (ATN) messages from the captured data.
  - Convert each filtered packet and append it to an output file in the Airtel Router Log format.
  - Use the "Airtel Protocol Decoder" (PDEC) utility to process the Airtel Router Log file and generate a `pdus.csv` output file.
  - Compare the generated `pdus.csv` file with the one from the previous processing iteration to determine whether any new messages have been received.
  - Create a "timestamped" CSV file using the filename format `YYYYMMDDHHMM_pdus.csv`, that contains only the new messages.
- Provide the "timestamped" CSV output files to an Elasticsearch Filebeat instance for forwarding to the Skyguide DLS Cockpit Cloud Platform.

1.2 Online Component

1.2.1 Functionality

The online component captures network traffic and exports the capture files to the offline environment using `rsync`.

1.2.2 Network Capture

The network capture functionality is implemented as follows:

- Network capture is implemented as a Bash script that runs the `dumpcap` utility.
- The `dumpcap` utility is configured to use the ring-buffer option to create capture files with a configurable (default=one-hour) duration.
- The network capture script is configured as the `ExecStart` action in a `systemd` service unit.
- Capture file cleanup is configured as an `ExecStartPre` action in the same `systemd` service unit.
- Pacemaker is configured to run the network capture `systemd` service as a managed resource on the MAIN node of the ATN Router cluster.

Example `dumpcap` invocation:

```
: "${ARCHIVE_DIR:=/archives/captures}"
: "${NETWORK_INTERFACE:=net3}"

hostname="$(hostname -s)"
capture_file="${ARCHIVE_DIR}"/"${hostname%%-*}"_"${NETWORK_INTERFACE}".pcap

# Use ring buffer with 72 files of 60 minutes each (total = 3 days)
dumpcap \
  -i "${NETWORK_INTERFACE}" \
  -p \
  -b files:72 \
  -b duration:3600 \
  -P \
  -q \
  -w "${capture_file}" &
```

1.2.3 Export to Offline Environment

Capture files are exported by an existing `rsync`-based mechanism that transfers log files to the offline environment. The `rsync` is executed by a Bash script (`sync_to_rli.sh`) that runs every minute as a cron job on both ATN router servers. Each `rsync` running on a server uses a distinct destination directory in the offline environment.

Because the script transfers multiple types of application and system log files, large files could delay transfer of capture files. If this is deemed problematic, a dedicated `rsync` for capture files can be implemented.

1.3 Offline Component

1.3.1 Functionality

The offline component is responsible for processing the online-generated capture files into CSV files suitable for ingestion by Filebeat.

1.3.2 Global Design

The offline component is implemented as a Python application deployed as a `systemd` service unit.

The application performs the following processing at regular intervals:

- Scan and select the latest capture files from two directories (one for each ATN Router server).
- Filter the relevant capture files based on IP address and protocol using the `tcpdump` utility.
- Convert packets to the Airtel Router Log format using the `rtcd_routerlog.awk` script provided by Skyguide.
- Create an Airtel Router logfile that contains at least the last hour of messages.
- Decode the Airtel Router logfile using the Airtel PDEC utility to generate a CSV output file containing the decoded PDUs.
- Determine entries that have been added to the CSV output file since the previous processing iteration.
- Store newly added entries in a "timestamped" CSV file to be ingested by Filebeat.

1.3.3 Processing

1.3.3.1 Capture File Scanning and Selection

1. Find the two most recent capture files (`latest` and `previous`) within the two `rsync` target directories.
2. Copy candidate files to an `input` directory to prevent conflicts with ongoing `rsync` transfers.

1.3.3.2 Packet Extraction and Transformation The application uses `tcpdump` and the `rtcd_routerlog.awk` awk script to filter and transform packets into single-line records.

For each capture file:

1. The `tcpdump` utility is executed on the `.pcap` file with the following options:
   - `-r <capture file>`: Read from capture file.
   - `-n`: Do not resolve hostnames.
   - `-e`: Output link-level headers.
   - `-x`: Output packet data in hex.
   - `-tttt`: Output detailed timestamp with sub-second precision.
   - `-l`: Line-buffered output.
   - Filter: `ip host <RTCD_SNIFFED_ADDRESS> and proto 80` (ISO-on-TCP).
2. The `tcpdump` output is piped to an `awk` script called `rtcd_routerlog.awk`, which transforms multi-line packet data into single-line records with the following fields:
   - Literal string: `ROUTER CLNS_DT_PDU`
   - Timestamp from the `tcpdump` header
   - Direction: `SENT` (source IP matches monitored IP) or `RCVD`
   - ATN PDU length (IP packet payload)
   - Remote IP address

- Raw ATN (CLNP) PDU as a hex string (IPv4 header removed)

The `awk` command is invoked with the following options: - `-v "RTCD_SNIFFED_ADDRESS=<IP address>"`: Set environment variable to be used in `rtcd_routerlog.awk`. - `-f rtcd_routerlog.awk`: Use `rtcd_routerlog.awk`

1.3.3.3 Protocol Decoding

The application uses the Airtel `pdec_clnp` utility to decode the Airtel Router logfile and generate a CSV output file called `pdus.csv`.

The `pdec_clnp` utility is executed with the following options:

- `-i <log file>`: Airtel Router logfile to be decoded.
- `-s <atsu file>`: File that provides mapping between ATN CLNP NSAP and facility.
- `--csv`: Generate CSV file with transport and application information.
- `--notxt`: Undocumented in Airtel-PDEC-USG-001 dated 31-10-2024.
- `--quiet`: Undocumented in Airtel-PDEC-USG-001 dated 31-10-2024.
- `--nointermediate`: Do not generate an intermediate file.

1.3.3.4 Airtel Router Logfile Decoding

The generated output for the selected capture files is concatenated into a single Airtel Router logfile to be used for decoding.

There are three distinct situations, each with its own processing logic:

1. Initial run.
2. Latest capture file is the same as in the previous run.
3. Latest capture file is newer than in the previous run.

1.3.3.4.1 Initial Run

The following processing steps are executed:

- The Airtel Router logfiles from the previous and latest capture files are concatenated into a single Airtel Router logfile, which is processed by the Airtel PDEC utility.
- The resulting `pdus.csv` file is copied as a timestamped file to the Filebeat input directory.
- The `pdus.csv` file is retained to allow comparison in the next processing iteration.

1.3.3.4.2 Latest capture file is the same as in the previous run

The following processing steps are executed:

- The Airtel Router logfiles from the previous and latest capture files are concatenated into a single Airtel Router logfile, which is processed by the Airtel PDEC utility.
- The resulting `pdus.csv` file is compared with the `pdus.csv` file from the previous processing iteration.
- Any new entries in the `pdus.csv` file are written to a timestamped file in the Filebeat input directory.
- The `pdus.csv` file is retained to allow comparison in the next processing iteration.

1.3.3.4.3 Latest capture file is newer than in the previous run

The following processing steps are executed:

- The Airtel Router logfiles from the last three capture files are concatenated into a single Airtel Router logfile, which is processed by the Airtel PDEC utility.
- The resulting `pdus.csv` file is compared with the `pdus.csv` file from the previous processing iteration.
- Any new entries in the `pdus.csv` file are written to a timestamped file in the Filebeat input directory.
- The `pdus.csv` file is removed.
- The Airtel Router logfiles from the previous and latest capture files are concatenated into a single Airtel Router logfile, which is processed by the Airtel PDEC utility.
- The `pdus.csv` file is retained to allow comparison in the next processing iteration.