

3COM ROUTER 5000 / 6000 RELEASE NOTES

Software V 2.21

Release Date October 2005

Software Release Filenames

- r5y02_21e.bin is the encrypted software agent running on 5012, 5232, 5642 and 5682 routers;
- r5y02_21v.bin is the non-encrypted software agent running on 5012, 5232, 5642 and 5682 routers;
- r6x02_21e.bin is the encrypted software agent running on 6040 and 6080 routers;
- r6x02_21v.bin is the non-encrypted software agent running on 6040 and 6080 routers.

Bootrom Version

- For 5012, 5232, 5642 and 5682 routers, the compatible Boot rom version is **9.13**
- For 6040 and 6080 routers, the Bootrom is included as part of the released software agent.

Introduction

These release notes supercede the V2.11 and V2.20 Release Notes.

These release notes address the following:

- New Features
- Software Upgrade Information
- Hardware Accessories Installation
- System Access
- SNMP
- System Management
- Interface Management

- Link Layer Protocol
- Network Protocol
- Routing Protocol
- Multicast Protocol
- Security / VPN
- Quality of Service
- Documentation Errors
- Resolved Issues

New Features

There is a new command:

```
'configure-user count 1-35'
```

Which allows the system administrator control over the number of users that have access to the System View.

New menu option:

In the bootrom menu, there is an additional menu option to "Reset Console Authentication" for password recovery. The new 5000 Router boot rom image v9.13 is required for this fix.

Software Upgrade Information

To obtain the latest version of the Router software, visit the 3Com website for software downloads.

Hardware Accessories Installation

The Router 2-Port 10/100 MIM, 3C13761 2FE AA version is incompatible with Router 5012 and will cause a system lock up. There are no compatibility issues with this module in the Router 5232, 5642, 5682. Please use the “display version” command to check for the hardware revision of your 2-Port 10/100 MIM. 3C13761 2FE AA has a hardware version of 2.0. Contact 3Com to RMA this module and obtain a replacement MIM, 3C13761 2FE.

The following new cards include hardware fixes, resolving issues with D4, D4/AMI , FDL Loop-back and loop-back LED's. The new V2.21 upgrade software supports these new hardware fixes. New T1's reflect solid amber LED activity for FDL Loop back. Refer to “3Com Router Modules Installation Guide” for the updated LED definition and behavior.

Description	3C#	Label	Revision
2-port T1	3C13769	MIM-2CT1	AB
1-port fractional T1 SIC	3C13720	SIC-FT1	AB

Please note that release V2.21 software supports the 2 port channelized T1 MIM and 1 port fractional T1 SIC interface cards with previous hardware revision with the existing behavior.

System Access

- The router does not allow configuring of an FTP server with Radius Authentication None option. FTP Anonymous login is not supported. A username and password is required for FTP access
- The FTP server does not support filenames containing spaces. 3Com recommends that using underscores instead of spaces as separation delimiters.
- To get ftp mputs to work properly from a client, ftp update normal must be set on the router.
SYSTEM ACCESS

SNMP

- The router does not respond to SNMP when the user is logged into the System View. This causes Network Management Systems such as 3Com Router Manager and 3Com Network Director to generate errors. To resolve this, exit the System View.

- The Frame Relay MIB does not use the latest version of the RFC 2115. As a result, public MIB variables for troubleshooting Frame Relay performance problems are not supported; (e.g. frCircuitLogicalIndex) from the current FRAME_RELAY-DTE-MIB (RFC 2115)
- The router will send an initial invalid trap packet upon link down/up event, followed by the correct trap packet. Ignore the first trap packet, the second packet is correct.

System Management

- Analog Modem debugging shows internal activity when no cable is connected. This indicates that the modem is active and ready to receive or make calls.
- When saving a configuration to a non-existing directory the following message displays: “Cannot open the configuration file, this may be caused by insufficient memory space”. This is an incorrect message and is displayed when the user is trying to save a file to a non-existent directory. To solve the problem, create the directory first.
- If the user cut and pastes within the BootRom menu to fill in fields (such as filenames for TFTP downloads) the display will only show a maximum of 8 characters. If the filename is longer it will be accepted by the system, but will not display characters beyond the initial 8.
- A 1-Port channel E3 MIM card will not operate if inserted in slot 0 on the 5642 or slot 1 on the 5232. Select a different slot for the E3.
- The “more” command truncates large config files(>17KB) on the 5012 routers. If the file needing to be read is not the saved configuration, transfer the file to a PC disk, and read it from there. If it is the saved configuration, read it with the “display saved-configuration” command.
- 5000 series routers report that the system returned to service via “power-on” even if the router is warm booted.
- Regardless of actual traffic running or not, T3 and E3 activity LED’s blink constantly.
- Display ft1 will display the same statistics multiple times, once for each Frame Relay interface/sub-interface configured.
- Display interface for an ATM interface with sub-interfaces will display the same cumulative statistical information - no individual statistics are provided; Instead use, display atm interface to show more individualized statistics.
- An ATM PVC that is set with rate limiting and is heavily oversubscribed with data, will fail to pass traffic. Other PVCs continue to work on the link.

Interface Management

- Interface statistics with a flow-interval of under 10 seconds are not accurate. Do not enter flow-interval values under 10 seconds.
- The Virtual-Ethernet interface protocol state is always down when running PPPoE. Use “ping” to verify that the interface is actually up and working properly.

- On an ISDN interface, the Line Protocol state is up when no cable is attached to the port on the interface. It is best to observe the interface's Current State. The Current State will be down if no cable is attached to the interface even though the Line Protocol will show it as up.
- A Frame Relay sub-interface that has been configured as 'Down' transmits packets.
- Displaying a Fractional E1 interface displays a Frame Format equal to NONE. The actual Frame Format is no-crc.
- Frame Relay Payload Compression is displayed for PVC even after it is removed. Reset the interface to resolve.
- The current IMA aggregate baud rate does not change when links are added or removed, when using the display interface command. This is a display problem only.
- Changing the speed on a modem interface resets the interface. Do not change the modem interface speed while a dialup session is active.
- The Gigabit Ethernet module does not support half duplex mode at 100 Mb setting.
- Display fr pvc statistics do not account for the outbound packets.

Link Layer Protocol

- Frame Relay PVCs can be modified when they are part of a PVC switching endpoint. Verify first that the interface is not a PVC endpoint before making any changes.
- There is no DEBUG support for Multilink Fragmentation (FRF.16.1).
- Status and statistics for Multilink Fragmentation (FRF.16.1) cannot be viewed
- There is no support for ISDN switch type AT&T for BRI U interfaces. The router Command Line Interface and the documentation specifically states that AT&T is only supported on PRI interfaces. The default isdn protocol-type dss1 will connect to switches using AT&T switch type on a BRI interface. This was tested with Lucent 5E, otherwise known as AT&T 5ess.
- The "bridge x mac-address" command for setting a static MAC entry for a gigabit Ethernet interface is not supported.
- The "bridge X mac_address XXXX-XXXX-XXXX permit interface" command is not an option for a Gigabit type interface. This command is not supported for Gigabit interfaces.
- Bridge-set traffic cannot be routed even though a bridge-set can be configured with an IP address.
- FRF.9 Compression is still displayed upon viewing of PVC statistics, after the PVC is re-mapped without FRF.9. After re-mapping a PVC to exclude FRF.9 compression, reset the interface in order to clear any reference to FRF.9
- When removing FRF.9 compression settings from a frame relay static address mapping, the interface needs to be reset (shutdown/undo shutdown) for the configuration to take place.
- CRC and PAD errors on the 1-Port ADSL Module interfere with even the lowest traffic loads, of expected normal operation - Example 256K traffic on 8Mb link.

Network Protocol

- Certain web sites cannot be accessed when using DSL interfaces. To resolve this, set the outgoing router (WAN) physical or virtual interface to 1410 as the maximum segment size for TCP.
- The DHCP Server does not remember the DHCP clients after a reboot. The DHCP lease expiration, client reboot or client renew request will repopulate the DHCP clients table transparent to the user.
- A Router running DHCP client cannot obtain the default gateway address automatically. This parameter must be manually configured.

Routing Protocol

- OSPF interface costs are not the same on peer DCE/ DTE Frame Relay Serial interfaces. If a Frame Relay DTE Serial interface is configured for OSPF, and the DCE has a differing baud rate, the interface has to be configured with the "virtualbaudrate" command. Configure this command using the same baud rate as the DCE. After configuring, shut down and restart the interface.
- BGP Auto-summary does not work for networks incorporated via the Network command. Only imported routes are auto-summarized.
- Undo RIP from interface view removes RIP globally. To remove RIP from interface view use the command, "Undo RIP work."
- BGP route dampening does not work for IBGP routes. BGP dampening is designed to work only for EBGP routes
- The 3Com router will not exchange RIP Updates with a 3rd Party vendor's equipment when MD5 "usual" implementation is configured. The 3Com router will only exchange RIP Updates with a 3rd Party vendor's equipment when MD5 'Non-Standard' implementation is configured. Use 'Usual' to exchange RIP Updates between 3Com routers.
- The BGP route is not advertised if the IGP route is present in the forwarding table. Import the route into BGP from the protocol which owns the route in the forwarding table.
- RIP Poison Reverse is not supported.
- IPX is not supported on Frame Relay, HDLC, and X25. IPX is only supported on Ethernet and PPP.
- The BGP received and advertised routes for a particular peer ("display bgp routing-table peer x.x.x.x received|advertised") are not displayed in numerical order.

Multicast Protocol

- The default value for the IGMP query interval does not match the recommended value in RFC 2236. Set the query interval to match the query interval of other routers in the network.
- PIM is not supported with IP unnumbered FR interfaces. An IP address must be assigned to the FR interface.
- PIM is not supported over an IPsec tunnel. PIM hellos are rejected over an IPsec Tunnel.

Security/VPN

- NAT traversal does not work in IKE Main Mode. IKE Aggressive Mode is required for NAT traversal to function properly.
- Packets with internal addresses appear outside the NAT boundary. NAT does not translate ESP or IGMP packets. NAT does not translate any IP protocols other than ICMP, TCP, UDP, and GRE (with respect to PPTP)
- The firewall drops FTP connections when ASPF is configured to filter TCP. ASPF must be configured with TCP and FTP together.
- With CRL checking enabled by default, certificate enrollment cannot be performed and an IPsec tunnel cannot be established without the CRL on the router. CRL checking must be disabled for certificate enrollment and the IPsec tunnel if the CRL is not on the router.
- Juniper's IPsec implementation does not interoperate with the 3Com Router 5000 Series Family with respect to IPsec Fragmentation. If possible, set the MTU to 1438 or lower on devices that will be using the tunnel to avoid having to fragment IPsec packets.
- If an undefined ACL is used in a configuration, a warning message is not displayed.
- In X.509 the CRL URL format determines which protocol is used to retrieve CRL from the CA server. Use one of the following CLI commands depending on specific Server support:
 - HTTP: `crl url http://<CA Server IP>/<CRL DP>`
 - LDAP: `crl url ldap://<CA Server IP>/<CRL DP>`
 - SCEP: `crl url "scep"`
- When a policy or ike peer is configured with an underscore character (“_”), the display current command of the begin filter will not recognize the underscore character. Use the backslash character (“\”) to bypass the underscore. Do not use an underscore with the configuration filter.
- IPSEC ACLs with deny rules before the “permit all” rule results in the system ignoring the deny rules.
- ACL matches for IPsec only count the first packet used to open the tunnel - subsequent packets will be logged in the IPsec SA; Also, IPsec does not support Fast Forwarding.
- Manual Ipsec only protects the first match in an ACL with multiple rules; Recommendation: make only one rule per ACL to protect all desired traffic.
- The first IKE peer with local-address defined will have its address be used for all IKE peers in the policy.
- Ike peer-name does not seem to work as documented in the NAT-Traversal Example; In order to get name authentication to work, both sides must have id-type name configured. Both sides must have remote-names configured, and one side must have remote-ip configured (the initiator).

Quality of Service (QoS)

- QoS CBQ can be configured on a dialer interface but it has no effect. Place the QoS Policy on the physical interface rather than the logical dialer interface.

- Once a QoS policy is applied use the CLI command “reset IP Fast Cache” to re-apply the QoS functions properly.

MPLS

- If there is no response, from pinging a CE Router from a PE Router within an MPLS/BGP L3 network use the command “ping -vpn -a xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx”, using the source address of the PE interface that is in the VPN of the intended target.
- If Loopback0 and LSR ID ip addresses are different, MPLS LDP will not work properly . The Loopback0 and LSR ID ip addresses must be match.

Documentation Errors

- Firewall ASPF UDP detection does not support the following UDP based applications: TFTP, SSH, DHCP
- Named access list is documented but not supported .
- Name based ACLs, as listed in the command reference manual, are not supported.

Resolved Issues

The following issues have been resolved since the last release (v. 2.11) of this software.

- In some specific circumstances, displaying virtual-access on a router with MLPPP may cause a reboot. To resolve this, use the command, Display Virtual Template instead.
- A baud rate setting of 786000 is not available on a serial interface.
- The state of Promiscuous mode on an Ethernet interface is not shown in the “display current” command. To view the state of Promiscuous mode, use the “display interface Ethernet x/x” command.
- Gigabit Ethernet interfaces will not forward traffic if they are assigned to a bridge-set. Gigabit interfaces should only be assigned to routed interfaces.
- When a bridge-set is removed from an Ethernet interface the message “Promiscuous operation mode was removed automatically” is displayed. However, promiscuous mode may not have been disabled on that interface. Manually verify that Promiscuous mode has been reset using the “display interface Ethernet x/x” command. If it has not been disabled, use the “undo promiscuous” command in the interface view.
- There is no support for ISDN switch type DMS100 .
- Frame Relay sub-interface definition types (P2MP, P2P) are not displayed. To determine the interface type, display the interface as follows: “Display fr pvc interface <interface> <dlci>.”
- Frame Relay Classes that contain Frame Relay QoS parameters can be applied to PVC’s even though Frame Relay Traffic Shaping is not enabled. Frame Relay Traffic Shaping must be enabled for PVC queues to be functional.

- When IPSec policies are configured on both the incoming and outgoing interfaces, one of the interfaces needs to have IPSec over GRE configured to allow multicast IP fragments to pass through the router without problems.
- The ability to add inline comments to describe an ACL as a whole is available, however the ability to add a specific description to a rule is not available. Example: if an ACL is long and complicated, inline comments for the rule cannot be added. Save the current configuration and then edit in descriptive comments to that configuration.
- FDL and remote loop back issues.
- B8ZS and ESF issues.
- LBO range issues.
- Alarm Threshold Settings issues.
- Issues with viewing current alarms and error registers.
- Various issues with Loop backs , local, payload and remote.
- DEBUG commands on the serial interface and physical layer characteristics of the router modules.
- UNDO of the DEBUG function.
- Constant DEBUG output issues on the FT1 SIC module.
- No indication of resetting (zeroing) traffic statistics.
- Lack of input and output rates displayed in bits per second as part of traffic statistics output.
- A logging error where VPN information is logged erroneously, when there was no actual VPN configuration.
- Only one system user at a time able to access the console.
- With the display interface command, packet flow shows double that of the Ethernet interfaces.
- Inaccurate display information with ACL statistics, not properly incrementing for permit statements.
- Frame Relay statistics discrepancies on the sub-interface packet counts.
- Statistics on the FT1 and T1 interfaces not properly zeroed upon reset command, "reset counter interface".
- Banner information being lost upon FTP or TFTP while obtaining router information.
- A packet loss problem with small packet sizes configured.
- No display of trap settings with status.

- IPsec tunnel does not get established with Cisco routers when a NAT device is in the communications path. NAT traversal is not compatible with Cisco routers.
- Only one security association is used for all traffic flows. IPsec SA is not flow based. IPsec SAs originated from 3COM routers will be ACL based. To obtain flow-based functionality, create multiple ACLs with one rule each.

The following issues have been resolved since the last release (v. 2.20) of this software.

- Changing the speed and duplex on the Gigabit Ethernet Module does not take effect without resetting the interface manually. A manual “shutdown” and then “undo shutdown” is required to have the changes take effect.
- Loopback LED remains lit solid after remote side sends the loop down code - No Loopback LED indicator
- Banners edited offline in the proper format will be discarded when loaded into the system via ftp/tftp
- D4, D4/AMI and ones density are not supported.
FDL AT&T payload option issues.
No `fdl-att-plb-up` and `fdl-att-plb-down` are available.
- Alarm LED - No Alarm LED indicator
- BERT issues - Bits received since test started and Bits received since latest sync do not match on a perfect loop
- NAT display issues - NAT sessions do not display "NO-PAT"

User Documentation issues resolved since the last release (v. 2.20) of this software.

- ACL numbering scheme is different from those documented in the Command Reference Manual. Use the following corrected numbering scheme:
1000-1099(Interface-based ACL)
2000-2099(Basic ACL)
3000-3099(Advanced ACL)
4000-4999(Ethernet Frame Header ACL)
- The Command Reference manual states that “reset ike sa” will clear both phase 1 and phase 2 security associations. “Reset ike sa” will only clear phase 1 security associations; “reset ipsec sa” will clear phase 2 security associations
- MPLS LDP loop detect cannot be configured after LDP is enabled on interface. An error is reported.
Enable LDP loop detect under system view before enabling LDP on the interface.
- The “virtualbaudrate” command is non-existent in the Command Index. Use the “virtualbaudrate” command in the Command Line Interface (CLI).
[XXXX-3-Serial2/0/4]virtualbaudrate?

300 only for async mode
600 only for async mode
1200 for syn & asyn mode
2400 for syn & asyn mode
4800 for syn & asyn mode
9600 for syn & asyn mode
19200 for syn & asyn mode
38400 for syn & asyn mode
56000 only for syn mode
57600 for syn & asyn mode
64000 only for syn mode
72000 only for syn mode
115200 for syn & asyn mode
128000 only for syn mode
384000 only for syn mode
2048000 only for syn mode