May, 2014

WORKING GROUP 9

Infrastructure Sharing During Emergencies

Wireless Network Subcommittee

Roaming During Disasters

Table of Contents

1 Results in Brief

1.1 Executive Summary

Natural disasters and other hazards can result in the destruction of vital communications assets, leading to communication disruptions in critical times. In recent years communications providers have explored various methods of sharing infrastructure and assets, such as back-up power assets and in-market roaming agreements, to compensate for the temporary loss of assets. This working group will examine these options and recommend a set of best practices that service providers could use to more rapidly apply infrastructure sharing methods to sustain communications in future emergencies.

The purpose of this document is to recommend best practices for the consideration and streamlining of establishing mutual roaming during disasters.

2 Introduction & Background

Roaming agreements are a longstanding "business as usual" practice among wireless service providers going back more than 20 years. Depending on a wireless carrier's organizational structure, roaming agreements are typically managed either at the regional or national level. All parties agree that roaming arrangements during disaster pose unique issues. In certain circumstances roaming may make sense and in others it may not.

Circumstances that may determine the suitability of mutual roaming include, but are not limited to: compatibility of native air interfaces; the overall health of a carrier's network including lack of power and/or backhaul connectivity to cell sites; wireless spectrum limitations; relative geographic coverage of each network; degree to which the network disaster impacts all infrastructure in one geographic area disproportionately, such that mutual roaming would not result in a significant improvement in customers' ability to originate calls; a network's ability to handle voice/data traffic from existing or potential roaming partners and technical feasibility. As smartphone use tends to drive larger and larger data requirements, potential roaming partners may wish to assess the degree to which incoming additional data traffic might degrade the network's ability to handle its own voice/data traffic.

The decision to modify or create a roaming agreement during disaster situations is often made at the senior leadership levels within each company. The Working Group emphasizes that nothing in this Guideline should be construed to require or mandate that a carrier engage in mutual roaming, that mutual roaming be established within set timeframes following onset of a disaster or emergency, or that the duration of mutual roaming be any fixed length, such as the duration of a government declared state of emergency. Often it is assumed that mutual roaming is done on a fully symmetrical basis between partners, i.e., categories of shared air interfaces and/or frequencies are identical. In reality, however, roaming is sometimes accomplished on an asymmetrical basis, including during disaster situations, as agreed upon by the roaming carriers.

The Working Group notes that the four national wireless carriers are also members of DHS's NCC – the National Coordinating Committee for Telecommunications, through a Center chartered for Information Sharing and Analysis (the Comm ISAC). During disaster situations, Comm ISAC members apprise the NCC of roaming arrangements they've made so that the federal government has situational awareness. Independent of this recommendation, smaller carriers may want to contact the NCC (703-235-5080) which can help them contact the national wireless carriers.

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Next Generation 911	Working Group 2: Wireless Emergency Alerts	Working Group 3: EAS	Working Group 4: Cybersecurity Best Practices Working	Working Group 5: Server-Based DDoS Attacks	Working Group 6: Long-Term Core Internet Protocol Improvements	Working Group 7: Legacy Best Practice Updates	Working Group 8: Submarine Cable Landing Sites	Working Group 9: Infrastructure Sharing During Emergencies	Working Group 10: CPE Powering

Table 1 - Working Group Structure

2.2 Working Group 9 Team Members

Name	Company
Jay Naillon, Chair	T-Mobile USA
Eric Panketh, FCC Liaison	FCC
Eric Woody, Wireless Network- Co-Chair	Union Wireless
Ernie Gallo, Wireless Network - Co-Chair	Ericsson
Denise Anderson	Financial Services Information Sharing & Analysis Center (FS-ISAC)
Shellie Blakeney	T-Mobile USA
Kent Bowen	AT&T
Lois Burns	PA PUC
Ingrid Caples	HHS
Kathy Catalano	Cat5 Resources
Mark Christian	American Tower
Mike Cybyske	CenturyLink
Carroll Demas	Valrico Ventures
Jarrett Devine	FEMA-DHS
Todd Dufur	Generac
Rose Fiala	T-Mobile USA
Kevin Frank	Sprint
Rick Griepentrog	AT&T
Arun Handa	Applied Communication Sciences
Arthur Jackson	T-Mobile USA
Brian Josef	CTIA
Lola Judge	Federal Reserve Bank of New York
Rick Kemper	CTIA
John Kim	Enersys
Kate Kingberger	US Dept. of Treasury

Steven Martin	AT&T
Chao-Ming Liu	Applied Communication Sciences
Julia Merette	Federal Reserve Bank of New York
Chris Oberg	Verizon Wireless
Bob Oenning	*Expert*
Eric Osterweil	Verisign
Wayne Pacine	Federal Reserve Bank
Jared Pierson	Generac
Richard Qualey	Pac-Power
Ed Roth	Larimer County, CO
Harold Salters	T-Mobile USA
John Schwarz	Ericsson
Steven Schwartz	Goldman Sachs
Dick Scott	Battery Corp.
Viqar Shaikh	Applied Communication Sciences
Jim Shortal	Cox Communications
Alland Sy	Goldman Sachs
Jason Thompson	Sunbelt Rentals, Inc.
Stephen Tibbs	Foster Fuels
Anil Trehan	Commscope
Lynette van Someren	Comcast
Kathy Whitbeck	Nsight
Geoffry Why	State of MA.
Gaspar Wosa	Ericsson

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective & Scope

The scope of this document is to provide a recommendation to the FCC and CSRIC IV Council regarding possible best practices and approaches which could potentially streamline the enabling of wireless roaming between carriers in times of disasters or emergencies. This document includes:

- Introduction and background
- Reference to existing Best Practices
- Example of Wireless Roaming Matrix
- Example of Wireless Contact List
- Example of roaming enabling process

3.2 Methodology

This document, best practices and other supporting materials within were generated through a cooperative effort and by majority consensus of subject matter experts belonging to the CSRIC IV Working Group 9 team member roster. This effort was led by the CSRIC IV WG9 Network Wireless Subcommittee. The existing best practices were pulled from NRIC and FCC documentation as referenced.

4 Recommendations

It is the recommendation of CSRIC Working Group 9 that the FCC should consider sharing the Roaming During Disasters document and associated Best Practices with licensed wireless service providers (WSP) within the United States, and further The Alliance for Telecommunications Industry Solutions (ATIS) should populate and work with WSPs, on a voluntary basis, to maintain the Wireless Roaming Matrix and Wireless Contact List included in the appendix of this report. ATIS should post the referenced information on a secured website.

In addition, based on BP 9-9-1001, Wireless Carriers should review and streamline their internal practices and document their business continuity processes in a disaster. An example of this is Appendix A, which demonstrates the process for inbound and outbound roaming process during a disaster.

4.1 Recommended Best Practices

Proposed New Best Practices: The group spent several meetings trying to draft one or more new best practices to focus on this matter. However, after deliberations spanning many meetings, that included comprehensive analysis of scores of wireless-related best practices, the Group came to the conclusion that it was two of the existing best practices, 9-9-1001 and 9-9-1031, that most completely captured the range of issues and would provide the needed guidance to industry.

Existing Best Practices: FCC 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.
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.

5 Conclusions

In this Report, the Working Group sets forth a basis for consideration of existing or modified Best Practices that may be needed to facilitate service provider roaming during disasters. In this process, existing Best Practices have been identified for reference. Importantly, a national matrix of Service Provider air interfaces and state/territorial coverage has been developed. This matrix should be of particular help to smaller carriers as they assess their roaming opportunities and should assist all parties toward understanding the opportunities and challenges inherent in establishing roaming during disaster situations. Process diagrams are also set forth for illustration.

Roaming is not new to the wireless industry and is done on an everyday basis as part of standard business procedures voluntarily entered into between carriers. Likewise, this Report emphasizes that roaming during disasters or other emergencies can only be undertaken on a voluntary basis as carriers evaluate their networks in the context of an event.

6 Appendices

A. Example Roaming During Disasters Process Document

Overview

Wireless service providers typically establish 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.

This document describes voluntary steps that could be used to restore service availability for wireless customers following a disaster (earthquake, hurricane, tornado etc.) by establishing or changing Inbound and/or Outbound Roaming relationships between WSPs.

For purposes of this discussion, these voluntary steps will be referred to as Disaster-Driven Roaming (DDR) so as to distinguish it from normal roaming practices. Normal roaming practices will refer to agreements such as those that already exist to govern non-disaster 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.

Audience

Audience includes Wireless Service Provider A (WSP A) and Wireless Service Provider B (WSP B) as well as Roaming Partners (RPs).

Document Scope

This document describes the roles, responsibilities and procedural steps for stakeholders in the disaster recovery process.

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

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

Assumptions and Constraints

- All wireless service providers 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, event-driven roaming will be bilateral as agreed upon by all parties. Therefore, frequent communication and updates between the wireless service providers are crucial to this process.

- Throughout this process Wireless Service Providers will continually send updates to provide situational awareness to the concerned parties and enhance network viability.

Authority

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 WPS 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 emergent 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 event-driven roaming.

Closure of Roaming as soon as best efforts should have resulted in a WSP restoring service to its own customers on its own network.

Example Procedure for Inbound Disaster

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.
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.

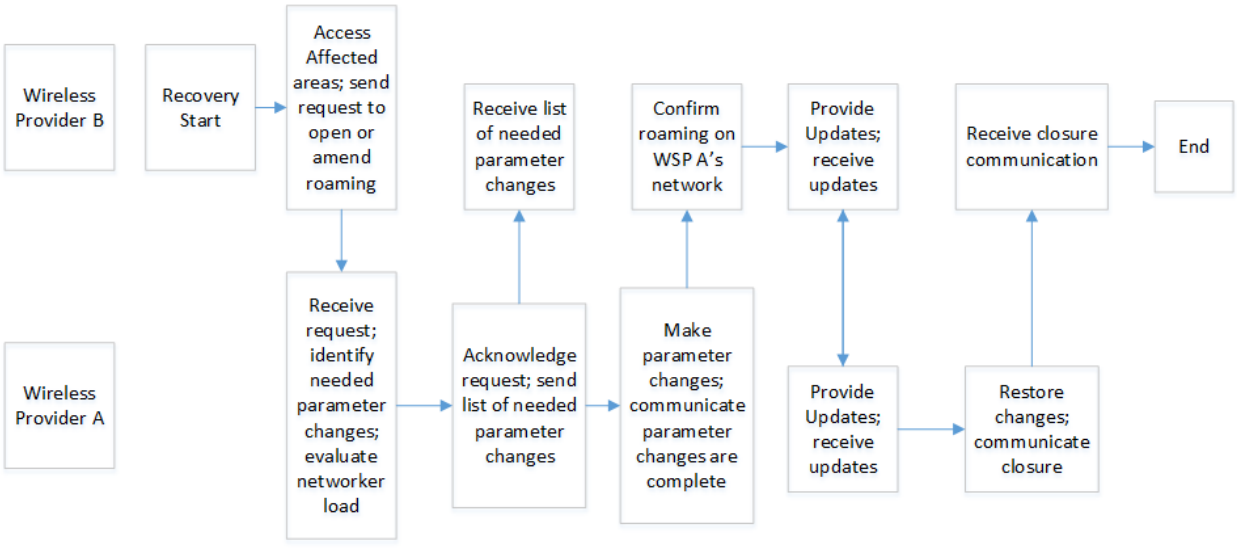
3. WSP A will need to notify the WSP B of progress in mitigating damage to their network. At the appropriate time, WSP B and WSP A will agree to terminate roaming.
4. WSP B takes necessary action to terminate roaming and communicates that information to WSP A. WSP A confirms roaming is terminated,

For an overview of process refer to Figure 1: Disaster Recovery Process in Conjunction with Event-driven Inbound Roaming between WSP A and WSP B.

Example Procedure for Outbound Disaster Roaming

1. WSP B assesses damage to network immediately following a disaster. They determine areas affected and contact WSP B to initiate Roaming. WSP B contacts WSP A with network data needing to open roaming. WSP A receives and acknowledges request.
2. WSP A communicates they agree. WSP A sends WSP B available network data after network assessment has been completed. If network can accommodate the additional load WSP A will open roaming. WSP A updates WSP B. As information may change; all updates are communicated between WSPs.
3. As WSPB is able to mitigate damage to their network; WS PB will keep WSP A apprised of any progress and updates.
4. Once WSP B network is viable; WSP B will communicate to WSP A that roaming can be closed. WSP A will agree. WSP A closes roaming and updates WSP B. WSP A closes roaming and sends closure notification to WSP B.

For an overview of process refer to Figure 2: Disaster Recovery Process in Conjunction with Event-driven Outbound Roaming between WSP A and WSP B.



B. Wireless Roaming Matrix

This matrix is provided only as a sample of information that ATIS should establish and maintain roaming during disasters, in order to restore service to their customers in the event of significant damage to their network and to their ability to respond. It is anticipated that ATIS would include information of greater granularity than demonstrated in this sample.

The presence of a particular carrier's information in this matrix is for sample purposes only and does not indicate that the carrier had adopted or endorsed.

		Technology/Spectrum					
State	Carrier	GSM	CDMA	EVDO	UMTS	LTE	WiMax
Alabama	AT&T	850, 1900	na	na	850, 1900	700, 1900, AWS	na
	Sprint	na	800, 1900	1900	na	na	2500
	T-Mobile	1900	na	na	1900/AWS	AWS	na
	Verizon	850	850, 1900	850, 1900	na	700,AWS	na
Alaska	Artice Slope	850, 1900	na	na	na	na	na
	AT&T	850, 1900	na	na	850, 1900	700, 1900, AWS	na
	GCI	1900	na	na	1900	na	na
	Sprint	1900	na	na	na	na	na
	Verizon	na	na	na	na	700,AWS	na
American Samoa							na
Arizona	AT&T	850, 1900	na	na	850, 1900	700, 1900, AWS	na
	C1AZ	850, 1900	na	na	na	na	na
	Commnet	850, 1900	na	na	na	na	na
	Sprint	na	800, 1900	1900	na	na	2500
	T-Mobile	1900	na	na	1900/AWS	AWS	na
	Verizon	na	850, 1900	850, 1900	na	700,AWS	na
Arkansas	AT&T	850, 1900	na	na	850, 1900	700, 1900, AWS	na
	Sprint	na	1900	1900	na	na	2500
	T-Mobile	1900	na	na	1900/AWS	AWS	na
	Verizon	na	850, 1900	850, 1900	na	700,AWS	na

C. Wireless Carriers Contact List

This list is provided only as a sample of information that ATIS should establish and maintain roaming during disasters, in order to restore service to their customers in the event of significant damage to their network and to their ability to respond. It is anticipated that ATIS would include information of greater granularity than demonstrated in this sample.

The presence of a particular carrier's information in this list is for sample purposes only and does not indicate that the carrier had adopted or endorsed.

Carrier	Name	Title	E-mail	NOC/Emergency
AT&T	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx
Sprint	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx
	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx
T-Mobile	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx
	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx
	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx
Verizon	xxxx	xxxx	xxxx@xxxx.com	xxx-xxx-xxxx