digital™

CUSTOMER RELEASE NOTES

DIGITAL GIGAswitch/Router
Firmware Version 2.1.0.1
February, 1999

INTRODUCTION:

This document provides specific information for version 2.1.0.1 of the system firmware for the DIGITAL GIGAswitch/Router (GSR) family of products.

Please review this release note thoroughly prior to installing or upgrading this product.

FIRMWARE SPECIFICATION:

Image Name	Version No.	Type	Release Date
gsr2101	2.1.0.1	Customer	February 1999
gsr2000	2.0.0.0	Customer	November 1998
gsr1200	1.2.0.0	Customer	September 1998
gsr1100	1.1.0.0	Customer	August 1998
gsr1010	1.0.1.0	Customer/Maintenance	June 1998
gsr1000	1.0.0.0	Customer	April 1998

HARDWARE COMPATIBILITY:

Part	Description	Minimum Firmware Version
DGSRA-BA	16-slot GIGAswitch/Router Chassis, Backplane and Modular Fan	1.2.0.0
DGSRP-AB	Power Supply for GSR-16	1.2.0.0
DGSRD-AA	Switch Fabric Module for GSR-16	1.2.0.0
DGSRA-AA	8-Slot GIGAswitch/Router Chassis, Backplane and Modular Fan	1.0.0.0
DGSRP-AA	Power Supply Module for GSR-8	1.0.0.0
DGSRC-AA	Control Module with 64 MB	1.0.0.0
DGSRC-AB	Control Module with 128 MB	1.0.0.0
DGSRC-BA	Revised Control Module with 64 MB	1.1.0.0
DGSRC-BB	Revised Control Module with 128 MB	1.1.0.0
DGSRT-AA	8-Port 10/100 TX Module (Cat 5 RJ-45) with 4 MB	1.0.0.0
DGSRF-AA	8-Port 100 FX Module (MMF SC) with 4 MB	1.0.0.0
DGSRS-AA	2-Port 1000 SX (Gigabit) Module (SCSX for MMF Only) with 4 MB	1.0.0.0
DGSRL-AA	2-Port 1000 LX (Gigabit) Module (SCLX for MMF or SMF) with 4 MB	1.0.0.0
DGSRT-AB	8-Port 10/100 TX Module (Cat 5 RJ-45) with 16 MB	1.0.1.0
DGSRS-AB	2-Port 1000 SX (Gigabit) Module (SCSX for MMF Only) with 16 MB	1.0.0.0
DGSRL-AB	2-Port 1000 LX (Gigabit) Module (SCLX for MMF or SMF) with 16 MB	1.0.0.0
3X-DGSRK-AA	4-Port Serial module with compression for GSR-8 and GSR-16	2.1.0.1
3X-DGSRK-AB	4-Port Serial module with compression and encryption for GSR-8 and GSR-16	2.1.0.1
3X-DGSRH-AA	2-Port HSSI module for GSR-8 and GSR-16	2.1.0.1

Note: The DGSRC-BA/BB Control Modules replace the DGSRC-AA/AB Control Modules. The DGSRC-BA/BB Control Modules have a 10/100 BASE-TX management port (as opposed to a 10 BASE-T port on the

DGSRC-AA/AB Control Modules). Otherwise, the functionality of the DGSRC-BA/BB Control Modules is identical to that of the DGSRC-AA/AB Control Modules.

BOOT PROM COMPATIBILITY:

This version of the firmware supports boot PROM version 1.0.0.0 and 1.1.0.0. The boot PROM resides in the internal flash on the Control Module. Its primary function is to load the firmware image.

For the **GSR-8**, the following table lists the Control Module, PROM image, and firmware image compatibility.

Control Module	Minimum PROM Image	Minimum Firmware Image
DGSRC-AA DGSRC-AB	prom-1.0.0.0	1.0.0.0
DGSRC-BA DGSRC-BB	prom-1.1.0.0	1.1.0.0

Note: It is recommended that you update the DGSRC-AA and DGSRC-AB PROM image to version 1.1.0.2 (prom-1.1.0.2).

For the **GSR-16**, the following table lists the Control Module, PROM image, and firmware image compatibility.

Control Module	Minimum PROM Image	Minimum Firmware Image
DGSRC-BA DGSRC-BB	prom-1.1.0.2-cm2	1.2.0.0

SUPPORTED FUNCTIONALITY:

New Features in Version 2.1.0.1	Support
Serial and HSSI WAN Modules The HSSI WAN modules for the GSR support leased-line service speeds up to STS-1 (52 Mbps), inclusive of Fractional T3/E3 and T3/E3 services. The Serial WAN modules for the GSR support leased-line service speeds up to E2 (8 Mbps), inclusive of Fractional T1/E1 and T1/E1/J2 services. The GSR WAN modules support true Layer 2/3/4 Switching, allowing consistent policy management for security and quality of service. The GSR supports PPP and Frame Relay. Industry leading WAN features include support for per-priority, per-PVC queuing, enabling Quality of Service to extend out of the WAN. Flow rate limiting, Weighted Random Early Detection (WRED), and Weighted Fair Queuing (WFQ) work in harmony to manage congestion. Traffic shaping is provided on a per-PVC basis, and BECN adaptive rate shaping is also supported. Detailed accounting information can be gathered using per PVC RMON, allowing easy confirmation that service level agreements are being met.	YES

INSTALLATION AND CONFIGURATION NOTES:

- **Password Recovery**

  If you forget the GSR password and are unable to log into the GSR or enter Enable mode, follow these steps to gain access to the system. You must execute the following steps at the system console; they cannot be executed through Telnet.

  1. Get to the system Boot PROM mode. To get to this mode, the GSR must either be rebooted or powered off, then on. When the GSR goes through its initialization, interrupt the normal boot sequence by pressing the Escape key. Typically, the GSR waits two seconds for user interruption before entering the normal boot sequence.

  2. At the gs/r-boot prompt, enter the boot command as follows:

     gs/r-boot> **boot file:/pc-flash/boot/gsr2101/ skipconfig=yes**

  3. Once the GSR is booted, it has no configuration information. Enter the system without a password. Go to Enable mode and enter the following command:

     gs/r# **copy startup to scratchpad**

     This copies the start-up configuration into the scratchpad without activating the commands.

  4. Go to Configure mode. You can now either change the password or remove the old password altogether by negating the system set password commands in the scratchpad. Once you do this, the commands in the scratchpad can be made active by either saving the active configuration in Configure mode or copying the scratchpad to active in Enable mode.
  5. To ensure that the new configuration survives the reboot, save the active configuration to the start-up configuration. At the next boot, enter the GSR with the new password you just set (or without a password if so configured).

FIRMWARE CHANGES AND ENHANCEMENTS:

Issues Resolved in Version 2.1.0.1
Note: The issues resolved in Version 2.1.0.1 are the same as those listed in Version 1.2.0.2. Version 1.2.0.2 was a limited-distribution release. The fixes for Version 1.2.0.2 were not made part of version 2.0.0.0, but they were made part of Version 2.1.0.1.
Under certain circumstances, packets received by the Control Module would be corrupted, causing the GSR to crash without a crash dump.This problem was fixed in this release.

Issues Resolved in Version 2.1.0.1
In certain QoS configurations involving IPX interfaces, the priority would get set to "low" even when the CLI command had "high" specified in it. This occurred when the “interface list” parameter was used; for example: **qos set ipx ipx35 high 0a010080 any any 0a010000 any any <*interface list*>** This problem was fixed in this release.
In previous releases, IGMP could not be run on more than ten interfaces. This problem was fixed in this release.
In certain configurations, an ARP request was sent out for every route in an update. This problem was fixed in this release.
Under certain circumstances, routes from other protocols (direct routes) were not redistributed into OSPF. This problem was fixed in this release.

Issues Resolved in Version 2.0.0.0
In previous releases, the port mirroring feature disabled the switching capability of the monitor port and all the ports on the monitor port’s line card. With this release, the switching capability of ***only*** the monitor port is disabled. The other ports on the monitor port’s line card work normally.
In previous releases, downloading an image to a PCMCIA flash card could take more than a few minutes. Since the CPU is busy while downloading the image, routes may have disappeared from the routing table until downloading was complete. This problem was fixed in this release.
The interface option in the **ip add route** command now works correctly.
In previous releases, if an IP interface was brought down and back up (using the **interface down** and **interface up** commands), the interface came up right away, but it took about 30 seconds for the interface route to appear in the routing table. The interface route now appears in the routing table immediately.
The command to display the ARP cache table was changed from **arp show host all** to **arp show all**.
Under some circumstances, executing an SNMP Get-Next operation on an OSPF MIB object caused a loop on that object. This problem was fixed in this release.

Issues Resolved in Version 2.0.0.0
In previous releases, the GSR forwarded a NAK from a DHCP server to the port where the client used to reside if the ARP entry still existed. If no ARP entry existed, the GSR forwarded the NAK to the IP VLAN where the client originally was a member. This problem was fixed in this release.

Issues Resolved in Version 1.2.0.2
Note: Version 1.2.0.2 was a limited-distribution release. The issues listed below were resolved in Version 1.2.0.2, but the fixes were ***not*** made part of Version 2.0.0.0. The fixes were made part of Version 2.1.0.1. This means that the following issues are resolved in Version 1.2.0.2 and 2.1.0.1, but ***not*** 2.0.0.0.
Under certain circumstances, packets received by the Control Module would be corrupted, causing the GSR to crash without a crash dump.This problem was fixed in this release.
In certain QoS configurations involving IPX interfaces, the priority would get set to "low" even when the CLI command had "high" specified in it. This occurred when the “interface list” parameter was used; for example: **qos set ipx ipx35 high 0a010080 any any 0a010000 any any *<interface list>*** This problem was fixed in this release.
In previous releases, IGMP could not be run on more than ten interfaces. This problem was fixed in this release.
In certain configurations, an ARP request was sent out for every route in an update. This problem was fixed in this release.
Under certain circumstances, routes from other protocols (direct routes) were not redistributed into OSPF. This problem was fixed in this release.

Issues Resolved in Version 1.2.0.1
The GSR may have experienced a memory leak if no route to the destination IP helper address existed in the IP routing table. This problem was fixed in this release.
Under certain circumstances, GSR crashed when trying to forward DHCP packets. This problem was fixed in this release.
Under certain circumstances, software timer interrupts would pre-empt network processing and cause the GSR to crash. This problem was fixed in this release.

Issues Resolved in Version 1.2.0.1
The IP stack limitation prevented the GSR from running OSPF simultaneously on more than 10 interfaces. This problem was fixed in this release.
Occasionally, the GSR received a packet with an invalid port of entry, which caused the GSR to crash. This problem was fixed in this release.

Issues Resolved in Version 1.2.0.0
The IPX ACL logging function did not work in previous releases of the firmware. This problem was fixed in this release.
In previous releases, the GSR may have crashed when applying an ACL filter (IPXGNS, IPXSAP, and IPXRIP) under the following circumstances: • If there was an IPXGNS filter defined on the output side, and a SAP server in the SAP list did not match the ACL. • If there was an IPXRIP filter defined on the output or input side and incoming/outgoing network did not match the ACL. • If there was a IPXSAP filter defined on the output or input side and incoming/outgoing SAP service did not match the ACL. This problem was fixed in this release.
In previous releases, the GSR may have crashed when you deleted an ACL with the ACL Editor. This problem was fixed in this release.
CPU resources were consumed by an ACL when you created or removed the ACL after a Layer 3 (IPX) flow was already created. This problem was fixed in this release.

Issues Resolved in Version 1.1.0.0
Sometimes executing SNMP Get or Get-Next operation on the Interface MIB object in MIB-2 caused the GSR to reboot. This problem was fixed in this release.
When the GSR is configured to advertise on its secondary interface using RIP Version 2, an invalid UDP checksum was calculated by the GSR. This problem was fixed in this release.

Issues Resolved in Version 1.1.0.0
Under certain circumstances, if a station was moved to a different port within the same IP/IPX VLAN, it was possible to lock up the CPU for a long time. This problem was fixed in this release.
The GSR rebooted if you put in the wrong command structure using the following sequence: 1. Enter the command **interface create ip** 134net **address-netmask** 134.141.1.1/24 **port** et.1.1 2. Press Ctrl-p to retrieve the command entered above. 3. Press Ctrl-b to edit the above line by changing the IP address to 134.141.2.1/24 and then change the word '**create**' to '**add**' This problem was fixed in this release.

Issues Resolved in Version 1.0.1.3
Sometimes DHCP packets were forwarded through that interface even though the helper address did not permit DHCP packets to go through. This problem was fixed in this release.
If you specify an IP helper address on an interface with primary and secondary addresses, the DHCP packets were not always forwarded. This problem was fixed in this release.
The GSR ignored the broadcast bit in the “flags" field of a DHCP packet and replied with unicast instead of broadcast. This problem was fixed in this release.
When a DHCP client sent multiple requests quickly, the relay agent did not process the queued up packets completely. As a result, the relay agent processed the packets in a delayed manner, with the reply coming back with an old BOOTP transaction ID. This problem was fixed in this release.

Issue Resolved in Version 1.0.1.1
In some instances, the GSR failed to learn some SAP or Route entries. This occurred when a large number of SAP or RIP packets were received on the IPX interface. During this time, the IPX Client may have been unable to login to a Novell Server. This problem was fixed in this release.

Issues Resolved in Version 1.0.1.0
Telnetting into the GSR after applying and removing a service ACL no longer causes the GSR to crash.
When defining an ACL to deny UDP packets, the destination port configured is now the same as what the user chose from the provided list of ports using the name of the port.

Issues Resolved in Version 1.0.1.0
The SNMP community table (read/write privileges) was inconsistent with the active configuration under certain circumstances. This problem was fixed in this release.
When the **input_encapsulation** is set to **forced-ethernet_ii** mode, Spanning-Tree Protocol now works properly.
Under certain conditions, when a port was configured for IP and IPX interfaces, the GSR crashed due to the hash bucket full condition. This problem was fixed in this release.

KNOWN RESTRICTIONS AND LIMITATIONS:

The following features are not supported in the current release of the firmware:

Hardware

Control Module
If you are using a DGSRC-BA/BB Control Module, you must place the PCMCIA flash card in slot0. Slot0 is the top PCMCIA slot on the Control Module.
A Control Module memory upgrade is recommended if a GSR reports the error message - "SYS-E-MEM 95% of heap memory is used". This condition may occur when a GSR is deployed in a configuration having many L2 MAC addresses and L3 flows.
The GSR-16 requires the new DGSRC-BA/BB Control Module. If you use the old DGSRC-AA/AB Control Module with the GSR-16, it will not boot.

PCMCIA Flash Card
You can copy system image software onto a PCMCIA flash card. Note that the GSR supports only PCMCIA flash cards obtained from DIGITAL.
The amount of time it takes for system image software to be added to (or deleted from) a PCMCIA flash card increases the first five or so times it is done.
The PCMCIA flash card cannot be re-initialized from the CLI. It is not normally necessary to re-initialize the card. However, if the PCMCIA flash card becomes corrupted and re-initialization is necessary, the procedure is as follows: **Note:** This procedure will erase the PCMCIA flash card. If you boot from the PCMCIA flash card, you must place the boot image on a TFTP server so you can temporarily boot over the network.

PCMCIA Flash Card

1. Get to the system Boot PROM mode. To get to this mode, the GSR must either be rebooted or powered off, then on. When the GSR goes through its initialization, interrupt the normal boot sequence by pressing the Escape key. Typically, the GSR waits two seconds for user interruption before entering the normal boot sequence.

2. After you press the Escape key, a gsr-boot prompt is displayed. Enter the following commands:

   gs/r-boot> **pcumount**
   gs/r-boot> **erasepcvfs**
   gs/r-boot> **pcmount -i**

Note that while this procedure will work in all cases, the **pcumount** and **erasepcvfs** commands work only if the card was able to mount successfully.

When you complete this procedure, you will have a PCMCIA flash card that lacks the boot image. You may have to use the **set** command to change the netaddr, bootaddr, netmask, and/or gateway parameters, if these have not already been set appropriately. To do this, enter the following commands:

gs/r-boot> **set netaddr** <*IPaddr-of-management-port*>
gs/r-boot> **set bootaddr** <*IPaddr-of-TFTP-host*>
gs/r-boot> **set gateway** <*IPaddr-of-default-gateway*>
gs/r-boot> **set netmask** <*default-netmask*>

You can then boot over the network by entering the following command:

gs/r-boot> **boot** <*IPaddr-of-TFTP-host*> <*directory*>***I***<*image-file-name*>

Then use the **system image add** command in Enable mode to copy the boot image from the TFTP server to the PCMCIA flash card:

gs/r# **system image add** <*IPaddr-of-TFTP-host*> <*directory*>***I***<*image-file-name*>

Finally, use the **system image choose** command to select the appropriate file as your boot image

gs/r# **system image choose** <*image-file-name*>

You can back up configurations onto the PCMCIA card from the boot flash. To do this, enter one of the following commands in Enable mode:

gs/r# **copy** <*filename-on-bootflash*> **to slot0:** <*filename*>

or:

gs/r# **copy active to slot0:** <*filename*>

When loading a configuration stored on the PCMCIA card, first copy the file to the scratchpad and then commit the configuration. Enter the following command:

gs/r# **copy slot0:** <*filename*> **to scratchpad**

PCMCIA Flash Card

Then go into Configure mode and press Ctrl-Z. This makes the configuration active.

Boot Flash

If you see the following message when trying to modify the GSR configuration:

%SYS-E-VFSBADINUSECNT, WriteConfig: open: invalid in-use count

it means the boot-flash is corrupted and must be reformatted. To reformat the boot flash, do the following:

1. Make a copy of the GSR configuration file. The information in this file is lost when you reformat the boot flash.

2. Get to the system Boot PROM mode. To get to this mode, the GSR must either be rebooted or powered off, then on. When the GSR goes through its initialization, interrupt the normal boot sequence by pressing the Escape key. Typically, the GSR waits two seconds for user interruption before entering the normal boot sequence.

3. After you press the Escape key, a gs/r-boot prompt is displayed. Enter the following commands:

   gs/r-boot> **umount**
   gs/r-boot> **erasevfs**
   gs/r-boot> **mount -i**

100Base-TX Module

In some instances, if a 100Base-TX module is configured to auto negotiate, link failure may occur due to incorrect implementation of the auto negotiation feature by the device, such as, Sun Microsystems Quad 10/100 Ethernet controller connected to a GSR port. The workaround is to manually set the port speed and duplex settings on the GSR.

100Base-FX Module

Using a single power supply, a maximum of five 100Base-FX modules (keeping two slots empty) can be installed in a GSR chassis. If a GSR has more than five 100Base-FX modules, then the GSR may not be able to boot. The workaround is to add a second power supply to the GSR.

1000Base-SX/LX Module

If you are connecting the 1000 Base-SX/LX module to another device that does not support auto negotiation, then both devices' link negotiation mode should be turned off. Be sure that both devices are set to same link negotiation mode.

WAN Module

The WAN hardware does not provide internal clocking. A CSU/DSU combination is required for packet framing.

Firmware

System
If a configuration has a large amount of table information (routing table entries, etc.), make sure that the screen length (terminal row) is not set to 0.
CLI commands cannot be executed if a Telnet session is started via rsh from a UNIX system.
Updating and erasing the system firmware image should not be done simultaneously.
If you are using DGSRC-AA/AB Control Modules, network performance on the network management port (en0) may be slow under certain circumstances. The workaround is to use one of the other network ports, e.g., et.2.1 to perform tasks such as upgrading the firmware image or Telnet.
The local file system on the GSR currently does not fully support filenames with mixed or uppercase characters. Please use filenames with **only** lowercase characters.

WAN Modules
The maximum allowed MTU size for WAN interfaces is 1500 bytes and cannot be changed.
If WAN ports are in the default VLAN, L2 traffic does not bridge on the WAN ports.
A configuration with an IPX interface used in a VLAN containing both LAN and WAN ports is not supported.
IPX is not supported in partially meshed WAN networks if nodes are using the same network address. Different IPX network addresses should be used for each node of the network.
Port mirroring, ACL, L2 filtering is supported on a per-WAN-card basis, not on a per-port basis.
Although the WAN hardware contains compression/encryption capabilities, the 2.1.0.1 firmware release does not support these capabilities at this time.
For PPP, IPX Network numbers for both the local and peer router must be the same. Mismatched network numbers may cause routing and other problems.

Maximum Transmission Unit Size
The maximum allowed MTU size for IP and IPX interfaces is 1500. Make sure to set the proper MTU for different output MAC encapsulation frame types so that the packet size does not exceed the maximum Ethernet packet size of 1518. For example, if the Ethernet SNAP frame format is used for an IP or IPX interface then the MTU size should be set to 1492. (1492 [MTU] + 26 [SNAP header] = 1518 [maximum Ethernet packet])

Port Statistics
The number for layer-2 MAC broadcast frames in the port statistics menu is incorrectly counted twice.
Packets less than 64 bytes in length are incorrectly counted as either CRC or Alignment errors instead of Runt Packet errors.
The statistics counters for IP, ICMP, UDP and TCP cannot be cleared to conform to the SNMP standard.

Bridging
Under some circumstances, SNA/DLC/Netbios traffic cannot be bridged across GSR ports.

802.1d
Only one instance of STP is used for the whole system, and STP can be enabled or disabled on a per-port basis.
One MAC address is used for all the layer-2 protocols.
The **stp filter-bpdu** command should be used to discard all incoming HELLO frames (BPDUs) on ports where STP is not enabled.

802.1Q
If a trunk port is created, the port is changed from access to trunk, but is not automatically added to any VLAN. Use the **vlan add port** command to add the trunk port to required VLANs.
Before a port is made part of an 802.1Q trunk, it cannot be assigned to any VLANs other than the default. You must make the port into a trunk port before adding VLANs to the trunk port.

Quality of Service (QoS)
The **interface name** parameter, which is the last possible parameter when configuring an IPX QoS entry, does not work. Do not enter an interface name when configuring an IPX QoS entry.
Certain L2 QoS configurations may not work when applied to a port set to “flow-bridging” mode. (The default setting for a port is “address” mode). The situation typically is found in a lab-test environment where two stations are sending traffic to each other (and to no one else), through a GSR configured so that the ports are in flow mode, and where QoS entries apply to their bi-directional traffic. This results in packets always going through the CPU and, consequently, degraded performance.

CPU Redundancy
You cannot hot swap an active Control Module.
If the GSR has a line card with OPP version 1, you cannot hot swap the secondary Control Module.
In a two-Control Module setup, the Control Module that comes up first becomes the active Control Module. The system assumes this active Control Module’s MAC address. If both Control Modules come up at approximately the same time, one will restart the other. The Control Module that does the restart becomes the active Control Module, and the Control Module that is restarted becomes the backup Control Module.
If the backup Control Module fails to receive a heartbeat from the active Control Module for a certain interval, the backup Control Module assumes the active Control Module’s role, including its MAC address. If you repair or replace the non-functional Control Module and then reboot the GSR, the new Control Module will have a different MAC address.

SmartTRUNKs
When Spanning Tree Protocol (STP) is enabled on a SmartTRUNK, one link in the SmartTRUNK participates in STP. If you use STP with a SmartTRUNK that consists of ports of the same type, DIGITAL recommends that the ports in the SmartTRUNK be neighbors (i.e., in consecutive order) on the same line card.
DIGITAL has tested SmartTRUNKs made up of eight ports. SmartTRUNKs comprised of both 10/100TX ports and 1000SX ports have also been found to work properly.
When the Control Module is too busy to send or receive Huntgroup PDUs, SmartTRUNK links may be affected. This may be an indication of other, more serious, problems as well; for example, routing information may not be accurate.

SmartTRUNKs

To carry traffic from multiple VLANs across a SmartTRUNK, you should first make the SmartTRUNK into an 802.1Q trunk, then add VLANs to the 802.1Q trunk. To do this, enter the following commands in Configure mode:

1. Create a SmartTRUNK:

   gs/r# **smarttrunk create st**.<*n*> **protocol no-protocol**
   gs/r# **smarttrunk add ports et.2.1-2 to st.**<*n*>

2. Make the SmartTRUNK into an 802.1Q trunk:

   gs/r# **vlan make trunk-port st**.<*n*>

3. Add a VLAN to the 802.1Q trunk:

   gs/r# **vlan add ports st.1 to** <*vlan*>

If a SmartTRUNK has been configured to carry traffic for an IP VLAN and you want to have it carry traffic for the L2 default VLAN as well, you must make the SmartTRUNK into an 802.1Q trunk, then disable and enable the SmartTRUNK.

To make the SmartTRUNK work as an 802.1Q trunk, enter the following command in Configure mode:

gs/r# **vlan make trunk-port st**.<*n*>

When you activate this change, the SmartTRUNK becomes an 802.1Q trunk. To activate the 802.1Q trunk, you must disable and then enable the SmartTRUNK. To disable the SmartTRUNK, enter the following command in Configure mode:

gs/r# **port disable st.**<*n*>

After you enter this command, exit Configure mode and activate changes. Then go back into Configure mode and enter the following command to negate the previous command and enable the SmartTRUNK:

gs/r# **no port disable st.**<*n*>

When you activate this change, the SmartTRUNK begins to function as an 802.1Q trunk and carry traffic for both the IP and the L2 default VLAN.

IP Routing

The en0 (Ethernet port on the Control Module) is a management port only and is not intended to and does not perform routing.

The **globals**, **timers**, **interfaces**, **active-gateways**, **interface-policies**, **import-policies** and **export-policies** options for the **rip show** command do not work.

IP Routing

The default value of the OSPF hello-interval for virtual links has been changed to 10 seconds from 60 seconds.

Under certain circumstances, the following message might appear on the console:

set_next_hop: rt->rt_routers [0x809ed870] is nill

This has no impact on the system. This is an extraneous message that will be removed at a later date.

A maximum of 120 IP interfaces can be created on a GSR switch.

The default metric of routes redistributed into RIP is 16 (unreachable). Thus, when redistributing any routes into RIP from a different protocol (OSPF, BGP, static, direct, or aggregates), you should specify a metric, or set the default-metric with the following command:

gs/r(config)# **rip set default-metric** <*value between 1-16*>

If there is a redistribute or export-related policy command in the configuration, such as the following:

ip-router policy redistribute from-proto ospf to-proto rip

then the default policies are superseded. To announce routes that would have been announced by default policies, you must explicitly redistribute from a protocol (OSPF, BGP, static, direct, or aggregate).

For example, by default, RIP announces the direct interfaces. When you redistribute OSPF into RIP on the GSR, you would have to then explicitly redistribute direct interfaces into RIP as well:

ip-router policy redistribute from-proto direct to-proto rip

Under certain circumstances, a direct route that is redistributed into OSPF may not be advertised as OSPF Type 5 LSA. In these cases, do one of the following:

- Run OSPF on that interface and set the hello interval to a high value (for example, 300 seconds) so that the overhead on the system is minimal. In this case, the interface would be advertised into OSPF as a stub network.
- Bring the interface down, and then bring it back up after 20 seconds using the following Enable mode commands:

  gs/r# **interface down** <*interface*>
  gs/r# **interface up** <*interface*>

If you have not configured a DNS server, or have disabled DNS lookup with the **ip disable dns-lookup** command, make sure you specify an IP address for the **gateway** and **gatelist** options of the **ip add route** command, rather than a hostname.

BGP

The **bgp show route default** command shows all routes, rather than just the default route.

IPX Routing

A maximum of 64 IPX interfaces can be created on a GSR switch.

Proxy ARP

By default, the Proxy ARP feature is enabled. To disable Proxy ARP, use the **ip disable proxy-arp** command.

When creating an IP interface, the **ip interface create** command requires a logical name for each interface. If you use a name that begins with “en” or “lo”, it causes the GSR to disable proxy ARP on some (if not all) IP interfaces.

DVMRP

If an interface that has DVMRP or IGMP enabled is deleted and added back again, the DVMRP and IGMP do not detect it. The workaround is to restart DVMRP by executing the **no dvmrp start** command and committing the change followed by executing the **dvmrp start** command and committing the change.

DVMRP scope does not work in the current release of the firmware.

A multicast packet is replicated to only one IP VLAN in an 802.1Q trunk port. Instead of an 802.1Q trunk port, you should use an access routed interface to forward multicast packets between two GSRs.

Access Control Lists

On rare occasions, when creating an IPXGNS ACL, a ServiceType of "4" gets translated to "FFFF".

The "implicit deny rule" is applied differently to an ACL for IPX than it is to an ACL for IP. For IP (and as stated in the documentation), once an ACL is defined at all, the implicit deny rule denies all traffic. You must then explicitly permit traffic as desired. However, for IPX, the implicit deny rule only applies to the specific traffic type the ACL addresses (RIP, SAP, etc.). So an ACL that permits RIP traffic from source address 10 will deny (implicitly) all other RIP traffic but will not effect any other type of traffic.

TACACS/RADIUS

The **system show users** command does not show the names of users that have been authenticated through TACACS or RADIUS.

RMON

The negate command does not work on RMON commands in an active configuration. If you negate an RMON command in an active configuration and enter a new command to replace it, the previous RMON command will still be in effect. The workaround is to reboot the GSR. This problem will be fixed in the next release.

GSR-16 Firmware

If you need to downgrade the GSR-16's system firmware from version 2.x.x.x code to version 1.2.x.x, make sure to power down the GSR and power up again before downgrading system firmware. If you do not do this, the GSR may not be operational, or you may see the following error message:

SYS_ERR: Transmit queue full

ARP

A new command, **arp set interface** <*interface name*> **keep-time**, was added to the 2.0.0.0 release. This command allows you to set ARP aging time for an IP interface.

DIGITAL clearVISN CoreWatch Software

Information about DIGITAL clearVISN CoreWatch is covered in a separate Release Note. The *DIGITAL clearVISN CoreWatch User's Guide* is located on the GSR Software and Documentation CD.

COMPLIANCE SUPPORT:

Compliance Level	Compliant
Year 2000	Yes

Known Anomalies: None

IEEE STANDARDS MIB SUPPORT:

Standard	Title
IEEE 802.1d	Spanning Tree
IEEE 802.1p	Traffic Prioritization
IEEE 802.1Q	Port Trunking
IEEE 802.3	10 Mbps Ethernet
IEEE 802.3u	100 BASE-T Ethernet
IEEE 802.3x	Full Duplex Ethernet
IEEE 802.3z	1000 Mbps Ethernet

IETF STANDARDS MIB SUPPORT:

RFC	Title
RFC 1058	RIP v1
RFC 1105	BGP
RFC 1157	SNMP
RFC 1163	BGP-2
RFC 1213	MIB-2
RFC 1253	OSPF v2 MIB
RFC 1265	BGP Protocol Analysis
RFC 1266	Experience with the BGP Protocol
RFC 1267	BGP-3
RFC 1293	Inverse ARP
RFC 1315	MIB for Frame Relay DTEs
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1349	Type of Service in the Internet Protocol Suite
RFC 1397	BGP Default Route Advertisement
RFC 1490	Multiprotocol Interconnect over Frame Relay
RFC 1493	Bridge MIB
RFC 1493	Definitions of Managed Objects for Bridges
RFC 1519	CIDR
RFC 1548	The Point-to-Point Protocol (PPP)
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1570	PPP LCP Extensions
RFC 1573	Interfaces MIB
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1583	OSPF v2
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1643	Ethernet Like Interface MIB
RFC 1656	BGP-4 Protocol Document Roadmap and Implementation Experience
RFC 1657	BGP-4 Definitions of Managed Objects

RFC	Title
RFC 1661	PPP (Point-to-Point Protocol)
RFC 1662	PPP in HDLC-like Framing
RFC 1723	RIP v2
RFC 1724	RIP v2 MIB
RFC 1757	RMON
RFC 1757	Remote Network Monitoring (RMON) Management Information Base
RFC 1771	BGP-4
RFC 1772	Application of BGP in the Internet
RFC 1812	Router Requirements
RFC 1966	BGP Route Reflection
RFC 1997	BGP Communities Attribute
RFC 2096	IP Forwarding MIB

DRAFT SUPPORT:

Function	Draft
DVMRP	Draft-ietf-idmr-dvmrp-v3-06.txt
802.1Q VLAN	IEEE Draft Standard P802.1Q/D9

IETF STANDARDS SNMP TRAP SUPPORT:

RFC	Title
RFC 1157	linkDown, linkUp, authenticationFailure Traps
RFC 1493	newRoot, topologyChange Traps

FRAME RELAY STANDARDS SUPPORT:

Standard	Title
Frame Relay Forum FRF.1.1	User-to-Network (UNI) Implementation Agreement
Frame Relay Forum FRF.3.1	Multiprotocol Encapsulation Implementation Agreement
ITU-T Q.922/ANSI T1.618	ISDN Core Aspects of Frame Relay Protocol
ITU-T Q.933	Access Signaling Annex A
ITU-T I.122/ANSI T1S1	Standards-Based Frame Relay Specification
ITU-T Annex D/ANSI T1.617	Additional Procedures for PVCs Using Unnumbered Information Frames

ENTERPRISE PRIVATE MIB SUPPORT:

ctron-trap-mib *version 1.1.0.3*	ctron-yago-config
ctron-yago-hardware	ctron-yago-l2
ctron-yago-l3	ctron-yago-service-status
ctron-yago-trap	novell-rip-sap-mib
ctron-lfap	ctron-policy
novell-ipx-mib	

Cabletron Private Enterprise MIBs are available in ASN.1 format from the Cabletron web site at:

http://www.cabletron.com/support/mibs/

Indexed MIB documentation is also available.

ACCESSING ONLINE INFORMATION:

DIGITAL Network Product Group Web Site

Further information on this network product or topic is available on the DIGITAL Network Product Group (DNPG) Web Site. The Web site maintains a common, rich set of up-to-date information on NPBG's products, technologies, and programs.

The Web Site can be reached at geological locations via the following:

Americas:	http://www.networks.digital.com
Europe:	http://www.networks.europe.digital.com
Asia Pacific:	http://www.networks.digital.com.au

For a listing of all the products available on the DNPG Web Site, please choose the "Technical Information" link, and from there choose the "Technical Information (Drivers, Manuals, Tech Tips, etc.)" link.