Network Maintenance Window

Contents

Contents

1.1 Purpose

This practice outlines the national GTE Network Maintenance Window Policy. This policy replaces all existing maintenance window documents. It is intended to clarify GTE's maintenance window policy at a national level and ensure uniform understanding and application for all Strategic Business Units (SBUs).

GTE's Maintenance Window is defined as 10:00 pm to 6:00 am local network time. 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.

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) will be performed between 12:00 Midnight and 4:00 am.

Outages and major service degradations (in progress) will **not** be deferred to the maintenance window unless Local Management (Customer Operations or Network Reliability) and the Network Operations Center (NOC) determines it is in the best interest of the customers to defer repair.

Maintenance Window Exceptions:

- It is recognized that exceptions to the maintenance window policy will occur in response to unforeseen circumstances. However, dual approval is required from Network Reliability and the appropriate NOC support group prior to High-Risk activity being performed outside of the stated maintenance window.
- Activities that will disrupt services to large customers (i.e., Microsoft, Bank of America) must be coordinated with the customer. If the activity is performed outside GTE's maintenance window, by customer demand, dual approval from Network Reliability and the NOC is required.
- Planned outages and critical High-Risk activities involving FCC reportable offices, must be performed between 12:00 Midnight and 4:00 am. For example, critical High-Risk activities that could disrupt services to FAA sites, Military installations, nuclear power plants, etc., for further detail refer to Practice 220-000-004. If the activity is to be performed outside GTE's maintenance window, by customer demand, dual approval from Network Reliability and the NOC is required.
- Refer to Section 8.6 for AIN and LNP maintenance 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 maintenance window so that activation can be performed shortly after the midnight time frame.

Notes:

1. The NOC is to be notified via High Risk Activity Notice for all High-Risk activity. Access the GTE Intranet at http://ems1.irngtx.tel.gte.com/accounts/global/highrisk.mv and distribute the notice per Practice 220-001-002.
2. Major GTE Network changes may require additional NOC notification. Refer to Network Change Management at http://nocwww.irngtx.tel.gte.com/OLS/main/OLShome.html.

1. General

1.2 Supersedures

This practice supersedes and cancels:

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

1.3 Responsibility

This practice was published by GTE Enterprise Services Department. For more information about this practice, contact GTE Network Reliability Support.

1.4 Disclaimer

This practice was prepared solely for the use of GTE Network Services. It must be used only by its employees, customers, and end users when installing, operating, maintaining, and repairing GTE Network Services' 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 GTE Network Services 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

(Continued)

Acronym or Term	Definition
CPU	Central Processing Unit
CPX	Common Peripheral Expander
CSD IXC	Circuit Switch Data Interexchange Carrier
DACS	Digital Access and Cross-connect System
DBM	Data Base Management
DCMS	Distributed Call Measurement System
DCS	Digital Crossconnect System
DS-1	Digital Signal Level 1
DS-3	Digital Signal Level 3
DSX	Digital Signal Crossconnect
EAS	Extended Area Service
EPG	Enhanced Products Group
ETC	Electronic Tele-Communication System
FGB	Feature Group B
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	InterOffice Facility
ISCP	Integrated Services Control Point
ISDN	Integrated Services Digital Network
ISP	Intelligent Service Peripheral
IXC	Interexchange Carriers
LCM	Line Concentrating Module
LCP	Local Calling Plans
LNP	Local Number Portability
LNPSCP	Local Number Portability SCP

(Continued)

Acronym or Term	Definition
LTF	Line and Trunk Frame
LVD	Low Voltage Disconnect
MF	Multi-Frequency
MOP	Method Of Procedure
MSHF	Memory Shelf
NOC	Network Operations Center
NPA	Numbering Plan Area
NPAC	Number Portability Administration Center
NXX	Seven Digit phone number
OLS	On-Line Support
OOS	Out Of Service
PIC	Primary Interexchange Carrier
PRT	Power, Ringing and Test Frame
PUF	Power Universal Frame
RTC	Real Time Clock
SCP	Service Control Point
SMDS	Switch Multimegabit 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
UPS	Uninterruptible Power Supply

2.2 References

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

See...	For Information About...
Practice 220-000-004	FCC Reporting and Notification Guideline
Practice 220-001-002	High Risk Activity Notice
Practice 740-035-010	Building Services Work Rules
Reference documentation DBM Maintenance Window Policy	Data Base Management maintenance window policies. http://dbmb.ftwyin.tel.gte.com/dba/PUBLISH/899840231/Content.html
Network Change Management	Major network changes, including software upgrades, patches, hardware modifications, and facility rearrangements. http://nocwww.irngtx.tel.gte.com/OLS/main/OLShome.html

3. When in Doubt Check it Out

3.1 When in Doubt Check it Out Policy

Prior to any High-Risk work activity being performed on the GTE network, the following "**When in Doubt Check it Out**" questions must be reviewed and answered by the technician.

1. Did I review recovery procedures?
   - Do I know why I'm doing this work and what the expected results will be when I'm done?
   - Do I know who to call for support?
   - Do I know who is "On Call" and have I checked to make sure he/she is available?
   - Do I have service recovery/restoral information available?

2. Have I identified impacts to services- internal users and end user customers?
   - Have I identified internal users and external customers that may be affected by the work I am going to perform?

3. Have I filed a High Risk Activity Report?
   - Have I completed a High Risk Activity Notification entry on the Intranet at http://ems1.irngtx.tel.gte.com/accounts/global/highrisk.mv, and distributed it per GTE Practice 220-001-002?
   - Prior to performing this work, have I contacted the local zone coach/maintenance supervisor to verify the High Risk Activity Report has been received, and he/she is aware this work is to be performed?

3.1 When in Doubt Check it Out Policy, continued

4. Do I have a Regression Test Plan?
   - Prior to performing this work, have I verified system integrity and stability?
   - Am I confident I have the proper tools and documentation required to correctly perform the activity?

5. Have the users been notified of the change?
   - Have I notified the users that I will be performing this work?
   - Do the users know what changes are being made, and have they agreed to the work window?

   Note: Technicians must coordinate any possible service affecting work with the end user and agree upon a "Work Window."

6. Have I checked to see if this work should be performed during the maintenance window?
   - Is this the correct time to perform this work?
   - Am I confident that performing this work, at this time, will least disrupt service?

7. Do I have a method of procedure (MOP)?
   - Is the work order and supporting documentation current and correct?
   - Have I previewed the work to be completed, reviewed the steps necessary to complete it and identified possible problem areas?
   - Have I asked a zone coach/supervisor or co-worker to review my method of procedure to identify things I might have missed?
   - Has my supervisor approved and signed off on my method of procedure?

8. Do I know whom to call in case of an outage?
   - Do I have an escalation procedure and supporting documentation?
   - Do I have correct contact telephone numbers to request assistance if needed?

9. Am I confident I can perform the work correctly and safely?
   - Do I have the necessary tools, equipment and documentation to thoroughly complete the assignment?
   - Do I have the proper training or is there someone on site with me who has more knowledge and experience that can assist me in this work?
   - Even though I have previously performed this type of work numerous times, have I reviewed all aspects of this specific work activity to ensure that I will not make a mistake?

4. Access Construction/Outside Plant

4.1 Access Construction Maintenance Window Activity Guidelines

GTE Network Service Access 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 followed in the “When in Doubt Check it Out” policy**.**

Local management has ultimate responsibility for the scheduling of High- Risk activities, and to ensure distribution of the High-Risk Notice per Practice 220-001-002.

4.1.1 Access Construction High-Risk Work Activities

The following work activities must be performed inside the maintenance 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 Maintenance Window Activity Guidelines

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

Local management has ultimate responsibility for scheduling of High-Risk activities that have the potential to disrupt service. Contact NOC/On Line Support if you are unsure about any equipment/activity not listed in this practice that could be High-Risk to GTE’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 4:00 am.

5.1 Central Office Installation Maintenance Window Activity Guidelines, continued

Examples of activities to be performed between 12:00 Midnight and 4:00 am include the following but are not limited to:

Any card replacement, diagnostics, backplane or growth activity on:

- 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 OLS for the technology in question.

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

5.1.1 COEI High-Risk Work Activities

The following list of central office construction work activities must be performed inside the maintenance window, which is defined as 10:00 pm to 6:00 am, except for planned outages and critical high-risk activities.

- 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 Practice 220-000-200 for equipment removal guidelines COE.
- 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.
- Activity associated with E911.
- Activities that require changing out in service printed circuit wiring cards.

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, DBM, etc, please refer to the appropriate section in this practice.

6. Data Base Management

6.1 DBM Maintenance Window Guidelines

These guidelines apply to all DBM employees performing any database activity, which includes provisioning, maintaining, or upgrading GTE'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 Centralized Support Group, Network Reliability and the NOC before performing activity that is identified as being in the “High-Risk" activity category.

Note: For further detail refer to reference documentation DBM Maintenance Window Policy at:
http://dbmb.ftwyin.tel.gte.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 maintenance 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 maintenance 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 Reliability/Customer Operations personnel. A listing of contacts, by area, may be viewed from the NEDAS decterm application by entering the command *network-contacts*.
2. Explain the reason for requesting approval to conduct the software changes outside of the maintenance window, and the consequences of delaying the changes.
3. Jointly determine whether additional safeguards are necessary.
4. Forward the Area Activity Notification to DBM Centralized Support with the:
    - reason why the change is being made outside the maintenance window.
    - name of the Network Reliability/Customer Operations contact agreeing to the deviation.

6.4 Risk Level Definitions

The following table provides the Risk Level definitions and Maintenance Window times.

Risk Level	Maintenance Window Parameters
High	All translation activity and testing must occur between 10:00 pm and 6:00 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 4:00 am.**
Moderate	All translation activity and testing must occur during low traffic periods between 7:00 pm and 7:00 am, 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 DBM. 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.

Risk	DBM Activity	Definition
Low Risk	Carrier Activity Cellular FGD FGB ALEC CSD IXC	This activity consists of building brand new routing and trunking for IXCs, cellular providers and ALECs. 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 DBM to make changes during the maintenance window, scheduling is performed at their discretion. The smaller IXCs dictate times according to their workforce. GTE-to-GTE local facility SS7 conversions should continue to be performed during the maintenance window.

(Continued)

Risk	DBM 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.*	GTE 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.

(Continued)

Risk	DBM Activity	Definition
Low Risk	Express Dialtone Add	This activity builds new translations for disconnected numbers enabling the GTE 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.
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.

(Continued)

Risk	DBM Activity	Definition
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.

*Task requires on-site technician.

7. Business Response - Enhanced Product Group

7.1 EPG Maintenance Window Activity Guidelines

The Business Response – Enhanced Products Group (EPG) is a centralized provisioning center responsible for data product service activation and data service platform configuration/commissioning. The EPG can be reached at 1-800-483-5325.

The following list identifies the risk factors associated with EPG activity.

- **High (H)** All engineering, configuration and common equipment maintenance activity must occur between 10:00 pm and 6:00 am, unless otherwise directed by GTE Management or disaster recovery procedures.

  Note: 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/remote) are performed between 12:00 Midnight and 4:00 am.

- **Moderate (M)** All routing, translation and data base activity must occur during low traffic periods between 7:00 pm and 7:00 am.
- **Low (L)** Work may be scheduled at any time. Includes off-line commissioning, service order recent change activity and subscriber line component maintenance.
- **Customer (C**) The customer directs the activity according to their business needs. An assessment of risk level must be considered. Intrusive testing requested by the customer may be scheduled at any time; however, work on common equipment may require high level (H) maintenance window scheduling if the activity places other customers at risk.

  Note: Any of the following High-Risk activities performed outside the maintenance window must have approval from EPG, the Network Operations Center (NOC) and Network Reliability.

Activity	Platforms & Modules						
	Frame Relay	**ATM**	**SMDS**	**ADSL**	**Flex-Grow**	**Routers**	**DACS**
Recent Change	L	L	L	L	L	L	L
Platform Engineering Configuration, Routing & Translation	H	H	H	H	H	H	H
New Platform Commissioning	L	L	L	L	L	L	L
Intrusive Circuit Testing	C	C	C	C	C	C	C
Data Base Recent Change	M	M	M	M	M	M	M
Version Release Upgrade	H	H	H	H	H	H	H

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. High-Risk notices are sent out 48 hours in advance of the work to be performed. 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 NOC Internal Network Maintenance Management group at 972-615-8179, if a Specialist is not available, do not proceed, wait until your phone call is answered.

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

- **H – High-risk**: all static reloads for new tables must occur between 10:00 pm and 6:00 am local network time.
- **M – Moderate-risk**: all static reloads for new tables must occur between 5:00 pm and 6:00 am 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 Maintenance Window

The SS7 Provisioning Group utilizes the Central Office maintenance window of 10:00 pm to 6:00 am 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

8.3 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/LNP ISCP

Risk Factor for Maintenance Activities on Associated Hardware

AIN/LNP	
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

8.5 Application Maintenance Risk Factors

High (H) All maintenance activity required to be performed during the maintenance window of 6:00am to 12:00 noon CST Sundays or 6:00 am to 6:00 pm 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 am (local time) maintenance window.
- All other faults are repaired during the next Sunday maintenance window.

8.6 LNP Network Element Maintenance Window Policy

Effective immediately and until further notice, all planned upgrades on all AIN/LNP and LNP nodes are done between the Normal NPAC maintenance window hours of Sundays 6:00 am to 12:00 pm (Noon) Central Time.

Note: Sundays 6:00 am to 6:00 pm Central Time is an Extended NPAC maintenance window the first Sunday of the month.

PLANNED UPGRADES VS. FAULT REPAIR ACTIVITIES

The policy above applies to PLANNED system upgrades.

- Faults which affect activation of LNP porting are repaired immediately.
- Faults which place an LNP network element in imminent jeopardy for failure are repaired during the next traditional 12:00 Midnight to 6:00 am (local time) maintenance window.
- All other faults are repaired during the next NPAC Sunday maintenance window.
- Extended maintenance 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 NOC-AIN department. Requests must be received by 4:30 pm Central Time on the Wednesday before the next Sunday maintenance window. This is required for NPAC notification. The NOC-AIN group issues the High-Risk notice.

PLANNED UPGRADES VS. FAULT REPAIR ACTIVITIES, continued

It is imperative that site personnel contact the NOC Internal Network Maintenance Management SS7 group at 972-615-8170 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. Reference the NOC Network Change Management documentation on the Intranet at:

http://nocwww.irngtx.tel.gte.com/OLS/main/OLShome.html

8.7 LNP Network Element Maintenance Window Time Zone Translator

Site	Node	Normal	Extended
VIRGINIA LNP SITES	(MNSS SPACE & NODE and OCQN NODE)	07:00AM to 13:00PM ET	07:00AM to 19:00PM ET
FLORIDA LNP SITES	(TAMP SPACE & NODE and CLWR NODE) (TAMP NSSC - ASMS)	07:00AM to 13:00PM ET	07:00AM to 19:00PM ET
INDIANA LNP SITES	(FTWY SPACE & NODE and GRRT NODE) (FTWY NSSC - ASMS)	07:00AM to 13:00PM EST 06:00AM to 12:00PM DT*	07:00AM to 19:00PM EST 06:00AM to 18:00PM DT*
TEXAS LNP SITES	(IRNG SPACE & NODE and DNTN NODE)	06:00AM to 12:00PM CT	06:00AM to 18:00PM CT
WASHINGTON LNP SITES	(EVRT SPACE & NODE and BOTH NODE)	04:00AM to 10:00AM PT	04:00AM to 16:00PM PT
CALIFORNIA LNP SITES	(LNBH SPACE & NODE and SNMN NODE)	04:00AM to 10:00AM PT	04:00AM to 16:00PM PT
HAWAII LNP SITES	(PNHO SPACE & NODE and WPHU NODE)	02:00AM to 08:00AM HST 01:00AM to 07:00AM DT*	02:00AM to 14:00PM HST 01:00AM to 13:00PM DT*

* 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 GTE's switching or transport network.

Local management has ultimate responsibility for scheduling of High-Risk activities which have the potential to disrupt service. Contact the appropriate NOC support group if you are unsure about any equipment/activity not listed in this practice that could be a High-Risk to GTE's network.

Any exceptions to allow planned work outside the maintenance window require DUAL approval from Network Reliability and the NOC Support group for the technology involved.

8.9 Central Office Maintenance Window Activity Guidelines

The following sub-sections are maintenance 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 maintenance window. The following exceptions apply.

NOTE: DO NOT attempt to restore the following hardware outside the maintenance window. Remote restoral of the following hardware is prohibited.

- 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 maintenance window. Service affecting faults in non-duplexed equipment should be referred to NOC OLS for the best corrective action. All power related activities not required to restore service, especially installation, should be performed in the maintenance 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 maintenance window. This activity must comply with the Data Base Management Translation Guidelines in Section 6.5.
- Level 1 Initializations or greater MUST be deferred to the maintenance window unless approved by NOC OLS and Network Reliability.

Software and Hardware Upgrades

All software and hardware upgrades must be performed in the maintenance window. Refer to the “Network Change Management Guidelines” for additional requirements.

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 maintenance window. The following exceptions apply.

NOTE: DO NOT attempt to restore the following hardware outside the maintenance window. NOTE: Remote restoral of the following hardware is prohibited.

- 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 maintenance 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 maintenance 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 maintenance window unless approved by NOC OLS and Network Reliability.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the maintenance window. Refer to the “Network Change Management Guidelines” for additional requirements.

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 maintenance window.

Card Replacement

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

The only exception to this policy is:

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

8.9.3 5ESS Switching System, continued

Initializations or Restarts

All Initializations or Restarts must be deferred to the maintenance window unless approved by NOC OLS and Network Reliability.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the maintenance window. Refer to the "Network Change Management Guidelines" for additional requirements.

DCO Switching System

Simplex Conditions

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

Card Replacement

All card replacement activity that is not related to outage recovery is to be deferred to the maintenance 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 maintenance window unless approved by NOC OLS and Network Reliability.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the maintenance window. Refer to the "Network Change Management Guidelines" for additional requirements.

8.9.4 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 maintenance window. The following exceptions apply.

NOTE: Do not attempt to restore the following hardware outside the maintenance window. Remote restoral of the following hardware is prohibited.

- 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 maintenance window. The only exception to this policy is Line Cards.

Initializations and Restarts

All Initializations and Restarts must be deferred to the maintenance window unless approved by NOC OLS and Network Reliability.

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the maintenance window. Refer to the "Network Change Management Guidelines" for additional requirements.

8.9.5 VIDAR SWITCHING SYSTEM

Simplex Conditions

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

Card Replacement

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

The only exceptions to this policy are:

- Line Cards
- Subscriber Switch Controllers
- DCMS maintenance work
- ETC card replacements
- Time Slot Interchanger maintenance
- Data Base Compatible (BW1) can be performed outside of the maintenance window with NOC OLS approval

8.9.5 VIDAR SWITCHING SYSTEM, continued

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the maintenance window. Refer to the "Network Change Management Guidelines" for additional requirements.

Adjunct or Peripheral Devices

Repair activity on any Adjunct or Peripheral device is to be performed during the maintenance window unless NOC OLS and Network Reliability approval has been obtained. (Examples: 4-Tel, INAS, Voicemail, etc.)

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 Maintenance Window unless approval is given by Network Reliability and NOC OLS.

Note: All planned outages and critical High-Risk activities (activities which could cause total switch outage) are performed between 12:00 Midnight and 4:00 am.

NOC OLS has identified the following work activities/routines as High-Risk. All activities listed below are done in the maintenance window.

- Battery Change-Out Activities
- Battery Rundown Testing - routine GS1PD
- Battery Strap Continuity – routine GS1PF (only if mv drop method is used)
- Power Alarms - routine GS1SP
- Power Board and Controller Functional - GS1P1 (Only LVD disconnect and re-connect settings)
- 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). MOP review can also be requested from NOC On-Line Support Power, a minimum of 48 hours prior to the scheduled activity.

The MOP must specify that all work is completed each day no later than 05:00 am to ensure all power systems are 100% functional prior to the end of the maintenance window.

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 maintenance window. he only exception to this policy is the removal or restoral of terminals (CRTs).

8.11 STP ALCATEL/TEKELEC/NORTEL, continued

Initializations and Restarts

N/A for these systems

Software and Hardware Upgrades

All software and hardware upgrades are to be performed in the maintenance window. Refer to the "Network Change Management Guidelines" 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 maintenance window.
- Customer (C) - The customer directs the activity according to their business needs. An assessment of the risk factor must be completed.

TRANSPORT	
H	Replace Digital Loop Carrier (DLC) batteries or a redundant rectifier.
H	Re-arrangements of working facilities from one route to another and/or 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 maintenance 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 maintenance window.
H	Work on DS-1 or DS-3 DSX patch panel cabling; cable re-arrangements or cable adds to the backplane area of a working DSX panel that could involve contact with existing in-service facilities.
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	Re-designs of circuits and facilities

(Continued)

TRANSPORT	
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.
L	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 (Bit Error Rate Test)readings at the monitor test jacks of in-service facilities. D) Taking BERT reading at the IN/OUT jacks of unassigned/non-working 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 maintenance window. Refer to the “Network Change Management Guidelines” for additional requirements.	

9. Support Assets

9.1 Support Assets Maintenance Window

Building Services 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 Practice 740-035-010 for additional requirements.

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

- Normally between the hours of 10:00 p.m. and 6:00 a.m. for network buildings.
- As defined by the user group at premium sites.

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

- Local Policies.
- Workloads.
- Schedules, etc.

When Building Services High-Risk work cannot be scheduled because of these factors, escalate the issue within Building Services unit to the General Manager-Network Reliability.

10. E-911

10.1 E-911

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 1-800-872-3356.

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 GTE 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; GTE Network Reliability; affected Exchange Carriers and E911 Public Safety Answering Points (PSAP) before attempting any changes to the equipment or network serving the Enhanced 911 system.

Maintenance 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.

11. Technical Support Telephone Numbers

11.1 Technical Support Telephone Numbers

The following NOC On Line Support telephone numbers are listed by technology.

DMS10	972-615-8115
DMS100	972-615-8110
GTD-5	972-615-8120
5ESS	972-615-8130
POWER	972-615-8195
DCO	972-615-8140
DLC/Fiber/Radio/DCS	972-615-8150
STP	972-615-8160
WIRELESS	972-615-8100
VOICE MAIL	972-615-8125
VIDAR	972-615-8135

The following support numbers are listed by Departments.

Enhanced Products Group (EPG)	1-800-483-5325
DBM Hotline	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.	1-800-872-3356