1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) Bulletin No. 2014-001, Planned Maintenance Related Outages December 2014

Background

The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) recently completed a study of outages that use the new set of cause codes related to planned maintenance activity. The new cause codes were introduced to the Network Outage Reporting System (NORS) following a study of outages related to procedural issues. The objective of the study was to address the Federal Communications Commission's (FCC) concern regarding what is described as an observed increase in the number of planned maintenance outage reports filed in NORS, based on the FCC's outage reporting thresholds.

Methodology

The ATIS NRSC examined "Planned Maintenance" outage reports from September 2013 to May 2014 by utilizing data from ATIS NRSC members provided by the FCC to an independent analyst. The reports provided by the FCC only included those for which a "Planned Maintenance" cause code was used in the root cause[1], the direct cause[2] or one of the contributing factors. Examination of the data did verify that the use of "Planned Maintenance" as a cause code was rising during the nine month period of the study. Additionally, it was observed that over 40% of these reports had either the direct or root cause (sub-category) as being "Planned Maintenance To Upgrade the System". Approximately 45% of the reports were filed as a result of the 900,000 wireless user minute criteria. The time of day analysis indicated the majority of the reports had their start time during what would normally be considered the maintenance window, and did not occur on a weekend.

Findings

The ATIS NRSC confirmed the observed increase in the number of reports filed based on the FCC's outage reporting thresholds. Findings indicate that the primary maintenance activity is network upgrade (largely in wireless networks). There is no evidence pointing to a common primary contributor within the data collected, therefore the ATIS NRSC believes that a review of the Best Practices related to planned maintenance would be beneficial to all communications stakeholders.

Recommendations

The ATIS NRSC recommends that appropriate entities revisit the Best Practices in this bulletin and continue to implement those that are applicable, which will contribute to the reduction of "Planned Maintenance" outages. The following Best Practices were selected from the most frequently cited Best Practices in the study as well as additional Best Practices suggested by ATIS NRSC members. These Best Practices address the following areas related to planned maintenance:

[1] Root Cause is the underlying reason why the outage occurred or why the outage was reportable and is the key problem which, once identified and corrected, will prevent the same or a similar problem from recurring.
[2] Direct Cause is the immediate event that results in an outage and the event, action or procedure that triggered the outage.

1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

- Training/MOP
- Communications
- Security/Testing
- Planning
- Review

Training/MOP:

Number	Best Practice
9-7-0589	Network Operators, Service Providers, and Equipment Suppliers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on production network elements, especially when new technology is introduced in the network.
9-7-0588	Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements.
9-9-0418	Network Operators and Service Providers should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.
9-9-5196	Network Operators, Public Safety and Service Providers should ensure that contractors and Equipment Supplier personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.
9-9-0697	Network Operators, Service Providers, Equipment Suppliers and Public Safety should employ an "Ask Yourself" program as part of core training and daily operations.
9-8-0590	Network Operators, Service Providers, and Equipment Suppliers should develop Methods of Procedure (MOP) for core infrastructure hardware and software growth and change activities and periodically review and update as appropriate.
9-9-0736	Network Operators should develop and implement a rapid restoration program for cables and facilities.
9-8-0755	Network Operators, Service Providers and Property Managers should document and communicate their installation and maintenance guidelines (e.g., MOP) and the expectation of compliance by all involved parties.

1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

Communications:

Number	Best Practice
9-9-0414	Network Operators, Service Providers, and Public Safety should establish plans for internal communications regarding maintenance activities and events that impact customers.
9-7-0407	Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Center) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).

Security/Testing:

Number	Best Practice
9-9-0536	As appropriate, Network Operators and Service Providers should deploy security and reliability related software updates (e.g., patches, maintenance releases, dot releases) when available between major software releases. Prior to deployment, appropriate testing should be conducted to ensure that such software updates are ready for deployment in live networks. Equipment Suppliers should include such software updates in the next generic release and relevant previous generic releases.
9-7-0559	Service Providers and Network Operators should consider validating upgrades, new procedures and commands in a lab or other test environment that simulates the target network and load prior to the first application in the field.

Planning:

Number	Best Practice
9-9-0595	Network Operators and Service Providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services.
9-9-5073	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should perform risk assessment on significant network changes (e.g., technology upgrades).
9-9-0745	Equipment Suppliers should design equipment so that changes and upgrades are non-service impacting.
9-7-0777	Equipment Suppliers should optimize equipment initializations to minimize service impact.
9-9-0750	Equipment Suppliers should provide a mechanism for feature activation or deactivation that is not service impacting to end-users (e.g., avoid re-boot, re-start or re-initialization).

Review:

Number	Best Practice
9-9-0548	Network Operators and Service Providers should have an internal post mortem process to complete root cause analysis of major network events with follow-up implementation of corrective and preventive actions to minimize the probability of recurrence. Network Operators and Service Providers should engage Equipment Suppliers and other involved parties, as appropriate, to assist in the analysis and implementation of corrective measures.