Applications Ware Software Release 7.3.R00A
Release Notice

Table of Contents

1 Overview

This notice contains update information for Release 7.3.R00A of the operating software for the following Vanguard platforms:

- Vanguard 3410
- Vanguard 3460
- Vanguard 6840
- Vanguard 7310
- Vanguard 3410W
- Vanguard 3480
- Vanguard 6841
- Vanguard 7330

The following Vanguard platforms are not supported in Release 7.3.R00A:

Platform	*Latest Supported Release*
Vanguard 100	Release 5.3M
Vanguard 200	Release 5.1M
Vanguard 242D/340 Enhanced/342	Release 7.2.R00A
Vanguard 300	Release 5.4
Vanguard 305	Release 5.5
Vanguard 311	Release 5.1M
Vanguard 311PLUS/312PLUS	Release 5.3M
Vanguard 320	Release 6.4.R00A
Vanguard 340	Release 7.0.R00A
Vanguard 6425/6430/6450	Release 6.0.R00A
Vanguard 6435/6455	Release 7.0.R00A
Vanguard 6520	Release 5.5
Vanguard 6560	Release 6.0.R00A
6500PLUS	Release 5.1M
650D	Release 5.0C
Voice feature on the Vanguard 100	Release 5.2

This notice supplements the full set of the Vanguard user documentation.

2 Applications Ware

This section explains how the Applications Ware software is organized, implemented, and modified.

2.1 Applications Ware Licenses and Upgrades

The Release 7.3.R00A Applications Ware is divided into four base licenses and four to five upgrade licenses (depending on the platform). Customers are required to purchase only one base license and can purchase optional upgrade licenses to add to the base license. Compatibility of upgrade licenses with base licenses and various products is dependent upon a specific product and its capabilities.

2.1.1 Applications Ware Base Licenses

- IP+ Applications Ware License (7310, 7330)
- IP SAFE Applications Ware License (3400 and 6800)
  - Note: Beginning with Release 7.1R00A, the IPSafe Applications Ware license includes SSH Server with external Radius Authentication and software based IPSec VPN
- SNA+ Applications Ware
- Multi-Service Applications Ware

2.1.2 License Upgrades

- Voice Applications Ware License Upgrade
- Encryption Acceleration Applications Ware License Upgrade
- AS/400 BSC Applications Ware License Upgrade
- Advance Voice (Premium Services + SIP)
- Security Services

Note: A license refers to both a legal document that allows a customer to use features and to the software that contains the features. One base license must be purchased for each hardware platform.

2.2 Default Software Images and Functionality

Each license contains a large number of software features and functions. In addition, each hardware platform has a default factory image that contains a subset of the full license. In some cases, the default image might not completely meet your needs. You can either create a new Vanguard customer image using the Software Builder application on the Vanguide CD-ROM, or use our Vanguard Customer Ware Program.

For details about all features in a particular Applications Ware License, refer to the appropriate section further on in this document.

2.3 Software Upgrade to 7.3.R00A Tech Tip

Always save a back-up of CMEM (configuration memory) file before upgrading. This backed-up CMEM file can be used to reload the configuration if you downgrade or lose the configuration.

Be aware that downgrading from 7.2.R00A to any prior release is not supported and note that problems will occur with the configuration memory. To properly downgrade, the configuration should be defaulted and then restored with the saved CMEM that was running in the prior release (DRCaa22736).

2.4 License Upgrades

The License Upgrades differ from standard Applications Ware packages in that they do not operate in a “stand-alone” capacity. For example, if you want the functions available in the SNA+ Applications Ware, you purchase that license and load it into your unit. However, a License Upgrade cannot be loaded into a unit by itself. You must:

- Purchase one of the standard Applications Ware packages
- Purchase the License Upgrade
- Use Software Builder to add the License Upgrade to the standard Applications Ware package.

2.5 Memory Requirements for Applications Ware Release 7.3R00A

The total memory required for each product at release 7.3.R00A is listed in this table:

Platform	Required Memory	Required FLASH
Vanguard 3410/3410W/3460/3480 RAM	64MB SDRAM	16MB Flash
Vanguard 6840, 6841	256MB DRAM	256MB Flash
Vanguard 7310, 7330 (V2, V3)	512MB DRAM	64MB Compact Flash

Notes:

- The table above lists the memory that is shipped.
- Release 7.3.R00A does not support the Vanguard 100, 200, 300, 305, 311, 311^{PLUS}, 312^{PLUS}, 320, 340, 242D, 342, 340E, 6425, 6430, 6450, 6435, 6455, 6520, 6560 platforms.

3 Products Supported

Products supported by Release 7.3R00A

Product	Support
Vanguard 3410, 3410W, 3460, 3480	Normal Product Release
Vanguard 6840, 6841	Normal Product Release
Vanguard 7310, 7330 (V2, V3)	Normal Product Release

Release 7.3.R00A is not supported on these discontinued products:

Product	Last Release Supported
Vanguard 100	Maintained at 5.3M.
Vanguard 200	Maintained at 5.1M.
Vanguard 300	Maintained at 5.4.
Vanguard 305	Maintained at 5.5.
Vanguard 311	Maintained at 5.1M.
Vanguard 31x+	Maintained at 5.3M.
Vanguard 320	Maintained at 6.4.R10A.
Vanguard 6425, 6430, 6450	Maintained at 6.0.R00A.
Vanguard 340	Maintained at 7.0.R00A.
Vanguard 6435, 6455	Maintained at 7.0.R00A.
6500+	Maintained at 5.1M.
650D	Product maintained at 5.0C
Vanguard 6520	Product maintained at 5.5
Vanguard 6560	Product maintained at 6.0.R00A
Vanguard 342, 340E	Maintained at 7.2.R00A.
Vanguard 242D	Maintained at 7.2.R00A.

4 New Features

The new features available for Release 7.3.R00A are described briefly below. Detailed descriptions of the new Release 7.3.R00A features can be found in the referenced documents. Each document can be accessed through the Vanguard Networks Public website at the following url:
http://www.vanguardnetworks.com/support-documentation-overview.htm

Instructions for obtaining on-line and CD versions of the documents that contain detailed explanations of these features appear in the “How to Obtain User Documentation” section in this document (Chapter 12).

4.1 New Hardware Platform – 3410W Access Services Gateway

The Vanguard 3410W provides a high performance, cost effective WAN CPE solution for Internet Access, Broadband VPN, MPLS, Frame Relay, or lease-line services. The 3410W ASG supports optional connectivity to Bisync, SNA, or Serial transactions devices (ATMs, bank controllers, POS devices, etc.) on today’s and tomorrow’s carrier transport technologies, enabling seamless migration without “ripping and replacing” non-IP applications or peripheral devices. The 3410W ASG has the performance and headroom needed in an all–IP future while Vanguard Networks’ customers are assured of investment protection for their existing applications.

Hardware details can be found in the user manual titled “3400 Installation Guide”. Software details can be found in the various software manuals on the Vanguard Networks website at:
http://www.vanguardnetworks.com/support-documentation-overview.htm

3410W Daughter Card Support:

Daughtercard		3400 Series Platform					
Description	Product Code	3410	3410W	3460		3480	
		DC Site 1	DC Site 1	DC Site 1	DC Site 2	DC Site 1	DC Site 2
2P-SDC (2-Port Serial)	1130-10004	---	Yes	Yes	Yes	Yes	Yes
56K DSU	68472	Yes	---	Yes	Yes	Yes	Yes
Dual E&M	65729	---	---	Yes	Yes	Yes	Yes
Dual FXS	68372	---	---	Yes	Yes	Yes	Yes
BRI Voice	68525	---	---	Yes	Yes	Yes	Yes
FT1 - 120 □	49666	Yes	---	Yes	Yes	Yes	Yes

FE1 - 75 □	49669		Yes	---	Yes	Yes	Yes	Yes
FE1 - 120 □	49716		Yes	---	Yes	Yes	Yes	Yes
FT1 - 120 □	1600-00001		Yes	---	Yes	Yes	Yes	Yes
FE1 - 75 □	1600-00075		Yes	---	Yes	Yes	Yes	Yes
FE1 - 120 □	1600-00120		Yes	---	Yes	Yes	Yes	Yes
FXS/FXO	80019		---	---	---	---	---	---
G.SHDSL	1152-10009		---	---	---	---	---	---
Quad FXO	1152-10035		---	---	Yes	Yes	Yes	Yes
Quad FXS	1152-10034		---	---	Yes	Yes	Yes	Yes
ISDN BRI S/T	68525		---	---	---	---	---	---
ISDN BRI S/T	1152-10005		---	---	Yes	Yes	Yes	Yes
ISDN BRI-U	68434		---	---	---	---	---	---
V.11 DCE (Serial)	49649		---	Yes	Yes	Yes	Yes	Yes
V.24 DCE (Serial)	46946		---	Yes	Yes	Yes	Yes	Yes
V.35 DCE (Serial)	49647		---	Yes	Yes	Yes	Yes	Yes
V.36 DCE (Serial)	49648		---	Yes	Yes	Yes	Yes	Yes
V.11 DTE (Serial)	49661		---	Yes	Yes	Yes	Yes	Yes
V.24 DTE (Serial)	49658		---	Yes	Yes	Yes	Yes	Yes
V.35 DTE (Serial)	49659		---	Yes	Yes	Yes	Yes	Yes
V.36 DTE (Serial)	49660		---	Yes	Yes	Yes	Yes	Yes
V.90 (Modem)	1152-10003		---	Yes	Yes	Yes	Yes	Yes

4.2 MD5 - BGP peer authentication

BGP Peer Authentication is the newest method to reduce security risks in a BGP network. The Vanguard implementation of BGP peer authentication uses the TCP MD-5 signature as specified in RFC 2385. This algorithm takes a key, the password entered during configuration, and performs an MD-5 hash on the key, and sends the resulting hash to the remote peer. The password itself is never sent over the connection.

Both sides of an authenticated BGP peer session must use the same password.

The authentication occurs in the TCP session not on the BGP peer session.

It provides added confidence that packets received from the TCP peer actually originated from the authorized TCP peer.

Though first released in patch 7.2P01D, the following parameter is new and is now generally available in release 7.3.R00A.

This new parameter “MD5 Password” can be found under “configure>configure router>configure BGP>Peer Parameters”.

MD5 Password

Range	1-25 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	Enter password for TCP MD5 Signature Option. A blank password means the feature is turned off.

4.3 NHRP (Next Hop Resolution Protocol)

Vanguard Networks Routers now support NHRP (Next Hop Resolution Protocol).

This was introduced in response to the demand for Vanguard Network routers to operate in the DMVPN (Dynamic Multipoint Virtual Private Network) model.

In the DMVPN model NHRP was required to address the burden of the HUB router in managing its remotes, primarily in the hubs requirement to add configuration for each of the remotes in the network. Using NHRP the Hub no longer has the need to modify/add to the configuration for any remotes added to the network.

The VG first release of NHRP support includes the following:

- Act as Spokes in the Hub & Spoke network
- Use GRE to transport data to the Hub (GRE only)
- Support dynamic IP addressing on the WAN interface.

The First release of Vanguard Networks NHRP implementation does NOT require the Vanguard routers to:

- Act as Hubs
- Be an NHRP Server
- Support direct Spoke-to-Spoke tunnels
- Support dynamic caching of mappings.

The Spokes will always have a static NHRP mapping for the Hub. The Hub must have a static IP address that is known by the Spokes.

4.3.1 GRE enhancements in support of NHRP

In support of the NHRP implementation an optional GRE Key (Tunnel Key) is needed to provide a way for the hub routers to map incoming GRE packets to specific tunnel interfaces. Each tunnel interface on a router must have a distinct GRE Key. All tunnels in a given DMVPN must have the same key.

NHRP is configured in the Tunnel configuration found from the main menu under; Configuration>Configure Router>Configure Tunnel

The new parameters added to 7.3.R00A are:

- Tunnel Key
- NHRP Network ID
- NHS Address
- NHRP Authentication
- NHRP Holding Time
- NHRP Registration Timeout
- Set NHRP Unique Flag

Here the new parameters are presented with the configurable ranges and brief description as they will appear in the Vanguard Routers Configuration menu.

Tunnel Key

Range	0-4294967295
Default	0
Description	This parameter enables the use of the optional Key field in the GRE header. A value of 0 indicates the GRE Key is not used.

NHRP Network ID

Range	0-4294967295
Default	0
Description	This is an identifier for a specific NHRP network. Each NHRP network must have a unique Network ID. All nodes in the network must have the same Network ID. A value of 0 indicates the Network ID is not used.

NHS Address

Range	A valid IP address in dotted notation.
Default	0.0.0.0
Description	This parameter specifies the address of the Next Hop Server (NHS). The router will register with the NHS.

NHRP Authentication

Range	0-8 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	This parameter specifies the authentication string used in NHRP messages. If blank, authentication is not used.

NHRP Holding Time

Range	0-65535
Default	7200
Description	This parameter specifies the holding time value in NHRP registration requests. The NHS will cache the registration request for the duration of the holding time value in seconds.

NHRP Registration Timeout

Range	0-65535
Default	2400
Description	Registration requests are sent out every [this parameter] seconds. If this parameter is set to 0, then registration requests are sent out every [1/3of holding time] seconds.

Set NHRP Unique Flag

Range	Yes,No
Default	Yes
Description	This determines whether to set the unique flag in registration requests. If the flag is set, the hub will prevent the mapping entry from being overwritten by a registration request with the same protocol address but with a different NBMA address. It's recommended to set this parameter to Yes if the tunnel's source address is static, to No if dynamic.

Statistics

Statistics supporting NHRP can be found from the main menu under through the Statistics>Router Stats> Tunnel Stats menu path. This is a sample of the menu structure:

```
Menu: Tunnel Statistics              Path: (Main.5.16.11)
  1. General Tunnel Statistics
  2. Tunnel RTP/UDP/IP Compression Statistics
  3. NHS Statistics
  4. NHRP Mapping
  5. NHRP Traffic
```

The statistics displayed are described in the following examples:

```
NHS Statistics
Node: vgnhrp1   Address: 100            Date: 16-AUG-2000  Time: 18:59:13
NHS Statistics
 NHS Addr        Reg Req (retry in)   Reg Repl   State    Last Reg Repl
Tnl 1:
 172.020.001.001   536     (NA)        527       Up       16-AUG-2000 18:41:02

 NHRP Mapping
Node: vgnhrp1   Address: 100            Date: 16-AUG-2000  Time: 18:59:21
NHRP Mapping
Iface     Proto Addr     NBMA Addr       Expiry  Type
Tnl 1      172.20.001.001   172.028.124.001   Never   Static

NHRP Traffic
Node: vgnhrp1   Address: 100            Date: 16-AUG-2000  Time: 18:59:26
NHRP Traffic
Sent via Tnl 1:
 Req Req 536, Err Ind 0
Received via Tnl 1:
 Reg Reply 527, Err Ind 0, Unsupported 0
```

4.4 7300 Platform System Card New Revision – V3

The 7300 system card (IBM750FX) has been revised.

The part number of the 7300 IBM750FX processor card is 76361G01, this can be found on the card itself and also in “Node Statistics” page 5, sample below.

```
System Controller:   Number of ports: 3  Status: Installed and functional
Assembly: 76361G01 V3  Version: D  Serial Number: 160064574
```

Notes:

- Previous revision is Revision B (76361G01)
- The latest revision is Revision D (76361G01)

- The Software revision to support the New Rev D System Controller Card (Product Code 1112-10037) is now 7.3.
- If the 7300 V3 System Card is configured with any previous software release, the following behavior may be encountered:
    - The date and time will not be updated correctly.
    - Power up Diagnostics will show failures in the two areas shown below, both of which are related to the revision changes.

```
Testing NVRAM >>-FAILED-<<
0 0   NVRM   0000 0000 0000 0000 0000
Testing Real Time Clock  >>-FAILED-<<
```

4.5 NULL ROUTES

Overview

A Null route is a static route that discards packets. It is used to engineer networks to prevent the use of the default route when the preferred route is lost. In many cases, when a preferred dynamic route is lost, the default route would cause routing loops if used.

A Null Route differs from an IP Filter in that it can be installed and removed from the routing table when its metrics are compared to other routes for the same subnet. IP filters, on the other hand are always in the table.

In 7.3.R00A the nexthop IP address for a static route can be configured as 255.255.255.255. This nexthop will drop packets. A Null route can be used to backup a route from a dynamic routing protocol to prevent routing loops.

Behavior

The default route is configured as a static route with a nexthop to discard the packet. It is configured to be less preferred than the dynamic route protects. Vanguard refers to this as a backup static route.

The Null route behavior differs in some ways from a backup static route.

The Null Route is not advertised. The Null route is not redistributed into another routing protocol.

From a dynamic routing protocol point of view (RIP, RIPv2, OSPF, BGP) a Null route is considered to be no route. That means, when a null route is installed in the routing table, the dynamic routing protocol will issue a WITHDRAW of the route to its neighbors.

A Subnet Route which has only a NULL route as a member of its summary range should not be advertised. If it has been previously advertised by a dynamic routing protocol, it should be withdrawn.

Configuration Requirements:

To activate the Null Routes feature, Override Static Routes in Configure IP Interface configuration Table must be enabled.

Then, configure Next Hop in Static Routes Configuration as 255.255.255.255 with a bigger number of Metric compared to other routes for the same subnet IP.

```
[1] Next Hop: 0.0.0.0/?
Range   = A valid IP address in dotted notation
Default = 0.0.0.0
```

The IP address of the next hop to the destination. The next hop itself must be on an IP network directly connected to the router. If the next hop is an unnumbered interface, enter 0.0.0.N where N is the (interface number - 1). If next hop is 255.255.255.255, the route is a null route.

4.6 IPSec Aggressive Mode

Overview

When the Juniper SSG router is configured to accept VPNs from peers with unknown IP addresses, they requires the ISAKMP Phase 1 negotiation to be in Aggressive mode and have a Peer ID to identify the remote peer.

Vanguard implemented Aggressive Mode with the ability to specify a Peer identifier for compatibility with the Juniper SSG family.

```
[1] ISAKMP Phase 1 Exchange Type: MAIN_MODE/AGRESSIVE_MODE/?
Range   = MAIN_MODE,AGRESSIVE_MODE
Default = MAIN_MODE
   ISAKMP Phase 1 exchange type:
    Main Mode - More secure option; generally preferred.
    Aggressive Mode - Less secure option. Used with dynamic local addressing
                it is necessary for interoperability with some VPN concentrators.
 [1] ISAKMP Username ID: (blank)/?
Range   = 1-63 alphanumeric characters, use the space character to blank field
Default = (blank)
   ISAKMP ID payload identifier.  This parameter is required, when configured
       for 'Aggressive' Phase I key change mode.  Both U-FQDN and FQDN are supported.
```

4.7 PP/IPCP Learned IP Address Line

When an interface is configured as unnumbered and the PPP Profile will negotiation and accept its address from its peer, the address will be installed in the router interface. Note that the subnet mask used will be the one configured by the user. If the router interface as a user configured IP address, PPP/IPCP will not install an IP address even if the address negotiated is different than the one configured by the user.

This feature may also be referred to as PPP/IPCP address negotiation

4.8 SSH

The SSH configuration parameters have been enhanced to include an idle timeout feature. The default timeout is 15 minutes.

SSH statistics now include SSH session statistics that show the current state of the SSH sessions, the username logged into the session, the authentication method, and the IP address and port of the user.

4.9 TCP Statistics

TCP statistics now include both a summary statistics menu entry and a detailed statistics entry. The summary statistics table displays counts for current TCP server-side sessions. The detailed statistics provide more information on each TCP session. Detailed statistics can be searched by server-side TCP port number. If the default port number 0 (zero) is used, all sessions will be displayed.

4.10 SIP Connect 1.0 Enhancements

SIPconnect 1.0 is a technical recommendation put out by the SIP Forum that describes the interface between a SIP service provider network and a SIP enterprise network. SIPconnect is the de facto standard for SIP Trunking. The following parameter changes have been made to our product to achieve this functionality.

4.10.1 SIP Connect 1.0 Parameters

Change From tag When Authenticating: Disabled/
Range = Disabled,Enabled
Default = Disabled
Disabled - If disabled, authentication requests sent in response to a challenge, which are outside of any dialog, will use the same values for the Call-ID and From tag as in the original request, and the CSeq number will be one higher than in the original request.
Enabled - If enabled, authentication requests sent in response to a challenge, which are outside of any dialog, will use new values for the Call-ID, From tag and CSeq number than those used in the original request.

SIP Signaling DSCP Value: 40/
Range = 0-63
Default = 40
Enter the DSCP value for SIP signaling packets.

SIP RTP DSCP Value: 46/
Range = 0-63
Default = 46
Enter the DSCP value for SIP RTP packets.

On Hold Media Attribute: Sendonly/
Range = Sendonly,Inactive
Default = Sendonly

This parameter specifies the media attribute to use in the SDP when sending an offer to put the remote end on hold.

Sendonly - Specify a=sendonly in SDP.
Inactive - Specify a=inactive in SDP.

4.10.2 Voice Switch Table change in support of SIP E.164 Numbering

Additional Voice Switching Features: NONE/
Range =NONE, H323_USE_INTERFACE_IP_ADDR,ENABLE_VOICE_MAIL,E_164_NUMBER
Default = NONE

Select Additional Voice Switching Features

NONE - no features enabled.
H323_USE_INTERFACE_IP_ADDR - Force all outbound H323 calls use the Interface IP address as the Source IP address in H.225, H.245 and media channel connection.
ENABLE_VOICE_MAIL - this switch entry specifies the call address of the voice mail port.
E_164_NUMBER - The digits specified in this entry represents a global E.164 number. The E.164 number syntax will be used in SIP requests.
Any combination of above specified by summing (e.g. H323_USE_INTERFACE_IP_ADDR+ENABLE_VOICE_MAIL..).

4.10.3 Voice Port Enhancement

The E&M interface type has been modified to operate slightly different from its original design for Transparent Voice Signaling (TVS) Mode. This parameter is only present when “Signaling Control” is set to Transparent. This new selection will allow the user to enable or disable audio when the signaling bits return to Idle. This is useful for eliminating Echo during some Radio Communication by implementing a forced Half Duplex operation.

Block Audio When Idle: Disabled
Range = Disabled,Enabled
Default = Disabled

This parameter enables/disables the blocking of audio packets toward the interface during the idle signaling state.

Disabled - Audio packets received from remote end will be sent to the interface when the interface is in the idle signaling state.
Enabled - Audio packets received from remote end will be discarded when the interface is in the idle signaling state.
Note: This parameter must be configured the same at both the local and remote ends of the TVS connection. Otherwise, a one way audio problem could result.

4.10.4 Fax Support Enhancement

The new T38_Override selection is introduced for those customers who choose to take advantage of the bandwidth savings of T.38 fax operation even when running G.711. Previous operation was for the voice port to stay running G.711 coder even if fax data was detected.

FAX Support:
Range = Disabled,Proprietary,Enabled,T38,T38_Override
Default = Proprietary

This parameter selects whether the FAX data is to be supported.

Proprietary - Detects presence of FAX data. If FAX data is detected, the voice port will spoof the local FAX machine and transmit the Proprietary FAX data to the remote end as 4800bps or 9600bps data.

T38 - Detects presence of FAX data. If FAX data is detected and the current codec is not G.711, the voice port will spoof the local FAX machine and transmit the T.38 standards based FAX data to the remote end. T.38 support fax data rates of 14.4kbps, 12.0kbps, 9.6kbps, 7.2kbps, 4.8kbps or 2.4kbps. If the current codec is G.711, the fax data will be transmitted transparently over G.711.

T38_Override - Detects presence of FAX data. If FAX data is detected, regardless of the current codec, the voice port will spoof the local FAX machine and transmit the T.38 standards based FAX data to the remote end. T.38 support fax data rates of 14.4kbps, 12.0kbps, 9.6kbps, 7.2kbps, 4.8kbps or 2.4kbps.

Disabled - FAX data will not be detected.

Enabled - Supported for backward compability, equivalent to Proprietary.

Notes:

T.38 Fax Requires release 6.3 or greater software, and is available by purchasing a software license. T.38 Fax text is not present if the T.38 Fax option is not loaded. Release 6.4 and greater includes the Fax feature in the Voice Applications Ware License for the Vanguard 34x, 6435 and 6455. The Vanguard 7300 includes the fax feature in the Multi-Service Applications Ware.

T38, T38_Override or Disabled must be selected for DSP Option 4
T38 and T38_Override cannot be selected for DSP option 1.

4.10.5 IP Classifier, Traffic Conditioner & QoS Mapper Profile Configuration:

This parameter range has been extended from its original range of 1-30 to 1-100.

Entry Number: 1/?
Range = 1-100
Default = 1

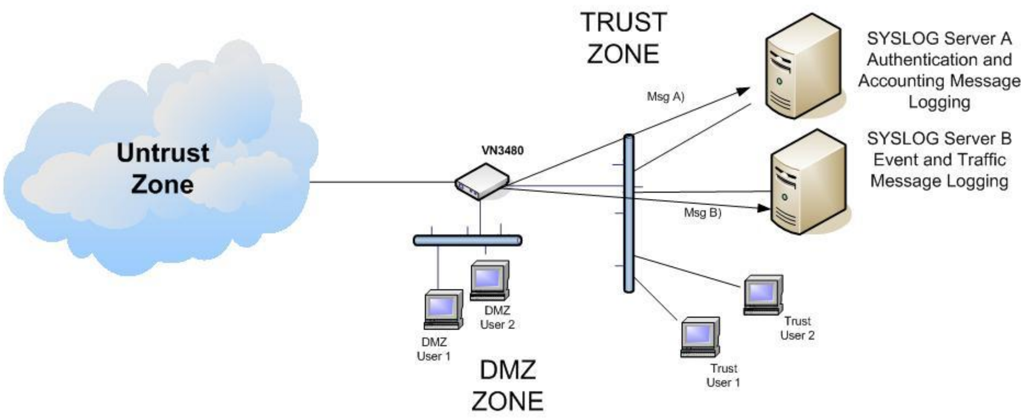
Entry number used to reference this table record.

4.11 SYSLOG Client

4.11.1 Overview

The SYSLOG Client Feature is available in Release 7.3.R00A with the installation of the Security Services License. The SYSLOG Client Feature allows the Vanguard Networks Router Products to send SYSLOG messages to up to two SYSLOG servers. It categorizes the SYSLOG messages into four message types: Authentication, Accounting, Event, and Traffic-Monitoring, and is capable of directing the SYSLOG messages to a particular Server based on the message type. Figure 1 shows an example of a VN3480 forwarding Authentication and Accounting messages to Server 1 and forwarding Event and Traffic messages to Server 2.

Fig 1 - Application of Vanguard Networks SYSLOG Client Feature



The 3480 sends SYSLOG Messages to Hosts A and B:

Msg A) Authentication and Accounting Type SYSLOG messages
Msg B) Event and Traffic Type SYSLOG Messages

4.11.2 SYSLOG Configuration

The SYSLOG Configuration consists of SYSLOG Global Configuration and SYSLOG Server Configuration. The SYSLOG Global Configuration consists of the “SYSLOG Global Enable” parameter. This enables or disables the SYSLOG Client Feature in the router. Figure 2 shows the Global Parameters Configuration.

SYSLOG Global Parameters Configuration

SYSLOG Global Enable:

Range: ENABLED, DISABLED

Default: DISABLED

Help Text: Enable/Disable SYSLOG in this router.

Figure 2 – SYSLOG Global Parameters

Figure 3 shows the SYSLOG Server Configuration parameters. The maximum number of SYSLOG Servers that may be configured is two. Each Server Connection can be enabled independently via the “SYSLOG Connection Enable.” The SYSLOG Server Protocol supported in Release 7.3 is UDP. As shown in Figure 3, the SYSLOG Server IP Address and UDP Port Number are specified in the SYSLOG Server Configuration. The Source IP Address associated with the SYSLOG connection defaults to 0.0.0.0. If it is left at 0.0.0.0, the router automatically assigns the source IP address to the UDP connection. The Source UDP Port number is not configurable. This is assigned automatically by the Vanguard Networks Router.

Also shown in figure 3 are the SYSLOG Type and SYSLOG Severity parameters. The SYSLOG Type parameter is used to specify which message types are sent across this SYSLOG Server Connection: Event, Authentication, Accounting, and/or Traffic Monitoring. The SYSLOG Severity Parameter serves a filtering function. Messages with their severity value specified here are allowed to traverse across this server connection to the attached SYSLOG server.

SYSLOG Server Configuration (cont)

SYSLOG Type:

Range: EVENT,TRAFFIC,AUTHENTICATION,ACCOUNTING

Default: EVENT+TRAFFIC+AUTHENTICATION+ACCOUNTING

Help Text:

The SYSLOG Type parameter selects the type of SYSLOG messages to forward across this SYSLOG Server connection:

EVENT - Forward Alarm messages

TRAFFIC - Forward Traffic messages

AUTH - Forward Authentication messages

ACCOUNTING - Forward Accounting messages

Any combination of above specified by summing (e.g. EVENT+TRAFFIC+. . .)

SYSLOG Severity:

Range: EMERGENCY,ALERT,CRITICAL,ERROR,WARNING,NOTICE,INFORM,DEBUG

Default: EMERGENCY+ALERT+CRITICAL+ERROR+WARNING+NOTICE

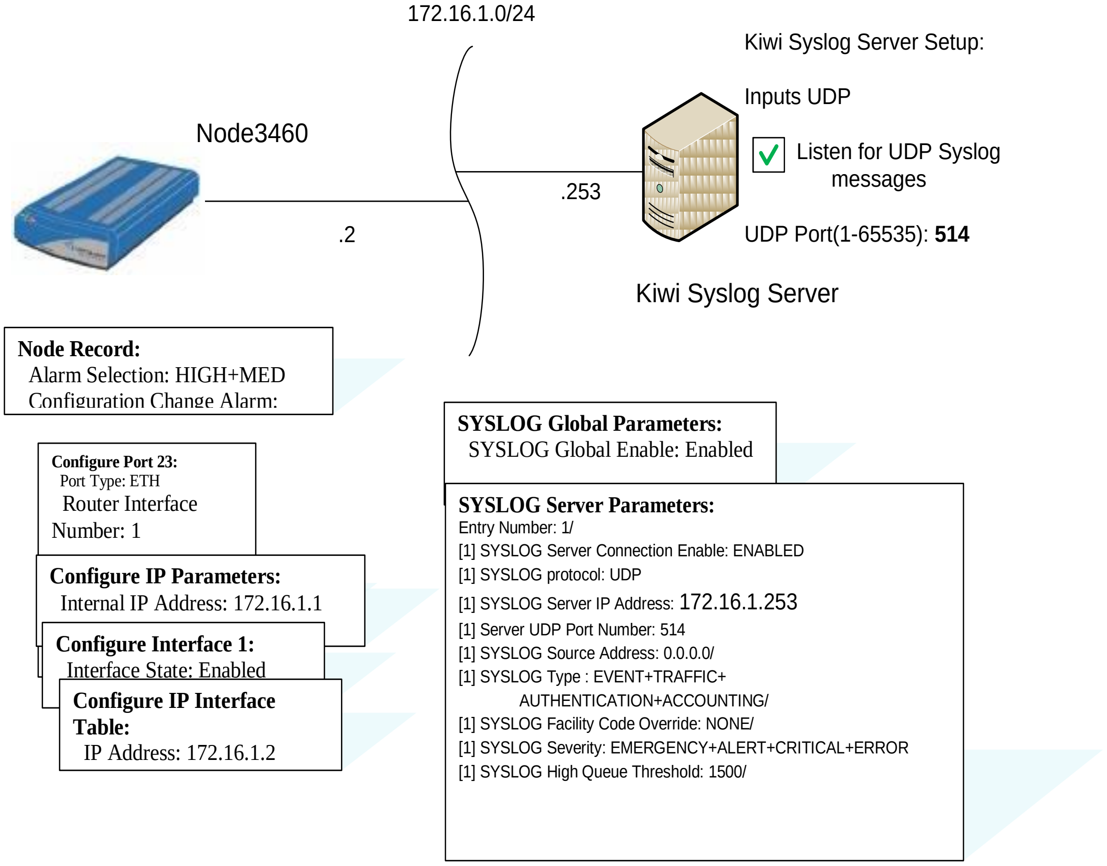
Help Text:

The SYSLOG severity parameter selects the severity of the SYSLOG message to forward to the SYSLOG Server. For TRAFFIC LOGGING Messages to be sent to the SYSLOG Server, you must include NOTICE in this Severity selection. Note: Any combination of above may be specified by summing. (e.g. EMERGENCY+ ALERT+. . .).

Figure 3 – SYSLOG Server Parameters (cont.)

4.11.3 SYSLOG Client Configuration Example

Figure 4 shows a configuration example of the SYSLOG Client Feature. In this example, a VN3480 is configured to send its SYSLOG messages to a Kiwi SYSLOG Server.



Kiwi Syslog Server Setup:

Inputs UDP

☑ Listen for UDP Syslog messages

UDP Port(1-65535): **514**

Node Record:
Alarm Selection: HIGH+MED
Configuration Change Alarm:

Configure Port 23:
Port Type: ETH
Router Interface Number: 1

Configure IP Parameters:
Internal IP Address: 172.16.1.1

Configure Interface 1:
Interface State: Enabled

Configure IP Interface Table:
IP Address: 172.16.1.2

SYSLOG Global Parameters:
SYSLOG Global Enable: Enabled

SYSLOG Server Parameters:

```
Entry Number: 1/
[1] SYSLOG Server Connection Enable: ENABLED
[1] SYSLOG protocol: UDP
[1] SYSLOG Server IP Address: 172.16.1.253
[1] Server UDP Port Number: 514
[1] SYSLOG Source Address: 0.0.0.0/
[1] SYSLOG Type : EVENT+TRAFFIC+
        AUTHENTICATION+ACCOUNTING/
[1] SYSLOG Facility Code Override: NONE/
[1] SYSLOG Severity: EMERGENCY+ALERT+CRITICAL+ERROR
[1] SYSLOG High Queue Threshold: 1500/
```

Figure 4: SYSLOG Client Configuration Example

4.12 Firewall Control-Plane polices and Firewall Intrazone Policies

4.12.1 Overview

Firewall Control-Plane polices and Firewall Intrazone polices control traffic destined to the firewall in the same way general firewall policies control traffic between zones across the firewall. These policies provide finer control to traffic terminating at the router itself.

Firewall policies will have an option to log traffic matching the firewall policy. These entries are recorded in the new Traffic Log.

4.12.2 Firewall Control-Plane Policies

Firewall control plane policies are used to filter traffic terminating at the router itself. A separate set of policies is advantageous for several reasons. In many cases traffic may not need filtering through the router. In these cases, subjecting all packets to the policies is known to significantly increase the CPU utilization. By separating the policy control for traffic to the router into a separate set, it also makes the intent of the configuration much clearer.

In Configure Firewall Policies, the following selections are added: Trust ->Control-Plane, Untrust ->Control-Plane, and DMZ->Control-Plane.

4.12.3 Firewall Intrazone Policies

Firewall intrazone policies are used to filter traffic sent between endpoints within the same zone.

In Configure Firewall Policies, the following selections are added: Trust ->Trust, Untrust ->Untrust, and DMZ ->DMZ.

```
Node: Node3463  Address: 3463           Date: 24-JUN-2010  Time: 13:56:17
 Menu: Configure Firewall Policies      Path: (Main.6.15.6.2)
  1. Trust->Untrust
  2. Untrust->Trust
  3. Trust->DMZ
  4. DMZ->Trust
  5. DMZ->Untrust
  6. Untrust->DMZ
  7. Trust->Control-Plane
  8. Untrust->Control-Plane
  9.   DMZ->Control-Plane
  10.  Trust->Trust
  11.  Untrust->Untrust
  12.  DMZ->DMZ
```

4.13 Denial of Service (Dos) Mitigation

The Firewall now includes support for DoS Mitigation. Under “Configure Firewall” there is a new menu “Configure DoS Mitigation”. Protection against various Denial of Service attacks may be enabled on a per zone basis.

Menu: Configure DoS Mitigation Path: (Main.6.15.6.3)

1. Trust Zone
2. Untrust Zone
3. DMZ Zone

Configure DoS Mitigation Trust Zone

[1] IP Packet Fragment Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of fragmented IP packets. If enabled, a packet is discarded if the More Fragments flag is set or the Fragment Offset field in the IP header is nonzero.

[1] SYN Fragment Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of fragmented TCP SYN packets. If enabled, a packet is discarded if the SYN flag is set, and the More Fragments flag is set or the Fragment Offset field in the IP header is nonzero.

[1] ICMP Fragment Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of fragmented ICMP packets. If enabled, a packet is discarded if the protocol is ICMP and the More Fragments flag is set or the Fragment Offset field in the IP header is nonzero.

[1] Large ICMP Packet Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of large ICMP packets. If enabled, a packet is discarded if the protocol is ICMP and the total packet length field in the IP header is greater than 1024 bytes.

[1] Bad IP Options Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets having an invalid IP options field in the IP packet header.

[1] Record Route IP Options Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets with the Record Route IP options bit set in the IP packet header.

[1] Timestamp IP Options Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets with the Timestamp IP options bit set in the IP packet header.

[1] Security IP Options Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets with the Security IP options bit set in the IP packet header.

[1] Stream IP Options Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets with the Stream IP options bit set in the IP packet header.

[1] Source Route IP Options Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets with the Loose Source Route or the Strict Source Route IP options bit set in the IP packet header.

[1] Unknown Protocol Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of IP packets with an unknown protocol value in the IP packet header. If enabled, a packet is discarded if the protocol value is 143 or greater.

[1] Ping Of Death Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of oversized ICMP packets. If enabled, a packet is discarded if the total packet size is greater than 65,535 bytes, even if the packet is fragmented.

[1] WinNuke Attack Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of TCP packets having a destination port of 139 and the Urgent flag set in the TCP header. This introduces a NetBIOS fragment overlap causing many Windows machines to crash.

[1] Land Attack Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of TCP packets having the SYN bit set with both the source and destination IP addresses the same in the IP packet header.

[1] SYN and FIN Flags Set Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of TCP packets having both the SYN and FIN flags set in the TCP packet header. This is an illegal TCP flags combination.

[1] FIN Flag Without ACK Flag Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of TCP packets having the FIN flag set without the ACK flag set in the TCP packet header. This is an illegal TCP flags combination.

[1] TCP Packet Without Flags Set Protection: Disabled/?
Range = Enabled,Disabled
Default = Disabled

This parameter controls the discarding of TCP packets having no flags set in the TCP packet header. This is an illegal TCP flags value.

When protection is enabled, a count is maintained to track the number of times each DoS attack occurs. Once per second, an alarm is logged for each counter having a non-zero value. Upon logging the alarm, the counter is cleared. The following is an example of a DoS alarm:

```
(2)     900 07-SEP-2003 01:07:11  DOS_Type=Timestamp IP Options Zone=Trust Src=
150.30.74.38 Dest=172.16.1.57 Proto=1 Count=1
```

5 Software Improvements

This section describes specific improvements to the Applications Ware software. It includes:

- Customer-initiated Change Requests
- New features to address new applications

These Change Requests were reported to Customer Service and interim patch releases were released to fix the problems. These Change Requests are incorporated into Release 7.3.R00A, and where applicable, interim patch releases have been replaced by Release 7.3.R00A:

Change Request (CR#)	***Interim Patch Release Replaced by Release 7.3.R00A***	***Problem Description***
16670	6.5.P03E	FXO ports are getting hung and a node boot is required to clear.
17376	70T16F	TCP header compression not working
17509	7.2.P03A	Need to implement more QoS IP CL,Tc Mapper profile entries
17561	7.1.T13A	3 party conference (REFER) is not working
17810	7.2iR00M	PPP/IPCP learned IP addr not shown in IP Interface stats
17851	7.0S100	BGP peer error, BGP - FSM Error - Peer 1 CurrState 0 CurrEvt 2
17869	Feature	Datapac 3201 protocol support on the 3400 platform
17886	70T16Z/Feature	Node freeze after reach 100% CPU. Need CPU reset to recover.
17890	7.2R00A	TOS Stat missing from Cache Statistics
17893	7.1R00a	Out of sequence large pings are failing with ACL, IP.51 rs ovfl alarms
17895	7.2R00A	Domain name field is too short
17904	7.2R00A	Unable to process fragmented ICMP messages when access control is
17909	7.2.R00A	Bypass stations buffer packets during heavy load and stop transmitting
17910	7.2R00A	DHCP Server issues with WIFI networks.
17911	7.2.P01B	arp may set data packet priority to exp_no_drop arputil.c #1091
17923	7.2R00A	Sudden Buffer Depletion when running SIP Voice Loading Test
17927	7.2R00A	Constant Node Crash when T1 ISDN is configured on Int. 1
17930	7.2.R01A	[Node Crash]:Memory Protection: PC stopped at _tcp_close.
17931	7.2.T01B	The rate limit feature was not included in the 342 & 242 platforms
17932	7.2.R01A	[IPSec Aggr Mode]:Node crash due to PPPoE Port configuration
17936	Feature	Add support for Bridge Priority to ethernet switch code
17942	7.1.S100	HTTPD will only accept the last address in an httpd access list
17954	7.2R00A	All IP Sec tunnels go down after booting IPsec parameters, no CTP
17955	7.2.T02A	Node boot needed to enable ISDN virtual ports once they have been
17962	7.2P01C	Node will not boot from alternate if current is corrupt.
17965	7.2.P02A	[Hardware Status]:7300s Hardware Status does not reflect the startup
17969	7.2.R00A	[ISDN BRI]:x.25 virtual port boot does not work.
17970	7.2.T02A	SNMP MIB does not reflect loss of carrier correctly.
17972	7.2.T02A	SSH password does not work
17986	7.2.P01F	BGP session fails to negotiate
17988	7.2.T02A	[6480]:BRI:Leased bonded 128K link does not work with 6840.
17992	7.2.P02A/Feature	Need TFTP image loading capability in 34xx bootprom
18011	7.2	BGP Load balancing produces an imbalanced result
18023	Feature	Implement a half-duplex audio path using E1 CAS signaling
18026	7.2.P01F/Feature	FW/PPoE:Cannot filter traffic destined to the router
18029	7.2	New T1/E1 cards not showing up in power up diagnostics with 3 Serial
18032	V7.1.T17A	MLPPP port not recovering after outage using T1 links w remote stand
18033	7.2R00A/Feature	MOI – Requests full support of Voice Billing Enhancements on 6.5T25C &
18034	7.2.T01E	PPPoE INITIALIZATION ERROR No thernet port context alarm after
18040	7.2.P01H	TCP port lock-up prevents remote access to the node – node must be
18042	NA	BGP hangs intermittently with 2 BGP Peers
18043	7.1P25A	Serial Frame Relay Port has constant CRC errors.
18044	7.1.S100	Qos not marking DSCP at IPSec over Ethernet WAN port
18059	7.2P01H/Feature	SSH is still stranding TCP sessions
18072	7.2.P01K	[Firewall]:No Policy Action Status on Firewall Session Table.
18100	7.2.P01M	[Firewall]:Stats:Wrong Firewall Flow Status with permitted fragmented
18103	7.2.R00A	PAD port configured for 5 data bits not working, supported?
18118	7.2R00A	BGP is not learning the external networks properly, stats do not show AS
18132	7.2P01P	Node restarts when stressing dual BGP peers with RIP redistribution

18134	7.2.T02C	Fax over G.711 is no longer working
18155	7.2.R00A	BGP is not learning external routes from Backbone properly
18187	7.2	SNMP MIB OID support for NHRP not available
18191	7.2	[IPSec]:The node stops ISAKMP negotiation
18192	7.2	NAT running does not allow BGP load balancing
18208	7.2	Unable to ping to the remote nodes tunnel interface over GRE tunnel
18213	7.2	VLAN encapsulated packets not utilizing IP Aggregated Cache
18219	7.2	Increase Aggregated Cache for 68xx and 34xx

Note: The enhancements associated with CR 16670 thru 18155 are also included within the 7.2S100 Service Pak.

6 Known Software Limitations

1) *CR17945 - For PAD Port Auto Baud Sequence DOT_DOT_CR, two or three "."'s are accepted prior to the "CR". More than three "."'s prior to the "CR" is not acceptable and may result in the Auto Baud Sequence to resynchronize and restart its search, for the DOT_DOT_CR sequence.*

   Workaround: The DTE Device connected to the PAD Port must ensure that it transmits two or three "."'s, and does not attempt to transmit more than three "."'s prior to the "CR".

2) *CR17916 - Invalid RFC1294 encapsulation errors when running an LCON, with RTP/UDP Header Compression, between Releases 6.5R00A and 7.0R00A or greater.*

   Work Around: Users must disable RTP/UDP Header Compression.

3) *CR16844 -GRE Tunnels may activate ISDN Encryption session keep-alive trigger GRE tunnels and ISDN calls even when there is no data to be sent.*

   Workaround: Increasing the session timeout in the encryption profile will decrease the frequency of the extra ISDN calls.

4) *CR16941 - Only the first 155 entries in the Virtual Port Mapping Table are valid. The available range in the VPMT is 1-255. If you use entries above 155 the mapped Voice port will become disabled.*

   Workaround: Limit configuration to the first 155 VPMT table entries.

5) *CR17539 BRI: Interface remains "IDLE" after the node is booted. If the node is booted while an ISDN call is active, the Interface may not recover and continue to pass data.*

Workaround: After booting the interface, Boot Virtual Port Boot. If unsuccessful, unplug and plug the cable back in.

6) *CR17579/17354 - Changing the Master Voice Port DSP Image Selection and Booting the Voice Port causes the DSP to reset.*

When the master voice port DSP Image selection is changed and the port is booted, the DSP associated with the Voice Port will reset requiring a Node Boot.

Workaround: Boot the node when modifying the DSP image selection.

7) *CR17595 - ISDN calls may be initiated with no data incoming. The node brings up ISDN calls after the previous connections were disconnected even when no data was incoming. It is caused by an inappropriate value configured in Idle Disconnect Timer.*

Workaround: Configure the Idle Disconnect timer to be at least 3 times as big as Add/Remove Bandwidth Wait Time. Here are configuration samples:

Working Configuration	***Non-Working Configuration***
Add Bandwidth Wait Time: 10	Add Bandwidth Wait Time: 10
Remove Bandwidth Wait Time: 10	Remove Bandwidth Wait Time: 10
Idle Disconnect Timer: 30	***Idle Disconnect Timer: 25***

8) *CR17872 - Incorrect Vanguide Builder Error Message when exceeding available flash size of the 34X.*

In Vanguide Software Builder selecting Products 340E, 342 or 242d, you may receive the following splash messages if the "Selected Option Size" (estimated calculation) exceeds 8,000,000 due to the image size exceeding the on board flash device limitation.

The on-screen message seen is as follows:

```
ERROR: No XRC file has been created in the TEMP directory!
Failed to create an XRC file! Please verify correctness of the settings in the "Settings"
dialog. Also ensure that there is at least 30MB available on your hard disk and that
available Virtual Memory is a least 16MB.
You should now review and save to a different location the .LOG files from the
installation's TEMP directory. Do you want to review and save the error logs?
```

Workaround: Deselect Feature/Protocols until the "Selected Option Size" is below 8,000,000. Note that this calculation will be corrected in the next release of Vanguide Software Builder.

9) *CR17677 - IP Parameter Boot may result in a BGP session boot. Any changes made to BGP related parameters under IP parameters and an IP parameter boot is performed, all BGP sessions will also be booted (reset). This will interrupt live BGP peer sessions and result in network BGP resynchronization.*

Workaround: Users should be aware that if a change is made to any of these parameters and a subsequent “IP parameter” boot is performed then all BGP peer sessions will reset to implement the change.

BGP to RIP Enable: Disabled/
BGP to RIP Default Filter: Deny/
BGP to RIP Nondefault Route Override: Disable/
BGP to RIP Default Route Override: Disable/
BGP to RIP Default Metric: 1/

To minimize the impact on the user, perform the IP parameter boot during a scheduled maintenance window to avoid network disruptions. There is no plan to correct this issue.

10) CR18164 - Bridging (total = 1)

Vanguard products support bridging of data traffic for Token Ring and Ethernet LANs. Bridging LAN traffic minimizes your networking costs by eliminating the need for redundant networks and maximizes the availability of dedicated facilities such as servers and printers, as well as public Frame Relay and X.25 services, across multiple LANs.

Note: *The Vanguard 3480 Switch does not support the Bridging feature.*

11) CR17762 - Problem Description: On the VN3480, when two Ethernet Ports (24 through 27) are configured with their Switch Capabilities set to SWITCH_TO_ROUTER_UPLINK and their associated the Router Interface has the same VLAN ID setting and the same subnet IP Address, the higher numbered port will have a Port Status of "MISCONFIG", when the router is Warm Booted.

Work Around: It is recommended that when more than one VN3480 Ethernet Port (24 through 27) is configured with a Switch Capabilities of SWITCH_TO_ROUTER_UPLINK, their associated Router Interfaces should be configured with a unique VLAN ID and with a unique IP Address.

Valid Configuration

[24] *Switch Capabilities:
SWITCH_TO_ROUTER_UPLINK
[24] *Router Interface Number: 2

Port 26:
[26] *Switch Capabilities:
SWITCH_TO_ROUTER_UPLINK
[26] *Router Interface Number: 4

IP Interface Configurations:

Entry Number:2
[2] Interface Number: 2
[2] IP Address : 192.168.3.1
[2] ***VLAN ID: 1***

Invalid Configuration

Port 24:
[24] *Switch Capabilities:
SWITCH_TO_ROUTER_UPLINK
[24] *Router Interface Number: 2
Port 26:
[26] *Switch Capabilities:
SWITCH_TO_ROUTER_UPLINK
[26] *Router Interface Number: 4

IP Interface Configurations:
Entry Number:2
[2] Interface Number: 2
[2] IP Address : 192.168.3.1
[2] ***VLAN ID: 1***

Entry Number:4

Entry Number:4
[3] Interface Number: 4
[3] IP Address : 150.30.1.1
[3] *VLAN ID: 2*

[3] Interface Number: 4
[3] IP Address : 150.30.1.1
[3] ***VLAN ID: 1***

7 Vanguard Feature Comparison Chart

Feature	***Vanguard 3410/3410W/3460/ 3480***	***Vanguard 6840/6841***	***Vanguard 7300***
T1 Network Interface Specification	Connectors: Dual RJ-45 (100 ohm) Framing: SF and ESF Line Coding: AMI, B8ZS Timing Source: Int, Receive T1 CSU: Built In	Connectors: Dual RJ-45 (100 ohm) Framing: SF and ESF Line Coding: AMI, B8ZS Timing Source: Int, Receive T1 CSU: Built In	Two card versions: **1.** 12 port T1 or E1 (RJ-45 120 ohm) **2.** 8 port T1 or E1 (RJ-45 120 ohm) E1-75 ohm support Future Node wide CLOCK control
E1 Network Interface Specification	Connectors: Dual RJ-45 (120 ohm) - Dual BNC (75 ohm) Framing: E1_CAS, E1_CAS_CRC, E1_CAS_FEBE Line Coding: HDB3, AMI Timing Source: Int, Receive	Connectors: Dual RJ-45 (120 ohm) - Dual BNC (75 ohm) Framing: E1_CAS, E1_CAS_CRC, E1_CAS_FEBE Line Coding: HDB3, AMI Timing Source: Int, Receive	T1 Framing: SF & ESF Line Coding: AMI, B8ZS Timing Source: Int, Receive T1 CSU: Built In E1 Framing: E1_CAS, E1_CAS_CRC, E1_CAS_FEBE Line Coding: HDB3, AMI
Channelized Data Support	Protocols Supported: X.25, FR, TBOP, PPP Maximum Number of Channels: 24 (T1) Maximum Number of Channels: 31 (E1) Maximum Aggregated rate: 1.984 Mbps	Protocols Supported: X.25, FR, TBOP, PPP Maximum Number of Channels: 24 (T1) Maximum Number of Channels: 31 (E1) Maximum Aggregated rate: 1.984 Mbps	Protocols Supported: X.25, FR, TBOP, PPP Max Number of Channels per T1/E1 port: 24 (T1), 31 (E1) Total No. of channels per card: (T1) 8*24=192, 12*24=288 (E1) 8*31=248, 12*31=372 Total No. of channels per System: (7310 T1) 192*4=768, 288*4=1152 (7310 E1) 248*4=992, 372*4=1488 (7330 T1) 192*7=1344, 288*7=2016 (7330 E1) 248*7=1736, 372*7=2604 *Note: all numbers subject to processing capabilities of the 7300.*

ISDN PRI Data Support	Switch Types (User Side Only): N/A Bundle (T1) NI-1, 4ESS, 5ESS, DMS100 European Bundle (E1) ETSI Asia Bundle (T1) NTT Switch Variants: None Required	Switch Types (User Side Only): N/A Bundle (T1) NI-1, 4ESS, 5ESS, DMS100 European Bundle (E1) ETSI Asia Bundle (T1) NTT Switch Variants: None Required	Switch Types (User Side Only): N/A Bundle (T1) NI-1, 4ESS, 5ESS, DMS100 European Bundle (E1) ETSI Asia Bundle (T1) NTT Switch Variants: None Required
Voice Signaling Support	CAS: E&M (Wink, Delay, Immediate Colisee, and Seizure Ack) (3460/3480) FXS (Loopstart) (3460/3480) FXO (Loopstart) (3460/3480)	CAS: E&M (Wink, Delay, Immediate Colisee, and Seizure Ack) FXS (Loopstart) FXO (Loopstart) CCS (2,3,4): • N/A Bundle (T1) – Q.Sig (Master/Slave) (5) – 5ESS (Network/User) (6) – NI-1 (Network/User) (6) – DMS100 (Network/User) (6) • Euro Bundle (E1) –ETSI (Network/User) –Q.Sig (Master/Slave) (5)	CAS: E&M (Wink, Delay, Immediate Colisee, and Seizure Ack) FXS (Loopstart) FXO (Loopstart) CCS (2,3,4): • N/A Bundle (T1) – Q.Sig (Master/Slave) (5) – 5ESS (Network/User) (6) – NI-1 (Network/User) (6) – DMS100 (Network/User) (6) • Euro Bundle (E1) –ETSI (Network/User) –Q.Sig (Master/Slave) (5)
Features	Trunking Gateway(3460/3480 E1 only)	Timeslot Bypass	Timeslot Bypass
Additional Clocking Features	Node Wide Network Clock Source (3460/3480 E1 only)	Node Wide Network Clock Source	Node Wide Network Clock Management Data Applications: Each Group of 4 T1/E1 ports can synchronize to a different carrier Voice & Data Applications: Each card has to be connected to one carrier
SDLC HPAD/TPAD	Protocols: SDLC Characteristics: HDX, FDX, TWA Network: QLLC/X.25/Frame Relay (Annex G) Host Interface: SDLC PTP, SDLC MP, X.25 (IBM NPSI) Physical Interface: V.21, V.24, V.35	Protocols: SDLC Characteristics: HDX, FDX, TWA Network: QLLC/X.25/Frame Relay (Annex G) Host Interface: SDLC PTP, SDLC MP, X.25 (IBM NPSI) Physical Interface: V.21, V.24, V.35	Same as 6840/6841except: Characteristics: no HDX

LLC2 (SNA) Conversion	Protocols: LLC2, X.25 (QLLC), SDLC, FR (RFC1490) Characteristics: HDX, FDX, TWA Network: QLLC/X.25/Frame Relay (Annex G) Frame Relay (RFC1490) Host Protocols: SDLC PTP, SDLC MP, X.25 (IBM NPSI), LLC2, Frame Relay (RFC1490) LAN: Ethernet 802.3 (10 mbps), Ethernet2. WAN Physical Interface: V.21, V.24, V.35	Protocols: LLC2, X.25 (QLLC), SDLC, FR (RFC1490) Characteristics: HDX, FDX, TWA Network: QLLC/X.25/Frame Relay (Annex G) Frame Relay (RFC1490) Host Protocols: SDLC PTP, SDLC MP, X.25 (IBM NPSI), LLC2, Frame Relay (RFC1490) LAN: Ethernet 802.3 (10 mbps), Ethernet2. WAN Physical Interface: V.21, V.24, V.35	Same as 6840/6841except: Characteristics: no HDX

5) Q.Sig Support now includes Basic Call, Supplementary Services and Segmentation.

6) Enblock Signaling Support only at this time.

AS/400 5494 Communications Server	Protocols: LLC2, X.25 (QLLC), SDLC, FR (RFC1490) Characteristics: HDX, FDX, TWA Network: QLLC/X.25/Frame Relay (Annex G) Frame Relay (RFC1490) Host Protocols: LLC2, Frame Relay (RFC1490) LAN: Token Ring (4 or 16 mbps), Ethernet 802.3 (10 mbps), Ethernet2. WAN Physical Interface: V.21, V.24, V.35	Protocols: LLC2, X.25 (QLLC), SDLC, FR (RFC1490) Characteristics: HDX, FDX, TWA Network: QLLC/X.25/Frame Relay (Annex G) Frame Relay (RFC1490) Host Protocols: LLC2, Frame Relay (RFC1490) LAN: Token Ring (4 or 16 mbps), Ethernet 802.3 (10 mbps), Ethernet2. WAN Physical Interface: V.21, V.24, V.35	Same as 6840/6841except: Characteristics: no HDX
Other SNA protocols	BSC3270 HPAD/TPAD BSC2780/3780 IBM 2260 PAD TCOP TBOP NCRBSC HPAD/TPAD Pad Scope	BSC3270 HPAD/TPAD BSC2780/3780 IBM 2260 PAD TCOP TBOP NCRBSC HPAD/TPAD Pad Scope	TBOP All others not supported
BSC3270 -to- SNA Conversion	256 Devices Supported	256 Devices Supported	2,000 Devices Supported

BSC2780/3780-to-SNA/LU0 Conversion	Supported on the 6455 256 Devices Supported	Supported on the 6455 256 Devices Supported	256 Devices Supported
Frame Relay	FRI, FRA, FRF.12 Support	FRI, FRA, FRF.12 Support	Same as 6840/6841 except no FRA and FRF.12 support
IP/LAN	VPN/IPSEC/3DES/AES	VPN/IPSEC/3DES/AES	VPN/IPSEC/3DES/AES.
ATM	Not supported	Not supported.	ATM supported over T3 or E3. UBR, VBR and CBR 4000 VCCs IP over ATM AnnexG over ATM
ATM	Not supported	Not supported.	ATM supported over T3 or E3. UBR, VBR and CBR 4000 VCCs IP over ATM AnnexG over ATM
VBIP (BSC3270 to TCP/IP Conversion)	Supported.	Not supported	Not supported
SNMP	The following MIB objects are supported only in 3400 platform. cdx6500T1E1VGTable	The following MIB objects are supported only in 6800 platform. cdx6500T1E1VGTable cdx6500TdmClkTable	The following MIB objects are supported only in 7300 platform. cdx6500PSTT1E1TGPortTable cdx6500PSTT1E1TGTable cdx6500STTdmtgClkGroup

1) **Al signaling types/variant combinations support user or Network side and T1 or E1.**
2) **Q.Sig/Euro ISDN support on T1 interfaces is now available in Release 6.5.R000, 7.0.R00A, 7.1.R00A, 7.2.R00A**
3) **NTT Signaling support is currently unavailable and is targeted to be added in a future release.**
4) **Transparent CCS can be supported manually by means of configuring the TBOP data channel for "Signaling" channel and Voice Bearer channels with none for signaling. Virtual port mapping table entries for voice ports must be TDM-VOICE.**
5) **Q.Sig Support now includes Basic Call, Supplementary Services and Segmentation.**
6) **Enblock Signaling Support only at this time.**

7.1 Software Configuration Limits

The following table lists the software configuration limits for:

- Physical Ports (physical port counts are set by software, not the actual number of physical ports)
- Frame Relay
- Sessions
- Network Services
- LAN - (IP specific)
- Voice
- SNA/IBM Support

Software Configuration	***7300 Series***	***6840/6841***	***3410/3460/ 3480***
Physical Port	***Maximum Limits***		
Ethernet ports per node - MPC750 CPU Ethernet ports per node - IBM750FX CPU Ethernet ports per node	5 20	2	2 (3410/3460) 5 (3480)
High speed (V.35) serial links per node	56	8	3460/3480 - 4 3410 - 2
Total LAN ports (ETH) per node (not bridged) MPC750 Total LAN ports (ETH) per node (not bridged) IBM750FX	5 20		
Devices supported per Ethernet segment (Relevant to Bridge operation)	255	255	255
T1/E1/PRI ports (data only) per node	84	4	3460/3480 - 2 3410 - 1
T1/E1/PRI voice only ports per node	14	4	0
T3/E3 ATM ports per node	2	0	0
Voice circuits per voice server card	60	60	0
Number voice calls per node (Number shown is E1 max.)	420	60	0
Number voice calls per node (Number shown is T1 max.)	336	60	0
Frame Relay			
Number of DLCIs per FR Port	820	820	820
Number of PVCs per FR Annex-G station	128	128	128
Number of SVCs per FR Annex-G station	512	512	512
Number of Voice SVC per Annex-G station	15	15	15
Number of DLCIs per node	8,000	1,024	1,024
Session			
Number of LCON	2,000	2,000	2,000
Number of Virtual Ports (FR, X25, PPP, Voice)	2,000	155	155
Max. Number of Multi-link PPP profiles	1,000	200	200
Max. Number of MLPPP switched links per MLPPP Profile	60	30	30
Number of UDP (SoTCP) sessions terminating in the node	2,000	188	188

Number of TCP (SoTCP) sessions terminating in the node	2,000	500	500
Number of simultaneous calls per node	8,000	2,000	2,000
Network Services			
Number of Network Services Tables Entries	1,000	128	128
Number of PVCs table entries	8,000	2,000	2,000
Number of mnemonic table entries	8,000	2,000	2,000
Number of Switch Service table entries	1,024	1,024	1,024
Number of X25 routing table entries	8,000	2,000	2,000
LAN IP (Specific)			
Routing table size	15,000	8,000	8,000
Routing Cache	8200	8200	8200
Accelerated/ Aggregated Route cache	512	512	512
Number of LCONs	8,000	2,000	2,000
Number of Interfaces	1,000	1,000	1,000
Access Control List table size	255	255	255
Policy based routing table size	255	255	255
Static ARP table	255	255	255
Number of static routes	8,000	8,000	8,000
MAC Filter Table Entries	1,200	300	300
RIP Route Control table	255	255	255
NAT table size	1023	1023	255
IP Multicast DVMRP Tables size	4,000	4,000	4,000
Maximum number of Multicast Interfaces supported	1,000	256	256
CIDR: RIP aggregate table	255	255	255
CIDR: Multi-home table size	255	255	255
Voice			

Number of voice switching table entries: Save your CMEM before configuring a large number of entries. If your CMEM becomes too large, the node may reset or default its configuration.	10,000	6,000	6,000
SNA/IBM Support			
Number of stations per LAN **interface** (SLAC) - *Note: Two LAN interfaces allowed per node -- 1,000 stations per interface,*	1,000	250	250
Maximum number of SLAC Stations supported for BSC/LU Devices	100	63	63
Number of stations per **Node** (SLAC) - *Note: Two LAN interfaces allowed per node -- 2,000 max stations per node.* **LLC LAN Conversion Stations:** Vanguard 7300 Series - 1,000 per interface, 2,000 per node (Release 6.0 and greater) Vanguard 3410/3460/3480- 250 per interface, 500 per node Vanguard 34x - 250 stations on one port **LLC FRI Conversion Stations:** Vanguard 7300 Series - 2,000 per node (Release 6.1 or greater) Vanguard 7300 Series - 1,000 per node (Prior to Release 6.1) Vanguard 34x, 3410/3460/3480 - 250 per node	2,000	500	500
Additional Limits			
Number of bridge links entries (7300 Series original size - 250)	1,000	1,000	1,000
ARP (queue size)	50	50	50
Max. number of IPX interfaces+	1,000	1,000	1,000

Number of OSPF routes	15000(G1)
	20000(G2)
		4000	4000

Max. SVCs per SoTCP session	64	50	50
Max. Total Data SVCs (SoTCP)	2,000	1,024	1,024
Max. Total Voice SVCs (SoTCP)	2,000	1,024	1,024
IP Broadcast Forwarding Table Size	255	255	255
UDP Broadcast Forwarding Table Size	255	255	255
Outbound Translation Table Entries (7300 Series original size - 1,600)	16,000	1,600	1,600

Additional Limits - ATM			
ATM Stations	4,000	*	*
Maximum FRST Entries	4,000	*	*
SAR Profile	500	*	*
X25 Profile	500	*	*
Maximum Compressed Data Connections	500		
Additional Limits - LAN			
Transparent Bridge Forwarding Table Size (7300 Series original size - 8,000)	16,000	255	255
Max. number of OSPF interfaces	255	255	255
BGP Policy Table	2,048	768	768

BGP Route Table	15000(G1)
	20000(G2)
		10000	10000

BGP to OSPF Import Policy Table	1,024	1,024	1,024
BGP Maximum peers	128	16	16
QoS - QCL Profiles	1,000	1,000	1,000
QoS - IP MF Classifiers	10,000	10,000	10,000
VLAN Sessions - 16 per port, 50 per node Vanguard 34x - 20 per node 50 per node 30 per node 30 per node	50 per node 30 per node 30 per node		

8 BOOT PROM SOFTWARE UPDATES

This section provides instructions for Cold loading the Boot prom using Software Loader or Procomm Communication software.

Caution

Backup your configuration. Upgrading to a new release could cause configuration loss. If you choose to downgrade to a previous release, you must reload the configuration saved from that release or risk corrupting the configuration.

8.1 Software Loader

Software Loader automatically upgrades or downgrades the boot prom. When an image is loaded and it requires a version of boot prom different from the one currently loaded, Software Loader changes the boot prom to successfully load the image. For more information on boot prom-image compatibility, refer to the Boot prom Directory table on page 28.

The boot prom can be uploaded and downloaded manually using a communication application such as Procomm.

8.2 Procomm Procedure

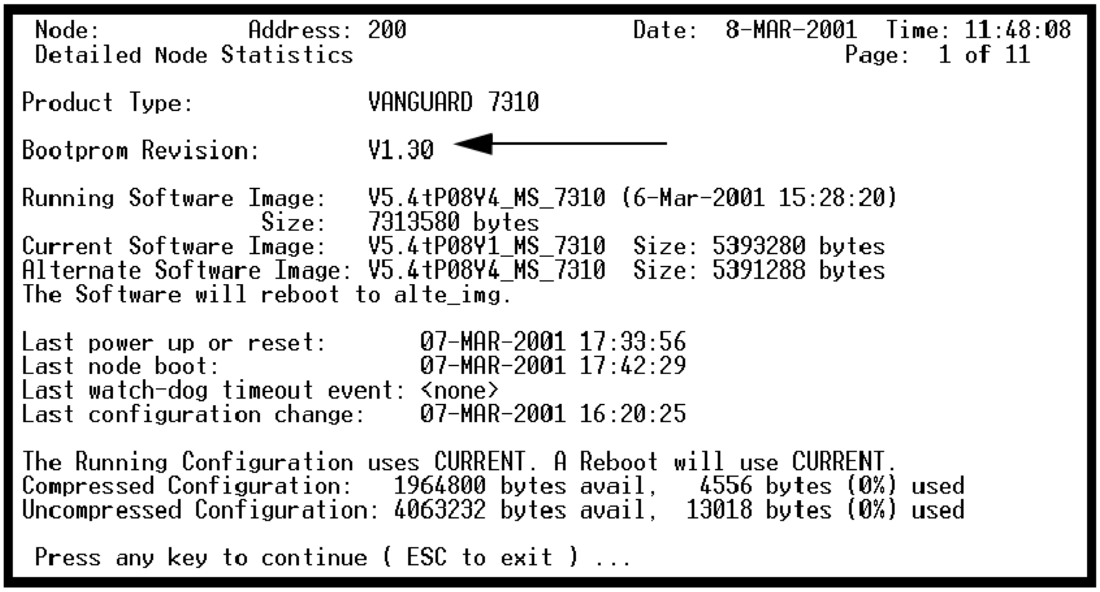
Below is a step procedure on how to cold load the Boot prom using Procomm Communication software. This procedure example was documented using a Vanguard 7300 Series router. The figure on page 29 shows the various product directories.

Note:

Boot prom revision 3.00 is current for release 6.5.R000 or greater 7300 series routers using the IBM750FX CPU and MPC750 CPU.

1) To determine the current version of Boot prom loaded on your Vanguard, perform these steps:

Step	***Action***
a)	Access the Console Terminal Program's (CTP) Main Menu.
b)	Select Option 5, **Status/statistics**.
c)	Select Option 1, **Node Stat**, from the Status/statistics menu. The Node Stats' displays the Boot prom Revision: 7300 Series Examples: Version 1.10, 1.11, 1.30, 1.40, 1.50, 1.51, Version 2.00, or Version 3.00. **Note:** Refer to the Boot prom Directory table in Step 9.



```
 Node:           Address: 200                  Date:  8-MAR-2001  Time: 11:48:08
 Detailed Node Statistics                                     Page:  1 of 11

Product Type:              VANGUARD 7310

Bootprom Revision:         V1.30

Running Software Image:    V5.4tP08V4_MS_7310 (6-Mar-2001 15:28:20)
                  Size:    7313580 bytes
Current Software Image:    V5.4tP08V1_MS_7310  Size: 5393280 bytes
Alternate Software Image:  V5.4tP08V4_MS_7310  Size: 5391288 bytes
The Software will reboot to alte_img.

Last power up or reset:        07-MAR-2001 17:33:56
Last node boot:                07-MAR-2001 17:42:29
Last watch-dog timeout event:  <none>
Last configuration change:     07-MAR-2001 16:20:25

The Running Configuration uses CURRENT. A Reboot will use CURRENT.
Compressed Configuration:   1964800 bytes avail,   4556 bytes (0%) used
Uncompressed Configuration: 4063232 bytes avail,  13018 bytes (0%) used

 Press any key to continue ( ESC to exit ) ...
```

2) Use the Procomm application to update the Boot prom. Open the Procomm application to get a Data Terminal Window. The settings should be 9.6k, N-8-1, and RAW-ASCII transfer mode. Use a regular Control Terminal Port (CTP) connection.

3) Activate a Force Cold-Load (16.12.y.y):

Flash Memory->Force-Cold-Load->yes

Cold Boot the node (7.5.y):

Boot->Node (cold)->yes

A Download Coldloader prompt from the (CTP) displays.

4) Choose an appropriate speed cold loader indicated in the current bank column of the table below. Typically the c73cv115.xrc file is used.

Current Bank	***Kbps***
c73cv115.xrc	115
c73cv192.xrc	19.2
c73cv288.xrc	28.8
c73cv384.xrc	38.4
c73cv576.xrc	57.6
c73cv96.xrc	9.6

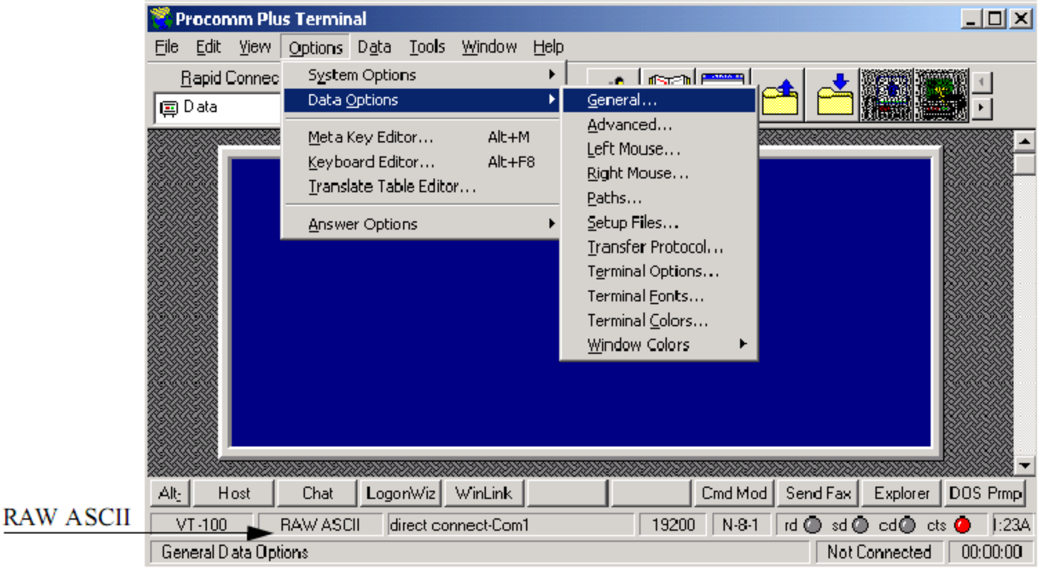
5) Download the appropriate cold loader to your PC for the correct Boot prom version, from the following directory example:

You must use the cold loader from the current bank column of the table in step 4 to load the Boot proms.

6) When using the Procomm application:
- Select Send File from the Procomm Data Menu
- Select RAW ASCII transfer mode
- Select 9600 for the Coldloader speed

The following figures show the Procomm application.

Note:
To ensure you are in RAW ASCII transfer mode in Procomm, check the setup file. Options->Data Options

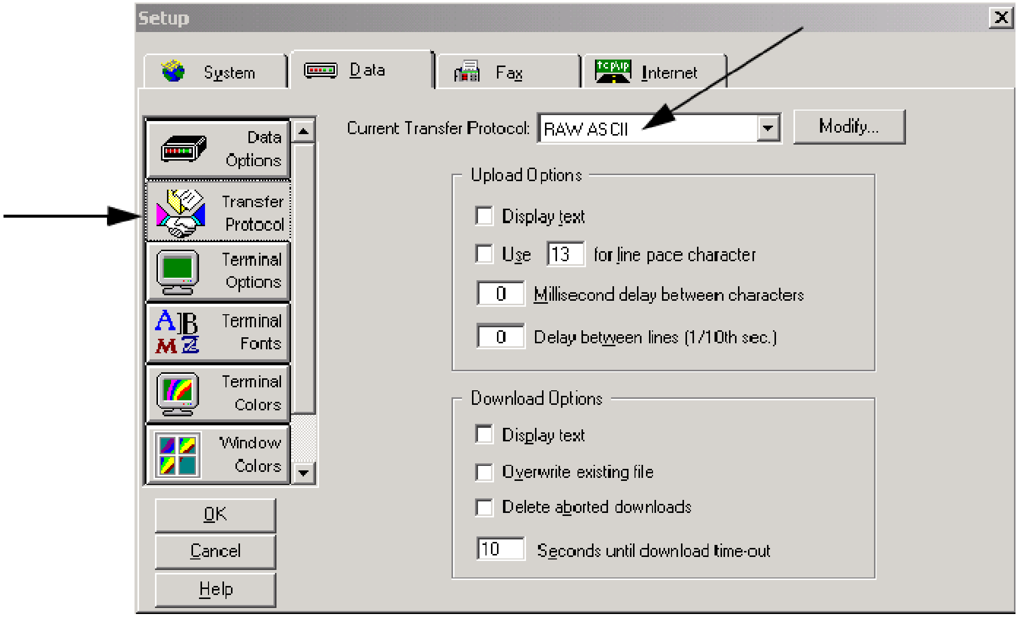


VT-100 | RAW ASCII | direct connect-Com1 | 19200 | N-8-1

General Data Options | Not Connected

8.3 Procomm Setup

When Options->Data Options->Transfer Protocol is selected, a Setup menu displays.
- Select RAW ASCII from the Current Transfer Protocol pull down menu.
- Click the Transfer Protocols button.



Current Transfer Protocol: RAW ASCII

Upload Options

□ Display text

□ Use 13 for line pace character

0 Millisecond delay between characters

0 Delay between lines (1/10th sec.)

Download Options

□ Display text

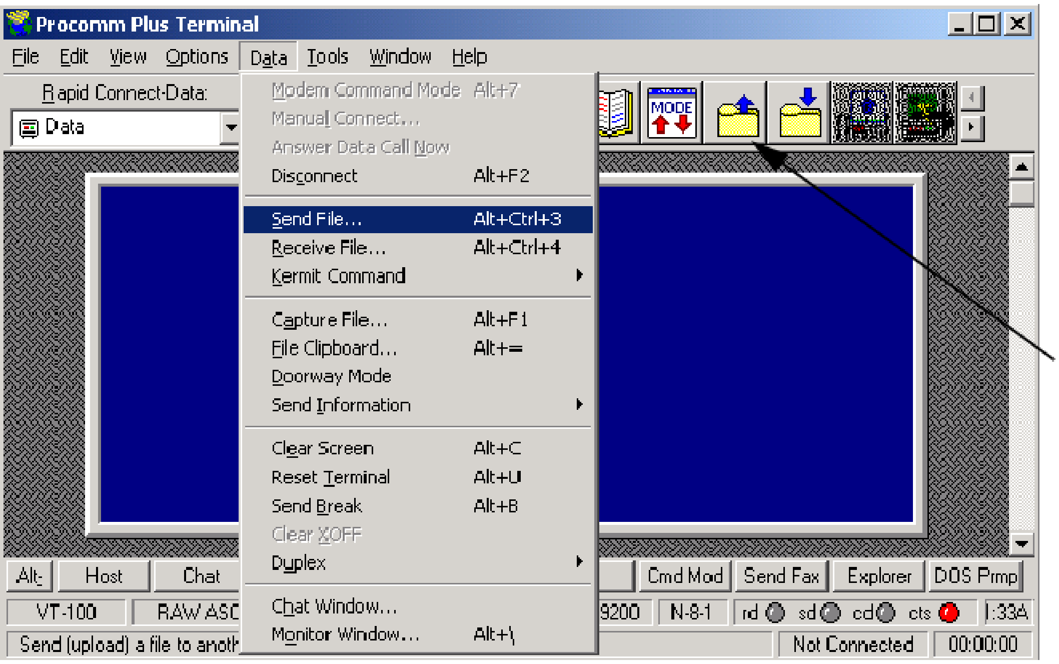
□ Overwrite existing file

□ Delete aborted downloads

10 Seconds until download time-out

8.4 Send File

To send a file, open the Procomm application. Under the Data Menu select Send File.



This button also Sends Files.

Send the correct file using one of the enclosed "c73 loaders" below:

c73cv115.xrc for 115 Kbps	c73cv288.xrc for 28.8 Kbps
c73cv192.xrc for 19.2 Kbps	c73cv384.xrc for 38.4 Kbps
c73cv576.xrc for 57.6 Kbps	c73cv96.xrc for 9.6 Kbps

Note:
To reduce the download time, Vanguard Networks recommends c73cv115.xrc for 115 Kbps.

7) Once the download is complete, change the terminal speed to the appropriate cold loader speed chosen in step 4. Download the Bootprom.xrc file. The required Boot prom version (such as T10BP111.xrc) can be acquired from the directory containing the same name:

C:\Vanguard\SFW_IMGS\73*0\COLDLOAD\T10BP1**

8) Open the Procomm Plus Terminal Manual application:
   a. Select Send File, under the Procomm Data Menu
   b. Select the correct boot prom version

9) Choose the correct boot prom directory that includes the cold loaders. The example below shows the 7300 Series Boot prom Directories.

\T10BP1** refers to:
T10BP110 T10BP150
T10BP111 T10BP151
T10BP130 T20BP200
T10BP140 T30BP300

Boot prom Directory	***ONS Image Compatibility***	***Boot prom Version***
T10BP110	5.4.P08A 5.4.P08B	1.10
T10BP111	5.4.P08# The pound sign "#" represents a letter from C to Z.	1.11
T10BP130	5.4.P0LA, 5.4.P0KA, and 5.4.P0JA Boot prom version 1.30 is required to run the 5.4 Point Release L software. The 1.30 version of the boot prom does not work with any earlier 5.4.P08* software. **If you have a new CPU card, use boot prom 1.40 or 1.50.** The asterisk "*" represents a letter from A to Z.	1.30 or greater
T10BP140	5.4.P0LB Boot prom version 1.40 or greater is required to run with the new CPU cards.	1.40 or greater
T10BP150	6.0.R00A, 6.1.R000, 6.2.R000, 6.3.R00A, 6.4.R00A, 6.4.R10A	1.50
T10BP151	6.0.R00A, 6.1.R000, 6.2.R000, 6.3.R00A, 6.4.R00A, 6.4.R10A	1.51

	Boot prom 1.51 is the latest for the MCP750 CPU. **Do not** use boot prom 2.00 on the MCP750 CPU.	
T20BP200	6.4.R00A and 6.4.R10A	2.00
	The IBM750 CPU must use boot prom 2.00	
T30BP300	6.5.R000 or greater	3.00
	Boot prom revision 3.00 supports IBM750 and MPC750 CPUs. Boot prom revision 3.00 is mandatory for Release 6.5.R000.	

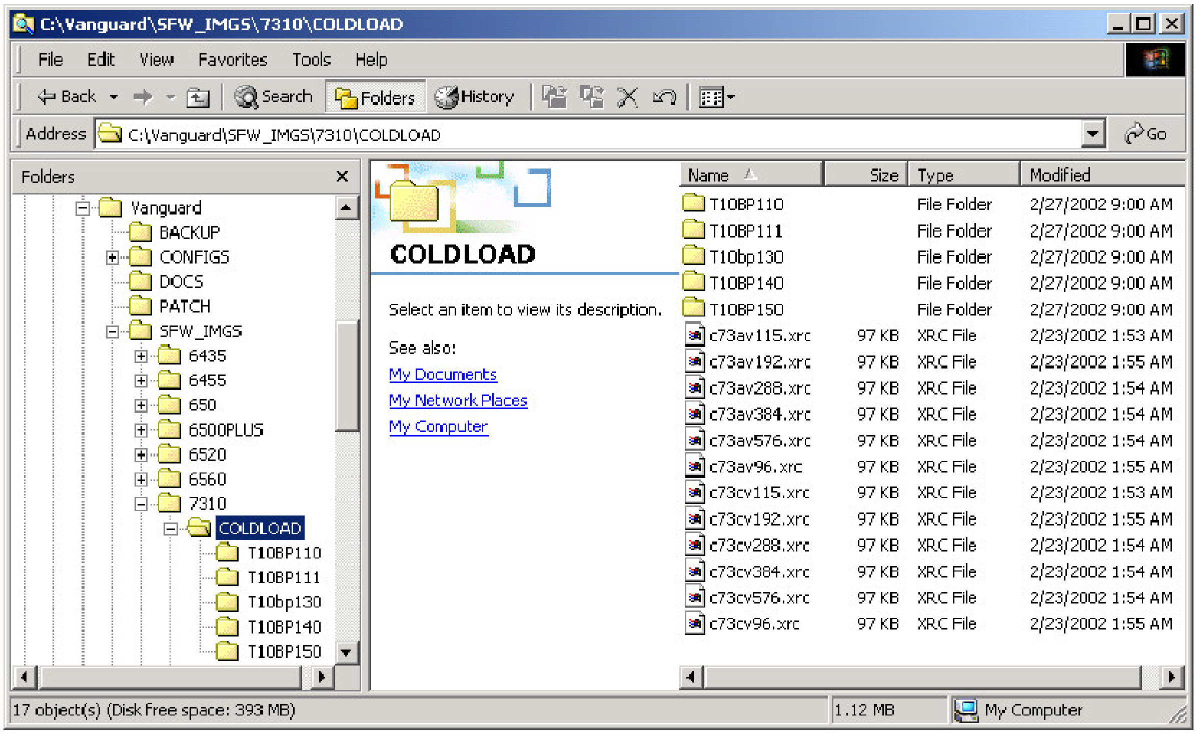
Note:
The respective.xrc file is contained in the directory with the same name.
Example: T10BP140.xrc would be found in the T10BP140 directory. T10BP150.xrc would be found in the T10BP150 directory.

8.5 Directory Example

The figure below shows a Vanguard 7310 Directory selected.
C:\Vanguard\SFW_IMGS\7310\COLDLOAD

Note: Under the SFW_IMGS directory all the Vanguard products are listed. To select a Vanguard 7310 the path would be:
C:\Vanguard\SFW_IMGS\7310\COLDLOAD

C: Vanguard
SFW_IMGS
7310
COLDLOAD


C:\Vanguard\SFW_IMGS\7310\COLDLOAD
File Edit View Favorites Tools Help
Back Search Folders History
Address C:\Vanguard\SFW_IMGS\7310\COLDLOAD
Go
Folders
Vanguard
BACKUP
CONFIGS
DOCS
PATCH
SFW_IMGS
6435
6455
650
6500PLUS
6520
6560
7310
COLDLOAD
T10BP110
T10BP111
T10bp130
T10BP140
T10BP150
COLDLOAD

Select an item to view its description.

See also:
My Documents
My Network Places
My Computer

Name	Size	Type	Modified
T10BP110		File Folder	2/27/2002 9:00 AM
T10BP111		File Folder	2/27/2002 9:00 AM
T10bp130		File Folder	2/27/2002 9:00 AM
T10BP140		File Folder	2/27/2002 9:00 AM
T10BP150		File Folder	2/27/2002 9:00 AM
c73av115.xrc	97 KB	XRC File	2/23/2002 1:53 AM
c73av192.xrc	97 KB	XRC File	2/23/2002 1:55 AM
c73av288.xrc	97 KB	XRC File	2/23/2002 1:54 AM
c73av384.xrc	97 KB	XRC File	2/23/2002 1:54 AM
c73av576.xrc	97 KB	XRC File	2/23/2002 1:54 AM
c73av96.xrc	97 KB	XRC File	2/23/2002 1:55 AM
c73cv115.xrc	97 KB	XRC File	2/23/2002 1:53 AM
c73cv192.xrc	97 KB	XRC File	2/23/2002 1:55 AM
c73cv288.xrc	97 KB	XRC File	2/23/2002 1:54 AM
c73cv384.xrc	97 KB	XRC File	2/23/2002 1:54 AM
c73cv576.xrc	97 KB	XRC File	2/23/2002 1:54 AM
c73cv96.xrc	97 KB	XRC File	2/23/2002 1:55 AM

17 object(s) (Disk free space: 393 MB) 1.12 MB My Computer

10) Once completed, the 7300 shows “Restarting”. Change your terminal speed immediately back to 9600. The unit should automatically reboot and go to ONS, provided that the boot prom and ONS images are compatible.

Note: If the ONS images are not compatible, the node responds by removing the current image and prompts the user with a “download cold loader” message. If you received this message check the table in step 9. The table contains the correct compatibility information. To load a compatible ONS image, repeat these steps substituting the ONS image instead of the boot prom image instruction in step 8.

11) Upon completion of loading a compatible image, the node restarts.

8.6 Boot Prom Information for the MPC750 Controller Card

Any MPC750 CPU controller card (numbered 75836G01) with revision D or greater REQUIRES the new boot prom code and must not be downgraded past 1.40. You must NOT load an earlier version of boot prom or attempt to load software with a Vanguide CD prior to release 5.4.P0LB. This card is functionally equivalent to the original card, but does require new boot prom code and cold loaders to operate. This new boot prom code is release 1.40 or greater.

The new 1.40 or greater boot prom is fully compatible with the original controller card and all software versions that worked with boot prom revision 1.30. If you use an older Vanguide CD to load an older image, it attempts to downgrade the boot prom which renders the controller card inoperable and it will have to be replaced.

In order to prevent inadvertently loading boot prom revision 1.30 onto a new system controller card, please discard any CD's previous to the 5.4.P0LB CD.

For more information, refer to the Vanguard 7300 Controller Card Hardware Advisory Notice (Part Number T0185-04) located on the web at:
http://www.vanguardnetworks.com/support-documentation-overview.htm

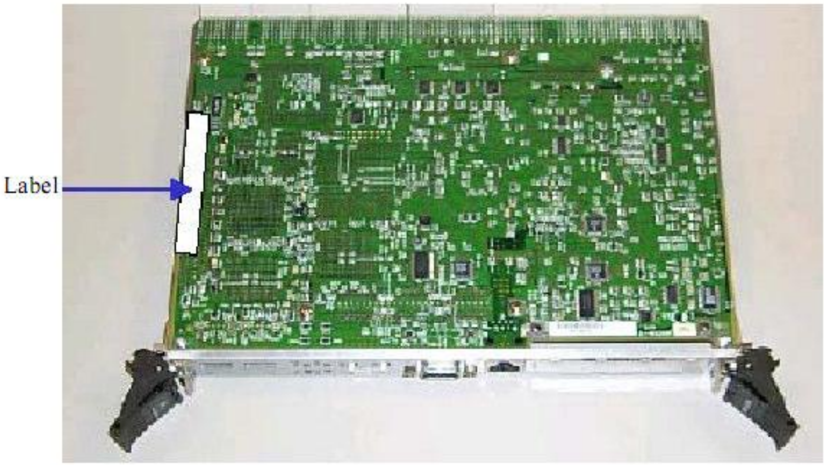
Also refer to the “Boot Prom Software Updates” section (Chapter 8) of this Software Release Notice.

Notes:
The most current boot prom for the MCP750 and IBM750 CPU card is 3.00. Do not use boot prom 2.00 on the MCP750 CPU card.

The IBM750FX CPU card available with release 6.4.R10A and greater must use Boot prom 2.00.

8.7 Controller Card Board Assembly Number Location

Refer to the figure below to locate your board assembly number:



8.8 Vanguard 7300 CPU Card Upgrade

The Vanguard 7300 Series MCP750 (part number 75836G02) system cards are supported by software releases 6.1.T14A and greater. If you have a part number 75836G02 system card and are running older versions of release 6.1, a new 6.1 software patch is required (6.1.T14A). The system cards have a different revision PCI-PCI bridge than previous system cards (part number 75836G01). The new system cards are not being recognized by software older than 6.1.T14A. Software patch 6.1.T14A must be installed when using part number 75836G02. For more information reference the 7300 Hardware Advisory Notice (part number T0258).

9 Boot Prom and Cold loader Matrix Upgrade

The following tables describe the valid combinations of released flash image, boot code, on-board flash, flash SIMM and DRAM for the Vanguard 34xx, 34x, 68xx, and 7300 platforms. In the following tables, the Status column can be Valid, Invalid and VR (Valid and Recommended). "Valid" means that the router is basically working, but some functionalities such as an option feature support, might not be available. "Invalid" means that the router is not working with such a combination. "VR" (Valid and Recommended) means that the combination is valid and recommended to use according to our current knowledge.

Vanguard 3400 Boot prom, Coldloader and Image Matrix

No.	*Release*	*Boot Code Version*	*Cold-loader from Release*	*On-Board Flash*	*Flash SIMM*	*Status*	*Comment*
1	7.0.P12A or earlier	1.04	7.0.P12A	16M	None	Valid	None
2	7.1.R00A	1.05	7.1.R00A	16M	None	Valid	64k CMEM, 4M image maximum
3	7.2.R00A	1.05	7.2.R00A	16M	None	Valid	64k CMEM, 4M image maximum
4	Factory/Aug 2010	1.06	7.2.R00A	16M	None	Valid	None

3400 Series Platform Notes: The installed 3400 SDRAM is 64Mbytes.

Vanguard 242 Boot prom, Coldloader and Image Matrix

No.	*Release*	*Boot Code Version*	*Cold- loader from Release*	*On-Board Flash*	*Flash SIMM*	*Status*	*Comment*
1	7.2.R00A or earlier	2.31	7.2	8M	8M or none	Valid	128K CMEM, 8M image maximum

Vanguard 340 Enhanced Boot prom, Coldloader and Image Matrix

No.	*Release*	*Boot Code Version*	*Cold-loader from Release*	*On-Board Flash*	*Flash SIMM*	*Status*	*Comment*
1	6.4 or 7.2.R00A	2.31	6.4	8M	8M or none	Valid	128K CMEM, 8M image maximum

Vanguard 340 Enhanced platform Notes: ECC is supported.

Vanguard 342 Boot prom, Coldloader, Image, ECC and FLASH SIMM Matrix

No.	Rel.	DRAM DIMM	Boot Code Versio n	Cold-loader from Release	On-Board Flash	Physi cal Flash SIMM	Status	Comment
1	6.2	32M from Micron	2.1	6.2	8M	8M or None	Valid	128k CMEM, 8M image maximum
2	6.2	32M from Micron	2.1	6.3 to 7.2	8M	8M or None	Valid	128k CMEM, 8M image maximum
3	6.2	32M from Micron	2.30	6.2	8M	8M or None	Valid	128k CMEM, 8M image maximum
4	6.2	32M from Micron	2.30	6.3 to 7.2	8M	8M or None	VR	128k CMEM, 8M image maximum
5	6.2	32M from Micron	2.31	6.2	8M	8M or None	Valid	128k CMEM, 8M image maximum
6	6.2	32M from Micron	2.31	6.3 to 7.2	8M	8M or None	VR	128k CMEM, 8M image maximum
7	6.2	32M from Viking	2.1 to 2.30	6.2 to 7.2	8M	8M or None	Invalid	Viking 32M DRAM DIMM works only with 2.31 boot code
8	6.2	32M from Viking	2.31	6.2	8M	8M or None	Valid	Viking 32M DRAM DIMM works only with 2.31 boot code
9	6.2	32M from Viking	2.31	6.3 to 7.2	8M	8M or none	VR	Viking 32M DRAM DIMM works only with 2.31 boot code
10	6.3 to 7.2	32M from Micron	2.1	6.2	8M	8M or none	Valid	128k CMEM, 8M image maximum. ECC not supported.
11	6.3 to 7.2	32M from Micron	2.1	6.3 to 7.2	8M	8M or none	Valid	128k CMEM, 8M image maximum. ECC not supported
12	6.3 to 7.2	32M from Micron	2.30	6.2	8M	8M or none	Valid	128k CMEM, 8M image maximum
13	6.3 to 7.2	32M from Micron	2.30	6.3 to 7.2	8M	8M or none	Valid	128k CMEM, 8M image maximum
14	6.3 to 7.2	32M from Micron	2.31	6.2	8M	8M or none	Valid	128k CMEM, 8M image maximum

15	6.3 to 7.2	32M from Micron	2.31	6.3 to 7.2	8M	8M or none	VR	128k CMEM, 8M image maximum
16	6.3 to 7.2	32M from Viking	2.1 to 2.30	6.2 to 7.2	8M	8M or none	Invalid	Viking 32M DRAM DIMM works only with 2.31 boot code
17	6.3 to 7.2	32M from Viking	2.31	6.2	8M	8M or none	Valid	Viking 32M DRAM DIMM works only with 2.31 boot code
18	6.3 to 7.2	32M from Viking	2.31	6.3 to 7.2	8M	8M or none	VR	Viking 32M DRAM DIMM works only with 2.31 boot code

Vanguard 342 platform Notes:

1) The Vanguard 342 uses 32Mbyte DRAM. If the DRAM DIMM's vendor is Viking (Viking Part Number VI8GU083236BTB) 2.31 boot code must be used.
2) Boot code 2.1 was released with 6.2.
3) Boot code 2.1.1 was based on 2.1 and is compatible with the old released software. It contains the watchdog FER changes. Boot code 2.1.1 was released with 6.2.S100.
4) Boot code 2.20 (which is not mentioned in the above matrix) is the same as 2.1.1 except for the version string.
5) Boot code 2.30 is released with 6.3.R00A. It is based on 2.1.1. The ECC card is supported by the Boot code 2.30 and release 6.3.R00A or later.
6) Coldloader in 6.3.R00A or later was improved by adding valid flash address checking.
7) Boot code should be updated to 2.31 for when a SDRAM DIMM from "Viking" is used.

Vanguard 6800 Series Boot prom, Coldloader, Image Matrix

No.	***Release***	***Boot Code Version***	***Cold-loader from Release***	***On-Board Flash***	***SAN-DISK***	***Status***	***Comment***
1	6.5.P30A	1.06	7.0.R00A	4M	256M	Valid	None
2	7.1.R00A	1.07	7.1.R00A	4M	256M	Valid	For 7.0.R00A and 7.1.R00A, 1.07 boot prom is mandatory
3	7.2.R00A	1.07	7.2.R00A	4M	256M	Valid	For 7.0.R00A, 7.1.R00A, amd 7.2.R00A 1.07 boot prom is mandatory

Vanguard 7300 Series Boot prom, Coldloader, Image Matrix

No.	Rel.	Sys. Module	Boot Code Version	Cold-loader from Release	Compact Flash	On board flash	Status	Comment
1	6.1 to 6.3	MPC750 CPU	1.50	6.1 to 6.4	32M	1M	Valid	2M CMEM Compressed
2	6.1 to 6.3	MPC750 CPU	1.51	6.1 to 6.4	32M	1M	VR	2M CMEM Compressed
3	6.1 to 6.3	MPC750 CPU	2.00	6.1 to 6.4	32M	1M	Invalid	2M CMEM Compressed
4	6.1 to 6.3	IBM750 FX CPU	1.50 to 3.00	6.1 to 6.4	32M or 64M	16M (curr) + 16M (alt)	Invalid	New System Module released in 6.4
5	6.4	MPC750 CPU	1.50	6.1 to 6.4	32M	1M	Valid	2M CMEM Compressed
6	6.4	MPC750 CPU	1.51	6.1 to 6.4	32M	1M	VR	2M CMEM Compressed
7	6.4	MPC750 CPU	2.00	6.1 to 6.4	32M	1M	Invalid	2M CMEM Compressed
8	6.4	IBM750 FX CPU	1.50 and 1.51	6.1 to 6.4	32M or 64M	16M (curr) + 16M (alt)	Invalid	1.5x boot code not working with IBM750FX CPU card
9	6.4	IBM750 FX CPU	2.00	6.1 to 6.3	32M or 64M	16M (curr) + 16M (alt)	Invalid	6.1 to 6.3 cold loader not working with IBM750FX CPU card
10	6.4	IBM750 FX CPU	2.00	6.4	32M	16M (curr) + 16M (alt)	Valid	2M CMEM Compressed
11	6.4	IBM750 FX CPU	2.00	6.4	64M	16M (curr) + 16M (alt)	VR	2M CMEM Compressed
12	6.5 to 7.2	IBM750 FX CPU	3.00	6.5	64M	16M (curr) + 16M (alt)	VR	2M CMEM Compressed

13	6.5 to 7.2	MPC750	3.00	6.5	32M	1M	VR	2M CMEM Compressed

Vanguard 7300 Series Platform Notes:

1) The MPC750 CPU system module has 128Mbyte DRAM.
2) For the MPC750 CPU system module, a feature was implemented in Boot code 1.51. It enabled the node to be booted from current bank or alternate bank in the cold load menu. This boot code was released with 6.3.
3) The IBM750FX CPU system module has 512Mbyte DDR RAM.
4) For the IBM750FX CPU module, boot code 2.00 should be used. It has all the functionalities in 1.51.
5) For the MPC750 CPU system module, boot code 2.00 should not be used.
6) The on-board flash is primarily used for boot code.
7) For Release 6.5, boot code 3.00 is mandatory.

10 User Documentation

User documentation supporting the 7.3.R00A Applications Ware is organized as:

- Basic Protocols
- IP and LAN Feature Protocols
- SNA Feature Protocols
- Serial Feature Protocols
- Multi-service Feature Protocols
- Multimedia Feature Protocols

Each of these sets, which are available on our website, consists of several manuals. The contents of each set and the manual part numbers are described below.

Note: For information about obtaining these documents, refer to the “How to Obtain User Documentation” section in this document (Chapter 12).

10.1 Applications Ware Basic Protocols Manual

The Vanguard Applications Ware Basic Protocols Manual (Part Number T0106) consists of these manuals:

- Vanguard Configuration Basics (Part Number T0113)
- Frame Relay (Part Number T0106-02)
- Trans Polled Async (Part Number T0106-03)
- SNMP (Part Number T0106-04)
- Async Bypass (Part Number T0106-05)
- SLIP (Part Number T0106-06)
- TELNET (Part Number T0106-07)
- Point to Point PPP & MLPPP (Part Number T0106-08)
- Command Line Interface (Part Number T0106-09)
- X.25 Configuration Basics (Part Number T0107)
- Configuration for APAD/ATPAD (Part Number T0110)
- Bandwidth Management (Part Number T0108)

10.2 Applications Ware IP and LAN Feature Protocols Manual

The IP and LAN Feature Protocols Manual (Part Number T0100) consists of these manuals:

- Vanguard Router Basics (Part Number T0100-01)
- Bridging (Part Number T0100-02)
- IP Routing (Part Number T0100-03)
- OSPF (Part Number T0100-04)
- SIP (Part Number T0100-05)
- SoTCP (Part Number T0100-06)
- IPX (Part Number T0100-07)
- AppleTalk (Part Number T0100-08)
- Protocol Priority (Part Number T0100-09)
- Quality of Service (Part Number T0100-10)
- Asynchronous Transfer Mode (Part Number T0100-11)
- 7300 Series T3 ATM (Part Number T0100-12)
- Border Gateway Protocol (BGP-4) (Part Number T0100-13)
- Traffic Monitor (Part Number T0100-15)
- Ethernet Basics (Part Number T0109)
- Token Ring Basics (Part Number T0111)
- Firewall-DMZ (Part Number T0293)

10.3 Applications Ware SNA Feature Protocols Manual

The SNA Feature Protocols Manual (T0101) consists of these manuals:

- BSC 2780/3780 (Part Number T0101-02)
- BSC 3270 (Part Number T0101-03)
- IBM 2260 (Part Number T0101-04)
- SDLC (Part Number T0101-05)
- XDLC (Part Number T0101-06)
- AS/400 Communication Server (Part Number T0101-07)
- BSC 3270-to-SNA Conversion (Part Number T0101-08)
- BSC 2780/3780-to-SNA LU0 Conversion (Part Number T0101-09)
- TN3270 Remoter Server (Part Number T0101-10)
- VBIP BSC3270 to TCP/IP Conversion (Part Number T0290)

10.4 Applications Ware Serial Feature Protocols Manual

The Serial Feature Protocols Manual (T0102) consists of these manuals:

- Burroughs Poll/Select (Part Number T0102-02)
- NCR BSC (Part Number T0102-03)
- TBOP (Part Number T0102-04)
- NCCP (Part Number T0102-05)
- TCOP (Part Number T0102-06)
- SHDLC (Part Number T0102-07)
- T3POS (Part Number T0102-08)
- 3201 (Part Number T0102-09)
- X.42 (Part Number T0102-10)
- TNPP (Part Number T0102-11)
- TPDU (Part Number T0102-12)
- SPP (Part Number T0102-13)
- AC100 (Part Number T0102-14)
- ALC (Part Number T0102-15)

10.5 Applications Ware Multi-Service Feature Protocols Manual

The Multi-Service Feature Protocols Manual (T0103) consists of these manuals:

- Internal DSD (Part Number T0103-02)
- Multipoint X.25 (Part Number T0103-03)
- Frame Data Compressor (Part Number T0103-04)
- Vanguard 6560/6520 ISDN (Part Number T0103-05)
- Vanguard ISDN (Part Number T0103-06)
- Remote DataScope (Part Number T0103-07)
- SMDS (Part Number T0103-08)
- Data Encryption (Part Number T0103-09)
- Virtual Private Network (Part Number T0103-10)

10.6 Applications Ware Multimedia Feature Protocols Manual

The Multimedia Feature Protocols Manual (Part Number T0104) consists of these manuals:

- Voice Technology Reference Guide (Part Number T0104-04)
- Vanguard Voice Manual (Part Number T0104-05)
- Vanguard Voice Hardware Reference Card (Part Number T0104-06)

10.7 Applications Ware Alarms and Reports Manual

This Alarms and Reports Manual (Part Number T0005) contains a listing of all alarm and report messages generated by the Vanguard Applications Ware. The manual explains the actions you must perform in order to correct unexpected network situations that might arise while using any of the Applications Ware licenses on Vanguard Products. The alarms and traps database is also available on the web by doing the following:

1) Access the web site: http://www.vanguardnetworks.com/support-alarm-search.htm
2) Search the alarms by alarm, text or SMNP trap number.

11 How to Obtain User Documentation

There are two ways to obtain software documentation:

- Download the most current, up-to-date document files from the on-line Library on our World Wide Web page.
- Keep a current set of documentation for Release 7.3.R00A.

11.1 Download from the World Wide Web

The latest Vanguard user documentation, including detailed descriptions of new features and enhancements, is available on the World Wide Web.

Find your information faster and easier when you use the Product Documentation website. Eliminate the need to flip through several documentation updates. For example, suppose feature enhancements are made to ISDN over the course of several software releases. Each release provided a separate document describing the details of those ISDN features. The details of the features are described in the ISDN Manual in context with the rest of the feature information.

The full set of Vanguard Documentation is available for download from the Vanguard Networks Product Documentation website:

http://www.vanguardnetworks.com/support-documentation-overview.htm

To read the files, you need a copy of Adobe Acrobat Reader with Search. This application is free from many locations on the World Wide Web. You can define how you use Acrobat with your Web browser.

11.2 Keep a Current Set of Manuals

Keep a current set of documentation for Release 7.3.R00A. To download a current printed set you will need access to a:

- Internet connection to the Vanguard Networks product documentation website:
  http://www.vanguardnetworks.com/support-documentation-overview.htm
- Printer
- Copy of Adobe Acrobat for your platform

Download manuals from the WWW for the desired features you need. Print the files, and replace the pages in your set of documentation with the new version.

12 Vanguide CD-ROM with Vanguard Software Builder

Vanguide and Vanguide Plus! CD-ROMs are consolidated into one CD-ROM called Vanguide CD-ROM with Software Builder. Vanguard Software Builder is now included on the Vanguide CD-ROM.

12.1 Vanguard Software Builder

Vanguard Products come with a factory default Applications Ware software image. However, you can create your own Applications Ware, with a specific mix of features by using Vanguard Software Builder. This application let's you create custom features sets with features and functions suited for your specific needs. The features available for selection depend on the Applications Ware License you purchased. Vanguard Software Builder operates on Windows XP, Windows NT, Windows 2000, 95 or 98 platforms.

Vanguard Software Builder is part of the Vanguide Application Set. This set also includes the Vanguide Application Manager which provides access to the Software Loader and Software Builder applications. Once Software Builder is installed, you can:

- Select a specific software release
- Choose the product which you are loading/configuring
- Create a name and 2-digit number for the Applications Ware Package you want to create
- Follow a series of command prompts to select features/protocols for your Package

For more information, refer to Vanguard Software Builder Manual (Part Number T0030).

13 Release 7.3R00A for the Vanguard 3410/3410W/3460/3480

Release 7.3.R00A supports the following Applications Ware for the Vanguard 3410, 3410W, 3460, and 3480. Each Applications Ware supports a suite of default features. Other features, however, can be added by using Vanguard Software Builder. For more information, refer to the "Vanguide CD-ROM with Vanguard Software Builder" section in this document (Chapter 13).

Notes:

1) When using Vanguard Software Builder, be sure to make note of the warnings regarding memory limitations.
2) Information about the Applications Ware is divided into four tables.
    a. The first two tables list each model's Applications Ware and file information.
    b. The last two tables list each model's Applications Ware and its default, optional, and add- on features.

3400 Applications Ware Name	***Source Filename***	***Version String***	***Description Filename***
IPSAFE Applications Ware	73R00Abb11.xrc	7.3.R00A_@IPSAFE_3400	73R00Abb11.des
SNA+ Applications Ware	73R00Abb12.xrc	7.3.R00A_@SNA+_3400	73R00Abb12.des
Multi-service Applications Ware	73R00Abb15.xrc	7.3.R00A_@MS_3400	32R00Abb15.des

Release 7.3	**VG3410/W** **VG3460** **VG3480**								
July 2010 Updates	Release 7.3								
UPGRADE LICENSE	Base			Upgrade License					**TRD**
Legend: **L**=in license **D**=in default image **A**=add-on feature (upgrade license)	IP SAFE	SNA+	MS	Voice	Security Services	Encryption Acc.(*)	AS400/BSC	Advanced Voice	**SPECIALS ($)**
Network Management									
SNMP v1	D	D	D						
SNMP v3	L	L	L						
TELNET	D	D	D						
TFTP	D	D	D						
CLI	D	D	D						
Embedded Web HTTPD	L	L	L						
Async									
ATPAD	D	D	D						
APAD	L	L	L						
ISDN									
ISDN BRI-NOAM									
ISDN BRI-EURO									
ISDN BRI-ASIA									
ISDN (T1/E1/PRI) Data (NA Default)		L	L						
ISDN (T1/E1/PRI) Data (European)	L	L	L						
ISDN (T1/E1/PRI) Data (Asia)	L	L	L						
ISDN (T1/E1/PRI) Voice (incl sign. NA)									
ISDN (T1/E1/PRI) Voice (incl sign. Euro)									
Vanguard Voice Relay (2 x E&M)									
G.723.1			D	A	**<<3460/80 only**				
G.729A			D	A	**<<3460/80 only**				
CVSELP			L	A	**<<3460/80 only**				
Centralized Voice Switching			D	A	**<<3460/80 only**				

Voice Routing Services							3460/80 only>>	A	
Half Duplex Radio			L	A	<<3460/80 only				
Vanguard Voice Relay (Quad FXS/FXO))									
G.723.1/G729A/G711(can't add T.38)			L	A	<<3460/80 only				
G.723.1/G711(can add T.38)			L	A	<<3460/80 only				
G.729AB/G711(can add T.38)			L	A	<<3460/80 only				
G.723.1/G729A/G711(T.38, but no VAD)			L	A	<<3460/80 only				
Centralized Voice Switching			D	A	<<3460/80 only				
Voice Routing Services							3460/80 only>>	A	
FAX ITU T.38			L	A	<<3460/80 only				
Digital Voice - 68XX and 73XX models									
Vanguard T1/E1/PRI Digital Voice Server									
Half Duplex Radio			L	A	<<3460/80 only				
Digital Voice - 7300									
T.38 w/ G.723&G.711 for T1/E1									
T.38 w/ G.729a & G.711 for T1/E1									
Voice Relay with G.723.1 and G.729a									
Voice Relay Encapsulated in IP (SoTCP)									
H.323 v.2 Standards Based Voice									
Voice Over IP									
H.323/H.323 Caller ID	L	L	L	<<3460/80 only					
VOICE-IP-ENCAPSULATION	L	L	L						
Advanced Voice (Premium License features included in Advanced Voice License for 3400, 6800 and 7300 Series)									
SIP/SIP Connect 1.0							3460/80 only>>	A	
Caller ID							3460/80 only>>	A	
Call Hold							3460/80 only>>	A	
Call Waiting							3460/80 only>>	A	
Call Transfer							3460/80 only>>	A	
Call Forward							3460/80 only>>	A	

3rd Party Conferencing							**3460/80 only>>**	A	
LAN									
Router IP	D	D	D						
Router IPX	L	L	L						
LAN Option Protocols									
LLC-Eth		D	D						
IPXWAN	L	L	L						
Appletalk	L	L	L						
Bandwidth on Demand (Ld-Bal)	L	L	L						
Router Proxy	D	D	D						
Router Discovery	L	L	L						
Network Address Transl	L	L	L						
Policy Based Routing	L	L	L						
RTP/UDP/IP Header Compression	L	L	L						
ETH-Bridge	D	D	D						
XLB-Bridge									
IP Tunnel (GRE)	L	L	L						
DHCP Server & Client	L	L	L						
UDP/Radius client	L	L	L						
Dynamic IP Address (Dynamic VPN)	D	D	D						
IP Multicast Protocols									
PIM Sparse Multicast	L	L	L						
DVMRP Multicast	D	D	D						
Network Protocols									
NHRP Registration	L	L	L						
OSPF	D	L	L						
BGP4	L	L	L						
BGP IGB to BGP route Filtering									
BGP Multipath Load Balancing									
BGP Same AS as in ASPath									
BGP/TCP MD5 Authentication									
VRRP	L	L	L						
FRF12	L	L	L						
FRA(only for back compatibility)		L	L						
FRI (includes FRA)	D	D	D						
FR SVC DTE Interface									**A**
X25	D	D	D						
SMDS									
PPP Auto-Dialer	D	D	D						

PPP	D	D	D						
PPP IP Header Compression	L	L	L						
PPPoE	L	L	L						
SoTCP (=Voice Relay Encap. In IP)	L	L	L						
Fractional T1/E1	D	D	D						
Trunking Gateway for E1 only	D	D	D						
ATM Protocols									
ATM									
ATM Congestion Control									
IBM NETWORKING									
AS/400 5494 Comm. Server						**3410 only>>**	**A**		
BSC2780 (HPAD/TPAD)									
BSC2780/3780 to SNA Conversion						**3410 only>>**	**A**		
BSC3270 (HPAD/TPAD)		L	L						
VBIP (BSC to IP Conversion)		L	L						
BSC3270 to SNA Conversion						**3410 only>>**	**A**		
IBM2260									**A**
TN3270 Rem. Server Conversion						**3410 only>>**	**A**		
LLC-ETH		D	D						
LLC-FR		D	D						
SDLC		D	L						
Serial Asynchronous Protocols (NON-IBM)									
ASYNC-BYPASS	D	D	D						
ADSPAD	L	L	L						
SLIP	D	D	D						
TNPP									**A**
TNPP-ROUT									
X.42 (GSC)									
T3POS									**A**
T3POS over TCP									**A**
DATAPAC/3101 PAD/3201									**A**
SPP-PAD									**A**
AC100									
Serial Synchronous Protocols (NON-IBM)									
SHDLC									**A**
TBOP		D	D	A					
TBOP-BYPASS		D	D						
X32									**A**
XDLC									
Serial Character Oriented Protocols (NON-IBM)									

BSTD (Burroghs Poll Select)									**A**
TCOP		D	D						
TCOP-BYPASS		D	D						
NCRBSC									**A**
RS366 (801 Autodialer Protocol)									**A**
TPDU Adaptors									
TPA-TPDU		L	L						
TPA-SDLC									A
TPA-3270									A
TPA-2780									A
TPA-TCP		L	L						
TPA-UDP		L	L						
Node Features									
ATCIF (AT Dial/Telnet)	L	L	L						
LBU	D	D	D						
DCP		D	L						
DSCOPE		L	L						
DSD			L						
NCCP									A
BCST									A
NUI (Northern Telecom Backbone)									A
QOS Features									
TOW									
QoS - Protocol Priority (5.3M)									**A**
QoS - Diff Serv	D	D	D						
Ethernet DiffServ QoS (WAN)	D	D	D						
MLPPP LFI			L						
FRAME Data Comp									
IP-FLOW o/MLPPP (NetFlow 5)	D	D	D						
Security and VPN									
Enhanced Firewall ** (DOS mitigation,, Intrazone, Interzone, Control Plane Policies)					A				
Syslog Client					A				
IPSec 3DES S/W based encryption	L	L	L						
IPSec Aggressive mode									
SSH	L	L	L						
Hardware Accelerated Encryption & VPN DES, 3DES and AES						A			
PKI & X.509 Digital Certificates						A			

	Enhanced SSH						A			

14 Release 7.3R00A for the Vanguard 6840/6841

Release 7.3.R00A supports the following Applications Ware for the Vanguard 6840/6841. Each Applications Ware supports a suite of default features. Other features, however, can be added by using Vanguard Software Builder. For more information, refer to the “Vanguide CD-ROM with Vanguard Software Builder” section in this document (Chapter 12).

Notes:

1) When using Vanguard Software Builder, be sure to make note of the warnings regarding memory limitations.
2) Information about the Applications Ware is divided into four tables.
    a. The first two tables list each model’s Applications Ware and file information.
    b. The last two tables list each model’s Applications Ware and its default, optional, and add- on features.

6840 Applications Ware Name	***Source Filename***	***Version String***	***Description Filename***
IPSAFE Applications Ware	73R00Aba11.xrc	7.3.R00A_@IPSAFE_6840	73R00Aba11.des
SNA+ Applications Ware	73R00Aba12.xrc	7.3.R00A_@SNA+_6840	73R00Aba12.des
Multi-service Applications Ware	73R00Aba15.xrc	7.3.R00A_@MS_6840	73R00Aba15.des

6841 Applications Ware Name	***Source Filename***	***Version String***	***Description Filename***
IPSAFE Applications Ware	73R00Aba11.xrc	7.3.R00A_@IPSAFE_6840	73R00Aba11.des
SNA+ Applications Ware	73R00Aba12.xrc	7.3.R00A_@SNA+_6840	73R00Aba12.des
Multi-service Applications Ware	73R00Aba15.xrc	7.3.R00A_@MS_6840	73R00Aba15.des

Release 7.3	**VG6840** **VG6841** (encryption module)								
July 2010 Updates	Release 7.3								
UPGRADE LICENSE	Base			Upgrade License					**TRD**
Legend: **L**=in license **D**=in default image **A**=add-on feature (upgrade license)	IP SAFE	SNA+	MS	Voice	Security Services	Encryption Acc.(*)	AS400/BSC	Advanced Voice	**SPECIALS ($)**
Network Management									
SNMP v1	D	D	D						
SNMP v3	L	L	L						
TELNET	D	D	D						
TFTP	D	D	D						
CLI	D	D	D						
Embedded Web HTTPD	L	L	L						
Async									
ATPAD	D	D	D						
APAD	L	L	L						
ISDN									
ISDN BRI-NOAM	L	L	L						
ISDN BRI-EURO	L	L	L						
ISDN BRI-ASIA	L	L	L						
ISDN (T1/E1/PRI) Data (NA Default)	L	L	L						
ISDN (T1/E1/PRI) Data (European)	L	L	L						
ISDN (T1/E1/PRI) Data (Asia)	L	L	L						
ISDN (T1/E1/PRI) Voice (incl sign. NA)			L	A					
ISDN (T1/E1/PRI) Voice (incl sign. Euro)			L	A					
Vanguard Voice Relay (2 x E&M)									
G.723.1			D	A					
G.729A			L	A					
CVSELP			L	A					
Centralized Voice Switching			L	A					
Voice Routing Services			L	A					
Half Duplex Radio				A					
Vanguard Voice Relay (Quad FXS/FXO))									

G.723.1/G729A/G711(can't add T.38)			L	A					
G.723.1/G711(can add T.38)			L	A					
G.729AB/G711(can add T.38)			L	A					
G.723.1/G729A/G711(T.38, but no VAD)			L	A					
Centralized Voice Switching			L	A					
Voice Routing Services			L	A					
FAX ITU T.38			L	A					
Digital Voice - 68XX and 73XX models									
Vanguard T1/E1/PRI Digital Voice Server			D	A					
Half Duplex Radio				A					
Digital Voice - 7300									
T.38 w/ G.723&G.711 for T1/E1									
T.38 w/ G.729a & G.711 for T1/E1									
Voice Relay with G.723.1 and G.729a									
Voice Relay Encapsulated in IP (SoTCP)									
H.323 v.2 Standards Based Voice									
Voice Over IP									
H.323/H.323 Caller ID									
VOICE-IP-ENCAPSULATION			L	A					
Advanced Voice (Premium License features included in Advanced Voice License for 3400, 6800 and 7300 Series)									
SIP/SIP Connect 1.0								A	
Caller ID								A	
Call Hold								A	
Call Waiting								A	
Call Transfer								A	
Call Forward								A	
3rd Party Conferencing								A	
LAN									
Router IP	D	D	D						
Router IPX	L	L	L						
LAN Option Protocols									
LLC-Eth		D	D						
IPXWAN	L	L	L						
Appletalk	L	L	L						
Bandwidth on Demand (Ld-Bal)	L	L	L						
Router Proxy	D	D	D						
Router Discovery	L	L	L						
Network Address Transl	L	L	L						
Policy Based Routing	L	L	L						
RTP/UDP/IP Header Compression	L	L	L						
ETH-Bridge	D	D	D						

XLB-Bridge	L	L	L						
IP Tunnel (GRE)	L	L	L						
DHCP Server & Client	L	L	L						
UDP/Radius client	L	L	L						
Dynamic IP Address (Dynamic VPN)	D	D	D						
IP Multicast Protocols									
PIM Sparse Multicast	L	L	L						
DVMRP Multicast	D	D	D						
Network Protocols									
NHRP Registration	L	L	L						
OSPF	L	L	L						
BGP4	L	L	L						
BGP IGB to BGP route Filtering									
BGP Multipath Load Balancing									
BGP Same AS as in ASPath									
BGP/TCP MD5 Authentication									
VRRP	L	L	L						
FRF12	L	L	L						
FRA(only for back compatibility)		L	L						
FRI (includes FRA)	D	D	D						
FR SVC DTE Interface									**A**
X25	D	D	D						
SMDS			L						
PPP Auto-Dialer	L	L	L						
PPP	D	D	D						
PPP IP Header Compression	L	L	L						
PPPoE	L	L	L						
SoTCP (=Voice Relay Encap. In IP)	L	L	L						
Fractional T1/E1	D	D	D						
Trunking Gateway for E1 only	D	D	D						
ATM Protocols									
ATM									
ATM Congestion Control									
IBM NETWORKING									
AS/400 5494 Comm. Server							A		
BSC2780 (HPAD/TPAD)		L	L						
BSC2780/3780 to SNA Conversion							A		
BSC3270 (HPAD/TPAD)		L	L						
VBIP (BSC to IP Conversion)									
BSC3270 to SNA Conversion							A		
IBM2260									**A**
TN3270 Rem. Server Conversion									
LLC-ETH									
LLC-FR		D	D						

SDLC		D	L						
Serial Asynchronous Protocols (NON-IBM)									
ASYNC-BYPASS	D	D	D						
ADSPAD									
SLIP	D	D	D						
TNPP									**A**
TNPP-ROUT			L						
X.42 (GSC)									**A**
T3POS		L	L						
T3POS over TCP		L	L						
DATAPAC/3101 PAD/3201									
SPP-PAD									**A**
AC100									**A**
Serial Synchronous Protocols (NON-IBM)									
SHDLC									
TBOP		D	D	A					
TBOP-BYPASS		D	D						
X32	L	L	L						
XDLC		L	L						
Serial Character Oriented Protocols (NON-IBM)									
BSTD (Burroghs Poll Select)									
TCOP		D	D						
TCOP-BYPASS		D	D						
NCRBSC									**A**
RS366 (801 Autodialer Protocol)		L	L						
TPDU Adaptors									
TPA-TPDU									
TPA-SDLC									
TPA-3270									
TPA-2780									
TPA-TCP									
TPA-UDP									
Node Features									
ATCIF (AT Dial/Telnet)	L	L	L						
LBU	D	D	D						
DCP		D	L						
DSCOPE		L	L						
DSD			L						
NCCP		L	L						
BCST									**A**
NUI (Northern Telecom Backbone)	L	L	L						
QOS Features									
TOW	D	D	D						
QoS - Protocol Priority (5.3M)	L	L	L						

QoS - Diff Serv	D	D	D						
Ethernet DiffServ QoS (WAN)	D	D	D						
MLPPP LFI			L						
FRAME Data Comp	L	L	D						
IP-FLOW o/MLPPP (NetFlow 5)	L								
Security and VPN									
Enhanced Firewall ** (DOS mitigation,, Intrazone, Interzone, Control Plane Policies)					A				
Syslog Client					A				
IPSec 3DES S/W based encryption	L	L	L						
IPSec Aggressive mode									
SSH	L	L	L						
Hardware Accelerated Encryption & VPN DES, 3DES and AES		**6841 only>>**				A			
PKI & X.509 Digital Certificates		**6841 only>>**				A			
Enhanced SSH						A			

15 Release 7.3R00A for the Vanguard 7310/7330

This section provides detailed information about the Applications Ware available for Vanguard 7300.

Release 7.3.R00A makes available the following Applications Ware for the Vanguard 7300. Each Applications Ware package supports a suite of default features. Other features, however, can be added by using Vanguard Software Builder.

Vanguard 7310 Applications Ware Name	***Source Filename***	***Version String***	***Description Filename***
IP+	7.3.R00At11.xrc	7.3.R00A_@IP+_7310	73R00At11.des
SNA+	7.3.R00At12.xrc	7.3.R00A_@SNA+_7310	73R00At12.des
Multi-Service	7.3.R00At15.xrc	7.3.R00A_@MS_7310	73R00At15.des

Vanguard 7330 Applications Ware Name	***Source Filename***	***Version String***	***Description Filename***
IP+	73R00Au11.xrc	7.3.R00A_@IP+_7330	73R00Au11.des
SNA+	73R00Au12.xrc	7.3.R00A_@SNA+_7330	73R00Au12.des
Multi-Service	73R00AAu15.xrc	7.3.R00A_@MS_7330	73R00Au15.des

Release 7.3	**VG7300 VG7310**								
July 2010 Updates	Release 7.3								
UPGRADE LICENSE	Base			Upgrade License					**TRD**
Legend: **L**=in license **D**=in default image **A**=add-on feature (upgrade license)	IP+	SNA+	MS	Voice	Security Services	Encryption Acc. (*)	AS400/BSC	Advanced Voice	**SPECIALS ($)**
Network Management									
SNMP v1	D	D	D						
SNMP v3	L	L	L						
TELNET	D	D	D						
TFTP	D	D	D						
CLI	D	D	D						
Embedded Web HTTPD	D	D	D						
Async									
ATPAD	D	D	D						
APAD	L	L	L						
ISDN									
ISDN BRI-NOAM									
ISDN BRI-EURO									
ISDN BRI-ASIA									
ISDN (T1/E1/PRI) Data (NA Default)	D	D	D						
ISDN (T1/E1/PRI) Data (European)	L	L	L						
ISDN (T1/E1/PRI) Data (Asia)	L	L	L						
ISDN (T1/E1/PRI) Voice (incl sign. NA)	D	D	D						
ISDN (T1/E1/PRI) Voice (incl sign. Euro)	L	L	L						
Vanguard Voice Relay (2 x E&M)									
G.723.1									
G.729A									
CVSELP									
Centralized Voice Switching									
Voice Routing Services									
Half Duplex Radio									
Vanguard Voice Relay (Quad FXS/FXO))									
G.723.1/G729A/G711(can't add T.38)									

G.723.1/G711(can add T.38)									
G.729AB/G711(can add T.38)									
G.723.1/G729A/G711(T.38, but no VAD)									
Centralized Voice Switching									
Voice Routing Services									
FAX ITU T.38									
Digital Voice - 68XX and 73XX models									
Vanguard T1/E1/PRI Digital Voice Server	D	D	D						
Half Duplex Radio									
Digital Voice - 7300									
T.38 w/ G.723&G.711 for T1/E1	L	L	L						
T.38 w/ G.729a & G.711 for T1/E1	L	L	L						
Voice Relay with G.723.1 and G.729a	D	D	D						
Voice Relay Encapsulated in IP (SoTCP)	D	D	D						
H.323 v.2 Standards Based Voice	D	D	D						
Voice Over IP									
H.323/H.323 Caller ID									
VOICE-IP-ENCAPSULATION	D	D	D						
Advanced Voice (Premium License features included in Advanced Voice License for 3400, 6800 and 7300 Series)									
SIP/SIP Connect 1.0								A	
Caller ID								A	
Call Hold								A	
Call Waiting								A	
Call Transfer								A	
Call Forward								A	
3rd Party Conferencing								A	
LAN									
Router IP	D	D	D						
Router IPX	D	D	D						
LAN Option Protocols									
LLC-Eth		D	D						
IPXWAN	D	D	D						
Appletalk									
Bandwidth on Demand (Ld-Bal)	D	D	D						
Router Proxy	D	D	D						
Router Discovery	D	D	D						
Network Address Transl	D	D	D						
Policy Based Routing	D	D	D						
RTP/UDP/IP Header Compression	D	D	D						
ETH-Bridge	D	D	D						
XLB-Bridge									
IP Tunnel (GRE)						A			

DHCP Server & Client	D	D	D						
UDP/Radius client	D	D	D						
Dynamic IP Address (Dynamic VPN)	D	D	D						
IP Multicast Protocols									
PIM Sparse Multicast	L	L	L						
DVMRP Multicast	D	D	D						
Network Protocols									
NHRP Registration	L	L	L						
OSPF	D	D	D						
BGP4	D	D	D						
BGP IGB to BGP route Filtering									
BGP Multipath Load Balancing									
BGP Same AS as in ASPath									
BGP/TCP MD5 Authentication									
VRRP	L	L	L						
FRF12	D	D	D						
FRA(only for back compatibility)									
FRI (includes FRA)	D	D	D						
FR SVC DTE Interface									**A**
X25	D	D	D						
SMDS									
PPP Auto-Dialer	L	L	L						
PPP	D	D	D						
PPP IP Header Compression									
PPPoE	L	L	L						
SoTCP (=Voice Relay Encap. In IP)	D	D	D						
Fractional T1/E1	D	D	D						
Trunking Gateway for E1 only									
ATM Protocols									
ATM			D						
ATM Congestion Control			D						
IBM NETWORKING									
AS/400 5494 Comm. Server							A		
BSC2780 (HPAD/TPAD)									
BSC2780/3780 to SNA Conversion		D	D						
BSC3270 (HPAD/TPAD)									
VBIP (BSC to IP Conversion)									
BSC3270 to SNA Conversion		D	D						
IBM2260									
TN3270 Rem. Server Conversion									
LLC-ETH									
LLC-FR		D	D						
SDLC		D	D						
Serial Asynchronous Protocols (NON-IBM)									

ASYNC-BYPASS									
ADSPAD									
SLIP									
TNPP									
TNPP-ROUT									
X.42 (GSC)									
T3POS									
T3POS over TCP									
DATAPAC/3101 PAD/3201									
SPP-PAD									
AC100									
Serial Synchronous Protocols (NON-IBM)									
SHDLC									
TBOP		D	D						
TBOP-BYPASS									
X32									
XDLC									
Serial Character Oriented Protocols (NON-IBM)									
BSTD (Burroghs Poll Select)									
TCOP									
TCOP-BYPASS									
NCRBSC									
RS366 (801 Autodialer Protocol)									
TPDU Adaptors									
TPA-TPDU									
TPA-SDLC									
TPA-3270									
TPA-2780									
TPA-TCP									
TPA-UDP									
Node Features									
ATCIF (AT Dial/Telnet)	D	D	D						
LBU	D	D	D						
DCP		D	D						
DSCOPE									
DSD									
NCCP									
BCST									
NUI (Northern Telecom Backbone)									
QOS Features									
TOW	D	D	D						
QoS - Protocol Priority (5.3M)									
QoS - Diff Serv	D	D	D						
Ethernet DiffServ QoS (WAN)	D	D	D						

MLPPP LFI			L						
FRAME Data Comp	D	D	D						
IP-FLOW o/MLPPP (NetFlow 5)	L								
Security and VPN									
Enhanced Firewall ** (DOS mitigation,, Intrazone, Interzone, Control Plane Policies)					A				
Syslog Client					A				
IPSec 3DES S/W based encryption									
IPSec Aggressive mode									
SSH									
Hardware Accelerated Encryption & VPN DES, 3DES and AES						A			
PKI & X.509 Digital Certificates						A			
Enhanced SSH						A			

16 MIB Download Steps for Third-Party SNMP Managers

This section lists Vanguard MIB files needed for SNMP management of Vanguard devices when using aa third-party non-Vanguard Networks SNMP Network Management System (NMS).

16.1 Obtaining MIB Files

Vanguard MIB files for your third-party NMS are available from the Vanguide 7.3.R00A CD-ROM. You can also download MIB files from the internet. The address for the server is:
http://www.vanguardnetworks.com/support-downloads-mibs.htm

On the internet, there is one ZIP file for the PC and one ZIP file for UNIX. You must unzip the ZIP file to get the MIB files. The contents of these two ZIP files are identical. However, the formats of the files in these two ZIP files are slightly different due to the way PCs and UNIX systems handle text files. Depending on the protocols and options provided by the Applications Ware image installed in your node, you might not need all the MIB files. See the Required Files and Loading section below for details on the files you should have to support SNMP management for Vanguard products.

16.2 Required Files and Loading

The following MIB files are required by your NMS to perform SNMP management of Vanguard products:

- rfc1213.mib
- cdx_6500.mib

These files must be loaded first and in the order shown. After you load these required files onto your NMS, you can load the MIB files for the options and protocols installed on your Vanguard hardware. See the MIB Files for Options/Protocols section below.

16.3 MIB Files for Options/Protocols

This table lists the contents of options and protocol MIB files for Vanguard products. Use this table to determine which MIB files you need to download.

Download this MIB File	If you want this option, protocol, or base MIB software
adspad_opt.mib	ADS Protocol
alc_opt.mib	ALC protocol
atm_opt.mib	Asynchronous Transfer Mode
bcst_opt.mib	Broadcast
bgp4_opt.mib	Border Gateway Protocol 4
bri_opt.mib	ISDN BRI protocol
bridge_opt.mib	Bridging option
bsc2780_opt.mib	BSC2780 protocol
bsc3270_opt.mib	BSC3270 protocol
bstd_opt.mib	Burroughs Poll/Select protocol
cdx_6500.mib	Required base MIB for Vanguard Products MIBs
dc_opt.mib	Data Compression option
dcp_opt.mib	Data Connection Protection option
de_opt.mib	Data Encryption option
dsd_opt.mib	Digital Sharing Device Option
e1_opt.mib	Physical E1 port
eia_opt.mib	EIA protocol (required file for serial protocol support)
eth_opt.mib	Ethernet option
eth_sw_opt.mib	Ethernet Switch Option
frdce_opt.mib	Frame Relay DCE option
frdte_opt.mib	Frame Relay DTE option
fri_opt.mib	Frame Relay option
fwall_opt.mib	Firewall Option
gsc_opt.mib	GSC protocol
hub_opt.mib	Ethernet Hub option
ibm2260_opt.mib	IBM2260 protocol
ipsec_opt.mib	IP Security
isdn_opt.mib	ISDN protocol
iso3201_opt.mib	3201 protocol
mx25_opt.mib	MX.25 protocol
ncrbsc_opt.mib	NCR Binary Synchronous protocol
ns_opt.mib	Network Service (required file)
pad_opt.mib	PAD protocol
pim_opt.mib	Protocol Independent Multicast
ping_opt.mib	Remote Ping Option

ppp_opt.mib	Point-to-Point protocol
pppoe_opt.mib	Point-to-Point protocol over Ethernet
qos_opt.mib	Quality of Service option - QoS-Kit- includes: QoS_CORE, QoS_CLSSIFIER and QoS_SCHEDULER
qos_pp_opt.mib	Quality of Service option - QoS-PP (Protocol Priority) includes: QoS_CCM, PACKET_CLASSIFIER and PACKET SCH-EDULER
radius_opt.mib	RADIUS
rfc1213.mib	MIB-II for managing TCP/IP -based internets
rfc1231.mib	IEEE 802.5 Token Ring MIB
rfc1286.mib	Definitions of managed objects for bridges
rfc1315.mib	Management Information Base for Frame Relay DTEs
rfc1398.mib	Managed objects for Ethernet-type interfaces
rfc1657a.mib	BGP4 MIB (Converted to SNMP version 1 from the ori-ginal rfc1657 mib).
rfc1850av.mib	OSPF Version 2 MIB
rfc1903v.mib	Textual conventions for version 2 of SNMP
rfc2496a.mib	DS3/E3 Interface Type MIB (Converted to SNMP version 1 from the original rfc2496 mib).
rfc2618a.mib	RADIUS Authentication Client MIB
rfc2620a.mib	RADIUS Accounting Client MIB
router_opt.mib	Routing option (required file)
rs366_opt.mib	EIA RS366 support
sdlc_opt.mib	SDLC protocol
shdsl_opt.mib	Symmetric High Speed DSL
slac_opt.mib	LLC Ethernet/Frame Relay/Token Ring Conversion option
snabsc_opt.mib	SNA to BSC3270 Conversion
spp_opt.mib	SPP protocol
ss_opt.mib	Switched Services (required file)
t1_opt.mib	Physical T1 port
t1e1_opt.mib	Virtual T1/E1 port mapping table
t1e1tg_opt.mib	T1/E1 for the 7300 Series
t1e1vg_opt.mib	T1/E1 for the 6840/3400/34X Series
tbop_opt.mib	TBOP protocol
tcop_opt.mib	TCOP protocol
tcpbsc_opt.mib	BSC3270 to TCP/IP Conversion
tdlc_opt.mib	TDLC protocol
tdmclk_opt.mib	TDM Network Clock option
tdmtgclk_opt.mib	TDM Network Clock option for the 7300

tftp_opt.mib	TFTP option
tn3270_opt.mib	TN3270 Remote Server
tnpp_opt.mib	Telocator Network Paging Protocol (TNPP)
tow_opt.mib	TOW option
tr_opt.mib	Token Ring option
traffic_monitor_opt.mib	Traffic Monitor
trap.mib	trap mib
v_opt.mib	Voice Relay option
vpmt_opt.mib	Virtual Port Mapping Table option
vrrp_opt.mib	Virtual Router Redundancy Protocol
wan_opt.mib	WAN support (required file)
x25_opt.mib	X.25 option
xdlc_opt.mib	XDLC protocol

17 Applications Ware RFC Compliance

RFC	Description
768	User Datagram Protocol. J. Postel. Aug-28-1980.
791	Internet Protocol. J. Postel. Sep-01-1981.
792	Internet Control Message Protocol. J. Postel. Sep-01-1981. Not all messages covered by RFC 792 are supported by Applications Ware.
793	Transmission Control Protocol. J. Postel. Sep-01-1981.
826	An Ethernet Address Resolution Protocol-or-Converting network protocol addresses to 48.bit Ethernet Address for Transmission on Ethernet hardware. D.C. Plummer. Nov-01-1982.
854	Telnet Protocol Specification. J. Postel, J.k. Reynolds. May-01-1983.
858	Telnet Suppress Go Ahead Option. J. Postel, J.K. Reynolds. May-01-1983.
877	Standard For The Transmission Of IP Datagrams Over Public Data Networks. J.T. Korb. Sep-01-1983.

894	Standard for the Transmission of IP data grams over Ethernet networks. C. Hornig. Apr-01-1984.
919	Broadcasting Internet Datagrams. J.C. Mogul. Oct-01-1984.
922	Broadcasting Internet datagrams in the presence of subnets. J.C. Mogul. Oct-01-1984.
950	Internet Standard Subneting Procedure. J.C. Mogul, J. Postel. Aug-01-1985.
951	Proposed Bootstrap protocol (BOOTP) for ARPA-Internet W. Croft, J. Gilmore. Sept-01-1985.
1009	Requirements for Internet Gateways R.Braden, J. Postel. Jun-01-1987.
1042	Standard For The Transmission Of IP Datagrams Over IEEE 802 Networks. J. Postel, J.k. Reynolds. Feb-01-1988.
1055	Nonstandard For Transmission Of IP Datagrams Over Serial Lines: SLIP. J.l. Romkey. Jun-01-1988.
1058	RIP Version 2 Carrying Additional Information. G. Malkin. January 1993.
1060	Assigned values used in network protocol implementations. J. Reynolds, J. Postel. Mar-01-1990.
1075	Distance Vector Multicast Routing Protocol. D. Waitzman, C Partridge, S. Deering. Nov-010-1988.
1091	Telnet Terminal-type Option. J. Vanbokkelen. Feb-01-1989.
1112	Host Extensions for IP Multicasting S. Deering. Aug-01-1989.
1122	Requirements for Internet hosts - communication layers. R.T. Braden. Oct-01-1989.
1123	Requirements for Internet hosts - application and support. R.T. Braden. Oct-01-1989.
1144	Compressing TCP/IP headers for low-speed serial links. V.Jacobson. Feb-01-1990.

1155	Structure And Identification Of Management Information For TCP/IP-based Internets. M.t. Rose, K. Mccloghrie. May-01-1990.
1156	MIB for Network Management of TCP/IP based Internets.
1157	Simple Network Management Protocol (SNMP). J.D. Case, M. Fedor, M.L. Schoffstall, C. Davin. May-01-1990.
1209	Transmission Of IP Datagrams Over The SMDS Service. D.m. Piscitello, J. Lawrence. Mar-01-1991.
1212	Concise MIB Definitions. M.t. Rose, K. Mccloghrie. Mar-01-1991.
1213	Management Information Base For Network Management Of TCP/IP-based Internets: MIB-II. K. Mccloghrie, M.t. Rose. Mar-01-1991.
1215	A Convention for Defining Traps for use with the SNMP. M. Rose, Editor, Performance Systems International. March 1991.
1231	IEEE 802.5 Token Ring MIB. K. Mccloghrie, R. Fox, E. Decker. May-01-1991.
1250	IAB Official Protocol Standards. J. Postel. Aug-01-1991.
1256	ICMP Router Discovery Messages. S. Deering. September 1991.
1286	Definitions Of Managed Objects For Bridges. E. Decker, P. Langille, A. Rijsinghani, K. Mccloghrie. December, 1991.
1293	Inverse Address Resolution Protocol. T. Bradley, C. Brown. Jan-01-1992.
1294	Multi-protocol Interconnect Over Frame Relay. T. Bradley, C. Brown, A. Malis. January 1992.
1315	Management Information Base for Frame Relay DTEs. C. Brown, F. Baker, C. Carvalho. April 9, 1992.
1332	PPP Internet Protocol Control Protocol (IPCP). G. McGregor. May 1992.
1334	PPP Authentication Protocols B. Lloyd, W. Simpson. Oct-01-1992.
1340	Status of Assigned Numbers J. Reynolds, J. Postel. July-01-1992.

1349	Type of Service in the Internet Protocol Suite P. Almquist. Jul-01-1992.
1356	Multiprotocol Interconnect On X.25 And ISDN In The Packet Mode. A. Malis, D. Robinson, R. Ullmann. August 1992.
1362	Novell IPX over Various WAN Media (IPXWAN). M. Allen. Sept-01-1992.
1398	Definitions Of Managed Objects For The Ethernet-like Interface Types. F. Kastenholz. January 1993.
1483*	Multiprotocol Encapsulation over ATM Adaptation Layer 5 Juha Heinanen, July 1993. *** See RFC 2684. RFC 2684 obsoletes RFC 1483**
1490	Multiprotocol Interconnect Over Frame Relay. T. Bradley, C. Brown, & A. Malis. July 1993.
1517	Applicability Statement For The Implementation Of Classless Inter-Domain Routing (CIDR). Internet Engineering Steering Group, R. Hinden. September 1993.
1518	An Architecture For IP Address Allocation With CIDR. Y. Rekhter & T. Li. September 1993.
1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. V. Fuller, T. Li, J. Yu, & K. Varadhan. September 1993.
1520	Exchanging Routing Information Across Provider Boundaries in the CIDR Environment. Y. Rekhter & C. Topolcic. September 1993.
1534	Interoperation between DHCP and BOOTP. R. Droms. Oct-01-1993.
1542	Clarifications and Extensions for the Bootstrap Protocol. W. Wimer. Oct-01-1993.
1576	TN3270 Current Practices. J. Penner. DCA, Inc. January 1994.
1577	Classical IP and ARP over ATM M. Laubach, January 1994.
1583	OSPF Version 2. J. Moy. Mar-01-1994.
1631	The Network Address Translator (NAT). K. Egevang, P. Francis. May 1994.

1634	The text/enriched MIME Content-type. N. Borenstein. Jan-01-1994.
1647	TN3270 Enhancements. B. Kelly. Auburn University. July 1994.
1661	The Point-to-Point Protocol (PPP). W. Simpson, Editor. July 1994.
1694	Definitions of Managed Objects for SMDS Interfaces Using SMIv2. T. Brown & K. Tesink, Editors. August 1994.
1700	Assigned Numbers. J. Reynolds, J. Postel. October, 1994.
1745	BGP/IDRP of IP - OSPF Interaction K. Varadhan, OARnet & ISI, S. Hares, NSFnet/Merit, Y. Rekhter, T.J. Watson Research Center, IBM Corp., December 1994.
1771	A Border Gateway Protocol 4 (BGP-4) Y. Rekhter, T.J. Watson Research Center, IBM Corp., T. Li, Cisco Systems, Editors. March 1995.
1793	Extending OSPF to Support Demand Circuits. J. Moy, Cascade. April 1995.
1812	Requirements for IP Version 4 Routers. F. Baker. June 1995.
1828	IP Authentication using Keyed MD5 P. Metzger, Piermont, W. Simpson, Daydreamer. August 1995.
1852	IP Authentication using Keyed SHA P. Metzger, Piermont, W. Simpson, Daydreamer. September 1995.
1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). J. Case, K. McCloghrie, M. Rose, S. Walbusser. January 1996.
1918	Address Allocation for Private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot & E. Lear. February 1996.
1990	The PPP Multilink Protocol (MP). K. Sklower, B. Lloyd, G. McGregor, D. Carr, T. Caradetti. August 1996.
1997	BGP Communities Attribute. R. Chandra, P. Traina, Cisco Systems, T. Li. August 1996.
1998	Application of the BGP Community Attribute in Multi-home Routing. E. Chen, MCI, T. Bates, Cisco Systems. August 1996.

2131	Dynamic Host Configuration Protocol (DHCP). R. Droms, Bucknell University, March, 1997.
2132	DHCP Options and BOOTP Vendor Extensions. S. Alexander, Silicon Graphics, Inc., R. Droms, Bucknell University. March 1997.
2236	Internet Group Management Protocol (IGMP), Version 2 W. Fenner-Xerox PARC. November, 1997.
2338	Virtual Router Redundancy Protocol (VRRP). S. Knight, D. Weaver, Ascend Communications, D. Whipple, Microsoft, Inc., R. Hinden, D. Mitzel, P. Hunt, Nokia, P. Higginson, M. Shand, Digital Equipment Corp., A. Lindem, IBM Corporation. April 1998.
2362	Protocol Independent Multicast-Sparse Mode (PIM-SM). D. Estrin, D.Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei, CISCO, UCL, USC, LBL, XEROX and UMICH. June 1998.
2364	PPP Over AAL5. G. Gross, Lucent Technologies, M. Kaycee, Paradyne, A. Lin, Shasta Networks, A. Malis, Ascend Communications, J. Stephens, Cayman Systems. July 1998.
2393	IP Payload Compression Protocol (IPComp). A. Shacham, Cisco, R. Monsour, Hi/fn, Inc., R. Pereira, TimeStep, M. Thomas, AltaVista Internet. December 1998.
2395	IP Payload Compression using LZS. R. Friend, R. Monsour, Hi/fn, Inc. December 1998.
2401	Security Architecture for the Internet Protocol. S. Kent, BBN Corp., R. Atkinson, @Home Network. November 1998.
2402	IP Authentication Header. S. Kent, BBN Corp., R. Atkinson, @Home Network. November 1998.
2403	The Use of HMAC-MD5-96 within ESP and AH. C. Madson, Cisco System Inc., R. Glenn, NIST. November 1998.
2404	The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, Cisco System Inc., R. Glenn, NIST. November 1998.
2405	The ESP DES-CBC Cipher Algorithm with Explicit IV. C. Madson, Cisco System Inc. N. Doraswamy, Bay Networks, Inc. November 1998.
2406	IP Encapsulating Security Payload (ESP). S. Kent, BBN Corp., R. Atkinson, @Home Network. November 1998.

2407	The Internet IP Security Domain of Interpretation for ISAKMP. D. Piper, Network Alchemy. November 1998.
2408	Internet Security Association and Key Management Protocol (ISAKMP) D. Maughan, National Security Agency, M. Schertler, Security, Inc., M. Schneider, National Security Agency, J. Turner, RABA Technologies, Inc. November 1998.
2409	The Internet Key Exchange (IKE). D. Harkins, D. Carrel, Cisco Systems. November 1998.
2410	The NULL Encryption Algorithm and Its Use with IPSEC. R. Glenn, NIST, S. Kent, BBN Corp. November 1998.
2411	IP Security. Working Group R. Thayer, Sable Technology Corp., N. Doraswamy, Bay Networks, R. Glenn, NIST. November 1998.
2451	The ESP CBC-Mode Cipher Algorithms. R. Pereira, TimeStep Corporation, R. Adams, Cisco Systems. November 1998.
2453	RIP Version 2. G. Malkin, Bay Networks. November 1998.
2474	Definition: Differentiated Services Field (DS Field) in IPv4/IPv6 Headers. K. Nichols, S. Blake, F. Baker, D. Black. December, 1998.
2475	An Architecture for Differentiated Services. S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. Dec. 1998.
2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links. S. Casner, V. Jacobson. Cisco Systems. February 1999.
2516	The Method for Transmitting PPP over Ethernet (PPPoE). L. Mamakos, K. Lidl, J. Evarts, UNET Technologies Inc., D. Carrel, D. Simone, RedBack Networks Inc., R. Wheeler, RouterWare Incorporated. February 1999.
2519	A Framework for Inter-Domain Route Aggregation. E. Chen, Cisco, J. Stewart, Juniper. February 1999.
2597	Assured Forwarding PHB Group. J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. June, 1999.
2598	An Expedited Forwarding PHB. V. Jacobson, K. Nichols, K. Poduri. June, 1999.

2618	RADIUS Authentication Client MIB B. Aboba, G. Zorn, Microsoft. June, 1999.
2620	RADIUS Accounting Client MIB B. Aboba, G. Zorn, Microsoft. June 1999.
2684*	Multiprotocol Encapsulation over ATM Adaptation Layer 5. D. Grossman, Motorola, Inc., J. Heinanen, Telia. September 1999. *** RFC 2684 replaces RFC 1483**
2686	The Multi-Class Extension to Multi-Link PPP. C. Bormann, Universitaet Bremen TZI. September 1999.
2715	Interoperability Rules for Multicast Routing Protocols. D.Thaler, Microsoft. October 1999.
2833	RTP Payload for DTMF Digits, Telephone Tones and Telephony Signals. S. Petrack, Metatel. May, 2000.
2865	Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, Livingston, A. Rubens, Merit W. Simpson, Daydreamer. June, 2000.
2866	RADIUS Accounting. C. Rigney, Livingston. June, 2000.
2976	SIP INFO Method S. Donovan, dynamicsoft, October 2000
3261	Session Initiation Protocol (SIP)
3276	Definitions of Managed Objects for High Bit Rate DSL - 2nd Generation (HDSL2) and Single Pair High Speed Digital Subscriber Line (SHDSL) Lines Processing. B. Ray, PESA Switching Systems, R. Abbi, Alcatel. May 2002.
3376	Internet Group Management Protocol (IGMP), Version 3 B. Cain-Cereva Networks, S. Deering, I. Kouvelas-CISCO Systems, B. Fenner-AT&T Labs, A. Thyagarajan-Ericsson. October, 2002.
3515	SIP REFER Method R. Sparks, dynamicsoft, April 2003

18 Appendix

18.1 CR17642 & CR17643 Enhancements: Special Upgrade Information

Prior to Release 7.0R00A the 7300 Platform used the “Group Subaddress (Hunt Group)” parameter to replace the four digit Virtual Port Number with a usable 3 digit Port Subaddress for connecting voice calls. This 3 digit Port Subaddress could also be used for a Hunt Group application. In Release 7.0R00A the PBX Services functionality was enhanced to include the ISDN Voice Interfaces and to enable PBX Services by default. This change created a conflict between the operation of Hunt Groups and PBX Services (Call Transfer) on the 7300 Platform.

Beginning in Release 7.2R00A, for the 7300 Platform only, a parameter has been introduced into the Virtual Voice Port Record. The new parameter is called “Port Subaddress”. This “Port Subaddress” parameter can now be used in place of the “Group Subaddress (Hunt Group)” parameter for connecting voice calls on the 7300 Platform. This restores the ability to use Hunt Groups and PBX Services together on the 7300 Platform.

The upgrade from any prior release to release 7.2R00A is handled in the following manner. The populated “Group Subaddress (Hunt Group)” field will be brought forward. The new “Port Subaddress” field will be left blank. This will insure backward compatibility without requiring reconfiguration for Hunt Group or Individual Group Subaddress functionality.

For customers that are not running with Hunt Group functionality and are using PBX Services (Call Hold/Transfer) or are installing a 7300 for the first time, it will now be required to utilize the new “Port Subaddress” parameter. This parameter will be used to represent the 3 digit port subaddress required for connecting voice calls on the 7300 Platform only. Like all subaddress values care must be taken not to create address conflicts by creating duplicate addresses.

IMPORTANT:
For PBX Services (Call Hold/Transfer) to function properly on the 7300 Platform, in Release 7.2R00A or later, it is required to configure the “Port Subaddress” parameter.

The following change will be made to the Vanguard Applications Ware Multimedia Feature Protocols Vanguard Voice Manual.

Port Subaddress (73xx Platform Only)

Range:	0-3 digits
Default:	Blank
Description	Specifies a Port Subaddress to uniquely identify this port. This parameter must be configured in order to use PBX services on the port. The Port Subaddress must not conflict with any other Port Subaddress or Group Subaddress configured in the node. * Note: For PBX Services (Call Hold/Transfer) to function properly on the 7300 Platform, in Release 7.2R00A or later, it is required to configure the “Port Subaddress” parameter. Also, to use the Group Subaddress for it’s intended purpose (Hunt Group).

19 Product Declarations and Regulatory Information

The following sections provide information about standards compliance, safety statements, and Type Approvals.

19.1 Warnings and Cautions

The following special notices apply to all equipment handling procedures in this installation guide.

Warning

Ports capable of connecting to ports on other apparatus are defined as Safety Extra Low Voltage (SELV). To conform with EN60950, ensure that these ports are only connected to ports of the same type on other apparatus.

Les ports qui sont susceptibles d'être connectés à des équipements sont désignés comme TBTS. Pour garantir la conformité à la norme EN 60950, n'interconnecte ces ports qu'avec des ports du même type sur des autres matériels.

Anschlusse, die mit anderen Geraten verbindet werden konnen, sind als SELV beschrieben. Um Konformitat mit EN 60950 zu versichern, sichern Sie es, daß diese Anschlusse nur mit den des selben Type auf anderen Geraten verbindet werden.

19.2 CE Marking

The mark in the following diagram appears on each Vanguard Series product, and the statement that follows explains its significance.

CE

This product is CE marked to indicate compliance with the following European Directives:

- 1999/5/EC Radio & Telecom Terminal Equipment (R&TTE)
- 73/23/EEC Low Voltage Directive (Safety)
- 89/336/EEC EMC Directive

19.3 Declarations of Conformity

English

Declaration of Conformity:
Hereby, Vanguard Networks declares that this Vanguard Router is in compliance with the requirement and other relevant provisions of Directive 1999/5/EC.

Danish

Konformitetserklærin g:
Hermed erklærer Vanguard Networks, at indestående Vanguard Router er i overensstemmelse med de grundlæggende krav og de relevante punkter i direktiv 1999/5/EF.

Dutch

Verklaring van overeenstemming:
Hierbij verklaart Vanguard Networks dat diens Vanguard Router voldoet aan de basisvereisten en andere relevante voorwaarden van EG-richtlijn 1999/5/EG.

Finnish

Vaatimustenmukaisuusvakuutus:
Vanguard Networks vakuuttaa täten, että Vanguard Router on direktiivin 1999/5/EC keskeisten vaatimusten ja sen muiden tätä koskevien säännösten mukainen

French

Déclaration de conformité :
Par la présente, Vanguard Networks déclare que ce routeur Vanguard est conforme aux conditions essentielles et à toute autre modalité pertinente de la Directive 1999/5/CE.

German

Konformitätserklärung:
Hiermit erklärt Vanguard Networks dass der Vanguard Router die grundlegenden Anforderungen und sonstige maßgebliche Bestimmungen der Richtlinie 1999/5/EG erfüllt.

Greek

Δήλωση Συμμόρφωσης :
Δια του παρόντος, η εταιρεία Vanguard Networks δηλώνει ότι η παρούσα συσκευή (δρομολογητής) Vanguard Router πληροί τις βασικές απαιτήσεις και άλλες βασικές προϋποθέσεις της Οδηγίας 1999/5/ΕK.

Italian

Dichiarazione di conformità:
Con la presente Vanguard Networks dichiara che il router Vanguard soddisfa i requisiti essenziali e le altre disposizioni pertinenti della direttiva 1999/5/CE.

Portuguese

Declaração de Conformidade:
Através da presente, a Vanguard Networks declara que este encaminhador Vanguard se encontra em conformidade com os requisitos essenciais e outras disposições relevantes da Directiva 1999/5/CE.

Spanish

Declaración de conformidad :
Por la presente declaración, Vanguard Networks declara que este encaminador Vanguard cumple los requisitos esenciales y otras cláusulas importantes de la directiva 1999/5/CE.

Swedish

Överensstämmelseförklaring:
Vanguard Networks förklarar härmed att denna Vanguardrouter överensstämmer med de väsentliga kraven och övriga relevanta stadganden i direktiv 1999/5/EG.