



ATIS-0300004

NETWORK INTERCONNECTION INTEROPERABILITY FORUM

(NIIF)

INTERCONNECTION TEMPLATE

(Network Interconnection Bilateral Agreement Template)

Issue 3.0



ATIS is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 21 industry committees, and its Incubator Solutions Program.

< <http://www.atis.org/> >

---

This document was developed by the Alliance for Telecommunications Industry Solutions' (ATIS) sponsored Network Interconnection Interoperability Forum (NIIF). The NIIF provides an open forum to encourage the discussion and resolution, on a voluntary basis, of industry-wide issues associated with telecommunications network interconnection and interoperability which involve network architecture, management, testing and operations and facilitates the exchange of information concerning these topics. The NIIF is responsible for identifying and incorporating the necessary changes into this document. All changes to this document shall be made through the NIIF issue resolution process as set forth in the NIIF Principles and Procedures.

This document is maintained and exclusively distributed by ATIS on behalf of the NIIF.

#### **Disclaimer and 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, WITH RESPECT TO ANY CLAIM, 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.

---

*ATIS-0300004, NIIF Interconnection Template (Network Interconnection Bilateral Agreement Template), Issue 3.0, Formerly NIIF-0003*

The NIIF Interconnection Template (Network Interconnection Bilateral Agreement Template), Issue 3.0 is an ATIS standard developed by the Network Interconnection Interoperability Forum (NIIF) under the **ATIS OAM&P Functional Group**.

*Published by*

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

Copyright © 2004 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/> >.

Printed in the United States of America.

# Table of Contents

I.	INTRODUCTION .....	7
1.	GENERAL .....	7
A.	Purpose .....	7
B.	Applicability .....	7
C.	Definitions .....	7
D.	NIIF Reference Document .....	7
2.	BASIC PREMISES .....	7
3.	CRITERIA .....	7
4.	SCOPE OF THIS DOCUMENT .....	7
5.	SERVICE PROVIDERS (SP) RESPONSIBILITIES .....	7
6.	SERVICE CUSTOMERS (SC) RESPONSIBILITIES .....	8
II.	REQUIREMENTS AND AGREEMENTS FOR PROVISIONING NETWORK INTERCONNECTION .....	9
1.	TARIFF IDENTIFICATION .....	9
A.	Lists of Services .....	9
B.	Unbundled Services .....	9
2.	EXPLICIT FORECASTING INFORMATION .....	9
A.	Direct Traffic .....	9
3.	DOCUMENTATION .....	10
4.	INTERFACE SPECIFICATIONS .....	10
A.	Service Provisioning Process* .....	10
B.	Specific Versions of Protocol and/or Interface Specifications .....	10
C.	Network Interface Standards, Versions Control (Backward Compatibility) .....	11
E.	Interface for Ordering/Pre-Ordering* .....	11
F.	Compatibility with Year 2000 Specifications* .....	11
G.	Specific References: GR 2945, 2000 Generic Requirements – System Interfaces (12/96), ISO8601* .....	11
H.	Ensure Compatible Date formats on Interface* .....	11
I.	Compatibility of Expanded Use of Information Digits .....	11
5.	NETWORK DESIGN PARAMETERS* .....	11
6.	NETWORK ADMINISTRATION OF NETWORK SECURITY .....	11
A.	Access Methodology .....	11
B.	Functional Partitioning .....	12
C.	Access Monitoring .....	12
D.	Password Control .....	12

E.	Encryption Control.....	12
F.	GATEWAY SCREENING (SS7 Network Interconnection Reliability and Security).....	12
G.	Calling Party Number Privacy Management.....	12
H.	Security Base Guidelines for Interconnected SS7 Networks.....	12
I.	Security Guidelines and Standards.....	12
7.	SERVICE INTERWORKING REQUIREMENTS.....	13
A.	Tandem Homing Arrangements.....	13
B.	Re-Sale Related Service Requirements*.....	14
C.	Operator Services/DA Routing and Branding.....	14
D.	Unbundling Related Service Requirements.....	14
E.	Directory Listings*.....	14
F.	Number Portability (NP).....	14
G.	National Services.....	14
8.	DIVERSITY AND SURVIVABILITY REQUIREMENTS.....	15
A.	Route Identification.....	15
B.	Diversity Definitions.....	15
9.	SPECIAL ROUTING TRANSLATIONS (SSP, STP).....	15
10.	PROTOCOL IMPLEMENTATION AGREEMENTS.....	15
A.	Specific References.....	16
B.	Timer Values.....	16
C.	Routeset Congestion Test (RCT) Messages.....	16
D.	Optional Parameters.....	16
E.	Switch Parameters.....	17
F.	Standard Protocols.....	17
III.	INSTALLATION AND MAINTENANCE GUIDELINES, PROCEDURES AND RESPONSIBILITIES.....	18
1.	GUIDELINES FOR MEETING MAINTENANCE PERFORMANCE SERVICE LEVELS.....	18
A.	Interface Specification.....	18
B.	MTBF/MTTR.....	18
C.	Performance Thresholds (Tolerance Range) *.....	18
D.	E9-1-1 Database Updates.....	18
E.	Measures for Specific Service Classes*.....	18
F.	Monitoring and Reporting Mechanisms.....	18
2.	DOCUMENTATION REQUIREMENTS.....	19
A.	Company Specific Contact Directory.....	19
B.	Contact Listing.....	19
3.	MAINTENANCE PROCEDURES FOR STATUS AND TROUBLE REPORTING.....	19
A.	Trouble Reporting, Trouble Resolution and Escalation Procedures.....	19

B.	Emergency Communication; Emergency Preparedness Plans .....	20
C.	Tones and Announcements for Unsuccessful Call Attempts and Toll Warnings.....	20
D.	Catastrophic Outages.....	21
4.	ACCEPTANCE TESTING .....	21
IV.	INTERCONNECTION TESTING PROCEDURES AND RESPONSIBILITIES.....	22
1.	RESPONSIBILITY ASSIGNMENTS.....	22
A.	Automatic Trunk Testing .....	22
B.	Pre-Cutover Inter-Network Connectivity Testing.....	22
2.	INTEROPERABILITY TEST RESULTS .....	22
3.	PROCESS FOR CIRCUIT LEVEL TESTING AND PERFORMANCE ANALYSIS OF UNBUNDLED NETWORK ELEMENTS .....	23
4.	SS7 AND OTHER CRITICAL INTERFACE INTER-NETWORK COMPATIBILITY TESTING.....	23
A.	SS7 Interconnection.....	23
B.	SS7 Diversity Verification and Validation .....	23
5.	INFORMATION SHARING .....	24
V.	NETWORK ADMINISTRATION AND MANAGEMENT GUIDELINES, PROCEDURES, AND RESPONSIBILITIES.....	25
1.	DOCUMENTATION REQUIREMENTS.....	25
A.	Network Configuration.....	25
B.	Contact Numbers* .....	25
2.	NETWORK TRAFFIC ENGINEERING.....	25
A.	Traffic Engineering Design Criteria and Capacity Management.....	25
B.	Alternate Routing Design .....	25
C.	Call Blocking Criteria.....	25
3.	NETWORK REARRANGEMENTS - MAJOR RE-HOMING.....	25
A.	Logical .....	25
B.	Physical .....	26
4.	SYNCHRONIZATION DESIGN AND COMPANY-WIDE COORDINATION CONTACTS .....	26
A.	Establish Conformance .....	26
B.	Identify Synchronization Contacts.....	26
C.	Coordination Administration .....	26
VI.	NETWORK TRANSITION CONSIDERATIONS.....	27
1.	NETWORK TRANSITION .....	27
2.	NPA SPLITS/OVERLAYS/REARRANGEMENTS AND NXX CODE OPENINGS/CHANGES .....	27
A.	NXX Code Establishment and/or Modifications .....	27
3.	MAJOR REHOMING, REARRANGEMENT PLANS*.....	28
4.	TRANSITION TO USE OF EMERGING TECHNOLOGIES SUCH AS PACKET BASED TECHNOLOGY.....	28
A.	Vendor Compatibility* .....	28

B.	Optional Capabilities*	28
C.	Feature Interactions*	28
VII.	BILLING CONSIDERATIONS	29
1.	ACCURACY OF DATA*	29
2.	INTERVAL OF RECORDS EXCHANGES*	29
3.	DISPUTE RESOLUTION*	29
4.	OBF DOCUMENTATION/BILLING RECORDS DATA EXCHANGE	29
VIII.	VENDOR REQUIREMENTS AND RESPONSIBILITIES	30
1.	WRITTEN REQUIREMENTS	30
2.	SOFTWARE VALIDATION	30
3.	OPTIONAL REQUIREMENTS	30
4.	TESTING	30
5.	TRAINING	31
6.	EMERGENCY EQUIPMENT AVAILABILITY	31
A.	Contact Lists	31
7.	INTERFACE SPECIFICATIONS FOR STANDARD ELEMENTS*	31
8.	PROCESS FOR CERTIFYING COMBINATION, INTERMINGLING, AND OPERATIONS OF NE'S*	31
IX.	ENVIRONMENTAL OPERATIONAL REQUIREMENTS	32
1.	SECURITY	32
2.	POWER & GROUNDING	32
A.	Power	32
B.	Grounding	33
3.	INTERFERENCE PROTECTION	35
4.	RADIO INTERFERENCE	35
X.	OPERATIONAL AND RELIABILITY REQUIREMENTS	36
1.	PROTOCOL ELEMENTS*	36
2.	INTERFACE MESSAGING*	36
3.	GATEWAY SCREENING*	36
4.	OVERLOAD CONTROLS	36
4.	FAULT DETECTION*	36
5.	NETWORK PERFORMANCE OBJECTIVES*	36
6.	COMPATIBILITY*	36
7.	NETWORK MANAGEMENT CONTROLS	36
8.	BACKWARD COMPATIBILITY*	37
9.	PERFORMANCE CRITERIA*	37
10.	NETWORK OUTAGES REPORTABLE TO THE FCC	37
A.	Failure Analysis Procedures	38

B.	Root Cause Analysis Processes .....	38
C.	Network Survivability Performance .....	38
XI.	GLOSSARY .....	39

# INTERCONNECTION TEMPLATE DOCUMENT

## I. INTRODUCTION

### 1. GENERAL

#### A. *Purpose*

The purpose of this document is to provide guidance to access SCs and access SPs when they are engaged in interconnection negotiations to ensure that all areas of network integrity from an interconnection perspective are addressed.

#### B. *Applicability*

This document is intended to be a living document, therefore subject to revision and upgrading under the Operating Procedures for ATIS Forums and Committees.

This document does not replace or supersede any existing Contracts, tariffs or any other legally binding document.

#### C. *Definitions*

In general the definitions for terms utilized within this document can be found in the Terms and Definitions section of the Network Interconnection Interoperability Forum (NIIF) Reference Document.

#### D. *NIIF Reference Document*

The NIIF Reference Document, its appendices and Company Specific Contact Directory referred to herein may be obtained by contacting the NIIF Committee Administrator at 1200 G Street NW, Suite 500, Washington, DC 20005, at the ATIS web site ([www.atis.org](http://www.atis.org)), or at 202-628-6380.

## 2. BASIC PREMISES

The use of an interconnection checklist enables the interconnection negotiations process to proceed more expeditiously and will provide assurance that appropriate areas for concern are addressed proactively.

## 3. CRITERIA

Information to be included in this document is a result of Network Interconnection Interoperability Forum agreements and pertains to interconnection negotiations between SPs and SCs.

## 4. SCOPE OF THIS DOCUMENT

The scope of this document is restricted to the interconnection negotiations between SPs and SCs as it pertains to providing assurance for the integrity of the interconnected networks, as related to the Interconnection template as initially provided by the Network Reliability Council Task Group II (NRC TG-II). All users of this document should understand that negotiations are encouraged to go above and beyond those subjects and questions identified in these template guidelines. During negotiations, interconnecting companies may impose additional subjects or questions, including some that are in areas other than those identified in this document.

## 5. SERVICE PROVIDERS (SP) RESPONSIBILITIES

The responsibilities of SPs as it pertains to interconnection have been addressed in the NIIF Reference Document for the various access services. See the NIIF Master Table of Contents.

## **6. SERVICE CUSTOMERS (SC) RESPONSIBILITIES**

The responsibilities of SCs as it pertains to interconnection have been addressed in the NIIF Reference Document for the various access services. See the NIIF Master Table of Contents.

In addition to the responsibilities stated in the NIIF Reference Document, the following guidelines should be established:

- Establish a business relationship with their SP of choice
  - Establish an account for service
  - Provide appropriate billing and account location information
  - Select from the appropriate service options offered by the SP
- Notify the SP of any problems which may occur with regard to the service(s) provided
- Notify the SP of any changes desired to the service(s) or features provided, or other changes to the SC's account information
- Remit payment for services billed and agreed to by the SC, when billed by the SP
- Notify the SP of the desire to discontinue service, if appropriate
- Utilize the service(s) in an appropriate manner

Has your company informed its customers of their responsibilities with regard to the service(s) your company provides to them?

## II. REQUIREMENTS AND AGREEMENTS FOR PROVISIONING NETWORK INTERCONNECTION

### 1. TARIFF IDENTIFICATION

All SPs in geographic areas are bound to some degree by state and federal tariffs and regulatory orders. It is imperative that prior to the commencement of interconnection negotiations all parties involved perform the appropriate research to ensure that they are in compliance with those tariffs and orders.

#### A. *Lists of Services*

At the time of interconnection negotiations the interconnecting parties should provide each other with a listing of the services for which your company will provide interconnection and where applicable, identify the tariff/order that covers the requirements of those services.

Questions that may be asked and answered to facilitate these negotiations are provided.

- “Does your company have a listing of the services and appropriate tariffs/orders of the services that you wish to interconnect?”
- “Are there additional services that your company wishes to interconnect to that are not covered by tariffs or orders? If the answer is yes what are they?”

#### B. *Unbundled Services*

Some SPs may offer unbundled elements of their service for interconnection. Where this potential exists interconnecting companies should provide the appropriate information.

Questions that may be asked and answered to facilitate these negotiations are provided.

- “Does your company offer unbundled services for interconnection?”
- “What unbundled services does your company offer for interconnection?”

### 2. EXPLICIT FORECASTING INFORMATION

This section discusses the need for accurate forecasting information being exchanged either during interconnection negotiations or as soon as available. These discussions will assist in ensuring the availability of both transport paths and required equipment needed for interconnection. It is suggested that interconnected parties exchange forecasting information and expectations for current and future traffic needs in a regular interval.

Discussions could include:

- How much direct and/or subtending/transiting traffic would your company anticipate sending?
- It is suggested that timetables be determined for sharing on-going forecasting information or equipment requirements if applicable.

#### A. *Direct Traffic*

This shared information will ensure that the necessary facilities and equipment are provided to allow for the exchange of the following types of traffic between Access Service Providers and Access Service Customers.

**Local Exchange** - Local traffic to be terminated on each party’s local network so that customers of either party have the ability to reach customers of the other party without the use of access codes.

**Exchange Access** - The offering of access to telephone exchange services or facilities origination and termination of intraLATA or interLATA toll services.

**IXC Transit** - The SP must provide intermediary network access service between an SC and SP for the purpose of completing interLATA and intraLATA toll traffic. Each carrier will provide their own network access services to the SC on a meet-point basis.

### **3. DOCUMENTATION**

Interconnected companies should agree on installation, provisioning and maintenance guidelines for interconnection. Recommended guidelines are identified in the NIIF Reference Document, Master Table of Contents.

### **4. INTERFACE SPECIFICATIONS**

#### *A. Service Provisioning Process\**

#### *B. Specific Versions of Protocol and/or Interface Specifications*

This Section describes characteristics of the Physical / Software interfaces needed to interconnect to other networks and network elements.

Specific versions of protocol – As a generic requirement for any interface with multiple versions and options within each version, interconnecting companies need to agree on what is optional and what is mandatory. Agreement must be reached on how much backward compatibility will be supported, and how to plan compatible migrations.

- What version of the protocol does your company use?
- What optional parameters are included?

The interface required to obtain connectivity/access to other networks, and network elements, is generally comprised of two elements: a physical interconnection device and compatible (software) protocol. The physical element includes both the hardware device that functions as the actual connection point (e.g., optical cross-connect panel connection using a fiber patch cord with an SC connector) and the electrical/optical requirements for transmitting/receiving information over that connector (e.g., bit rates, voltage ranges, optical wavelengths, etc.).

The software element is the specific protocol used for formatting the addressing, administrative and application information that is transmitted over the interface.

These elements are included within specific levels of the OSI Reference Model, or other protocol stacks such as TCP/IP, which organize communication protocols into logical groups or layers. Each layer specifies a protocol standard that describes a physical or software interface requirement.

The physical/software interconnection requirements for connectivity to specific networks and network elements are detailed in one or more technical documents published by various manufacturers, standards bodies, technical publishing companies, or individual network providers. They are usually referenced within the tariffs or interconnection agreements published by the service provider offering access to their network/network elements.

The physical/software interfaces used to interconnect networks should conform to existing tariffs, technical standards and government regulations.

- Is your company aware of the physical/software interconnection requirements for each network element to which it intends to establish connectivity with a particular service provider?
- Does your company know how to obtain the necessary technical documentation, which describes the interconnection requirements specified by a particular service provider?

#### **1. Tariffs**

Tariffs are documents filed by a regulated common carrier with state public utility commissions or the Federal Communication Commission. The tariff describes the pricing and conditions under which services are offered by the common carrier to all potential customers.

#### **2. Technical Standards**

Technical Standards are performance-based or design-specific technical specifications and related management system practices. Technical Standards are developed or adopted by voluntary consensus standards bodies.

### **3. Government Regulation**

Interconnection specifications are typically used as a means to carry out policy objectives or activities determined by government agencies, departments, and commissions.

### **4. Network Interconnection Point**

A network interconnection point is defined as a physical point at which ownership or responsibility for operating or maintaining facilities passes from one party to another. Normally non-intrusive tests can be performed at the network interconnection point without interference to other equipment or facilities.

#### *C. Network Interface Standards, Versions Control (Backward Compatibility)*

Specific versions of protocol – As a generic requirement for any interface with multiple versions, interconnecting companies need to agree on how much backward compatibility will be supported, and how to plan compatible migrations.

- What protocols are used by your network?
- For each protocol, what version is used?

#### *E. Interface for Ordering/Pre-Ordering\**

#### *F. Compatibility with Year 2000 Specifications\**

#### *G. Specific References: GR 2945, 2000 Generic Requirements – System Interfaces (12/96), ISO8601\**

#### *H. Ensure Compatible Date formats on Interface\**

#### *I. Compatibility of Expanded Use of Information Digits*

Automatic Number Identification (ANI) Identification Information (II) digits are a digit pair sent with the originating number. These digits identify the type of originating station. The expanded use of ANI II digits will continue to support service offerings and system capabilities. In an interconnected environment, compatibility in application and transporting these digits, where available, is important for enhanced services and systems to be workable when interconnected to service providers and/or service customers.

- Does your company intend to pass these ANI II digits?
- Does your company adhere to the ANI II digits as assigned within the Industry?
- Does your company use other information digits not commonly used within the Industry?

## **5. NETWORK DESIGN PARAMETERS\***

## **6. NETWORK ADMINISTRATION OF NETWORK SECURITY**

This section is designed to provide guidance to interconnected parties in regards to Network Administration and Security Management as it pertains to accessing network nodes. This information should not be interpreted as a complete compendium of all security measures in place, but merely a minimum set of recommendations.

It is recommended that interconnected companies proactively share their respective security requirements for interconnection during their interconnection negotiations.

The following list addresses some specific areas of security that should be discussed during interconnection negotiations as well as specific references where information can be obtained:

#### *A. Access Methodology*

It is recommended that all interconnected parties develop and have in place access methodologies that inhibit unauthorized personnel from gaining access to network elements and support systems.

## *B. Functional Partitioning*

Where appropriate, systems should be partitioned in such a manner as to enable company personnel to perform only those functions for which they are authorized. The partitioning should inhibit unauthorized personnel from migrating from one functional area/system to another.

## *C. Access Monitoring*

Administrative tools that monitor partitioned access, whether administrative or network related, should be mutually developed and maintained.

## *D. Password Control*

It is recommended that, where appropriate, password controls be developed and implemented to protect access to systems, whether administrative or network related.

## *E. Encryption Control*

Where appropriate and practical, encryption should be utilized to protect data as it traverses the interconnected network.

## *F. GATEWAY SCREENING (SS7 Network Interconnection Reliability and Security)*

SS7 network providers are responsible for ensuring the reliability and security of their own SS7 networks with respect to defending against the propagation of abnormal SS7 signaling messages when interconnected with other networks. This responsibility should ensure protection against unexpected SS7 messages, SS7 messages with protocol errors, attempts at sabotage, or any other harmful conditions that may be propagated across interconnected SS7 networks.

It should be noted that SS7 network intermediate nodes generally examine those parts of incoming messages with respect to routing of the message. The SS7 destination node examines additional information for the proper processing of the message, and this may include additional security considerations. Examination of the content of every message routinely is not done, and may not be practical. Various methods of protocol analysis that further examine message content are available to detect and resolve troubles, but are generally utilized only on an exception basis.

A variety of processes and responsibilities intended to ensure reliability, network security, and risk minimization associated with SS7 network interconnection are outlined elsewhere in the document.

## *G. Calling Party Number Privacy Management*

The FCC requires the linking of the calling number and calling name such that the presentation status is either "presentation allowed" or "presentation restricted". In order to reduce unnecessary queries to the calling name (CNAM) database, the carrier should rely on the Calling Party Number Parameter field in the IAM to control whether or not the name and number be delivered to the called party. If the presentation status in the IAM is set to "presentation allowed", the carrier may reveal both the calling number and the calling name to the called party. If the presentation status in the IAM is set to "presentation restricted", the carrier will not reveal the caller's number or name to the called party. No calling name in the CNAM database should be preset to "private" or "public".

- Does your company adhere to the appropriate regulatory guidelines for the "Calling Party Privacy" feature? "Calling Party Privacy" feature includes:
  - The called party's switch blocks the transmission of the calling party's number to an electronic display mechanism and prevents use of Call Return Feature.

## *H. Security Base Guidelines for Interconnected SS7 Networks*

The NIIF Reference Document, Part III, has outlined a set of guidelines for application in the SS7 interconnected network (SS7 Network Security Base Guidelines).

## *I. Security Guidelines and Standards*

For more information related to security guidelines and standards, readers may wish to visit the ATIS Telecom Security site, as well as other industry sites.

## 7. SERVICE INTERWORKING REQUIREMENTS

**Tandem Switch** - A tandem switch connects one trunk to another and serves as a trunk concentration and distribution function to minimize direct end office interconnection. A tandem switch is an intermediate switch or connection between an originating switch and the final switch call destination. A tandem switch does not allow origination or termination of telephone calls. Tandems serve a designated geographic area consisting of specific rate centers.

### A. Tandem Homing Arrangements

There are three levels of regulatory jurisdictions and six types that define tandem homing arrangements.

- Your company needs to be aware of the tandem homing arrangements.

NOTE: A particular switch can be one of the following types or a combination.

**Local** - A Local Exchange Carrier (LEC) switching system specifically identified as a local tandem which provides a traffic concentration and distribution function for local traffic originating and/or terminating within a local calling area as defined in the state tariffs on file with the appropriate regulatory body. A local tandem provides trunk to trunk connections to more than one end office within a local calling area.

Although interconnection at more than one local tandem may be required to provide access to all end offices within a local calling area, only the homing or subtending interconnection is reflected in the Telcordia LERG Routing Guide.

A host/remote scenario does not constitute a local tandem homing arrangement. Nor should an office be considered a local tandem if local traffic is rerouted to that office solely for emergency or special routing arrangements, e.g., type 2A Interconnected Wireless.

**Intra-LATA** - An intra-LATA tandem switch connects one trunk to another and serves as a trunk concentration and distribution function of intra-LATA toll traffic to minimize direct end office interconnection. Intra-LATA tandem traffic can be either intrastate intra-LATA or interstate intra-LATA as defined in the tariffs on file with the appropriate regulatory body. It is a switch that completes billable toll messages that originate and terminate within the same LATA.

**Inter-LATA** - An inter-LATA tandem switch connects one trunk to another and serves as a trunk concentration and distribution function of inter-LATA toll traffic to minimize direct end office interconnection. The inter-LATA tandem serves as an Access Tandem that provides distribution of originating and terminating traffic between subtending end offices and Interexchange Carriers (IXC).

**Intermediate** - Independent Operating Companies can provide an Intermediate Tandem between end offices and the LATA Access Tandem. The design of the Intermediate Tandem must be done so that it poses no impediment to the Inter-LATA Toll Network. The Intermediate Tandem follows the United States Telecom Association (USTA) specification TID 93-002, "The Intermediate Tandem Interconnection Consideration With Access Tandems".

**Operator Services Tandem** - An Operator Services (OS) tandem switch serves as the concentrated distribution point for providing a host of services that may include toll and intercept. The OS tandem is an integral part of the network as it performs alternate billing services, automated coin telephone service, AMA teleprocessing, and automatic call distribution for operator handling of calls.

**E9-1-1 Tandem** - The main characteristic of E9-1-1 service is the capability of the E9-1-1 tandem to selectively route a 9-1-1 call originated from any devices in the E9-1-1 service area to the correct primary (or controlling) Public Safety Answering Point (PSAP) designated to serve the originating devices' location. In emerging network architectures, the functions provided by the E9-1-1 tandem in traditional networks may be provided by different network elements, e.g., the Selective Router function and database may be separate from the network elements that provide the network access interfaces to the PSAPs.

*B. Re-Sale Related Service Requirements\**

*C. Operator Services/DA Routing and Branding*

- Can/Does your company support multiple billing options, e.g. calling/credit card, collect, etc.?
- Can/Does your company support multiple call types normally associated with operator services, e.g. bids for directory assistance, person to person, coin, etc.?
- Can/Does your company support operator assist platforms, e.g. inward, busy line verification, “hand-off trunks”, etc.?

*D. Unbundling Related Service Requirements*

- Dialing Plan Requirements
- Network Element Requirements

*E. Directory Listings\**

*F. Number Portability (NP)*

NP is a circuit-switched network capability that allows an end-user to change Service Provider (SP), Location, and/or Service type without having to change their telephone number.

The three types of NP are:

1. Service Provider Portability - allows an end-user to change Service Provider while retaining his/her telephone number.
2. Location (Geographic) Portability - allows an end-user to change from one geographic area to another (the current Location Routing Number (LRN) model does allow limited location portability within the rate boundaries) while retaining his/her telephone number.
3. Service Portability - allows an end-user to change service (e.g., CENTREX to POTS, etc.) while retaining his/her telephone number with the same Service Provider.

*G. National Services*

National Services are universally available within the North American Numbering Plan (NANP). Examples of such services include:

- 800- 8XX Toll free service
- 500 & 900 Services
- Line Information Database (LIDB)
- Enhanced 9-1-1 Emergency Service
- 211 Community Information and Referral Services
- 311 Non-emergency Police and Government Services
- 511 Travel Information Services
- 711 Telecommunications Relay Service
- Is your company aware of and capable of complying with existing industry guidelines involving national services?

## **8. DIVERSITY AND SURVIVABILITY REQUIREMENTS**

This section covers Diversity Requirements necessary to foster network survivability for interconnection from a trunking and signaling perspective.

### *A. Route Identification*

It is recommended that all routes for SS7 links be readily identified as outlined in the NIIF Reference Document, Installation, Testing & Maintenance Responsibilities for SS7 Links and Trunks Installation & Maintenance, Section III, Dual STP Failure Prevention Procedures, SS7 Component Identification.

- Does your company adhere to and support the NIIF agreements in regards to route identification of SS7 links?
- Does your company have in place the appropriate processes to identify/mark SS7 links?

### *B. Diversity Definitions*

SS7 route diversity, which assumes a network that encompasses interconnecting mated STPs, is defined as signaling link sets that are on physically and electrically separate routes. (See the NIIF Reference Document, Installation, Testing & Maintenance Responsibilities for SS7 Links and Trunks Installation & Maintenance).

The architecture of STPs connected to STPs requires three-way physical diversity of SS7 link facilities. The architecture of STPs connected to SPs/SSPs or SCPs requires two-way physical diversity of SS7 link facilities. Three-way diversity between STPs means that no two failures should simultaneously disable all three physically diverse link sets between the STPs. Two-way diversity between an STP and an SP/SSP or SCP means that no single failure should simultaneously disable the two physically diverse link sets between the STP and the SP/SSP and SCP. (See the NIIF Reference Document, Installation, Testing & Maintenance Responsibilities for SS7 Links and Trunks Installation & Maintenance).

- Does your company adhere to and support the Industry standards and NIIF agreements in regards to the diversity of SS7 links?
- Does your company have in place processes to ensure SS7 link diversification?

## **9. SPECIAL ROUTING TRANSLATIONS (SSP, STP)**

This section addresses the need for the exchange of information as it pertains to “Special Routing Translations for SSPs and STPs”.

It is recognized that each individual network provider has special requirements as it pertains to their network; however, in the interest of network integrity it is in the best interest of interconnecting parties to share the appropriate information during their interconnection negotiations.

The following questions should, at a minimum be asked and answered wherever possible during the interconnection negotiations or provided prior to the turn up of service:

- Does your company have requirements for Special Routing Translations for your SSPs and STPs?
- Who or what department should be contacted in regards to reconciling problems or questions for the maintenance of these special translations?
- Will your company provide sufficient prior notification to facilitate changes to these special translations in order to maintain network integrity?

## **10. PROTOCOL IMPLEMENTATION AGREEMENTS**

This section covers implementation agreements on SS7 timer values, route set congestion test messages, optional parameters, switch parameters and other standard protocols used between interconnected networks.

#### A. *Specific References*

Interconnecting network providers should review the following information sources to ensure network integrity and reliability:

- TR-246 Operations, Administration, Maintenance, and Provisioning (OAM&P) - Information Model and Services for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record Exchange (CARE)
- T1.111, Signaling System No.7, Message Transfer Part
- T1.112, Signaling System Number 7 (SS7) - Signaling Connection Control Part (SCCP)
- T1.113, Signaling System No. 7 (SS7) - Integrated Services Digital Network (ISDN) User Part (Revision of T1.113-1995; includes two Supplements: T1.113a-2000 & T1.113b-2001)
- T1.114, Signaling System Number 7 (SS7) - Transaction Capabilities Application Part (TCAP)
- T1.116, Signaling System Number 7 (SS7) - Operations, Maintenance, and Administration Part (OMAP) (Revision and consolidation of T1.116-1996 and T1.116a-1998)
- T1.631, High Probability of Completion HPC Network Capability
- GR-2931, High Probability of Completion Network Capability FSD 15-10-0000
- GR-317, Switching Systems Generic Requirements for Call Control Using the Integrated Services Digital Network Users Part (ISDNUP)
- GR-394, Switching Systems Generic Requirements for Inter-Exchange Carrier Interconnection using ISDNUP

#### B. *Timer Values*

To ensure network integrity and reliability, SS7 timer values (MTP level 2 and level 3, ISUP and SCCP) should be exchanged at the time of interconnection negotiation.

- Does your company subscribe to the NIIF agreements in regards to timer values?
- Does your company agree to exchange timer values prior to interconnection?
- What are your company's timer values?

#### C. *Routeset Congestion Test (RCT) Messages*

It is recommended that interconnected networks adopt the practice of responding to Transfer Controlled (TFC) messages by assigning Route-Set-Congestion Test (RCT) messages using Signaling Link Selection (SLS) codes that ensure an equal distribution on all the links in the linkset. Prior to SS7 interconnection the interconnecting companies should exchange RCT methodologies.

- Does your company agree to the above recommendations?
- What are your company's RCT methodologies?
- Does your company utilize and acknowledge ACC messages?

#### D. *Optional Parameters*

Companies with ISDN capabilities have a need to communicate to their interconnected network providers the passage of such parameters. In addition, all interconnecting SS7 partners should pass 3.1KHz audio and speech. As per local agreements, all interconnecting companies utilizing Automatic Congestion Control (ACC) should acknowledge and respond when ACC messages are received.

- Does your company have any optional ISDN parameters in your network?
- What are they?

#### *E. Switch Parameters*

Interconnected companies should address the needs of specific vendor switches, which may have unique requirements. For example, a switch may require that the Trunk Circuit Identification Code (TCIC) and the trunk number be the same value. Switches of the interconnected companies should be identified to determine the extent of testing that would take place.

- Does your company's switches have any specific vendor unique requirements that need to be shared?
- What are these unique requirements?

#### *F. Standard Protocols*

Network providers who intend to interconnect their networks should perform a minimum set of tests prior to interconnection. This will ensure that their switches are compatible and function appropriately using standard SS7 protocols.

Network providers implementing ISUP trunk interconnection should perform standard ISUP protocol testing to ensure that their switches are compatible and function properly with SS7 signaling.

- Does your company subscribe to the NIIF agreements in regards to a minimum set of tests to be performed prior to trunk interconnection?
- Will your company perform the ISUP protocol tests for ISUP trunk interconnection as outlined in the NIIF Reference Document?

Network providers implementing ISDN services should perform standard ISUP protocol testing to ensure that their switches are compatible and function properly with SS7 signaling.

- Does your company subscribe to the NIIF agreements in regards to a minimum set of tests to be performed prior to interconnection?
- Will your company perform the ISUP protocol tests for ISDN services tests outlined in the NIIF Reference Document?

Network providers implementing ISDN services should be equipped to utilize standard and/or default cause code treatment as defined in NIIF Reference Document Part III, Attachment H.

Prior to network interconnection, both providers should share their Gateway screening information to ensure that essential, desired SS7 messages traverse their networks.

- Does your company subscribe to the NIIF agreements in regards to a minimum set of tests to be performed prior to interconnection?
- Will your company perform the Gateway screening tests?

### III. INSTALLATION AND MAINTENANCE GUIDELINES, PROCEDURES AND RESPONSIBILITIES

#### 1. GUIDELINES FOR MEETING MAINTENANCE PERFORMANCE SERVICE LEVELS

##### A. *Interface Specification*

The NIIF Reference Document has identified the maintenance parameters and performance thresholds (tolerance range) in the guidelines for the various access services classes and the interconnected facilities between companies. Each type of access service classes and the interconnecting facilities service levels are within the various “Installation and Maintenance Responsibilities” sections as listed in the NIIF Reference Document, Master table of Contents.

##### B. *MTBF/MTTR*

Two forms of calculation that can be used for determining certain service levels within the various “Installation and Maintenance Responsibilities” are:

**MTBF (Mean Time Between Failures)** - Mean Time Between Failures is an average mean time between failures of a particular equipment type. For example, a single piece of equipment with an estimated MTBF of 840 hours could or would potentially fail once every five weeks ( $7 \times 24 = 168 \times 5 = 840$ ).

**MTTR (Mean Time To Repair)** - Mean Time To Repair is the average “mean” time to restore a failed piece of equipment to service. For example, the MTTR for a given piece of equipment could include the following depending on location, redundancy, availability of repair parts needed, etc.:

- Detection of a problem
- Diagnostics on the failed equipment (manual and/or auto)
- Transportation time to the failed equipment site
- Repair/s to the failed equipment
- Restoration of the equipment to full service

Does your company:

- Have a pre-determined time limit to repair discrepancies?
- Have a reporting mechanism to advise customers or SPs when MTTR is not met?
- Provide a means to monitor MTBF / MTTR?
- Analyze root causes when MTBF becomes frequent?

##### C. *Performance Thresholds (Tolerance Range) \**

##### D. *E9-1-1 Database Updates*

During interconnection negotiations, E9-1-1 Database updates will need to be included in those agreements. These updates should be part of the service order process to transition the customers’ data between Service Providers’ E9-1-1 databases without loss of services to the customer.

##### E. *Measures for Specific Service Classes\**

##### F. *Monitoring and Reporting Mechanisms*

The integrity of the network and customer satisfaction depends on the ability to maintain and correct discrepancies within the interconnecting facilities and the access services as soon as possible.

- Does your company have in place mechanisms to monitor performance of various services or facilities?
- Does your company monitor Links and Trunks in the SS7 network?
- Does your company have automatic trunk testing?

## **2. DOCUMENTATION REQUIREMENTS**

This section outlines the requirements for documentation that relates to interconnection. During interconnection negotiations both parties need to discuss and agree upon the required documentation to ensure network reliability once interconnection has taken place.

### *A. Company Specific Contact Directory*

The NIIF Company Specific Contact Directory lists specific functions for interconnected company contacts. These functions are critical to the reliability of the network during emergency situations and modifications of the network.

- Testline Coordinator Contact
- Network Management Contact
- Network Management Escalation
- Catastrophic SS7 Network Failure Contact
- Media Stimulation Calling Event Contact
- Non-circuit Specific Trouble Referrals Contact
- Synchronization Coordinator Contact
- Inter-Company LIDB Contact
- Mutual Aid Contact
- CO Code Company Contact
- Other Company Contact e.g. Network Modification Notification Contact

### *B. Contact Listing*

- Does your company have contacts listed in the NIIF Company Specific Contact Directory for these specific functional responsibilities?
- If not, for which specific functions will your company provide contact numbers?
- Will these contacts be available 24 hours?

## **3. MAINTENANCE PROCEDURES FOR STATUS AND TROUBLE REPORTING**

Detailed procedures are outlined in the NIIF Reference Document for the various facilities, and access services as listed in the Master Table of Contents.

### *A. Trouble Reporting, Trouble Resolution and Escalation Procedures*

- Does your company have the NIIF Reference Document?
- Does your company support the maintenance procedures as outlined in the NIIF Reference Document, relating to trouble reporting, trouble resolutions and escalations?
- Does your company adhere to the time duration for status reporting to interconnecting companies?
- Does your company have a 7 by 24 contact number(s) for maintenance, trouble reporting, trouble resolution, escalation, and trouble status?

## *B. Emergency Communication; Emergency Preparedness Plans*

The NIIF Reference Document recommends that each interconnected company have plans for Emergency Communications between other interconnected companies. Part VI, Appendix A, of the NIIF Reference Document identifies Emergency and Restoration Planning Considerations, and the intent to subscribe to a communication system other than the PSTN. In Part VI, Network Management Guidelines, Section 7, Emergency Communications, Subsection A, the recommendation is to subscribe to Public Packet Switched Network (PPSN). This emergency contact is to be accessed only during such catastrophic failures on the SS7 Network.

- Does your company have plans for disaster preparedness & recovery?
- Does your company list a contact for the Disaster Preparedness & Recovery function in the NIIF Company Specific Contact Directory?
- Does your company have emergency communications links with other interconnected companies?
- Does your company provide communication access other than PSTN, during a catastrophic SS7 failure?
- Does your company list a contact for any catastrophic failures in the NIIF Company Specific Contact Directory?

**Equipment Supplier Participation** - SPs are encouraged to negotiate agreements with their equipment suppliers to support emergency preparedness and emergency communications. Mutual Aid is an agreement with equipment suppliers and other SPs to loan equipment and/or manpower during catastrophic outages so as to restore the PSTN back to service as soon as possible.

- Does your company subscribe to Mutual Aid agreements?
- Does your company have Mutual Aid Agreements with your equipment suppliers or other SPs?
- Does your company list your Mutual Aid contact in the NIIF Company Specific Contact Directory?

**Security Management Participation** - Companies are encouraged to involve their Security organizations in emergency and network outage situations.

- Does your company involve your Security organization in network outages that maybe caused by vandalism or deliberate sabotage?
- Is the Security contact number posted for quick reference within your control locations?

**National Security/Emergency Preparedness** - During interconnection negotiations, companies should provide assurance to each other that they have in place an Emergency Preparedness plan and provide the contact name and number of the person responsible for this plan.

- Does your company have in place an Emergency Preparedness plan?

Telecommunication Service Priority (TSP) Guidelines - The NIIF Reference Document has identified the requirements for NSEP access service installation and maintenance. (See Part I, Section 3, TSP GUIDELINES)

This section provides TSP installation and maintenance guidelines for access services and provides generic administrative procedures and interfaces between Access SCs and Access Service Providers.

The TSP system provides for priority treatment of National Security Emergency Preparedness (NSEP) telecommunication services in order to prioritize their installation and maintenance.

- Does your company adhere to the NIIF guidelines for TSP?

## *C. Tones and Announcements for Unsuccessful Call Attempts and Toll Warnings*

There are two resources for Tones and Announcements information that are recommended by the NIIF:

- The NIIF Cause Codes document may be found in the NIIF Reference Document Part III Attachment H – SS7 Cause Codes & Tones and Announcements. This document contains recommended Cause Code applications for network failures.
- Issue 9 of BR780-200-020, Tones and Announcements

*D. Catastrophic Outages*

The NIIF Reference Document contains a directory of company contacts to be utilized during major outages.

- Does your company have a copy of this NIIF Company Specific Contact Directory?
- Is your company listed in this directory?

*4. ACCEPTANCE TESTING*

The NIIF Reference Document identifies the parameters and specifications for the various access services and the interconnecting facilities for acceptance in the sections for “Installation and Maintenance Responsibilities”

- Does your company adhere to the acceptance parameters and specifications as outlined in the various NIIF Documents for Acceptance Testing?

## **IV. INTERCONNECTION TESTING PROCEDURES AND RESPONSIBILITIES**

### **1. RESPONSIBILITY ASSIGNMENTS**

The NIIF Reference Document identifies the responsibilities of SPs for interconnection testing. Each type of access service and interconnecting facility are identified in the various NIIF Documents as listed in General Section 1, subsection 3.

#### *A. Automatic Trunk Testing*

Where automatic trunk testing capabilities are available, specific guidelines on the usage of automatic trunk testing should be agreed to during interconnection negotiations.

- Does your company have automatic trunk testing capabilities?
- Will your company have automatic trunk testing capabilities scheduled on a regular basis for maintenance purposes?
- Who will perform the testing (the type of interconnection will determine who will do the testing, e.g., LEC to LEC, IXC to LEC, etc.)?

#### *B. Pre-Cutover Inter-Network Connectivity Testing*

Interconnection tests for SS7 and Local Number Portability are outlined in the NIIF Reference Document; however, it must be understood that these are a recommended set of tests and companies may wish to perform additional tests to provide assurance for the integrity of the network. Additional interconnection tests may be outlined in individual tariffs or may be negotiated by the interconnecting parties.

During interconnection negotiations the following questions may be discussed:

- Does your company have network interface specifications in place?
- Does your company have pre-cutover testing procedures in place?
- Is your company following testing recommendations as outlined in the NIIF Reference Document?

### **2. INTEROPERABILITY TEST RESULTS**

This section covers interoperability testing as it pertains to interconnection. There are a number of sources from which interconnection connectivity testing results can be obtained. They are:

- Vendor testing (LAB Environment)
- SP testing (LAB Environment)
- SP testing, third party (LAB Environment)
- Network testing (LAB Environment) performed by the Internetwork Interoperability Test Coordination (IITC) Committee
- Inter-company testing

Based on the sources of information, their availability and proprietary nature, interconnected companies are encouraged to share information that may adversely affect each other. The IITC has developed and agreed upon a set of guidelines for the sharing of such information in the interest of enhancing network integrity.

- During interconnection negotiations the following questions should be addressed:
- Do you participate in any of the testing venues listed above?

- Do you participate in any other type of testing venue not listed above?
- Will you proactively share any information gleaned during testing that may adversely affect our interconnected network?
- Do you subscribe to and support the Information Sharing Guidelines as developed by the IITC?

The IITC provides the opportunity for the telecommunications industry to perform interoperability tests in a laboratory environment where negative impact to the resident interconnected networks cannot occur. The use of IITC methodology will ensure rainy day scenarios can be tested with no negative impacts in the resident interconnected networks. SPs and vendors/manufacturers of telecommunications equipment (hardware/software) participate in the IITC to ensure that the highest standards of network reliability, integrity and customer satisfaction are maintained. Participation in this venue is encouraged. For more information, contact ATIS on the ATIS home page at [www.atis.org](http://www.atis.org) or at 202-662-8662.

### **3. PROCESS FOR CIRCUIT LEVEL TESTING AND PERFORMANCE ANALYSIS OF UNBUNDLED NETWORK ELEMENTS**

This section addresses the circuit level testing and performance analysis of unbundled network elements that are available to interconnected parties. Unbundled network elements are elements from several networks that may be used when establishing a single end-to-end service. Both the users and owners of unbundled network elements must reach a mutual understanding of requirements and capabilities of each element. The ability to evaluate and test the various unbundled network elements contributing to the service is essential to providing a quality product.

- What unbundled network elements are available for interconnection?
- Is your company willing to perform end-to-end testing on services that use unbundled network elements?
- When testing is performed, is your company willing to share test results according to the NIIF Information Sharing guidelines?

### **4. SS7 AND OTHER CRITICAL INTERFACE INTER-NETWORK COMPATIBILITY TESTING**

This section covers MTP, ISUP, SCCP and Gateway Screening inter-network compatibility testing from an interconnection negotiation perspective. The tests are outlined in the NIIF Reference Document, Installation, Testing and Maintenance Responsibilities for SS7 Links and Trunks, and in the appropriate attachments.

#### *A. SS7 Interconnection*

- Interconnected companies should address SS7 interconnection and the appropriate service protocol/message set tests to be performed.
- Does your company use a specific questionnaire for SS7 interconnection?
- Will your company share this information?
- Is your company familiar with and does your company have a copy of the NIIF documentation described above?
- Does your company support the NIIF recommended MTP, ISUP, SCCP and Gateway Screening tests?
- Will your company perform the recommended NIIF tests, and where applicable, correct any problems encountered prior to interconnection?
- Is your company willing to share the test results according to the NIIF information sharing guidelines?

#### *B. SS7 Diversity Verification and Validation*

Interconnected companies should discuss and negotiate procedures for verification and validation of SS7 routes. Link diversification validation guidelines are covered in the NIIF Reference Document under SS7 Signaling and the appropriate attachments.

- Does your company have verification procedures for verification and validation of SS7 routes?
- Does your company subscribe to the NIIF recommendations on link diversification validation guidelines as listed in the above document?

## **5. INFORMATION SHARING**

This section covers the sharing of information between interconnected companies for analysis and problem identification.

The NIIF Reference Document provides a set of recommendations for the sharing of information between interconnected companies as well as with their respective vendors.

Real time analysis of network problems and their results should be shared between interconnected parties. Such sharing agreements should be based on local negotiations.

Interconnected parties should determine the appropriate processes for the sharing of trouble analysis information.

- Do you adhere to and support the NIIF Information Sharing Guidelines?

## **V. NETWORK ADMINISTRATION AND MANAGEMENT GUIDELINES, PROCEDURES, AND RESPONSIBILITIES**

### **1. DOCUMENTATION REQUIREMENTS**

#### *A. Network Configuration*

Interconnection interoperability for any network configuration is critical to network reliability. Although conformance to standards does not ensure interoperability, it is a desirable first step. In addition, interoperability testing is needed to ensure operation at the interface point. Unique protocol options for the information channel, signaling channel and OAM&P channel interfaces are critical to reliable interconnections. Participation in national industry standards development forums would benefit new service providers or new service customers.

- Does your company participate in the development of industry standards?
- Does your company participate in industry interoperability testing?

#### *B. Contact Numbers\**

### **2. NETWORK TRAFFIC ENGINEERING**

This section provides specific areas of network traffic engineering that need to be addressed during interconnection negotiations.

#### *A. Traffic Engineering Design Criteria and Capacity Management*

- Does your company utilize a hierarchical or flat routing scheme?
- Are your switches capable and configured to accept calls on a tandem basis?

#### *B. Alternate Routing Design*

Where alternate routing requirements are provided or offered, specific details as to the customer SP shall be identified prior to implementation of alternate routing.

- Does your company want to have alternate routing provided?

#### *C. Call Blocking Criteria*

- What formula or tables does your company utilize to measure call blocking?
- What percentage of blocking is your network engineered for?

### **3. NETWORK REARRANGEMENTS - MAJOR RE-HOMING**

The NIIF Reference Document addresses any rearrangements or re-homing activity as a modification to the network. The NIIF Document has identified the responsibilities of each interconnecting company when modification to the network is planned to avoid failure to the network. Network modification and the required notification process is identified in all the various parts of the NIIF Reference Document. Also listed are Suspension Periods when modification is restricted.

#### *A. Logical*

See section II subsection 7-A, Tandem Homing Arrangements above.

## *B. Physical*

The NIIF Reference Document has outlined specific requirements for SPs and SCs to notify each other prior to engaging in any major network activities that may affect the interconnected network.

The information required for exchange between interconnected companies is outlined in the maintenance portion of each part of the NIIF Reference Document.

- Does your company adhere to and support the guidelines for network modifications as listed in Part II of the NIIF Reference Document?
- When any major modifications are planned within your network, will your company follow the NIIF recommendations in regards to major modifications and rehomings?

## **4. SYNCHRONIZATION DESIGN AND COMPANY-WIDE COORDINATION CONTACTS**

This section covers the synchronization expectations as they pertain to interconnection negotiations.

### *A. Establish Conformance*

Improper synchronization can result in circuit impairments that should be investigated and synchronization problems corrected.

If either of the interconnected companies has its own primary frequency standard that meets the International Telephone Union (ITU) standard for national networks (G.811, G.822), synchronization of the digital SS7 link(s) will be by the plesiochronous method of operation. If either network does not conform to the ITU standard, the non-conforming company will use loop timing to accept SS7 link(s) timing from the conforming company.

- What synchronization standards does your company conform to in your network?
- Does your synchronization clock conform to the ITU standard?
- Does your company have a synchronization back-up plan in case of failure?
- Does your company have major/minor alarms on your synchronization network?

Listed below are documents that outline industry standards that may be utilized for reference purposes:

- T1.101, Synchronized Interface Standard
- Telcordia Special Report, SR 2275, Telcordia Notes on the Networks

### *B. Identify Synchronization Contacts*

The NIIF Company Specific Contact Directory has listed each interconnecting company's Synchronization Coordinator and their contact number.

### *C. Coordination Administration*

If one of the interconnected companies does not conform to the industry standard, it is imperative that a bilateral agreement is established and loop timing be used to accept SS7 link(s) timing from the conforming company.

## **VI. NETWORK TRANSITION CONSIDERATIONS**

### **1. NETWORK TRANSITION**

SPs should provide timely notification to their SCs of all changes in their access network architecture, which may affect SC routing or rating of calls, such as:

- Tandem homing arrangements
- Switch reconfigurations affecting rating or routing
- New or changed NXX
- New or changed NPA
- Changes in rate centers

NIIF-0008 guidelines entitled “Recommended Notification Procedures to the Industry for Changes in Access Network Architecture” should be followed during access network reconfigurations.

- Has your company identified all affected SCs?
- Has your company advised SCs of planned changes?
- Has your company advised SCs of estimated due dates for each change?
- Has your company followed the above mentioned industry notification guidelines dealing with changes in access network architecture?

### **2. NPA SPLITS/OVERLAYS/REARRANGEMENTS AND NXX CODE OPENINGS/CHANGES**

The following principles should be followed during NPA code relief planning:

- “NPA Code Relief Planning & Notification Guidelines”, INC 970404-16
- Communications should be established with all affected companies, appropriate regulatory bodies, and the North American Numbering Plan Administrator (NANPA). This should be initiated immediately after the need for NPA code relief has been determined.

#### *A. NXX Code Establishment and/or Modifications*

During the entire NXX code establishment and/or modification process, it is essential that effective communications be established with all affected SPs based on the following industry guidelines:

- Central Office Code (NXX) Assignment Guidelines, INC 95-0407-008
- Recommended Notification Procedures to the Industry for Changes in Access Network Architecture, NIIF-0008
- NIIF Reference Document, Part X, Interconnection between LECs Operations Handbook.
- Has your company established communications with all affected companies?
- Will your company have the required interconnection trunking and switching facilities in place prior to establishing and/or modifying the code?
- Has your company followed the above mentioned industry guidelines dealing with CO code establishment and/or modification?

- Does your company have an AOCN? If so, has your company notified the affected company of this establishment and/or modification?
- Has your company notified NANPA of this modification?
- Has your company allowed for proper industry notification as recommended in NIIF-0008?

### **3. MAJOR REHOMING, REARRANGEMENT PLANS\***

As mentioned above in Subsections 1 and 2, any network modifications that may affect interconnected companies must be properly documented and coordinated to avoid failures to the network. The NIIF has provided a Network Modification Notification form and documentation for any major rearrangements (This form can be found as Attachment B of Part VI of the NIIF Reference Document). Also see Section V; Subsection 3, - Network Rearrangements - Major Rehoming.

- When any major modifications are planned within your network, will your company follow the NIIF recommendations in regards to major modifications and rehoming?

### **4. TRANSITION TO USE OF EMERGING TECHNOLOGIES SUCH AS PACKET BASED TECHNOLOGY**

As the network evolves, compatibility with older types of equipment must be ensured.

- Does your company have plans to test the interoperability between both old and new types of equipment?
- Does the future technology fit with your current embedded base and network planning methods to:
  - Provide standardized transmission rates, formats, and physical interfaces?
  - Utilize standardized message-based OS protocols?
  - Integrate operations functions based on standard interfaces?

A. *Vendor Compatibility\**

B. *Optional Capabilities\**

C. *Feature Interactions\**

## **VII. BILLING CONSIDERATIONS**

### **1. ACCURACY OF DATA\***

### **2. INTERVAL OF RECORDS EXCHANGES\***

### **3. DISPUTE RESOLUTION\***

### **4. OBF DOCUMENTATION/BILLING RECORDS DATA EXCHANGE**

The following questions should be asked and answered when negotiating interconnection agreements from a provisioning perspective.

- What is your company's preferred method (e.g., EDI, EC-LITE, CORBA etc.) and media for passing order information?
- What type of network interconnection for passing orders (e.g. private line, frame relay, the Internet) does your company prefer?
- Does your company plan to support development and use of an industry standard process to support the pre-order process?
- What is your company's preferred method to receive pre-order information?
- What is the response time we may expect for pre-order inquiries from our gateway to your OSS(s) and back?
- Will your company support a pre-order process for address validation, customer telephone number reservation, appointment scheduling, customer service inquiries, directory inquiries, and feature service availability inquiries?
- Will your company process pre-order inquiries and transactions in real-time?
- Will your company support and use the Firm Order Confirmation (FOC)/Design Layout Record (DLR) process, as defined by the Ordering and Provisioning committee of the Ordering and Billing Forum (OBF)?
- Does your company support and use the Local Service Request (LSR) process, as defined by the OBF?
- What procedures does your company propose to use to handle rejected orders?
- Are there any limits to the number of orders for service your company can accept and process? If the answer is yes, what are they?
- What is your company's preferred method and media for passing information used in billing for the service you provide?
- Does your company support and use the Customer Account Record Exchange (CARE) process, as defined by the Subscription Committee of the OBF?

## **VIII. VENDOR REQUIREMENTS AND RESPONSIBILITIES**

### **1. WRITTEN REQUIREMENTS**

Vendors have responsibilities within technical/operational interconnection agreements based on their product capabilities. Vendor documentation is also critical to achieving network reliability. Poor documentation could result in network failures, and could affect interconnected companies. Interconnecting companies may desire additional vendor support in achieving proper interconnection, especially with regard to emerging technologies. Examples of this support may include how to properly test a network element and how can it be managed once the network is in place.

- Do the products used in your company's network conform to North American interconnection standards?
- Are the products used in your company's network compliant with human factors requirements for equipment to improve network reliability, such as GR-2914-CORE?
- Are the products used in your company's network compliant with requirements for supplier provided documentation, such as GR-454-CORE?
- Does your company have agreements in place with your vendors for product support?
- Does your company's vendors provide information on compatibility with other vendors' products?
- Are your vendors willing to share technical information that is required for interconnection testing and maintenance?
- Will your vendor participate in the testing of their telecommunications equipment before any interconnection testing takes place, such as tests offered by the IITC? (See the Interoperability Test Results Section)
- Is your vendor's equipment compatible with other vendors' equipment? Has this compatibility been tested? Are there any major outstanding faults that remain to be resolved?

### **2. SOFTWARE VALIDATION**

The NIIF Reference Document has defined VENDOR/MANUFACTURE SOFTWARE VALIDATION CRITERIA, in Part III, Attachment J, SS7 Software Validation. This information may be found in the sections listed below.

- Section 6, Part A: Vendor/ Manufacture Software Validation Criteria, Vendor/Manufacture Requirements

### **3. OPTIONAL REQUIREMENTS**

The NIIF Reference Document has defined VENDOR/MANUFACTURE PRODUCT IMPLEMENTATION, OPTICAL REQUIREMENTS, in Part III, Attachment J, SS7 Software Validation. This information may be found in the sections listed below.

- Section 7, Part A: Vendor/Manufacture Product Implementation, Optional Requirements

### **4. TESTING**

The NIIF Reference Document has defined VENDOR/MANUFACTURE PRODUCT TESTING, TESTING ENVIRONMENT, in Part III, Attachment J, SS7 Software Validation. This information may be found in the sections listed below.

- Section 8, Part A: Vendor/Manufacture Product Testing, Testing Environment
- Will your vendor participate in the testing of their telecommunications equipment before any interconnection testing takes place such as tests offered by the IITC? (See the Interoperability Test Results Section)

- Is your vendor's equipment compatible with other vendors' equipment? Has this compatibility been tested? Are there any major outstanding faults that remain to be resolved?

## **5. TRAINING**

Any entity that provides telecommunication services or products should ensure that their personnel are properly trained in the installation and maintenance of the company's services or products. This responsibility pertains to, but is not limited to, service providers, and vendor/manufacturers.

- Does your vendor/manufacturer have training programs for your company's technicians on the products and services that you purchased from them?

## **6. EMERGENCY EQUIPMENT AVAILABILITY**

- Are your vendors willing to participate in a resource lending agreement in the event that your company's telecommunications equipment becomes damaged beyond repair?
- Does your company have a formal or informal resource lending agreement with your vendors or other telecommunications utilities in the event of an emergency restoration process?

### *A. Contact Lists*

- Does your company have a contact listed in the NIF Company Specific Contact Directory responsible for such resource lending agreements (Mutual Aid Listing)?

## **7. INTERFACE SPECIFICATIONS FOR STANDARD ELEMENTS\***

## **8. PROCESS FOR CERTIFYING COMBINATION, INTERMINGLING, AND OPERATIONS OF NE'S\***

## **IX. ENVIRONMENTAL OPERATIONAL REQUIREMENTS**

### **1. SECURITY**

- Does your company have a per site security arrangement for all employees, contractors, and visitors?
- Does your company have a contractor agreement arrangement for educating and enforcement of all security and environmental guidelines to be used at any of your company sites?
- Does security information vary from site to site? (Security arrangements and agreements are to be verified on a per site basis.)
- Does your company provide a means to prevent unauthorized persons from obtaining access to secured areas? Is this provided 24 hours a day / 7 days a week?
- Does your company provide company identification badges?

Company/contractor ID badges should be worn and displayed at all times when on company premises. The ID should display the following:

- Company Name
- Employee Name
- Photo of Employee/Contractor (if available)
- Expiration Date
- Building or Site Code/ID (if applicable)
- Hours/Days of Week (if applicable)
  
- Does your company monitor equipment movement on and off company premises?
- Does your company have in place guidelines for establishing temperature and humidity requirements for all telecommunications equipment in central offices and remote buildings?
- Does your company have in place a system and procedures for monitoring, alerting, responding, resolving and escalating environmental alarms and their trouble conditions 24 hours a day / seven days a week?

### **2. POWER & GROUNDING**

This section covers Power & Grounding information for all telecommunications equipment (Switches, STPs, DCSs, DSXs, SLCs, etc.) in Central Office buildings, Remote Sites, Controlled Environmental Vaults (CEV), that should be shared at the time of interconnection:

#### *A. Power*

Typical power systems for switching offices consist of the elements listed below:

- AC Power System
  - AC input switch gear
  - Standby AC plant (where appropriate)
  - AC distribution system (essential and non-essential loads)
  - AC backup systems for un-interruptible loads and protected loads.

- DC Power System
  - Rectifiers and plant controls
  - Storage batteries
  - DC distribution system.
  
- Does the power equipment installed in your serving area satisfy the space and environmental requirements described in GR-63, Network Equipment Building Systems (NEBS) Requirements: Physical Protection and in GR-1089-CORE Electromagnetic Compatibility and Electrical Safety – Generic Network Criteria for Network Telecommunications Equipment?
- Does your AC power system comply with the National Electrical Code (NEC) and ANSI Standard National Fire Protection Association NFPA 70 FCC?
- Does your company's DC power system meet the requirements defined in the following guidelines?
  - GR 347 CORE, Generic Requirements for Telecommunications Power Cable – April 2002
  - T1.311, DC Power Systems - Telecommunications Environment Protection
  - TR-NWT-000154, Generic Requirements for 24-, 48-, 130- and 140- Volt Central Office Power Plant
  - GR-512-CORE, LATA Switching System Generic Requirements (LSSGR)- Reliability
- Does your company have a service interruption prevention plan that also includes power installation, rearrangements, and loss of power?
- Does your company have Tier II support arrangements with the various vendors and their equipment suppliers?
- Does each of your company's sites have standby power capabilities? Where generators are used, are they equipped with automatic start and transfer capabilities?
- Does your company have access to portable backup generators and appropriate fuel supplies? Is the connection point to the portable generator clearly marked and accessible?
- Are fault detectors installed in each type of power plant equipment?
- Are all fault detection alarms monitored on power plant equipment and telecommunications equipment 24 hours a day / 7 days a week?
- Does your company provide for routine testing of all standby power plant equipment and alarming capabilities to ensure the reliability of essential telecommunications equipment loads?
- Does your company monitor, manage and maintain central office operating loads automatically for power adjustments?
- Does your company utilize charge and over-current protection devices to limit distribution currents to values that can be tolerated and protect the equipment?
- Is all power equipment securely fastened and anchored per Method of Procedure and industry standards or requirements?
  - Reference documents: GR-513-CORE – LATA Switching System Generic Requirements (LSSGR) – Power

*B. Grounding*

**Telecommunications Systems:** The purpose of a Central Office ground system for telecommunications equipment is to provide:

- Common Grounding for all telecommunications equipment
- Earth Potential common reference for communications equipment
- Lightning discharge paths for entrance cable protectors
- Ground current paths for equalization of DC power voltages
- An engineered primary low-impedance path to ground
  
- Does your company use all or some of the components listed below as their CO ground?
  - Office Principal Ground Point Bus
  - Vertical Equalizers
  - Horizontal Equalizers
  - CO Ground Buses
  - Main Ground Bus (MGB) - Centered in the Ground Window.
  
- Is all equipment grounded according to industry standards or requirements, and if applicable the appropriate job Method of Procedure?
- Is equipment grounding verified by an authorized inspector or quality control representative?
- Is a Supplementary Ground Bus (SGB) being used for additional connections separate from the Main Ground Bus (MGB)?
- Are all MGB's and SGB's clearly stenciled for identification purposes?
- Is the grounding bus for the switch external to the AC entrance of the switch gear and connected to the AC neutral bus?
- Are ground fields installed on all telecommunications equipment within central offices, and/or remote locations?
- Have the following been verified?
  - Insulation test
  - Low/High Voltage tests
  - Isolated Ground Plane Noise tests
  - Multi-grounded AC and DC Power Sources
  
- Have grounding principles prescribed by your vendor, for your particular switch type, been followed?
- Each site may house "various communication devices, e.g. Roof Mounted Towers, Radio Room equipment, Computer Systems.
  - Are all these various devices grounded per the device specifications?
  - Has your company complied with industry recognized grounding principles for interconnecting facilities?

**Power Plants:**

- Is the "frame" of the power plant grounded to the nearest ground reference?
- Is the -48V return bus used as the "ground window"?

- Is the -48V return grounded at the ground window?
- Is the return bus in the power plant insulated from the power plant framing?
- There are three possible ways to accomplish grounding internal AC and DC power supplies:
  - Grounded to the nearest ground reference (preferred way).
  - Current flow over -48V return (which can induce noise).
  - Current flow through the frame.
- If using either 2 or 3 then the following must be provided:
- Data that specifies the maximum impedance that can be in the external short circuit path and still permit sufficient short circuit current to flow, so that over-current detectors can operate satisfactorily.
- Test data showing when a short to a frame occurs, the transient disturbances generated do not interfere with the operation of other equipment.
- What grounding solution (1, 2, 3, as mentioned above or other) is your company utilizing at their sites?
- Are all power feeds, battery and battery return conductors run in pairs and closely coupled with the plant frame ground wire and plant grounding conductor to minimize noise?
- Does your company perform periodic grounding audits or surveys on all telecommunications equipment within the central office, ORM or CEV?
- Are drawings for each site listing the various components and their CO grounding systems readily available?

Reference Documents:

- TR-NWT-00295 – Isolated Ground Planes Definition and Application to Telephone Central Offices
- National Electrical Code (NEC)

### 3. INTERFERENCE PROTECTION

The FCC has released Report and Order FCC 97-303, which includes ET Docket No. 93-62, Guidelines for Evaluating the Environmental Effects of Radio Frequency Radiation, and OET Bulletin 65 issued 10/15/97 regarding guidelines and methods on the evaluation of the environmental effects of RF electromagnetic fields.

- Does your company adhere to the recommendations as listed in the above document?
- Are procedures in place to respond to a negative environmental evaluation?

### 4. RADIO INTERFERENCE

The FCC has released Report and Order FCC 97-303, which includes ET Docket No. 93-62, Guidelines for Evaluating the Environmental Effects of Radio Frequency Radiation.

Within this document are guidelines are established for dealing with FCC-regulated transmitters.

- Does your company adhere to the recommendations as listed in the above document?
- Are there any transmitters in your company's equipment?
- Does your company's equipment meet the FCC RF (Radio Frequency) Radiation Rules?
- Does your company monitor for antenna release power emissions?
- Does your company provide RF monitoring where necessary?
- Does your company monitor Radio Equipment for ERP (Effective Radiated Power)?

## **X. OPERATIONAL AND RELIABILITY REQUIREMENTS**

### **1. PROTOCOL ELEMENTS\***

### **2. INTERFACE MESSAGING\***

### **3. GATEWAY SCREENING\***

### **4. OVERLOAD CONTROLS**

Overload Control features are in place in most switch vendors' products to protect the network by reducing and/or re-routing call volumes, in the event of Network Node overloads and/or failures. These controls are implemented via SS7 messages.

Available Overload Controls are:

- ACC – Automatic Congestion Control
- ACG – Automatic Call Gap
- TFR – Transfer Restricted
- TFP – Transfer Prohibit

A description of these controls may be found in the NIIF Reference Document, Part III, Installation, Testing and Maintenance Responsibilities for SS7 Links and Trunks.

- Does your company's switch nodes contain features necessary to implement overload controls?
- Does your company support automatic response to ACG and ACC messages?
- Does your company support automatic response to TFR and TFP messages?

### **4. FAULT DETECTION\***

### **5. NETWORK PERFORMANCE OBJECTIVES**

- Do you have a method for measuring blocked calls between interconnected companies?

### **6. COMPATIBILITY\***

### **7. NETWORK MANAGEMENT CONTROLS**

Part VI of the NIIF Reference Document contains Network Management (NM) Guidelines. A list of key network management contacts can be found in the Company Specific Contact Directory, which is a stand-alone NIIF Document. A copy of both of the above documents can be obtained from ATIS at [www.atis.org](http://www.atis.org) or by contacting the NIIF Administrator at (202) 628-6380.

The NM Guidelines address:

- Minimum set of network management controls
- Terminating reroutes involving an Interexchange Carrier
- SC Switch or network failures or extended outages
- Mass Call Events

- SS7 Network Failures
- Emergency Communications
- Termination of Access Service
- Responsible Organization (Resp Org)
  
- Does your company have personnel who are trained in network management functions?
- Does your company have network management control (automatic and/or manual) capabilities available in all of your interconnecting network elements?
- Does your company have a network management center and a network management surveillance system?
- Does your company proactively and reactively monitor and respond to network management traffic alerting conditions in your network?
- Does your company agree with and adhere to the NIIF Network Management Guidelines?
- Does your company agree with and adhere to the NIIF defined minimum set of network management controls?
- Are disaster and/or congestion terminating reroutes available in your company's network?
- Does your company have any reciprocal agreements in place in the event of switch or network failures?
- Does your company agree with the NIIF Mass Calling Event Guidelines, e.g., does your company use the NIIF Mass Calling Event Notification Form or an electronic version of the form? (Attachment A Part VI of the NIIF Reference Document)
- Does your company agree with and use the NIIF guidelines for Network Modification Notification as listed in the NIIF Reference Document?
- Are there procedures in place within your company to coordinate a restoral of the SS7 Network?
- Does your company have a Dual STP Failure Prevention Plan?
- Does your company have an Emergency Communications Plan in place as covered in the NIIF Reference Document?

**8. BACKWARD COMPATIBILITY\***

**9. PERFORMANCE CRITERIA\***

**10. NETWORK OUTAGES REPORTABLE TO THE FCC**

Common Carriers that operate switches and/or owned/leased transmission facilities under FCC jurisdiction are required to notify the FCC of significant service outages. Common Carriers must also file an initial report and a final report on these significant outages to the FCC providing a detailed analysis and cause of each failure. This section addresses the outage reporting criteria from a regulatory perspective as well as from an interconnection perspective.

- Does your company have guidelines and procedures in place to meet the FCC criteria for reporting outages?
- Does your company support the NIIF guidelines for intercompany notification for outages?
- Does your company intend to utilize the standard data elements that the NRSC has developed for the collection of outage data?

*A. Failure Analysis Procedures*

This section covers the analysis procedures to assist Common Carriers in determining which network element failed on an outage. The basic procedure is to isolate the service outage to a specific element, i.e., local switch, tandem switch, signaling system, transmission facility, local cable, power, overload, or natural disaster affecting the telecommunications network, determine how many customers are affected, and determine the length of the outage. An example of questions that may be asked during interconnection negotiations could include:

- Are failure analysis procedures in place?
- Are reporting procedures or guidelines in place in the event of a significant failure?

*B. Root Cause Analysis Processes*

Common Carriers are required to perform a root cause analysis of significant failures and provide it to the FCC on either the initial or final report. The root cause analysis identifies the cause of the outage. Examples of typical root causes can be found on the NRSC Free Documents web page at <http://www.atis.org/ATIS/NRSC/freedocument.htm>.

*C. Network Survivability Performance*

Committee T1 Technical Report No. 24 on Network Survivability Performance addresses the survivability of telecommunications networks. The report provides a basis for analyzing service outages and determining their impact. To obtain a copy of the report, visit the ATIS Document Store, accessible through [www.atis.org](http://www.atis.org) or contact the T1 Administrator at (202) 628-6380 and order a copy of T1 Technical Report No. 24.

## **XI. GLOSSARY**

This section is a glossary of acronyms used in the NIIF Templates Document:

AC – Alternating Current  
ACC – Automatic Congestion Control  
ACG – Automatic Call Gap  
ANSI - American National Standards Institute  
ATIS - Alliance for Telecommunications Industry Solutions  
ATM - Asynchronous Transfer Mode  
CARE – Customer Account Record Exchange  
CEV – Controlled Environment Vault  
CO – Central Office  
CORBA – Common Objective Request Broker Architecture  
DC – Direct Current  
DLR – Design Layout Record  
EDI - Electronic Data Interchange  
ERP – Effective Radiated Power  
FCC - Federal Communications Commission  
FOC – Firm Order Confirmation  
GR – Generic Requirement  
ID - Identification  
INC - Industry Numbering Committee  
ISDN - Integrated Services Digital Network  
ISUP - Integrated Services Digital Network User Part  
ITU – International Telephone Union  
IXC – Inter-exchange Carrier  
LEC - Local Exchange Carrier  
LSR - Local Service Request  
LSSGR – LATA Switching System Generic Requirements  
MGB – Main Ground Bus  
MTBF – Mean Time Between Failures  
MTTR - Mean Time to Repair  
MTP – Message Transfer Prohibited  
NANPA - North American Numbering Plan Administrator  
NE - Network Element  
NEBS - Network Equipment Building Systems

NEC – National Electrical Code  
NFPA - National Fire Protection Association  
NIIF - Network Interconnection and Interoperability Forum  
NM – Network Management  
NPA – Numbering Plan Area  
NRC TG - Network Reliability Council Task Group  
NRSC - Network Reliability Steering Committee  
NXX – Usually referenced with the definition of the 10-digit code (N= digits 2-9, X= digits 0-9).  
OBF - Ordering and Billing Forum  
OSS - Operations Support Systems  
PSTN – Public Switched Telephone Network  
PPSN – Public Packet Switched Network  
RCT- Route-Set Congestion Test  
Resp Org – Responsible Organization  
RF – Radio Frequency  
SCCP - Signaling Connection Control Part  
SCP - Service Control Point  
SGB – Supplementary Ground Bus  
SLC – Subscriber Loop Carrier  
SLS – Signaling Link Selection  
SONET - Synchronous Optical Network  
SP – Service Provider  
SR – Special Report  
SS7 - Signaling System 7  
SP/SSP – Signaling Point/Signaling Switch Point  
STP - Signaling Transfer Point  
TCIC – Trunk Circuit Identification Code  
TFC – Transfer Controlled  
TFP – Transfer Prohibited  
TFR – Transfer Restricted  
TR – Technical Requirement  
TSP – Telecommunications Service Priority

\* The NRSC and the NIIF consider these sections as important points of discussion during interconnection negotiations, however at the present time there is no verbiage in the NIIF Reference Document to support/stimulate this discussion. As contributions are brought forward to enhance the NIIF Reference Document, the Interconnection Template will be updated. All items that require further information and contributions are marked with an asterisk throughout the Interconnection Template.