



ATIS-0100054

ATIS Standard on -

DISASTER ROAMING GUIDE AND RESOURCE



As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [<http://www.atis.org/legal/patentinfo.asp>] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0100054, *Disaster Roaming Guide and Resource*

Is an ATIS Standard developed by the **ATIS Network Reliability Steering Committee (NRSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2015 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

ATIS-0100054

ATIS Standard on

Disaster Roaming Guide and Resource

Alliance for Telecommunications Industry Solutions

Approved April, 2015

Abstract

This document provides a guide that Wireless Service Providers can use as a checklist of procedures and available resources to facilitate roaming during disasters.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The ATIS Network Reliability Steering Committee (NRSC) was formed at the request of the first Network Reliability Council (NRC-1) to monitor network reliability. NRSC is a consensus-based industry committee that analyzes the communications industry's reporting of network outages, makes recommendations aimed at improving network reliability, distributes the results of its findings to industry, and, where applicable, refers matters to appropriate industry forums for further resolution. The NRSC also reviews regulatory developments affecting network reliability and submits consensus-developed comments on matters of common interest to NRSC members.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NRSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NRSC, which was responsible for its development, had the following leadership:

S. Hartman, NRSC Co-Chair (CenturyLink)

R. Krock, NRSC Co-Chair (Alcatel-Lucent)

ATIS Standard on –

Disaster Roaming Guide and Resources

Executive Summary

This document provides a guide that Wireless Service Providers (WSPs) can use as a checklist of procedures and available resources to facilitate roaming during disasters. This guide should be reviewed well in advance, recognizing that the onset of an emergency or network disaster is not the time to be taking first steps to contact parties with whom a WSP would wish to conclude mutual roaming agreements.

The following document lists the 12 Best Practices that taken as a whole address mutual aid roaming between WSPs, and serve to remind WSPs that business continuity and network disaster recovery, including mutual roaming agreements during emergencies, are part of an ongoing process that requires carrier attention. This document provides guidance in contacting other WSPs for formulating roaming agreements during disasters, and provides guidance for informing federal authorities when roaming agreements during disasters are invoked.

Roaming agreements between WSPs and planning for potential roaming during disasters should be planned for (as much as possible) in advance. This is not to say that WSP A and WSP B must have a predefined agreement in place prior to a disaster; but that WSP A has identified other WSPs who share the commonalities needed to roam in the event of a disaster.

This document is broken up into five areas of interest:

- Roaming Overview and Examples
- Best Practices Applicable to Roaming During Disasters
- Roaming Considerations
- Contacting other WSPs
- Resources

Disaster Driven-Roaming

Many WSPs have established business agreements with one another that in many circumstances allow customers of one service provider to “roam” onto and use the network of another service provider. These “normal roaming practices” will refer to already existing agreements that govern non-disaster circumstances.

In addition to these established business arrangement, the following are voluntary steps that could be used to restore service availability for wireless customers following a disaster (earthquake, hurricane, tornado etc.) by re-purposing or changing Inbound and/or Outbound roaming relationships between WSPs. For example, in normal circumstances, roaming partners may restrict the ability of their subscribers to roam on the other’s network, particularly in geographic areas where both have infrastructure.

However, during network disasters, natural or man-made forces may asymmetrically impact one or both carriers’ networks even in the same market. For purposes of this discussion, these voluntary steps will be referred to as Disaster-Driven Roaming (DDR) to distinguish it from normal roaming practices. DDR may be particularly effective in such circumstances. The purpose of DDR is to facilitate roaming between WSPs licensed in a particular market in order to mitigate the effects on a WSP’s customers until the WSP can restore services to its own network.

The disaster recovery process is defined with the following starting and ending point:

- Start: anticipation of a severe storm event or aftermath of a disaster event requiring network mitigation.
- End: as soon as best efforts have resulted in a WSP restoring service to its own customers on its own network.

Assumptions and Constraints

- All WSPs will take steps to provide as much network availability as practicable to their own affected customers and DDR arrangements will be purely voluntary.
- To the extent necessary, DDR will be bilateral as agreed upon by all parties. Therefore, frequent communication and updates to provide situational awareness between the WSPs involved are crucial to this process.
- If inbound and outbound roaming cannot be symmetrical, preference should be given to outbound roaming from subscribers in the disaster area so that emergency communications from the disaster zone can have some precedence. Such precedence, of course, would have to be feasible and consistent with carrier network design and (surviving) capacity.
- When invoked at the time of the network disaster, the parties to DDR arrangements should inform the FCC and the NCC so that public safety authorities can be made aware of the steps taken. Similarly, when terminated, the parties to DDR arrangements should also inform the FCC and the NCC.

Process

Formal requests to open Outbound Roaming should be initiated by WSP A to WSP B as soon as practicable to mitigate the impact of network outage on users.

Formal requests to open Inbound Roaming should be initiated by WSP B to WSP A as soon as practicable to mitigate the impact of network outage on users.

Triggers

Disasters, and their impact on WSP networks, are unpredictable. However, when there is a predicted event such as a hurricane, WSPs should evaluate the threat and determine if the event is likely to affect network viability and confirm their DDR-related communications and procedures as part of their event preparation. For no-notice events such as earthquakes, WSPs should similarly confirm communications and procedures early in the response process if there is any likelihood of DDR being needed once network assessment is complete.

Implementation

WSPs will exchange network data required for network viability as soon as practicable following a disaster and a decision to implement Disaster-Driven Roaming.

Termination of the DDR agreement should occur as soon as best efforts of both carriers to restore service to its own customers on its own network have been completed. Nevertheless, there may be circumstances where traffic volumes, network capacity considerations or other factors being experienced by one roaming partner require termination of the DDR agreement.

Network loads and different types of traffic (voice/SMS/data) may require the carriers to tailor DDR to allow or curtail different traffic types as necessary.

Example Procedure for Disaster Roaming

1. WSP A assesses affected areas following an event and determines that Roaming is needed from WSP B. WSP A contacts WSP B with network data needed to implement roaming (see example below). Note: WSP A and WSP B positions in scenario can of course be flipped.
2. WSP B confirms request and assesses network load. If network can accommodate the additional load, WSP B sends network data to WSP A. WSP B takes necessary action to implement roaming and communicates that information to WSP A. WSP A confirms Roaming on WSP B's network.
3. Both WSP A and B mutually keep the other apprised of progress in mitigating damage to its network. At the appropriate time, both WSP A and B will agree to terminate roaming.
4. Each WSP takes necessary action to terminate roaming and communicates that information to the other. Each confirms to the other when roaming is terminated.

Network Data Needed to Implement Roaming

The example below is for descriptive purposes (will vary depending on the air interface jointly used by the parties).

Inbound roaming (WSP A on WSP B):

WSP A's subscribers roaming on WSP B

WSP B's MSS communicates with WSP A's HLR and SCP (if CAMEL/IN system)

WSP B provisions MNC of WSP A's MSS so that Update Location Messages can be sent to WSP A's HLR

Outbound roaming (WSP B on WSP A):

WSP B's subscribers roaming on WSP A

WSP A's MSS communicates with WSP B's HLR and SCP (if CAMEL/IN system)

WSP A provisions MNC of WSP B's MSS so that Update Location Messages can be sent to WSP B's HLR

Acronyms

CAMEL	Customized Applications for Mobile networks Enhanced Logic
IN	Intelligent Network
HLR	Home Location Registry
MNC	Mobile Network Code
MSS	Mobile Soft-Switch Solution/Mobile Switching Server
SCP	Service Control Point

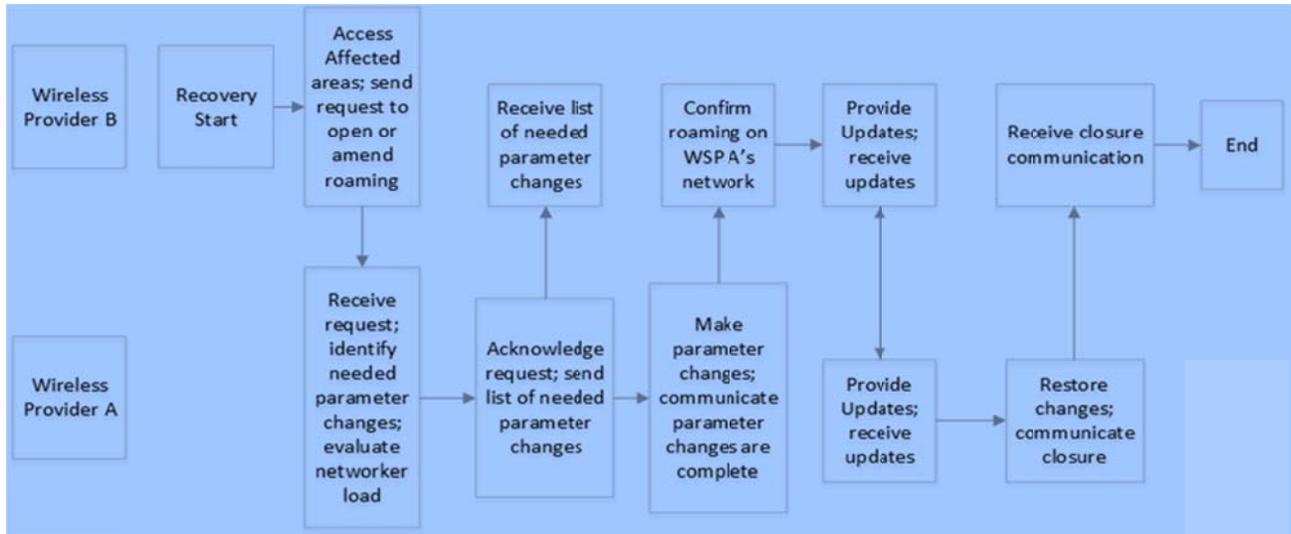


Figure 1 - Example Diagram of DDR

Applicable Best Practices

Number	Priority	Description
9-9-1001	Critical	Network Operators, Service Providers, Equipment Suppliers, Property Managers, and Public Safety should formally document their business continuity processes in a business continuity plan covering critical business functions and business partnerships. Key areas for consideration include: Plan Scope, Responsibility, Risk Assessment, Business Impact Analysis, Plan Testing, Training and Plan Maintenance.
9-9-1031	Highly Important	Network Operators, Public Safety and Service Providers should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC website. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.
9-7-0407	Highly Important	NOC Communications: 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).
9-7-0607	Highly Important	Inter-Provider Fault Isolation: Network Operators and Service Providers should ensure that bilateral technical agreements between interconnecting networks address the issue of fault isolation.

ATIS-0100054

Number	Priority	Description
9-7-0609	Highly Important	Network Operators and Service Providers should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes.
9-8-8651	Highly Important	Service Provider should have a documented Business Continuity and Disaster Recovery Plan.
9-9-0513	Highly Important	Network Operators and Service Providers should maintain a 24x7x365 contact list of other providers and operators for service restoration of inter-connected networks and as appropriate share with Public Safety and Support providers.
9-9-0608	Highly Important	Network Operators and Service Providers should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks. Interconnecting companies should address the control of overflow conditions in their bilateral agreements.
9-9-0617	Highly Important	Route Controls: Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions.
9-9-1032	Highly Important	Network Operators, Public Safety and Service Providers should document their critical equipment suppliers, vendors, contractors and business partners in their Business Continuity Plans along with an assessment of the services, support, and capabilities available in the event of a disaster.
9-9-1037	Highly Important	Network Operators, Public Safety, Service Providers, Equipment Suppliers and Public Safety Authorities should use a disaster recovery support model that provides a clear escalation path to executive levels, both internally and to business partners.
9-7-1045	Important	Network Operators and Service Providers should use their escalation process, as needed, to address resource issues identified through damage and resource assessments.

Disaster Roaming Considerations

What spectrum will I need to roam?	CDMA, TDMA, GSM or LTE
Who shares similar spectrum in my network area and where can I find that information?	FCC Universal Licensing System http://wireless.fcc.gov/uls/index.htm?job=home
Where can I find contact information for those who offer the spectrum?	FCC Universal Licensing System http://wireless.fcc.gov/uls/index.htm?job=home National Coordinating Center for Communications (NCC Watch) 703-235-5080 ncc@hq.dhs.gov http://www.dhs.gov/national-coordinating-center-communications
What type of roaming do I need/want?	Voice/Data
How long will I need to roam?	Dependent on restoration to your network

Contacting Other WSPs

As stated previously in the document, preparation and planning for DDR should be made well in advance of an event. This includes having the contact list of names and numbers for WSPs with whom you may need to roam with. However, in the event that you do not have the information needed to contact other WSPs about DDR, it is recommended that you contact the National Coordinating Center for Communications (NCC). The NCC has contact information that should enable you to connect your WSP with an appropriate WSP for possible DDR.

NCC Watch

<http://www.dhs.gov/national-coordinating-center-communications>

24 hours a day/ 7 days a week/ 365 days a year

703-235-5080

ncc@hq.dhs.gov

Resources

There are a variety of resources available to help with disasters, disasters preparedness and roaming. The following list is not exhaustive, but can assist WSPs with preparing for and working through disasters and roaming.

FCC Universal Licensing System

This website allows users to search for spectrum via market, channel, frequency and company for prospective roaming partners:

<http://wireless.fcc.gov/uls/index.htm?job=home>

ATIS NRSC Hurricane Checklist

In response to Hurricane Katrina, the NRSC prepared a checklist for industry members to use to prepare for future hurricanes. This document, ATIS-0100019, *NRSC Hurricane Checklist*, is available from the Alliance for Telecommunications Industry Solutions (ATIS):

< <https://www.atis.org/docstore/product.aspx?id=25649> >.

ATIS NRSC Pandemic Checklist

The NRSC compiled a checklist of voluntary industry Best Practices and relevant links as a reference in preparation for a pandemic event. This document, ATIS-0100018, *NRSC Pandemic Checklist*, is available from the Alliance for Telecommunications Industry Solutions (ATIS):

< <https://www.atis.org/docstore/product.aspx?id=25648> >