Verizon Safe Time Window Practice

Contents

NOTICE
Not for use or disclosure outside
Verizon Communication except under written agreement.

Page 2 of 40

1. General

1.1 Purpose

This practice outlines the national Verizon Safe Time Window Practice. This practice replaces all existing safe time and maintenance window documents. It is intended to clarify Verizon's safe time window policy at a national level and ensure uniform understanding and application for all Strategic Business Units (SBUs).

Verizon's Safe Time Window is defined as 11:00 p.m. to 7:00 a.m. local network time for all services except 911. High-risk work activity on or near network elements must be performed during this low traffic period in order to minimize disruption to customer service.

Various departments within Verizon establish Safe Time windows for their specific operations which may require a tighter window. But all departments will work within the safe time window when doing high risk activities. The exception to this would be if the work was specifically required to be done outside of the window by a Verizon customer i.e., E911 database activity.

Outages and major service degradations (in progress) will **not** be deferred to the safe time window unless Local Management (National Operations or Network Operations) and the Centralized Network Operations Group (CNOG) Technical Support Services determines it is in the best interest of the customers to defer repair.

Safe time window Exceptions:

- It is recognized that exceptions to the safe time window policy will occur in response to unforeseen circumstances. However, dual approval is required from Network Operations and the appropriate CNOG Technical Support Services group prior to high-risk activity being performed outside of the stated safe time window.

- Activities that will disrupt services to large customers private networks or leased facilities (i.e. Bank of America) must be coordinated with the customer. If the activity is performed outside Verizon's Safe Time Window, by customer demand, dual approval from Local Network Operations and the CNOG Technical Support Services Group is required.

- All work performed during the Safe Time Window must insure that sufficient time is planned so a graceful backout can be completed within the Safe Time Window if trouble is encountered.

- Refer to Section 8 for safe time window exceptions.

- Due to the length of time required to load a switch software upgrade, it may be necessary to load software prior to the safe time window so that activation can be performed shortly after the midnight time frame.

- Due to the nature of 911 service, safe time is defined as being, between the hours of 2:00 a.m. and 2:00 p.m.

1. General, (Continued)

1.2 Supersedures

This practice supersedes and cancels:

fBA 002-300-100 Bell Atlantic Regional Operations Safe Time Practice.

fGTE 06-220-100-300 Network Maintenance Window practice

Any other document which provides information contrary to the information contained in this practice.

1.3 Responsibility

This practice was published by Verizon Network Operations - Process Assurance Department. For more information about this practice, contact Andy.Kops@verizon.com.

1.4 Disclaimer

This practice was prepared for the use of Verizon Network Operations. It must be used only by its employees, customers, contractors and end users when installing, operating, maintaining, and repairing Verizon Network Operations equipment, facilities, and services. Any other use of this practice is forbidden. The information contained in this practice might not be applicable in all circumstances and is subject to change without notice. By using this practice the user agrees that Verizon Network Operations has no liability (to the extent permitted by applicable law) for any consequential, incidental, special or punitive damages that might result.

2. Overview

2.1 Definitions

The following table provides definitions for acronyms and terms used in this practice.

Acronym or Term	Definition
ACDC	Administrative Control and Display Complex
ACP	Activity Concentration Point
ADSL	Asymmetric Digital Subscriber Line
AIN	Advanced Intelligent Network
ALEC	Alternative Local Exchange Carriers
ANI	Automatic Number Identification
ATM	Asynchronous Transfer Mode
BMC	Billing Media Converter
CIC	Carrier Identification Code
CLEC	Competitive Local Exchange Carrier
COEI	Central Office Equipment Installation
CPU	Central Processing Unit
CPX	Common Peripheral Expander
CSD IXC	Circuit Switch Data Interexchange Carrier
DACS	Digital Access and Cross-connect System
DCMS	Distributed Call Measurement System
DCS	Digital Cross-connect System
DS-1	Digital Signal Level 1
DS-3	Digital Signal Level 3
DSX	Digital Signal Cross-connect
EAS	Extended Area Service
EPG	Enhanced Products Group
ETC	Electronic Tele-Communication System
FGB	Feature Group B

2. Overview, (Continued)

Definitions
The following table provides definitions for acronyms and terms used in this practice.

Acronym or Term	Definition
FGD	Feature Group D
GPU	General Processing Unit
HVAC	Heating, Ventilation, and Air Conditioning system
I/O	Input/output
INSCP	Intelligent Service Control Point
INT SS7	Internal Network SS7 Group
IOF	Inter-Office Facility
ISCP	Integrated Services Control Point
ISDN	Integrated Services Digital Network
ISP	Intelligent Service Peripheral
IXC	Inter-exchange Carriers
LCM	Line Concentrating Module
LCP	Local Calling Plans
LNP	Local Number Portability
LNPSCP	Local Number Portability SCP
LTF	Line and Trunk Frame
LVD	Low Voltage Disconnect
MF	Multi-Frequency
MOP	Method Of Procedure
MSHF	Memory Shelf
fGTE NOC	former GTE Network Operations Center
NPA	Numbering Plan Area
NPAC	Number Portability Administration Center
NXX	Office Prefix

2. Overview, (Continued)

Definitions
The following table provides definitions for acronyms and terms used in this practice.

Acronym or Term	Definition
OOS	Out Of Service
PIC	Primary Inter-exchange Carrier
PRTF	Power, Ringing and Test Frame
PUF	Power Universal Frame
RTC	Real Time Clock
SCP	Service Control Point
SMDS	Switch Multi-megabit Data Service
SS7	Signaling System Seven
SSP	Signal Switching Point
STP	Signal Transfer Point
TAS	Trouble Administration System
TDS	Translation Data Set
TPC	Telephony Processor Complex
TSS	Technical Support Services
UPS	Un-interruptible Power Supply

2. Overview, (Continued)

2.2 References

References

The following table provides sources of supplementary information relating to this practice.

See...	For Information About...
fGTE Practice 220-000-004	FCC Reporting and Notification Guideline
fGTE Practice 740-035-010	Building Services Work Rules
Reference documentation NOTD Safe Time Window Policy	Network Operations Translation Design safe time window policies. http://dbmb.ftwyin.tel.Verizon.com/dba/PUBLISH/899840231/Content.html
fBA Practice 780-002-100	Practice BA 780-002-100 FCC Mandated Reporting of Network Disruptions or Outages

3. PAUSE

3.1 Prevent All Unplanned Service Events Policy

Prior to any High-risk work activity being performed on the Verizon network, the following "PAUSE" questions must be reviewed and answered by the technician.

"Everyone Agrees!"

PAUSE

*P*revent *A*ll *U*nplanned *S*ervice *E*vents!

Ask Yourself:

- Why am I doing this?
- Should this be done during safe time?
- What is the expected result of my actions?
- Do I have a safe backout procedure?
- Do I know how to contact Tier 1 and Tier 2 support?
- Is this service-affecting?
- If service-affecting, whom do I notify beforehand?
- Does anyone need to be aware of the consequences of my actions?
- Should anyone be online with me?
- Am I comfortable with this method of procedure?
- Do I have all of the tools that I need to complete the task?
- Do I need a pre-test and post-test procedure for this task?
- How do I know that I did this task properly?
- Have I completed appropriate paperwork, labeling, database changes, or other records work?
- Am I willing to sign my work?

If you answer no to any of these questions, or feel that you cannot complete the job safely…

Do Not attempt the job! Call your supervisor immediately.

4. National Operations Construction/Outside Plant

4.1 National Operations Construction Safe time window Activity Guidelines

Verizon National Operations Construction personnel or any firm acting on their behalf will adhere to this practice while performing any activity deemed high-risk by this policy. All guidelines are to be followed in the "Prevent All Unplanned Service Events" policy**.**

Local management has ultimate responsibility for the scheduling of High-risk activities

4.2 National Operations Construction High-risk Work Activities

The following work activities must be performed inside the safe time window.

- All interoffice facility (IOF) cable route activity (copper and fiber).

- Any activity impacting Host – Remote cable facilities and/or in-service fiber optic cable.

- Permanent fiber restoration after an outage.

- Any cable facility installation, cable maintenance, or cable transfers that directly impact emergency networks which include:
    - 911 Circuitry
    - Hospitals
    - Ambulance Services
    - Police
    - Governmental Agencies
    - Medical Facilities
    - Major Customer Networks

- Any cable activities that could result in multiple or extended service disruptions or service degradation.

5. Central Office Equipment Installation (COEI)

5.1 Central Office Installation Safe time window Activity Guidelines

These guidelines apply to all Verizon central office installation technicians and contractors performing any installation activities on or around Verizon's switching or transport network.

All work performed during the Safe Time Window must insure sufficient time is planned so a graceful backout can be completed within the Safe Time Window if trouble is encountered.

Local management has ultimate responsibility for scheduling of High-risk activities that have the potential to disrupt service. Contact CNOG Technical Support Services if you are unsure about any equipment/activity not listed in this practice that could create a high-risk to Verizon's network.

All planned outages and critical High-risk activities (activities which have high probability to cause severe service degradation, or total switch outage to a base unit or remote) are performed between 12:00 Midnight and 5:00 a.m.

Examples of activities to be performed between 11:00 p.m. and 7:00 a.m. include the following but are not limited to:

Any card replacement, diagnostics, or growth activity on working equipment:

- MDC (Message Distributor Circuit) - GTD-5
- APC (Administrative Processor Complex) - GTD-5
- Common memory - GTD-5
- Memory - All types of CO Equipment
- TPC (Telephony Processor Complex) - GTD-5
- CPX (Common Peripheral Expander) - GTD-5
- CPU (Central Processing Unit) - All Switch Types
- Installation or removal of cable directly above a CPU - All Switch Types

For further details contact CNOG Technical Support Services for the technology in question.

Note: See Section 8 of this practice for additional detailed information and clarification of central office High-risk activities.

5.2 COEI High-risk Work Activities

The following list of central office construction work activities must be performed inside the safe time window, which is defined as 11:00 p.m. to 7:00 a.m. except for planned outages and critical high-risk activities which must be performed between 12Midnight and 5:00 a.m.

- Activity that will result in a simplex condition of a switching or transmission network, (See simplex condition in Section 8.9).

- Activity in the backplane area of switching or transmission equipment.

- Any power related activity, See Section 8.10.

- Activity involving cable or fiber rearrangements that affect IXC traffic or remote/pair gain spans.

- Any activities on SS7 links in live SS7 offices.

- Activity that requires the installation or removal of equipment (Including cabling) above or adjacent to in service equipment that has the potential to severely impact customer service. See fGTE Practice 220-000-200 or fBA 002-300-100 for equipment removal guidelines COE.

5. Central Office Equipment Installation, (Continued)

- Any activity that involves swapping transmission or switching network equipment from the active to the standby side.

- Any "point code routing changes" which are potentially service affecting.

- Activities that require changing out in-service printed circuit wiring cards.

Note: Activities associated with E911 must be conducted between 2:00 a.m. and 2:00 p.m. the safe time window for E911 service.

All potential high-risk activities may not be listed in this practice, and each work activity must be evaluated for potential service degradation or outage.

When COEI is performing work activities functions that may be classified as central office maintenance, NOTD, etc, please refer to the appropriate section in this practice.

5.3 Equipment Contractor Guidelines

Any supplier that provides equipment or services for Verizon's network must follow the appropriate practice Verizon IP 72202 issue 1 "Installation Suppliers Standards". This standard address equipment installation, Method of procedures, access to buildings, job status reports. workmanship, equipment removal, and safety.

No work may take place by any employee or contractor in a working equipment aisle or within 10 feet of working equipment, without the concurrence of local operations management personnel.

No work may take place by any employee or contractor in a working power equipment aisle, or within 10 feet of working power equipment, without the concurrence of local operations management personnel.

No work may proceed unless documented in a properly approved Method of Procedure (MOP).

Equipment suppliers must follow Verizon's Safe Time policy as described in this practice and must detail that requirement when providing a Method of Procedure at the start of any job.

For purposes of this practice, the term "supplier" is intended to include any personnel performing work operation on, in, or around any Network Equipment. This includes, but is not limited to contractors, Operational personnel, Outside Plant personnel, Telco Installation personnel.

6. Network Operations Translation Design

6.1 NOTD Safe time window Guidelines

These guidelines apply to all NOTD employees performing any database activity, which includes provisioning, maintaining, or upgrading Verizon's network.

6.2 Additional Required Notification

An "Area Activity Notification" is required when undertaking any activity with service - affecting possibilities. This notice is forwarded to the NOTD Centralized Support Group, Network Operations and the Network Service Assurance Center, (NSAC) before performing activity that is identified as being in the "High-risk" activity category.

Note: For further detail refer to reference documentation NOTD Safe time window Policy at: http://dbmb.ftwyin.tel.Verizon.com/dba/PUBLISH/899840231/Content.html

6.3 Deviation Steps for Policy Exceptions

When there is an urgent reason to perform database activity outside the safe time window, the steps outlined in the "Policy Deviation Steps" (below) must be followed.

Conditions required for policy deviation:

- Severe impacts on extreme or highly competitive market segments are likely if the activity is delayed until the safe time window period.

- There is a greater risk to the integrity of the network if this change is delayed.

Policy Deviation Steps:

1. Contact appropriate local Network Operations personnel, Network Control Center personnel.

2. Explain the reason for requesting approval to conduct the software changes outside of the safe time window, and the consequences of delaying the changes.

3. Jointly determine whether additional safeguards are necessary.

4. Forward the Area Activity Notification to NOTD Centralized Support with the:

    - reason why the change is being made outside the safe time window.

    - name of the local Network Operations/Network Control Center contact agreeing to the deviation.

6. Network Operations Translation Design, (Continued)

6.4 Risk Level Definitions

The following table provides the Risk Level definitions and Safe time window times.

Risk Level	Safe time window Parameters
High	All translation activity and testing must occur between 11:00 PM and 7:00 am, unless all deviation steps have been completed. **Note:** **Translations that have a high probability to cause an outage must be performed between 12:00 Midnight and 5:00 a.m.**
Moderate	All translation activity and testing must occur during low traffic periods between 7:00 p.m. and 7:00 a.m., unless all deviation steps have been completed.
Low	Translations and testing may be done at any time.
Variable	The customer directs the activity according to their business needs. An assessment of risk level must be completed.

6.5 Translation Risk/Task Matrix

The following table defines activities being performed by NOTD. The risk factor associated with each service is based on the impact to the network and/or market segment.

The risk factors are the same for the following technologies:

GTD-5, DMS 100, DCO, 5ESS, DMS 10, VIDAR, EWSD.

Risk	NOTD Activity	Definition
Low Risk	New Establishes of Carrier Activity; Cellular FGD FGB ALEC CSD IXC	This activity consists of building brand new routing and trunking for IXCs, cellular providers and CLECs. These activities include building new tables and trunk members. Trunks are installed in the "installation busy," or "pre-cut state" for the switching technicians to turn up with the carrier on the due date.
Variable Risk: Customer Driven	MF to SS7 Conversions* ECIC* Reroute CIC for Carriers*	These changes consist of modifying existing signaling and may affect live traffic. Although most of the major ICs (AT&T, MCI, Sprint) require NOTD to make changes during the safe time window, scheduling is performed at their discretion. The smaller IXCs dictate times according to their workforce. VERIZON-to-VERIZON local facility SS7 conversions should continue to be performed during the safe time window.

6. Network Operations Translation Design, (Continued)

Risk	NOTD Activity	Definition
Low Risk	CLASS Adding new, or changing existing features.	When this task involves implementation of new features it can be done anytime. However, when changing existing features, exercise caution, it may require work to be performed in low peak time or in accordance with customer schedules.
Variable Risk: Customer Driven	9-1-1 Adding new, or changing existing service.*	This work involves adding new 9-1-1 service or changing existing service. The customer defines the time of performance based on their dispatch activity.
High Risk	E9-1-1 Selective Router Routing & Translation Impact. Adding new, or changing existing service.*	VERIZON initiated activities: • This work involves adding new 9-1-1 selective routers or changing existing service. • Test calls should include at least one test call to each PSAP. Customer Driven activities: • This work involves customer requested activities. The customer defines the time of performance based on their dispatch activity. • Test calls should include at least one test call to each PSAP.
Low Risk	Local Calling Plans New*	This activity establishes new local calling plans based on regulatory rulings and may be performed at anytime.
High Risk	Local Calling Plans Changing*	This activity affects existing call traffic and should be considered high risk.
High Risk	NPA Splits (ANI) New activity*	This activity requires a change to the ANI information on working numbers due to new NPA activity and requires changes to existing translations in the switch.
High Risk	Intralata Prepositioning Prepositioning activity	This activity involves prepositioning the switch for multiple PIC access for Intralata traffic. The actual cut occurs when recent change activates the customer directory numbers. (Considered to be low risk when live traffic is not affected.)
Low Risk	SS7I Conversion Prepositioning	Adding new translations.
High Risk	SS7I Conversion Cut* Changes*	This activity involves converting MF routing and trunking to SS7 signaling and momentarily disrupts traffic.

6. Network Operations Translation Design, (Continued)

Risk	NOTD Activity	Definition
Low Risk	Express Dialtone Add	This activity builds new translations for disconnected numbers enabling the VERIZON Service Center to establish new service.
Variable Risk: Customer Driven	DID/DOD Adds Changes	This activity includes activating new services as well as changing existing services. New services may be implemented at anytime. Changing or cutting in-service should be coordinated with the customer's schedules.
Moderate Risk	Switch Conversion Equal Access Prepositioning / New Translations	This activity involves adding translations for new switches or new remotes to existing host offices.
High Risk	Switch Conversion Equal Access Cut or Changes that may affect traffic.	This activity involves activating new offices or cutting equal access.
Low Risk	Business Services / Preloads New Services	This activity involves entry of translations needed to supply service for new Centranet customers.
Variable Risk: Customer Driven	Business Services / Preloads Modify existing service	This activity involves day-to-day service changes requested by the customer.
Moderate Risk	DT1 (End-Office) GTD-5 Only-Preposition	This activity involves pre-positioning work to enable consolidation of TDSs in the GTD-5 switches. This activity may be performed in the moderate risk window because of the size of the file.
High Risk	DT1 (End-Office) GTD-5 Only-Cut	Redirecting traffic to the new TDSs.
Moderate Risk	DT1 (Tandem) GTD-5 Only-Preposition	This activity involves pre-positioning work to enable consolidation of TDSs in the GTD-5 switches.
High Risk	DT1 (Tandem) GTD-5 Only-Cut*	Redirecting of incoming traffic from end offices to the new TDSs.
Low Risk	800 SSP Preposition	Prepositioning work to prepare 800 to route to the SCP.
High Risk	800 SSP Cut*	Changing 800 service to launch a query at the SCP level.

6. Network Operations Translation Design, (Continued)

Risk	NOTD Activity	Definition
High Risk	Rehomes Rerouting traffic*	This activity involves rerouting traffic from one point to another, e.g., reroute an end office to a different tandem location.
High Risk	STP Rehomes Transfer of SS7 links*	Transferring existing SS7 links terminations to a different STP location.
Low Risk	Code Activities Adding new prefix's	Translations to add new NXXs
High Risk	Code Activities Changes	Changes to existing codes. Verify NPA/NXX additions for conflicts with Local, Remotes, EAS, LCPs existing codes.
Variable Risk: Customer Driven	ISDN New and changing activity.	This activity involves building and changing new ISDN customer services. This is the same as Centranet activity. The customer defines work window.
Low Risk	AIN Preposition	This activity involves the preposition/set triggers for associated features for AIN services.
Low Risk	Trunk Translations Add members Delete members	This activity adds or deletes members from new or existing trunk groups.
Moderate Risk	Trunk Translations Grooming*	This activity involves consolidating trunk members on various hardware assignments to make room for additions or to free up hardware for reuse.
High Risk	Hardware Adding/Initializing new hardware.	This activity involves initialization of new hardware so that it may be assigned/placed into service.
High Risk	Charge Registers-Adding charge registers in a GTD-5	This activity involves allocating memory to enable more customers to place billable calls.
Low Risk	AIN Customer Order Provisioning	This activity involves updating SPACE to provision individual customer service requests.
Moderate Risk	AIN Monthly Table Maintenance	This activity involves updating tables in SPACE for normal maintenance activities such as monthly code additions. NPA Splits, NPA Overlays, new local calling plans or calling plan additions.
High Risk	AIN Logic Platform Updates	This activity involves updating SPACE to modify the Service Logic for provided AIN services or to add new Service Logic for new service offerings.

*Task requires on-site technician.

7. Fast Packet Group & xDSL

7.1 Fast Packet Safe time window Activity Guidelines

The Fast Packet Group is composed of 3 separate departments; DSPC, the Data Services Provisioning Center; DSAC, Data Services Assurance Center; and the DSNOC the Data Services Network Operations Center, under the umbrella of the DSNO, Data Services Network Operations. The DSPC provisions customer circuits, the DSAC covers maintenance of existing circuits and the DSNOC provisions, repairs and monitors the Fast Packet infrastructure, including switches and trunks.

The Safe Time Policy and escalation process affects the following fast packet network elements:

Lucent CBX500

Lucent GX550

Lucent B-STDX9000

Marconi ASX200-BX

Marconi ES-3810

Newbridge 36170

Sahara 600

Sahara 1200

Siemens Cluster (45 meg)

Siemens Cluster (140 meg)

Xylan Omni5

Note: If newly installed Fast Packet equipment is not on this list contact the DSNO for Safe time guidelines.

The following software functions should normally be performed only during the

Safe Time:

Growth Recent Changes

Generic Loads *

*GENERIC AND PARAMETER CHANGES SHOULD BE SCHEDULED DURING SAFE TIME TO MINIMIZE TROUBLES IN THE EVENT OF A SOFTWARE PROBLEM.

This procedure describes the rules regarding Safe time work as they apply to Fast Packet group activities:

NO intrusive work will be done on any switch outside the safe time window (Midnight to 6:00 a.m.) without prior DSNO Director or VP approval. (TS-GEN-002 Issue 2)

This includes but is not limited to:

Module replacement

Module PRAM and RESET

Processor Toggling/Switch to Standby

Processor PRAM and RESET

In general, any work that MAY be service affecting or can possibly result in a total or partial outage.

7. Fast Packet Group & xDSL, (Continued)

In extreme cases, it may become necessary to perform work outside of the safe time window. Before performing any emergency work of this nature, the relevant escalation should be followed, i.e. the relevant Manager should be contacted. The Manager will in turn escalate to the Director who will escalate to the VP. Once approval has been attained, the work may continue with due care and diligence.

Failure to comply will result in disciplinary action.

7.2 xDSL

This section describes the rules regarding Safe time work as they apply to xDSL group activities:

The Safe Time Policy and escalation process affects the following xDSL network elements:

Cisco 7500 Router

Cisco 2500 Router

Cisco AS5200 Terminal Access Server

Cisco Catalyst 5000 Ethernet Switch

Cisco 3600

Cisco 6509

Cisco 7206

Alcatel ASAM 1000*

Alcatel ASAM 7300*

Alcatel 36120

Alcatel 36170

Litespan 2000 (CAP DSL, PART [RT DSL])

Redback SMS 1000

Redback SMS 10000 (FOA 3rd Qtr, 2002)

Fujitsu Speedport

Lucent CBX500 (AND ATM Switch)

The following software functions should normally be performed only during the

Safe Time:

Growth Recent Changes

Generic Loads *

*GENERIC AND PARAMETER CHANGES SHOULD BE SCHEDULED DURING SAFE TIME TO MINIMIZE TROUBLES IN THE EVENT OF A SOFTWARE PROBLEM.

7. Fast Packet Group & xDSL, (Continued)

Safe-Time Guidelines for ADN ATM Switches

NO intrusive work will be done on any switch outside the safe time window (Midnight to 6:00 a.m.) without prior ASG DNOC Director or VP approval. (TS-GEN-002 Issue 2)

This includes, but is not limited to:

> Module replacement
>
> Module PRAM and RESET
>
> Processor Toggling/Switch to Standby
>
> Processor PRAM and RESET
>
> In general, any work that MAY be service affecting, or can possibly result in a total or partial outage.

*The following are safe time guidelines pertinent to turn-up and acceptance of Alcatel's ASAM 1000 and ASAM 7300 and Fujitsu Speedport.

Safe-Time Requirements for DSLAM Equipment:

Guideline

- ♦ **A New DSLAM System - with No Working Customers**

    This work can be performed during normal business hours for all post installation, work functions required for the test and turn-up of that system.

- ♦ **Existing DSLAM Systems - with Working Customers**

    LT/ATUC Card & Splitter Card Shelf Augments - existing spare shelves with working EXT

     cards.

    This work can be performed during normal business hours. This procedure should be controlled and supervised by Verizon Advanced Services DNOC. Only the new spare shelf should be affected by the placement of the new cards. (DNOC Process - place LT/ATUC/SSM cards).
    Working FRC, NT and EXT card replacements affect service to an entire system or shelf, and must be replaced immediately under the direction of the Verizon Advanced Services DNOC.

    LT card replacements affecting 5 or more working customers must be conducted during the safe time window.

- ♦ **Daisy Chain and Shelf Augment - i.e. initial installation installed 6 channel banks; new order for augmentation of remaining 6 channel banks to the existing system.**

    The following procedure will be performed during safe-time only. The Daisy chain connection and the new bay alarm breaker test must be performed during safe-time to prevent a customer outage. These procedures should be controlled and supervised by Verizon Advanced Services DNOC see (Note 1).

    The LT/ATUC cards and alarm test of LT/ATUC card may be performed during normal business hours. This procedure should be controlled and supervised by Verizon Advanced Services DNOC see (Note 2).

7. Fast Packet Group & xDSL, (Continued)

♦ **Shelf Replacement**

Shelf replacements will be performed during safe-time only, as this work entails disruption of both data and dial tone services. These procedures should be controlled and supervised by Verizon Advanced Services DNOC.

♦ **Fan Filter Replacements**
Fan filter replacements will be performed as recurring, proactive maintenance during normal business hours.

♦ **Throughput and SYNC Testing**

This work can be performed during normal business hours or off tour for all work functions required for the test and turn-up to that system.

♦ **Alarm Testing**
The Alarm Breaker Test must be performed during safe-time to prevent a customer outage. These procedures should be controlled and supervised by Verizon Advanced Services DNOC see (Note 1).

All other alarm tests can be performed during normal business hours.

NOTES:

1. The alarm breaker test should be scheduled at the same scheduled time the daisy chain is connected (Project Management Process). A potential exists to overload the NT system card if the breaker alarm test is performed during a non safe-time. This overload could disrupt existing customer service.

All other alarm tests are not viewed as intrusive since alarms are normal event notifications to network management systems for action and are considered BAU and do not require safe-time.

2. The VERIZON ADVANCED SERVICES DNOC requests all LT/ATUC card additions are placed by 10 AM, prior to customer traffic impacts to the system.

8. Network Maintenance

8.1 X.25

These guidelines apply to the X.25 Provisioners performing any software table installation on the Sprint TP (Telenet Processor) products and/or on the ECI Telematics ACP50 products.

The X.25 Provisioners are responsible for scheduling those High-risk activities that have the potential to disrupt service. The only exception is an "Emergency Situation" which requires reloading a device to correct hardware or software faults. The determination of an "Emergency Situation" is made by the Internal Network Management staff. No activity involving X.25 devices is performed without prior notification of the CNOG Internal Network Maintenance Management group at 972-615-8179.

The following list identifies the risk factors involved in reloading software tables.

- **H – High-risk**: all static reloads for new tables must occur between 11:00 p.m. and 7:00 a.m. local network time.

- **M – Moderate-risk**: all static reloads for new tables must occur between 5:00 p.m. and 6:00 a.m. local network time.

- **L – Low-risk**: static reloads may be completed at any time.

PAD Type	Static Reload	Dynamic Reload	Restart
TP4900	H	L	N/A
TP8000-Switch	H	L	N/A
TP8000-Conc.	M-L	L	N/A
TP3XXX	M-L	N/A	N/A
ACP Switch	N/A	N/A	H
ACP PAD	N/A	N/A	M-L

8.2 SS7 Provisioning Safe time window

The SS7 Provisioning Group utilizes the Central Office safe time window of 11:00 p.m. to 7:00 a.m. local network time. All critical high-risk activities are performed during this window.

SS7 High-risk Activities	
H	SS7 NODE RE-HOMES
H	SS7 ROUTE SET CHANGES
H	GLOBAL TITLE CHANGES THAT RE-ROUTE ENTIRE SERVICES
H	LINK ADDITIONS TO EXSISTING LINK SETS

8. Network Maintenance, (Continued)

8.3 ISCP/ISP

The following list for Maintenance Activity on Associated Hardware has been rated High-risk.

ISCP/ISP	
H	All R24 Processors
H	All Summa 4 Circuit Packs and Control Equipment
H	SCSI Integrated Controllers
H	Token Ring Network adapters
H	Digital Trunk Dual Adapters
H	Digital Trunk Packs
H	Memory Cache
H	Micro-0 Channel Expansion Boards
H	Hard Disk Upgrades
H	Sims Upgrades

8.4 AIN/NDB ISCP

Risk Factor for Maintenance Activities on Associated Hardware

AIN	
H	Control Processor Card
H	Controller Cards
H	Memory/Firmware Maintenance
H	CSU/DSU to SS7 Link Activity
H	Ethernet Switch
H	SS7 Front End
H	Router
H	Disk
L	Tape Unit
L	Local MOC
L	Remote MOC
L	Dial-in Modem

8. Network Maintenance, (Continued)

8.5 Application Maintenance Risk Factors

High (H) All maintenance activity required to be performed during the safe time window of 2:00 a.m. to 8:00 a.m. CST Sundays or 12:00 Midnight to 11:00 a.m. CST on the first Sunday of the month.

Low (L) Any activities that will not impact provisioning or customer traffic.

H	Application Release Upgrade
H	Operating System Level Upgrade
H	Shutdown/Reboot Application or O.S.
L	MOC growth procedure
L	Workstation growth procedure
L	SS7 Link Soft Restart
H	Oracle Database Maintenance

Note:

- Faults which affect activation of LNP porting are repaired immediately.
- Faults which place an LNP Network element in imminent jeopardy are repaired during the next traditional 12:00 Midnight to 6:00 a.m. (local time) safe time window.
- All other faults are repaired during the next Sunday safe time window.

8.6 LNP Network Element Safe time window Policy

Effective immediately and until further notice, all planned upgrades on all LSMS (Local Service Management System)

LNP nodes are done during safe time windows.

Note: The first Sunday of the month is an Extended NPAC maintenance window from 12:00 Midnight to 11:00 a.m. (Central Time), all other Sundays normal NPAC maintenance window is 2:00 a.m. to 8:00 a.m. (Central Time).

Planned Upgrades vs. Fault Repair Activities

The policy above applies to PLANNED system upgrades.

- Faults which affect LNP porting are repaired immediately.
- Faults which place an LNP network element in imminent jeopardy of failure are repaired during the next traditional 12:00 Midnight to 6:00 a.m. (local time) safe time window.
- All other faults are repaired during the next NPAC Sunday safe time window.
- Extended safe time windows on other than the first Sunday of a month normally require a 30 day advance notice to the NPAC.

Any scheduled upgrade activity must be coordinated through the appropriate CNOG INO CCSN department. Requests must be coordinated by the appropriate CNOG INO CCSN group.

NOTICE
Not for use or disclosure outside
Verizon Communication except under written agreement.

Page 24 of 40

8. Network Maintenance, (Continued)

Planned Upgrades vs. Fault Repair Activities, continued

It is imperative that site personnel contact the appropriate CNOG INO Maintenance Management SS7 group before starting, and after completing, any SS7 related activity. This activity includes SS7 Links, SS7, all types of SCPs, and C.O. Switches. This group may deny a High-risk activity based on higher priority work being performed which could cause conflict between the two High-risk activities

fBA center numbers; Cambridge covers Northeast (NY and NE) 617-551-1500, Washington covers all Mid-Atlantic except PA 202-479-5721, Ft Washington covers PA 215-540-2052.

8.7 LNP Network Element Safe time window Time Zone Translator

Site	Node	Normal	Extended
FORT WAYNE NSS (Provisions Indiana eagle LNP NPDB's)	INDIANA LSMS	07:00AM to 13:00PM ET 06:00AM to 12:00PM DT*	07:00AM to 19:00PM ET 06:00AM to 18:00PM DT*
COPPELL NSSC (Provisions California Eagle LNP NPDB's)	TEXAS LSMS	06:00AM to 12:00PM CT	06:00AM to 18:00PM CT

- INDIANA & HAWAII do not observe Daylight Savings Time.

8.8 Central Office Maintenance

These guidelines apply to all technicians performing installation or maintenance activities on or around Verizon's switching or transport network.

8.9 Central Office Safe time window Activity Guidelines

The following sub-sections are safe time window guidelines listed by technologies.

8.9.1 GTD-5 Switching System

Simplex Conditions

Only one attempt can be made, via input command, to restore simplexed equipment. Further restoral activity is deferred to the safe time window. The following exceptions apply.

NOTE: DO NOT attempt to restore the following hardware outside the safe time window.

- Message Distribution Circuit (MDC)
- Common Memory Unit (CMU) or any memory subsystem (e.g. CMCL,CMI,CMB,DMB)
- Network Clock Unit (NCU)
- Space Switch Interface Controller (SSIC)
- Administrative Processor Complex (APC)
- Single TPC Site
- Dedicated Memory (DM)
- Common Memory Unit 9CMU – Type: CPMM CCM, AND COM
- Common Memory 4MW Expansion (CM4E)
- CPX
- ACDC

Card Replacement

Any switch maintenance activity not related to outage restoration recovery is to be deferred to the safe time window. Service affecting faults in non-duplexed equipment should be referred to CNOG Technician Support Services for the best corrective action. All power related activities not required to restore service, especially installation, should be performed in the safe time window.

The only exceptions to this policy are:

- Line Cards - which can be changed with proper monitoring to eliminate customer impact.
- Non-customer affecting hardware without direct switch interaction (i.e., GPU).
- Level 0 Initializations required as a result of Recent Change Activity may be made outside of the safe time window. This activity must comply with the Network Operations Translation Design Guidelines in Section 6.5.
- Level 1 Initializations or greater MUST be deferred to the safe time window unless approved by CNOG Technician Support Services and local Network Operations manager.

Software and Hardware Upgrades

All software and hardware upgrades must be performed in the safe time window

NOTICE
Not for use or disclosure outside
Verizon Communication except under written agreement.

Page 26 of 40

8. Network Maintenance, (Continued)

8.9.2 DMS100/200/250/300 –TOPS Switching Systems

Simplex Conditions

Only one attempt can be made, via input command, to restore simplexed equipment. Further restoral activity is deferred to the safe time window. The following exceptions apply.

NOTE: DO NOT attempt to restore the following hardware outside the safe time window.

- CPU 0 or 1

- Any equipment where the switch drops clock synchronization (except during REX testing)

Card Replacement

Any switch maintenance activity that is not related to outage restoration recovery is to be deferred to the safe time window.

The only exceptions to this policy are:

- Line cards.

- Span interface cards (traffic dependent - only when no trunk groups will be taken out of service).

- Terminal controller I/O cards.

- Other activities that may be performed outside of the safe time window:

    - Reloading peripherals.
    - Performing warmswacts on peripherals (if currently Rexed).
    - Simplexing LCMs (to isolate trouble).

Initializations or Restarts

All Restarts must be deferred to the safe time window unless approved by CNOG Technical Support Services and local Network Operations.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the safe time window.

8.9.3 5ESS Switching System

Simplex Conditions

Only one attempt to restore simplexed equipment can be made, via input command, before restoral activity defers to the safe time window.

Card Replacement

All switch maintenance activity that is not related to outage recovery is to be deferred to the safe time window. Service affecting faults in non-duplexed equipment should be referred to CNOG Technical Support Services for the best corrective action. All power related activities not required to restore service, especially installation, should be performed in the safe time window.

8. Network Maintenance, (Continued)

8.9.3 5ESS Switching System, continued

The only exception to this policy is:

Grid/Line/AIU cards – which can be changed with proper monitoring to eliminate customer impact.

Initializations or Restarts

All Initializations or Restarts must be deferred to the safe time window unless approved by CNOG Technical Support Services and local Network Operations.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the safe time window.

8.9.4 DCO Switching System

Simplex Conditions

Only one attempt to restore simplexed equipment can be made, via input command, before restoral activity defers to the safe time window.

Card Replacement

All card replacement activity that is not related to outage recovery is to be deferred to the safe time window.

The only exceptions to this policy are:

- Line Cards and Line Group Access cards in local or remote line frames
- Non-Integrated Billing Collector (BMC)
- Non-Integrated Ringing Equipment (Bulk Ringing)
- Out-Board Test devices (4TEL, etc.)
- Line and Trunk Frame (LTF) Cell Common Equipment
- LTF Cell Port Cards
- PRT Frame
- PUF Frame
- Test Access (TAS) Network Equipment

Initializations or Restarts

All Initializations or Restarts must be deferred to the safe time window unless approved by CNOG Technical Support Services and local Network Operations.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the safe time window.

8. Network Maintenance, (Continued)

8.9.5 DMS-10 SWITCHING SYSTEM

Simplex Conditions

Only one attempt to restore simplexed equipment can be made, via input command, before restoral activity defers to the safe time window. The following exceptions apply.

NOTE: Do not attempt to restore the following hardware outside the safe time window.

- CPU 0 or 1
- RTC
- MSHF
- CLK 0 OR 1

Card Replacement

All card replacement activity that is not related to outage recovery is to be deferred to the safe time window. The only exception to this policy is Line Cards.

Initializations and Restarts

All Initializations and Restarts must be deferred to the safe time window unless approved by CNOG Technical Support Services and local Network Operations.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the safe time window

8.9.6 EWSD Switching System

Simplex Conditions

Only one attempt to restore simplex equipment can be made, via input command, before restoral activity defers to the safe time window.

Card Replacement

All card replacement activity that is not related to outage recovery is to be deferred to the safe time window.

Recoveries or Restarts

All Initializations or Restarts must be deferred to the safe time window unless approved by CNOG Technical Support Services and local Network Operations.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the safe time window.

The Safe Time Policy affects the following hardware items:

8. Network Maintenance, (Continued)

8.9.6 EWSD Switching System, continued

CENTRAL CONTROL HARDWARE
ACRONYM

Coordination Processor	CP 113
Message Buffer	MB
Central Clock Generator	CCG
Switching Network	SN
Automatic Message Accounting Teleprocessing System	AMTPS

NETWORK FRAMES

Line Trunk Groups	LTG
Digital Line Units	DLU
Common Channel Signaling Network Control	CCNC
Packet Handler	IPH

COMMON CONTROL CARDS/TRUNKS/ PERIPHERAL EQUIPMENT

Digital Line Unit Control	DLUC
Subscriber Line Carrier	SLCI
Subscriber Line Modules	SLM
Digital Interface Unit for DLU	DIUD
Digital Interface Unit	DIU
Group Processor	GP
Line Interface Unit	LIUA
RAD PADS	RAD
MICOM PADS	MICOM

8. Network Maintenance, (Continued)

8.10 CO Power Systems

Any work activity involving Central Office building AC electrical circuits and DC power plant is considered High-risk. All power work is to be deferred to the Safe time window unless approval is given by CNOG Technical Support Services and local Network Operations.

Note: All planned outages and critical High-risk activities (activities which could cause total switch outage) are performed between 12:00 Midnight and 5:00 a.m.

The Power Control Center has identified the following work activities/routines as High-risk. All activities listed below are done in the safe time window.

- Battery Change-Out Activities

- Battery Rundown Testing remove or add fBA

- Battery Strap Continuity

- Power Alarms

- Power Board and Controller Functional

- DC Power Rearrangements

- DC Power Growth/Degrowth Activities

All AC and DC Central Office power system activity must be detailed on an approved Method of Procedure (MOP). The completed MOP is the responsibility of the person performing the actual work (COEI or Vendor). Each MOP is reviewed and approved by COEI (DC), and Support Assets (AC). The MOP must specify that all work is completed each day no later than 06:00 a.m. to ensure all power systems are 100% functional prior to the end of the safe time window.

8. Network Maintenance, (Continued)

8.11 STP ALCATEL/TEKELEC/NORTEL

Simplex Condition and Card Replacement

All switching system card replacements and equipment restoral activity that is **not** related to outage recovery is to be deferred to the safe time window, subject to recommendations by tier II support. The only exception to this policy is the removal or restoral of terminals (CRTs).

Alcatel STP

The Safe Time Policy affects the following hardware items:

DEFINITION	ACRONYM
ADMIN PROCESSOR EQUIPMENT	
Admin Processor	ADMIN
Common Channel Manager	CCM
Common Channel Distributor	CCD
Traffic Monitor/Measurement Processor	TM&M
Signaling Engineering Administration System	SEAS
Initial Problem Report Processor	IPR
Communication Processor	COMM
Datalink Processor/TermLk Processor	DATALINK
Interrupt Cut Through	ICT
DISK	
DISK DIA CONTROLLER	
MESSAGE TRANSPORT NETWORK	MTNC
PROCESSOR/CONTROLLER	
Digital Clock Generator	DCG
Time of Day Card	TDC
Admin Ext Memory	AEM
Clock Distribution Board	CDB
Message Transport Network Subsystem	MTN
Tape Drive	MTD
Power Supplies	PS

8. Network Maintenance, (Continued)

TEKELEC - EAGLE STP

The Safe Time Policy affects the following hardware items:

DEFINITION	ACRONYM
MAINTENANCE and ADMINISTRATION SYBSYSTEM	MAS
MAS Communications Application Processor	MCAP
Terminal Disk Module (DSOA Clock Timing)	TDM
Maintenance Disk and Alarm Card	MDAL
Inter-processor Message Transport Bus	IMT
Inter-processor Message Transport Card	IPMX
APPLICATION SUBSYSTEM	
Application Service Module	ASM
Application Communication Module	ACM
Link Interface Modules	LIM
Digital Clock Distribution (Telecom Solution 523)	DCD
Signaling Engineering and Administration System	SEAS

Initializations and Restarts

N/A for these systems

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the safe time window. Refer to the appropriate INO CCSN for additional requirements.

8.12 Transport (DCS/Fiber/Digital Loop Carrier) Systems

Risk factor for maintenance activity on associated hardware.

- Low Risk (L) - Work activity may be performed any time.

- High-risk (H) - Work activity must be performed inside the safe time window.

- Customer (C) - The customer directs the activity according to their business needs. An assessment of the risk factor must be completed.

8. Network Maintenance, (Continued)

	TRANSPORT
H	Replace Digital Loop Carrier (DLC) batteries or a redundant rectifier.
H	Re-arrangements of working facilities from one route to another, from one piece of hardware to another.
H	Upgrading in-service hardware - even if hardware has a protect side.
H	Replace failed cards where service has successfully switched to a protection card.
H	Upgrading system software.
H	Replacing disc drives - both floppy and hard.
H	Routines on testing hardware protection switching.
H	Working on AC or DC power; not associated with an outage; in a Base or Host C.O. will always be done during the safe time window.
H	Working on AC or DC power; not associated with an outage at a DLC (cabinet or hut), SONET terminal, or DCS that has working facilities.
H	New equipment additions at a working DLC that requires power or common equipment wiring activities, must be performed during the safe time window.
H	Work on DS-1 or DS-3 DSX patch panel cabling; ABAM or COAX cable re-arrangements/adds to the backplane area of a working DSX panel that could involve existing in-service facilities. - This does not apply to normal jumper running to provide service.
H	Working on fiber optic patch panel, performing re-arrangements or connecting new equipment to existing working equipment.
H	Fiber optic splicing activity on cables carrying live traffic.
C	Work can be done on circuits/facilities during the day; when those circuits/facilities are out-of-service (OOS) failed. Note: Service switched to protection is not considered an out-of-service; as long as the circuits are working on the protect side of the facility.
H	Replacing a non-redundant DLC rectifier or working on a power related problem while only the batteries are powering the system.
L	Installing new customer service or modifying an existing customer's service (with prior clearance from customer) on facilities or office DSX-1 or DSX-3 patch panels that does not involve contact with other in-service facilities.
L	Working on equipment or performing a routine that will not normally cause a service interruption. Examples: A) Testing cooling fans; changing filters. B) Taking voltage readings on front panel hardware test points. C) Taking BERT readings at the monitor test jacks of in-service facilities.
L	Installing and turning-up new facilities and hardware; where the new hardware is not yet physically connected to in-service hardware.
L	Collecting alarm and performance data, locally or remotely, via a systems I/O port.
	Software and Hardware Upgrades
All software and hardware upgrades are to be performed in the safe time window.	

9. Real Estate Operations

9.1 Real Estate Operations Safe Time Window

Real Estate employees and contractors are required to be familiar with all sections of this practice and follow as many of the rules and/or use whatever means required to prevent service outages.

See fGTE Practice 740-035-010 for additional requirements.

See Draft Verizon Practice REP 400-401-401 for additional requirements.

The period of time during which high risk activity can be performed:

- Normally between the hours of 11:00 p.m. and 7:00 a.m. for network buildings.

- As defined by the user group at premium sites.

Requirements for Network Operations personnel to be present during performance of high risk activity can vary according to:

- Local Policies.

- Workloads.

- Schedules, etc.

When Real Estate High-risk work cannot be scheduled because of these factors, escalate the issue within Real Estate unit to the Area Manager-Network Operations.

NOTICE
Not to be disclosed outside
Verizon Communications except under written agreement.

Page 35 of 40

10. E-911

10.1 General

Safe time window hours for Basic and Enhanced 911 systems may or may not coincide with normal safe time practices. Many times the heaviest 911 traffic will occur during what is normal safe time and overlap into what is considered normal High Risk time.. Generally the High Risk time for 911 service is between the hours of 2 p.m. through 2 a.m. the following morning and 911 safe time is considered to be 2 a.m. to 2 p.m. To ensure the correct determination of 911 safe time, it is recommended that before any high risk work is done with 911 service that the local 911 Service Manager be consulted. E911 work activity should not be performed until such time as proper notifications/authorizations have been secured. Enhanced 911 services, including hardware and software, are to be considered critical in all aspects of provisioning and maintenance and treated with the highest respect relative to moves, adds or changes to existing systems.

10.2 911 Network

911 Tandems/ Selective Routers

Lucent 5E and Nortel DMS100 Selective Routers.

All of Verizon - East and parts of Verizon West use either the 5E or the DMS 100 Class 5 switches as a 911 Selective Router. Since the 911 Selective Router feature is shared with the local network switch features, there will, at times, be conflicts between 911 service and local service as to what would be considered the correct Safe Time guideline to use. In these cases both local maintenance forces and 911 personnel must work together and use good judgement to determine the appropriate safe time to perform critical 911 maintenance tasks. Any task that is high risk to both Local switched services and 911 must be worked in safe time that is coincident for both switched services.

CML 911 Selective Router

The CML selective router is exclusively used in Verizon - West and is dedicated to the sole purpose of selectively routing 911 calls to the correct PSAP. Save time for the components of the CML are as follows:

Equipment Item	Defined Save Time
DCM Card	911 Safe Time Window
Power Feeders	911 Safe Time Window
Power to New Shelf	Central Office Safe Time Window
CPU	911 Safe Time Window
Mixer/Memory	911 Safe Time Window
SPM Boards	911 Safe Time Window
Data Card	911 Safe Time Preferred But Time Can Be Determined Locally
Generic Update	911 Safe Time Preferred But Time Can Be Determined Locally

10. E-911, (Continued)

10.3 PSAP Equipment

Safe time for PSAP equipment and PSAP trunking will be worked locally between the 911 Service Manager and local PSAP Management.

10.4 Interoffice Transport

All interoffice transport carrying 911 traffic will be worked on during the overlap of the Central Office Safe Time Window and 911 Safe Time.

E911 Database

10.5.1 INTRADO Platform - VZ East

ALISA Systems - (Blue Hill, Burlington, Freehold and Fairland)

Maintenance Window - Monday through Thursday 4:00 a.m. to 6:00 a.m.

All scheduled changes and activities are done during the maintenance window. This Time frame has historically had the lowest call volume for E911 calls. Anytime it's necessary to do an upgrade, install a patch, correct a problem, fix the hardware, make a change in the network etc. the change is scheduled during the maintenance window. If the activity requires more than the two hour window, an extension is scheduled and the Users are notified.

DBMS Systems - (Blue Hill DBMS, Freehold DBMS)

Maintenance Window - Monday through Friday 6:00 p.m. to 8:00 p.m., Saturday & Sunday All Day

All scheduled changes on the DBMS systems are done during the maintenance window. The maintenance hours are negotiated with the External Users who must be notified seven (7) days in advance, unless there's an emergency. The User Hours are frequently extended by E911 - System Administration when requested.

10.5.2 New Jersey - STRATUS Platform

Maintenance Window

Changes typically made during the week if short in duration, but on the weekends if the systems needs to be down for an extended time. All changes must be coordinated with the State.

DBMS/SOP

Maintenance Window

Minor changes done during the week and extended changes done on the weekend. Changes do not need to be coordinated with the State unless the ALIRS updates will be held for more than 24 hours.

10. E-911, (Continued)

10.5.3 INTRADO Platform - VZ West

ALISA Systems - (Everett, Fort Wayne, Long Beach and Tampa)

Maintenance Window -Tuesday through Thursday 10:00 p.m. to 4:00 a.m. (Local system time)

All scheduled changes and activities are done during the maintenance window. This applies to upgrades, installation of patches, correct problems, fix hardware, data network changes etc. If the activity requires more than the normal window, an extension is scheduled and the Users are notified.

DBMS Systems - (Long beach DBMS, Tampa DBMS)

Maintenance Window - Monday through Friday 6:00 p.m. to 10:00 p.m., Saturday and Sunday all Day.

All scheduled changes on the DBMS systems are done during the maintenance windows. The Saturday maintenance hours are negotiated with the External Users who must be notified seven (7) days in advance, unless there's an emergency.

10.5.4 HP 3000 ALI Systems

For HP 3000 - E911 ALI systems, the safe time is customer determined. Before a system is taken down, the customer is contacted for a preferred downtime. Typically suggested is 9:00 a.m. to 11:00 a.m. so that HP hardware support is readily available if needed.

For the Gateway, safe time is 7:00 p.m. to 10:00 p.m. That is a time where customer access is at a minimum and system processing is also at a low point.

10.6 National Trouble Reporting Centers

10.6.1 911 Control Center for Mid Atlantic and New York State

The 911 Control Center is located in Piscataway, NJ. The Control Center serves as the Central PSAP trouble reporting Point for the Mid Atlantic States and New York State. All PSAPs in this geography report their 911 troubles/outages to the 911 Control Center.   Before any critical 911 work is performed in this region the 911 Control Center must be notified. The Control Center can be reached on 800 - 773 - 7911. Further information on the Control Center can be obtained from the Verizon internal web Site at the URL shown below.

http://911cc.bell-atl.com/

10.6.2 911 Service Response Center (SRC) for New England States

The SRC is located in Andover, Massachusetts The SRC serves as the Central trouble reporting Point for all of the New England States served by Verizon. All PSAPs in New England report their 911 troubles/outages to the SRC.   Before any critical 911 work is performed in this region the SRC must be notified. The SRC can be reached on 800 - 391 - 1435.

10. E-911, (Continued)

Generally, since all PSAPs have two links to ALISA, software releases or hardware maintenance in performed Monday through Thursday between 8:00 a.m. and noon on the ALISA or DBMS. This is considered to be a "low traffic" time for PSAP call activity. First, one of the "mated" ALISAs is updated, restored to "normal" service, and then the other is updated. Before any software updates are installed in the Verizon West ALISAs, the (VZW) CNOG INMM group must review and approve the proposed date and time of the installation of the new release. Since the THIRD PARTY WIRELESS routers are not part of any IP network, no IP network activity will affect them. Any work performed on these routers requires notification of the National E911 Technical Support Group and the (VZW) CNOG INMM work group, prior to commencement of such activity.

The current network and customer support organization is the National E911 Technical Support Group. This organization can be reached at 1-877-483-3911. The current PSAP to ALISA Network and THIRD PARTY WIRELESS Routers, in Verizon West, are supported by the CNOG Intelligent Network Maintenance Management (INMM) personnel at 972-615-8179, 24 hours a day, 7 days a week.

Enhanced 911 services include the four basic platforms (Nortel, Lucent, CML and Rockwell) of central office equipment. Personnel assigned to make modifications to an existing system should work within the Verizon Network Services organization to insure that, prior to any activity, the proper notifications have been made. Planned maintenance/repair activity should include notification to the National E911 Technical Support Group; Verizon Network Operations; affected Exchange Carriers and E911 Public Safety Answering Points (PSAP) before attempting any changes to the equipment or network serving the Enhanced 911 system. Additionally, if this work involves PSAPs which are connected to an ALISA, or the THIRD PARTY WIRELESS routers, in Verizon West, (VZW) CNOG INMM must be notified.

Enhanced 911 services, including hardware and software, are to be considered critical in all aspects of provisioning and maintenance and treated with the highest respect relative to moves, adds or changes to existing systems. The current network and customer support organization is the National E911 Technical Support Group. This organization can be reached at 1-877-483-3911. The current PSAP to ALISA Network and THIRD PARTY WIRELESS Routers, in Verizon West, are supported by the CNOG Intelligent Network Maintenance Management (INMM) personnel at 972-615-8179, 24 hours a day, 7 days a week.

Enhanced 911 services include the four basic platforms (Nortel, Lucent, CML and Rockwell) of central office equipment. Personnel assigned to make modifications to an existing system should work within the Verizon Network Services organization to insure that, prior to any activity, the proper notifications have been made. Planned maintenance/repair activity should include notification to the National E911 Technical Support Group; Verizon Network Operations; affected Exchange Carriers and E911 Public Safety Answering Points (PSAP) before attempting any changes to the equipment or network serving the Enhanced 911 system. Additionally, if this work involves PSAPs which are connected to an ALISA, or the THIRD PARTY WIRELESS routers, in Verizon West, (VZW) CNOG INMM must be notified.

Safe time window hours for Enhanced 911 systems are customer driven. Any E911 work activity should not be performed until such time as proper notifications/authorizations have been secured. Generally, since all PSAPs have two links to ALISA, software releases or hardware maintenance in performed Monday through Thursday between 8:00 a.m. and noon on the ALISA or DBMS. This is considered to be a "low traffic" time for PSAP call activity. First, one of the "mated" ALISAs is updated, restored to "normal" service, and then the other is updated. Before any software updates are installed in the Verizon West ALISAs, the (VZW) CNOG INMM group must review and approve the proposed date and time of the installation of the new release. Since the THIRD PARTY WIRELESS routers are not part of any IP network, no IP network activity will affect them. Any work performed on these routers requires notification of the National E911 Technical Support Group and the (VZW) CNOG INMM work group, prior to commencement of such activity.

11. Technical Support Services Telephone Numbers

Technical Support Services Telephone Numbers

The following are the three main Technical Support Services telephone numbers.

(West) 972-615-6200 and (East) 215-440-0226 or dial the 800 number - 877-733-5250 and you will be routed to the appropriate pilot number based on were you originated the call (Lata routing).

The following support numbers are listed by Departments.

Fast Packet	1-800-483-5325
NOTD Hot Line	972-399-5400
AIN/SCP Group (SCP activity)	972-615-8198
NOC INT SS7 group (SS7 Link/Service, STP activity)	972-615-8170
National E911 Technical Support Group.	1-877-872-3911
NOC INT INO Group (X25, DPN, E-911, OSN/COAMN)	972-615-8179
NOC - Potomac	800-695-3006
NOC - Garden City	800-696-4200 / 517-832-8722
NOC - Taunton	888-684-6656 / 508-884-1300