DiviTrackIP™ 2.0
Application Note

NMX 5.0 Release

Revision 5.0.0.00
May, 2009

Harmonic Inc. Proprietary and Confidential
The targeted timeframes, products, features and/or functionality described herein are estimates only, shall not be relied on, may be changed at any time at Harmonic's sole discretion, and shall not be interpreted as an obligation or deliverable for current or future orders, and shall not be incorporated into any contract. Obligations and deliverables are defined on an independent basis pursuant to the individual contract terms and will default to current performance capabilities. Nothing herein shall create or impose any obligation on the part of Harmonic.

Revision	Date	Authors	Comments/changes
1.0	3/5/05	J. Koehler	Original version
1.1	3/23/05	J. Koehler	Incorporation of changes provided by Bill Kaiser and comments from Rebecca Barnes.
1.2	4/12/05	J. Koehler	Changed to official name DiviTrackIP and added recommendations for VLAN/subnet configurations
1.3	4/15/05	J. Koehler	Updated with changes provided by Pat Waddell
1.4	2005/08/23	B. Kaiser	Added IGMP appendix
1..5	9/19/05	J. Koehler	Reworded section 5.1 regarding prevention of network flooding. Added comments regarding auto-negotiation settings in section 5.2. Added comments in section 7 to clarify the use of IGMP-capable switches.
1.6	10/4/05	P. Waddell	Moved IGMP into main body. Minor fixes and clarifications throughout.
1.7	7/6/06	H. Lane	Updated document to reflect DT/IP changes, including a new section about products that support DiviTrackIP. Edited content.
1.8	March 2007	J. Koehler	Updates for the NMX 4.5 system release
1.9	2007/10/31	Bk	Revised for NMX 4.7, added Appendix A,B,C,D,E
4.8.1.006	2008/02/22	Bk	Incorporated review comments, revision agrees with NMX
4.8.2.00	20080404	Bk	Min. pool OH, redundancy, must be same mux for MC enc.
4.8.2.002	20080408	Bk	Review corrections, clarified multiple ProStar ports for redundant DT messages.
4.9.2	20081103	Bk	Clarify IP switch requirements. Removed §6.4.
5.0.0	20090501	Bk	Revised for 2.0 new features

Table of Contents

1 Preface

This document is intended for new deployments and people not familiar with DiviTrackIP™. If you are upgrading an older system already running DiviTrackIP, there is a separate document (DiviTrackIP 2.0 Upgrade Guide) that will help you with understanding the upgrade process and assisting your transition from the previous software version.

This release of DiviTrackIP 2.0 has the following enhancements:

- Longer network delay can be tolerated (150 ms each way max, up to 10 ms jitter)
- Increased number of encoders per pool (had been 24, now tested with 64)
- Improved video quality possible with larger pool size and reduced statistics delay
- Fast response to network route changes, adaptive protocol with intelligent history
- Better resilience to network packet loss on DiviTrack control channel
- Reduced PCR slew rate for lower transport stream timing deviations
- Better visibility into subsystem status to ease debugging and failure analysis
- Overflow protection possible in future. One misbehaving encoder will not affect other pool channels

This application note does not detail the internal implementation of DiviTrackIP2.0; instead, it intends to provide a simplified overview of the message exchanges between the components so you can install a system or diagnose problems with an already-installed system.

2 Introduction to DiviTrackIP

2.1 What is DiviTrackIP?

DiviTrackIP is Harmonic's statistical multiplexing system that uses IP transport for exchanging information between encoders and multiplexers. This configuration supports distributed network equipment – the encoders can be in many different locations and the multiplexers in yet another.

DiviTrackIP allows for encoders and the multiplexer participating in a statistical multiplexing pool to be in the same rack or geographically distributed, in the next room or in another city. The overall bitrate of a pool is a constant, and the encoders in that pool will share the available bits dynamically, depending on the video motion, scene changes, etc. As in prior versions of DiviTrack™, the system uses encoder-multiplexer messaging to statistically combine encoder channels. The primary difference is in the IP connectivity between the encoders and DiviTrack Controller (Multiplexer). Figure 1 shows an example of a DBS application of the system.

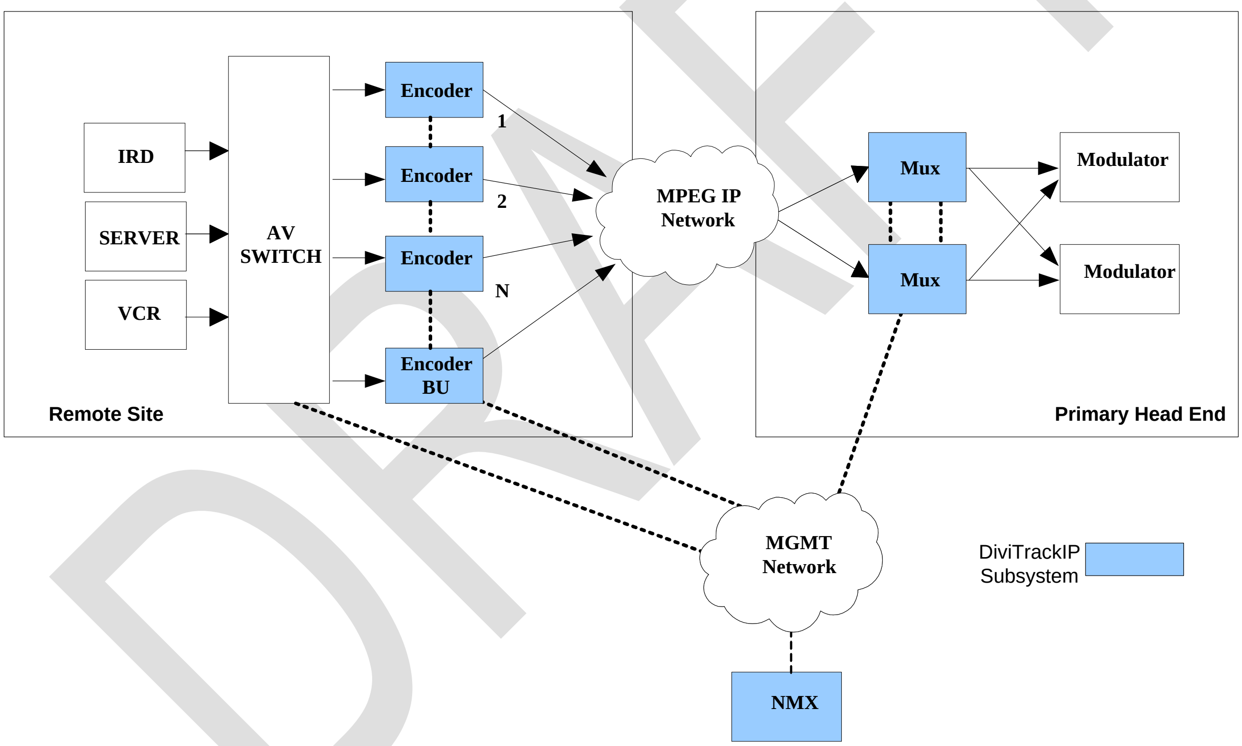


Figure 1. Example of a Typical DiviTrackIP System Configuration in a Distributed Architecture

Encoders are arranged in a N+1 (or N+M) redundancy configuration at one or more remote sites, and the primary/backup multiplexers are arranged in a 1+1 redundancy configuration at the primary head end. Each encoder at the remote site participates in the same DiviTrackIP pool controlled by the multiplexer in the primary head-end. Remote encoder sites can be added until the maximum video circuit count (per pool) of 64 is reached. Multiple pools can expand the video circuit count to any number beyond 64 as needed, subject to the maximum encoder and pool limits per-DiviTrack controller.

The ProStream 1000 DiviTrackIP controller can support up to 8 pools, with a maximum of 2 pools per transport, subject to an overall IP socket limitation of 128 input sockets total.

Some of the advantages of the DiviTrackIP system include:

- Ability to geographically distribute encoders and multiplexers, permitting contribution sites to be remote from uplink sites.
- Any-to-any mapping of encoders and multiplexers, by which any service can be flexibly added or removed from any statmux pool. This provides ease of transport grooming to optimize bandwidth utilization.
- More powerful device-initiated redundancy operations, which can be used to limit the downtime of redundancy operations and improve failover times.
- Simplified cabling configuration and connectivity.

Note: Regarding the MPEG IP Network cloud in Figure 1, NMX does not monitor or control any IP network devices such as IP switches, routers, or protocol adapters. However, NMX does provide the customer with network packet-related alarms detected by the devices. Examples of some DiviTrackIP network configurations are provided later in this application note.

3 DiviTrackIP and the IP Network

Encoders/muxes report their status to NMX, and NMX sets up (provisions) the encoders and muxes via a unicast management IP network that is separate from the audio/video IP traffic. This unicast network can run at a lower bitrate compared to the video network. WAN configurations may take advantage of this to reduce line charges.

The video/audio traffic is carried over a multicast-capable IP network. Multicast is required because of the redundancy architecture and the need to broadcast rate control messages to many encoders simultaneously. The multicast traffic is bidirectional. See the Appendix for expected bitrates required for each direction.

3.1 Data and Messaging Required for General Device Control

The network management system uses SNMP, UDP, TFTP, HTTP, and bootp for code loading, provisioning, alarm reporting, and status checks of the remote devices. This traffic is separate from the encoder-multiplexer MPEG/IP connection and can be provisioned with reduced priority and lower bandwidth than the video traffic.

3.2 Data and Messaging Required for DiviTrackIP

IP Multicast technology allows the DiviTrackIP system to provide the same redundancy protection against single points of failure as in the ASI DiviTrackXE system. Several types of message traffic must flow correctly between the encoders and the multiplexer for the DiviTrackIP system to function properly:

1. The MPEG content stream containing the encoded service, sent from encoders to multiplexer.
2. The video complexity statistics being sent from the encoder to the multiplexer
3. The rate allocation messages sent from the multiplexer to the encoders. This message specifies each individual encoder’s output bitrate.
4. Mux clock timing reference. The encoders sync their timebases to the DiviTrack controller using timing information sent from the multiplexer contained in this message. This is also referred to as the STC (System Time Clock) pool, or the pilot pool.
5. The FEC packets (if this feature is selected) sent from the encoder to the multiplexer
6. Out-of-band messaging for monitoring network characteristics. These may include unicast ranging packets, multicast ranging packets, and heartbeat messages. (future capability)

MPEG video/audio packets are encapsulated in HRTP/UDP (Harmonic extensions to RTP/UDP) that are *multicast* by each encoder to the multiplexer. *Unicast is not an option*. HRTP is a proprietary extension to standard RTP with the addition of individual timestamps for each MPEG packet, located in the message header. These are used by the “pool” devices to stay in sync.

Video complexity data from encoders to multiplexers are encapsulated in the same MPEG/IP multicast address as the video traffic. Depending on the FEC mode, complexity (sent as MPEG PID 0x000F) may be on the same UDP socket or a different socket as the video MPEG traffic. More specifics about this will be covered in the FEC section.

Video rate allocation messages from the multiplexer are multicast to the encoders via HRTP (for the legacy-format protocol) and simultaneously via UDP (for the new-format 2.0 protocol).

3.3 Upstream and Downstream Network Delays and Jitter

Make sure your network has less than one hundred fifty milliseconds of peak delay and also ten milliseconds maximum of jitter. The DiviTrackIP algorithm will not work with larger values.

3.4 Forward Error Correction (FEC) in DiviTrackIP Applications

Your network packet drop and packet reordering characteristics should be very low or else FEC should be employed. Local-area networks typically do not use FEC, whereas wide-area networks typically do.

3.4.1 When to use FEC

Dropped or reordered IP packets translate directly into lost MPEG traffic. Using FEC can improve uptime. Service loss due to packet drop and packet reordering can be nearly eliminated for packet drop rates up to 2% and good performance has been measured for drop rates as high as 5%.

3.4.2 SMPTE 2022 FEC

SMPTE 2022 FEC protects data integrity with parity packets that are calculated from the payload IP packets. In case an IP packet has been lost, the parity of the protection packet together with the other IP packets that were not lost are used to reconstruct the lost packet.

Correction packets are added to the regular video/audio MPEG packet stream. The FEC packets are sent on a different UDP socket from the MPEG data. This lets you receive the MPEG IP stream on a simple monitoring device, like a laptop running VNC, even if it doesn't support FEC decode, by listening to the data socket only.

The MPEG payload packets are transmitted on UDP socket "n" (n is any user configurable value from 2 to 65530, must be an even value), the column FEC packets are transmitted on socket n+2 and the row FEC packets are transmitted on socket n+4. ***In this release, no row protection packets are sent. In this release, only column protection packets are transmitted for the traffic from the encoders to the mux.***

Note that the complexity and rate message packets are not protected by FEC, and in rare cases a rate allocation or complexity packet may get dropped. Redundancy in the messaging protects against this loss.

3.4.3 DiviTrackIP and FEC Setup

Before you set up the NMX map, decide if you want FEC used in the system. Making a change from non-FEC operation to operation with FEC requires that the service flow be deactivated before the (extensive) map changes are made and then reactivated after the editing has been finished. This can be lengthy.

DiviTrackIP requires that either all services in a pool use FEC or none of the services in the pool uses FEC. Even though NMX allows setting FEC on or off individually for each service, you must make sure all services are set the same way when setting up DiviTrackIP. If you plan to use the NMX Any-to-Any feature (any service to any mux; services are allowed to move between transports), make sure you use the same FEC mode for all services.

Some operational limitations and considerations apply:

1. When FEC mode is enabled in the system, all DT/IP services will be delayed by up to 2.1 seconds to absorb worst case FEC encode-decode. .
2. DT/IP services include all VBR services as well as any CBR services that have the potential to be included in a DT/IP pool.
3. All services in a pool must use FEC (LAN and WAN) or else none of the services in a pool uses FEC. This is required to insure that redundancy works correctly.

With ALL new DiviTrackIP 2.0 pools, (excluding legacy unconverted MV-encoder pools), the video/audio IP traffic flows on a separate socket than the video complexity/rate data. This is termed “3-socket” mode. With this configuration, packets carrying complexity and rate data bypass the delay of the interleaver and parity corrector. Note that these rate and complexity packets are only protected against loss by means of duplicate transmission from the backup mux and history data for previous intervals in each message PDU.

The advantage of having the complexity and rate allocation data on a non-FEC (i.e., non-delayed) socket is that encoders can see farther ahead into the upcoming future video to request more bits for difficult sequences, while still running on a network having substantial delay. Otherwise, network latency would decrease the prediction buffer length, resulting in reduced video quality.

Key parameters for setting up DT/IP pools with FEC:

1. Setting the NMX Cross-Connect icon DiviTrack mode to “3 Socket With FEC”
2. FEC “L” value indicating the number of columns (**L**ength) in the FEC matrix
3. FEC “D” value indication the number of rows (**D**epth) in the FEC matrix
4. Minimum TS rate which limits the minimum bit rate for each encoder’s IP transport in the DT/IP pool (null stuffing is added at the encoder output to maintain the minimum TS rate)
5. In the NMX service configuration properties, the “Intermediate TS FEC enabled” check box is on.

Note: In NMX, when you assign specific multicasts to services, instead of letting NMX choose the multicasts, the “Intermediate TS FEC enabled” property of the service configuration needs to be set. This field is only configurable when no addresses have been specified for services, pools, or STC pools. Set this at the beginning of NMX configurations, otherwise there will be a lot of editing work to clear out the addresses before the GUI will allow changing the state of this property.

3.4.4 Calculating Network Bandwidth for FEC

Note that FEC imposes a bandwidth penalty in terms of an additional overhead bit rate to support

Choosing limited LxD (length by depth correction matrix) values may increase bandwidth up to 50% of maximum. For best protection against burst errors, use the largest number of columns possible. For least overhead, use the smallest number of columns possible. You can balance the protection against the bandwidth cost depending on your network error rate and carrier charges. The least overhead is the LxD setting of (5, 20) with 5% extra packets. Most customers use this setting.

Refer to the appendix for more details about calculating overhead for FEC and WAN links.

3.4.5 System Delay and FEC

Since the data block of LxD packets has to be checked as a group for errors, the data from the error checker for this block of packets is delayed until the entire block and correction packets has been received. This causes an extra lag between the source video and the DiviTrack controller output. In most cases this is not important. However, if the FEC delay is an issue for the system being deployed there are several ways to control the maximum delay introduced by FEC. They include:

1. Limit the FEC LxD to less than the maximum value (this increases the WAN bandwidth overhead). If the interleaver matrix is smaller, it fills faster, and can therefore start sending the corrected block of packets sooner.
2. Use a higher minimum transport rate on the service (null packet filling). This also increases the WAN link bandwidth.
3. Reduce the number of MPEG packets encapsulated per IP datagram.

Null-packet filling adds extra network bandwidth required to carry the services from the remote site to the central head end. Even with static video running at the encoder's minimum video bitrate, the encoder output will be sending a larger value of the minimum transport rate. This puts a floor on the minimum WAN bandwidth. Since the WAN has to carry the maximum bitrate of each service, the network needs to be provisioned for either the sum of each encoder's maximum bitrate, or the overall pool bitrate, whichever is less.

3.4.6 NMX FEC Settings

Choose your protection level of FEC in the IP Cross Connect properties page under "General Properties", "DiviTrack Mode".

The FEC mode is selected in the IP Cross Connect switch by right-clicking the Properties page for "DiviTrack Mode" and selecting either "Normal" or "FEC". Within the IP Cross Connect (double-click this to open it) icon, the level of FEC protection is set in the IP Network tab, where the FEC length by depth values (LxD) are selected for each connected encoder

3.5 Prerequisites for a Network to Support DiviTrackIP

To set up a DiviTrackIP network, you need the following basics:

- TCP/IP connectivity for NMX and all elements in the DiviTrackIP system for setup and provisioning messages. These messages are carried on the customer's management network separate from the program services (MPEG traffic) network.
- Network switches and routers that are capable of multicast operation. Layer 2 switches are required as a minimum but Layer 3 switches are preferred.
- There must be enough 1000-baseT ports to connect the multiplexers (ProStream 1000, as these do not support 10/100 Mbit/s speeds.
- UDP/IP multicast network connectivity for transport of MPEG content and DiviTrack messaging required from the encoder to the multiplexer
- UDP/IP multicast network connectivity for transport of the DiviTrackIP messaging required from the multiplexer to the encoders. These are the bit rate allocation messages transported via HRTP/UDP over the customer's program content network
- IGMP version 2 support is also recommended, and IGMP snooping is desirable. IGMP version 3 is desirable. The encoders and muxes can use IGMPv2 or v3 messages to receive only the traffic in which they're interested. If IGMP support is not available, the IP switch will flood multicast traffic to every port -- this can cause port overflow, especially with 100-baseT ports. Otherwise, you can use VLANs to separate each pool's traffic.

- The maximum network delay must be less than 150 ms and the network jitter must not exceed 10 ms (each way). This is the design limit. You will lose data if you attempt operation on networks with values beyond the limit.

- Values of packet drop rates and packet drop profiles. Choose whether to use FEC before the system is put on-air.

- Plan for networking address allocation. Before you start to deploy DiviTrackIP, consult with your network operation group to choose multicast addresses and port ranges. It's easier to monitor a system where each service has a unique IP multicast address, rather than varying the UDP port number (with a constant address) to distinguish the services.

- VPN/Firewall/Encryption. If any portion of the network is exposed to the public Internet (this is not common) you need to protect your equipment and traffic from external threats. Many program providers require video links to be protected against third-party interception.

3.6 Configuring the NMX Network Connections

3.6.1 The NMX IP Cross-Connect

Encoder to multiplexer (multiplexer) connections in NMX must always be over an IP Cross Connect as shown in the figures within this section.

Encoders and the multiplexer communicate only through multicast messages. No unicast addresses are used. This makes the most efficient use of network bandwidth, as multiplexers may be operated as a redundant pair, both of which receive the same "downstream" messages.

One multicast address and two ports per pool are required for each pair of redundant muxes, plus one additional address/port for the STC (system time clock; timing reference) pool, again, per mux pair. To repeat, pool addresses are the same for the primary and the backup multiplexer. It is better to use multiple multicast IP addresses rather than multiple sockets to distinguish between the pools for ease of debugging, although it is permissible to simply change the port number.

Only one of the two ports (per pool) you need is used today, in the mux-to-encoder direction of traffic. Start this port allocation with an even-numbered value. Future control messages may be added to the protocol on the odd-numbered, reserved port.

If the "Normal" DiviTrackIP mode had been selected on the cross connect (for older-protocol DiviTrackIP), each encoder service would only use two ports for traffic from the encoder to the mux. With the new protocol for DiviTrackIP 2.0, this selection is not allowed; there are always three IP sockets used, and the required selection for the cross-connect must have "3 Socket" mode, with or without FEC.

You need to allocate a minimum of six ports per service on the cross-connect from the encoder to the mux. These port addresses must start on an even number.

Note: the multicast addresses and ports can be either specified explicitly for each MPEG service or auto-generated by NMX based on the address ranges you entered on the IP cross connect device. Many customers want to lock the multicasts to the services; this is recommended to make debugging and monitoring easier. You must define a sufficiently large address range on the Cross-Connect to include all the multicast addresses used by the MPEG services. See the NMX help for details

3.6.2 DiviTrackIP Complexity Messages

Two destination multicast address/port numbers are used for sending the video/audio and DiviTrackIP complexity messages from the encoder to the multiplexer. The video flows on the first port, *N*, and the complexity flows on port *N+1*. Use only even port numbers to set the NMX; this avoids port conflicts.

NMX configures each encoder with a multicast address/port number (all stream data and DiviTrackIP messages from the encoder will have this as the Destination Address). The multiplexer will be listening on this multicast address/port number to receive stream data and DiviTrackIP messages from this particular encoder.

3.6.3 DiviTrackIP Rate Allocation Messages

Two destination multicast address/port number pairs are configured on the multiplexer (per pool) for sending DiviTrackIP rate allocation messages between the multiplexer and all the encoders in that pool; one port – the base-numbered port -- is used for legacy-format DiviTrackIP messages, and the port value one higher is used for new DiviTrackIP 2.0 rate messages. Both messages are sent simultaneously; you need to know this for planning channel bandwidth. You cannot turn off the unused protocol port.

The upstream DiviTrackIP rate allocation messages from the multiplexer are sent to a common multicast address/port combination. NMX configures both of these addresses on the multiplexer for transmitting rates and configures on each encoder one of these addresses (depending if the encoder is running new or old protocol) for receiving its rates. The backup multiplexer, if present, also listens on this multicast address to synchronize its DiviTrack clock to the primary's DiviTrack timing source. This prevents a clock frequency and phase jump when switching to the backup mux.

Another multicast address/port number for the STC pool (with pool ID 999) will be defined if any pools are provisioned on the mux. This address/port will be the same for the primary and the backup multiplexer.

Each pool needs two rate message address/ports, so if there are multiple pools, be sure you plan for this extra network traffic, in addition to the STC (pilot) address/port. Make sure there are enough ports allocated in the NMX cross-connect icon, and make sure that you don't have a port conflict because of the two-ports-per-pool requirement for both old and new rate message traffic.

3.6.4 Typical Network Configurations

A few typical network configurations are:

- IP output from multiple encoders (via IP ports) in an N+1 configuration and IP input to a single multiplexer.
- IP output from multiple encoders (via IP ports) and IP input to two multiplexers in a hot-hot configuration (1+1 multiplexer redundancy).
- IP output from multiple encoders (via IP ports) in an N+M configuration and IP input to two multiplexers in a hot-hot configuration.
- IP output from multiple encoders (via IP ports) and IP input to two multiplexers in different multiplexing groups.

The following figure shows an example of the second configuration.

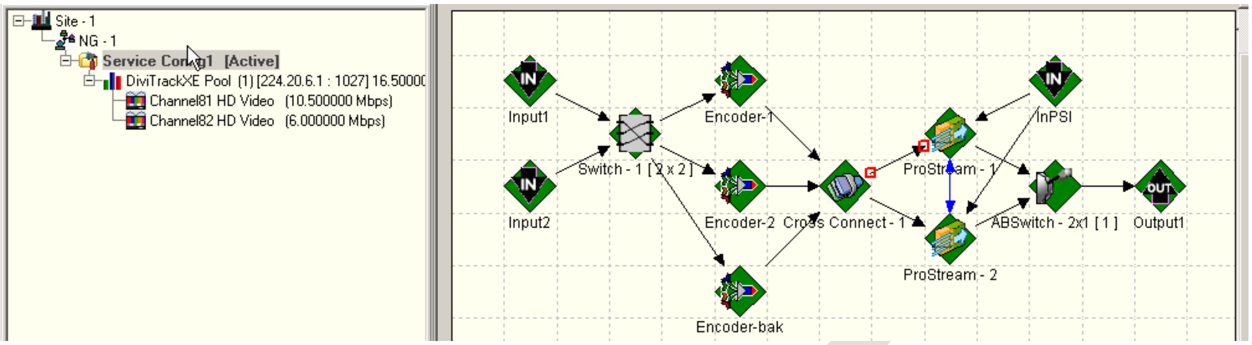


Figure 2. Example of a Typical Map Configuration

If you are familiar with the NMX GUI for setting up DiviTrackXE, the following are updates from previous, non-DiviTrackIP versions of NMX:

- A new dialog box with multiple tabs on the IP cross connect device configures the transport stream data, DiviTrackIP data multicast address/port ranges, and IP network parameters, such as MTU, TTL, source UDP port number, and the number of transport stream packets in an IP packet.
- An enhanced stream list dialog box showing the configured multicast address/ports on the intermediate MPEG streams.
- An enhanced statistical multiplexing tab in the service view showing the configured multicast address/ports on the pool objects.
- A multiplexer properties page enhanced to show the STC pool multicast address and port that has been configured by NMX.

4 Preparing to Set Up DiviTrackIP

4.1 Pre-deployment Preparations

Prepare for configuring DiviTrack IP by doing the following:

1. Verify that your network supports a multicast IP environment for both local and remote encoding facilities.

2. Coordinate IP network addressing ranges within your production network. You need to plan for a block of IP addresses for the management ports of the encoding equipment, a block of addresses for the primary MPEG output ports on the encoders, and a block of addresses for the backup MPEG output ports of the encoders and multiplexers.

3. Reserve a sufficient number of IP switch physical ports for the MPEG primary ports of the encoders and multiplexers, and, when port redundancy is used, additional physical switch ports for the encoder backup MPEG-IP outputs. Assign these to VLANs if desired.

4. Determine the MPEG traffic multicast addresses that will be set on each video/audio service. You need to reserve one multicast address and port combination (MC) for each channel. For example, Channel 1 might be assigned the MC of 225.1.1.1 and 50001. Channel 2 could be set to 225.1.1.2:50001, or you could pick 225.1.1.1:50002. Your network may be better suited to one style or the other. See your networking expert for guidance.

5. Determine the STC Pool and DiviTrackIP Pool control multicast addresses for each pool. You need one MC (and two ports) for each pool in your system plus one extra MC/port per DiviTrackIP primary controller. The backup DiviTrackIP controller uses the same MC addresses as the primary and does not need separate MCs. For example, you have three DiviTrackIP pools on a single DiviTrackIP controller. You need four MC addresses: one for the controller and one for each of three pools. If you have five DiviTrack controllers, each with one pool, ten MC addresses for control will be required: one for each pool plus one for each controller; times five totals ten. Redundant DT/IP controllers do not add to the control MC count.

6. If you are not using IGMPv3, determine the HHP multicast addresses that will be set on each encoder or mux. Every device using HHP needs a MC allocation, including DiviTrackIP backup controllers. Do not turn HHP on if you use IGMPv3. Most customers prefer to use the newer IGMPv3 for protection against multiple senders. HHP is an older, legacy method.

7. Determine the need for WAN adapters, firewalls, or other auxiliary networking equipment.

8. Make a network diagram to document your selections and speed up the data entry into NMX.

4.2 Choosing Multicast Addresses for DiviTrackIP Operations

The addresses you choose in the configuration must be unique in the network. You cannot reuse a multicast address/port combination in the MPEG data network and the HHP network.

To allocate the required addresses:

1. Verify the HHP multicast address for the encoders, if HHP is used. Specify a unique multicast HHP address for each encoder (and multiplexer). *HHP is not compatible with IGMPv3* in this release.

2. Verify the destination multicast address/port number for each MPEG program. Each output service from an encoder is carried over a unique multicast address/port combination. The downstream (encoder-to-multiplexer) DiviTrackIP messages are carried in band on the same multicast address/port combination (MC).

3. Verify the destination multicast address/port number for exchanging DiviTrack rate allocation messages between the multiplexer and all the encoders. The upstream DiviTrack rate allocation messages from the multiplexer to all the encoders are sent to a common MC.

4. Verify the STC pool multicast address/port number for HRTP based communication between the encoder and the multiplexer.

4.3 Address and Rate Configurations

Multicast address port ranges must be reserved on the IP cross connect switch.

1. The GUI allows for multiple ranges of multicast addresses to be entered on the cross connect device. Ranges for transport stream data and DiviTrack messages are specified.

2. You need to reserve one multicast address/port combination for each service.

3. NMX defines one multicast address/socket port per statistical multiplexer pool. This multicast address/socket port is the same for the primary and the backup multiplexer.

4. One multicast address/port for the STC pool should also be defined. This is the same for the primary and the backup multiplexer.

5. You must retain some free bandwidth available in the output transport beyond the allocated pool bitrate. Harmonic recommends allowing at least 200 kbit/s of free space in the output transport. For example, in a 38.8 Mbit/s transport, allocate only 38.6 Mbit/s of committed traffic, leaving 0.2 Mbit/s free.

4.4 Video Circuit Configurations

Set the customer desired minimum and maximum VBR rates for the video circuit in the Edit Configuration page. For DiviTrackIP operations, the minimum allowable video circuit bit rate is 0.3 Mbit/s and the maximum allowable bit rate is 24 Mbit/s for HD-AVC, and 8 Mbit/s for SD-AVC.

There is a second minimum to consider that applies to the overall transport rate from the encoder. Where FEC is used, the transport rate (including audio and null packets) must be higher than 2 Mbit/s. The video minimum is allowed to be smaller – say 0.3 Mbit/s – but you must reserve bandwidth on the WAN link from the encoder to allow sending at least 2 Mbit/s at all times from every remote encoder.

This means you have to calculate multiple possible scenarios to put a bound on the bandwidth used by the remote site. It may be possible that the overall pool bandwidth you choose is smaller than sum of all the encoder minimum transport rates at 2 Mbit/s. If you have a mix of LAN and WAN encoders, it may be possible that all the WAN encoders may need max bitrate while the LAN encoders are at minimums. Look at the worst-case combination and provision the WAN link accordingly.

4.5 Connecting to the “IP Cloud”

The connection of the encoders and multiplexer through an IP network requires an aggregation (“edge”) Layer 2 switch for the encoder IP outputs to gain access to the IP cloud to which the multiplexer is also connected. Depending on the number of encoders in the DiviTrackIP system, you will need one or more encoder aggregation switches.

These encoder aggregation switches will be connected into the core network via a core access switch. You must connect the multiplexer to the core network via a core network switch or router. Note that when using the ProStream 1000 you can connect both GbE ports to the network. This connectivity allows a duplicate rate message stream to be sent from the ProStream 1000 to the encoders (except when using MV-series encoders) and provides a level of robustness to poor network conditions where packet drops are an issue. The cost of this is the increased WAN bandwidth of the second rate control streams from the backup ProStream GbE port. This is about 66 packets per seconds extra.

For the development and testing of the DiviTrackIP feature, Cisco switches were used in all cases. The models employed were Cisco 2950, 3550, 3560, and 3750. Other Cisco switches and switches from other vendors may be used provided their interfaces and operations support at least Layer 2 switching and IGMPv2 support. NMX does not support the management or monitoring of these switches. You must configure the switches and routing equipment separately from the encoders and services.

There a few important considerations for the switches employed for DiviTrackIP. First, they must support at least 100-BaseT connections for the encoders. Second, to connect to the multiplexers, they must have either 1000-BaseT links for copper connections, or 1000-BaseSX links for fiber-optic connections. All connections must be full duplex. For details on the configuration of Harmonic devices with Ethernet connectivity to IP network, see the Harmonic application note “Network Connections of Harmonic Devices with Ethernet Interfaces.”
Using a backup DiviTrackIP controller for multiplexer redundancy requires a multicast-capable network path between the MPEG GbE ports of the primary and backup DiviTrackIP controllers. HHP redundancy for the encoders requires that a network path exists between the primary and backup encoders.

4.6 Switch Example Information

Encoder aggregation switch (typical)

- Cisco Catalyst 2950
- Layer 2 Switch
- 24 10/100 Base-T ports
- 2 GBIC ports
- Internet Group Management Protocol (IGMP) “snooping” support
- Able to auto-negotiate speed and duplex operation on 10/100 Ethernet ports, or can be set to fixed value manually (see the section on auto-negotiation).

Core edge access switch

- Cisco Catalyst 3550 Layer 3 Switch
- 2 10/100/1000 Base-T ports
- 10 GBIC slots for Fiber/copper GbE links
- Hot Standby Routing Protocol (HSRP) and Internet Group Management Protocol (IGMP) support
- Able to auto-negotiate speed and duplex operation on 10/100/1000-BaseT Ethernet ports or can be set manually (see the discussion in Section 6 on auto-negotiation).

The encoder aggregation switches must be configured in a 1+1 configuration to support redundancy.

Harmonic recommends that for both the multiplexers and the encoders, each of their dual IP ports be always placed on physically separate subnets to ensure the highest possible system availability in the event of switch failures in the “IP Cloud.” This type of network configuration was used in all development and QA testing of DiviTrackIP. Not all customers may be able to deploy in this manner based on cost or restrictions on their networks.

The following figure shows one example of DiviTrackIP devices connected over the IP cloud using Cisco IP switches and routers. While the encoder aggregation switches (labeled as “access switches”) do not show a redundancy tie, this is required. See the appendix for an example of an IP addressing and connection scheme.

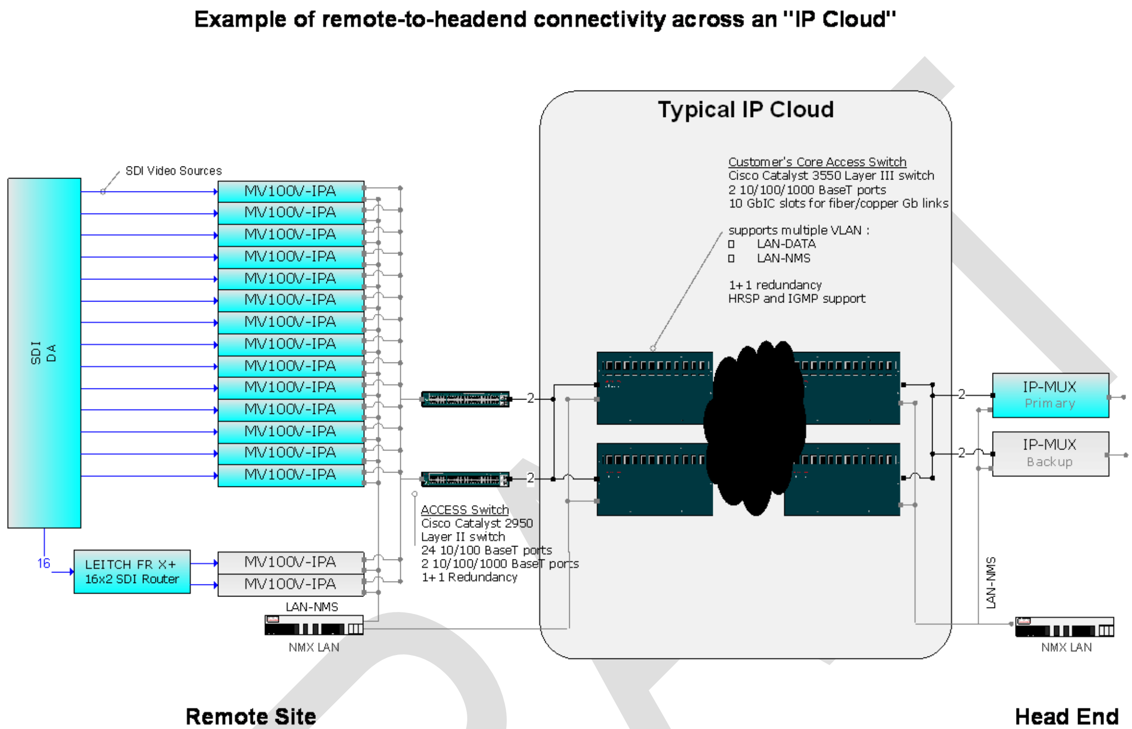


Figure 3. Example of a Remote Site Connection through an IP Cloud

5 Setting Up DiviTrackIP on NMX

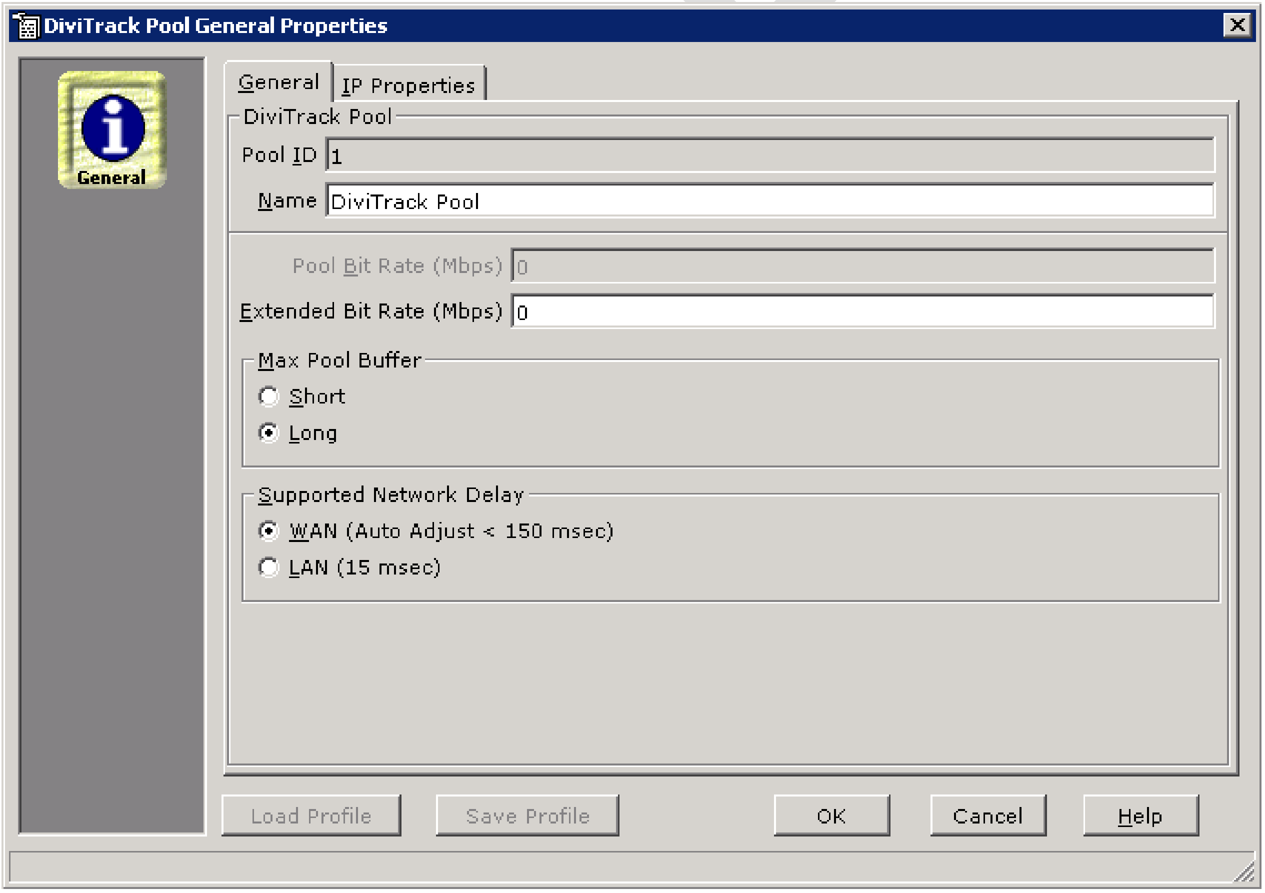
5.1 Creating a Map

Place all of the required encoders, multiplexers, and switches on your map and make the appropriate connections to the devices. If you need help with this, see the online help provided with NMX. Before working with any IP connectivity and addressing setups, be sure to review the address configuration information given in the previous sections and verify that it is consistent with the your network addressing scheme.

The remainder of these sections focus on the IP network connectivity and device settings required for setting up a DiviTrackIP service configuration on an NMX map.

5.2 New NMX Pool Properties

In the Edit Service Configuration window, after you create a pool, there are two new properties you will set. These are the Pool Buffer and Network Delay selections. See the screenshot below.



The Max Pool Buffer controls the encoder VBV delay. You can trade off between higher video quality (long) against faster channel change time (short).

If your MPEG IP network is entirely local – no offsite encoders – select the LAN delay value. This provides faster settling times for startup since the network jitter and delay is bounded. When you use remote encoders, the WAN setting is required, which allows dynamic changes to the network delay.

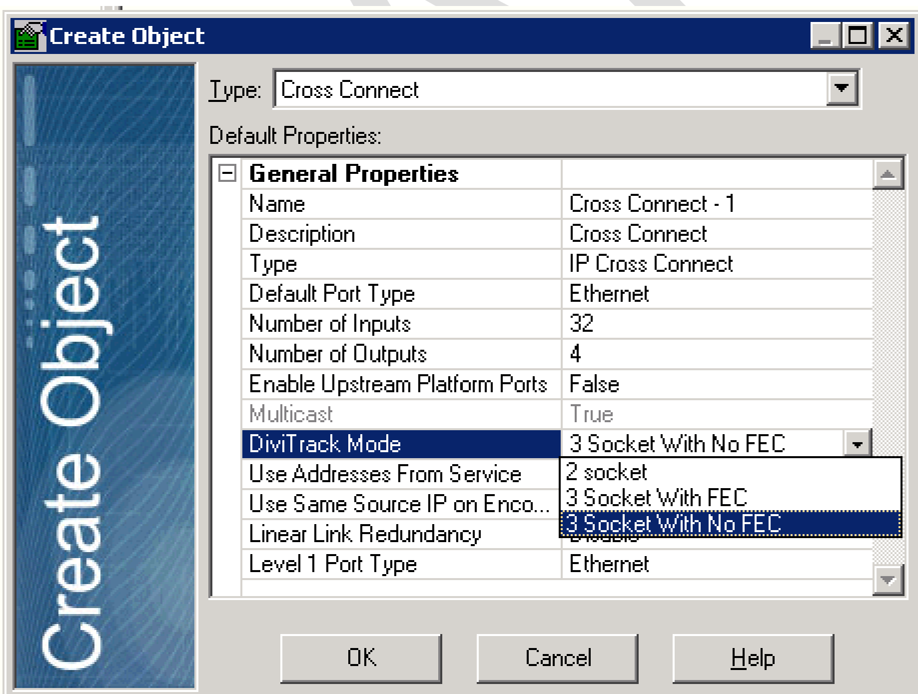
5.3 IP Cross-Connect Multicast Address and Port Range Configuration

For NMX 4.5 and later releases, a new property “DiviTrack Mode” has been added for the Cross Connect icon. This property has two legal values for DiviTrackIP 2.0. Do not select the 2-socket mode. 2-socket mode is to allow legacy pools to operate temporarily during the NMX upgrade process.

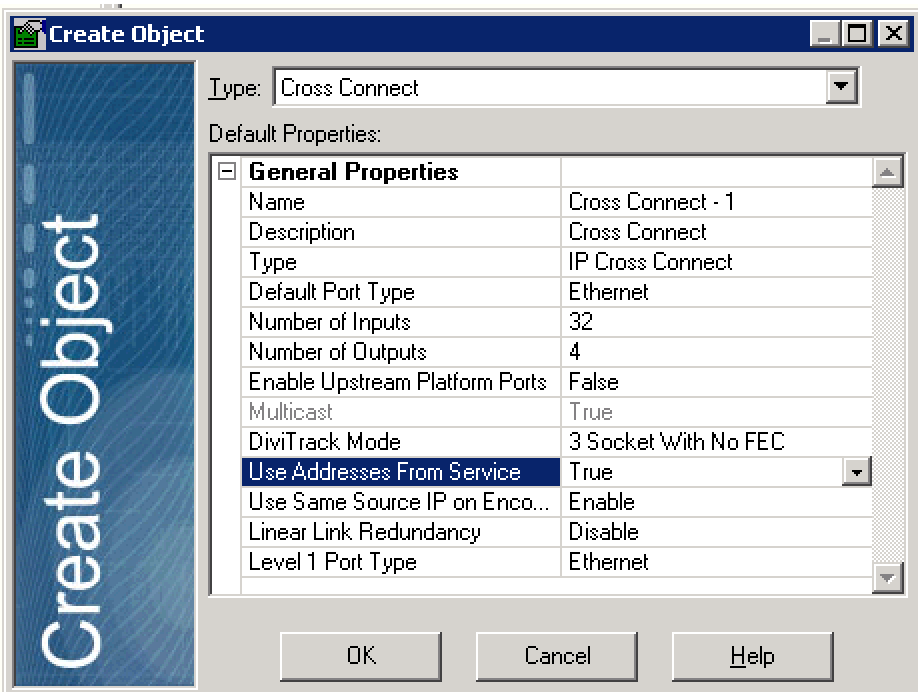
1. 3-Socket with no FEC
2. 3-Socket with FEC

If you will be using FEC in your DiviTrackIP system (i.e., you select “3 Socket With FEC” property), skip this section and start your setup of the IP cross connect with section 3.3 “Configuring the Cross Connect Switch with FEC and IP Addressing”. If you select the no FEC property then follow the procedures in this section:

1. Set the properties of the IP cross-connect by opening the properties page. The “Number of Levels” and the “Multicast” properties will not be shown on the IP cross connect device property page. The “Default Port Type” will always be “Ethernet” and cannot change. The only entry to make on the page is the cross-connect name. Since you have decided not to use FEC, the DiviTrack Mode should be set to *no FEC*. See the screen shot below.



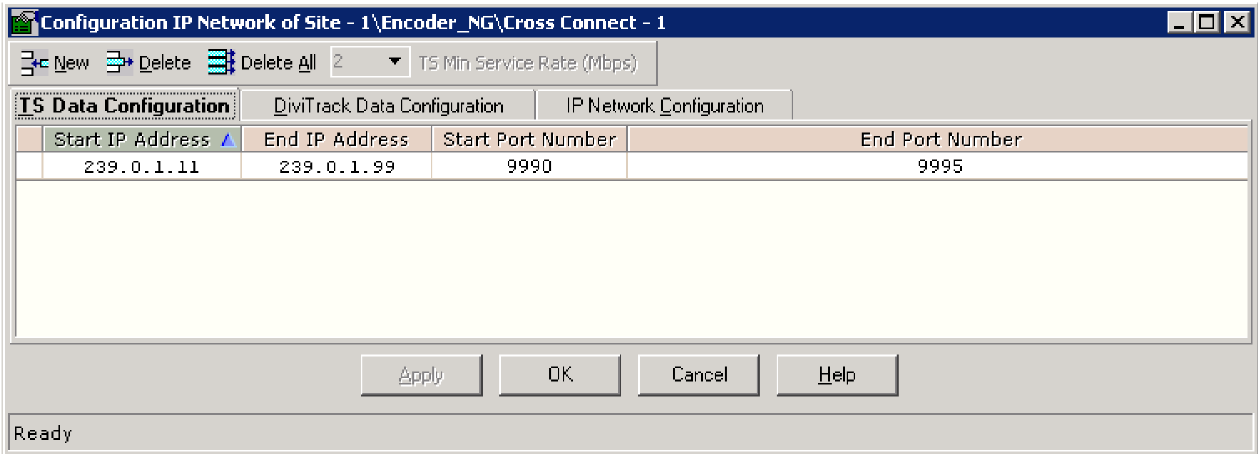
2. Before you close the Properties page, choose if you would like to have random multicast addresses assigned to the intermediate streams, or deterministic addresses you link to a particular channel. Select the latter by setting to *True* the property called *Use Addresses From Service* shown below.



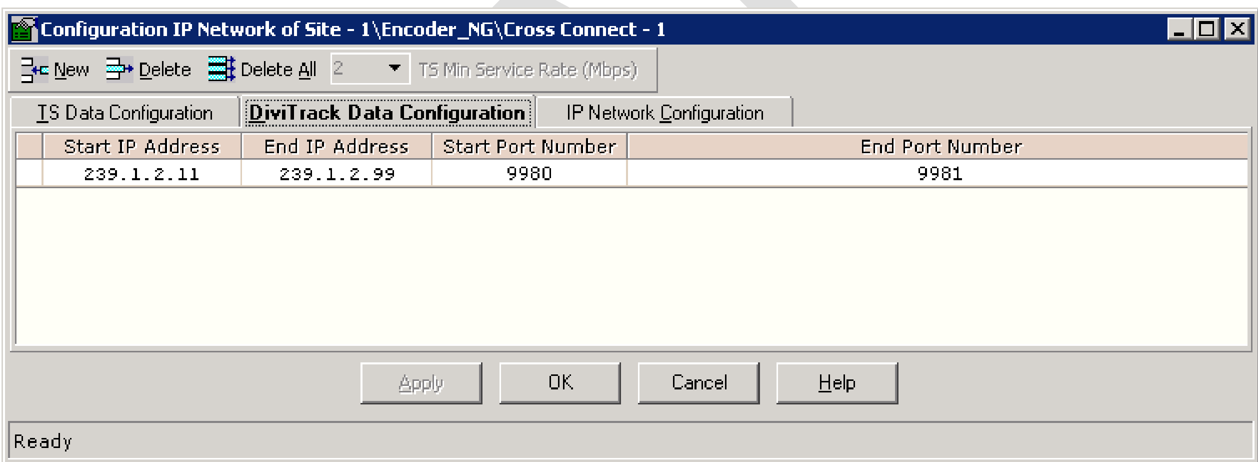
3. Specify the ranges of multicast addresses and port numbers on the IP Cross-Connect icon. Right click on the Cross-Connect icon and select “Configure IP Network.” You will set the address ranges for transport stream data and DiviTrackIP messages here as well as some other IP properties for the multicast streams.

4. On the TS Data configuration tab, set the multicast address and the associated port ranges. This example shows incremental port numbers with constant IP address; you can choose to have constant port numbers and incremental IP addresses as well (preferred). You may have more addresses in this table than actual services in use, but you may never have fewer addresses reserved than you plan to use. There will be an error if you run out of reservations.

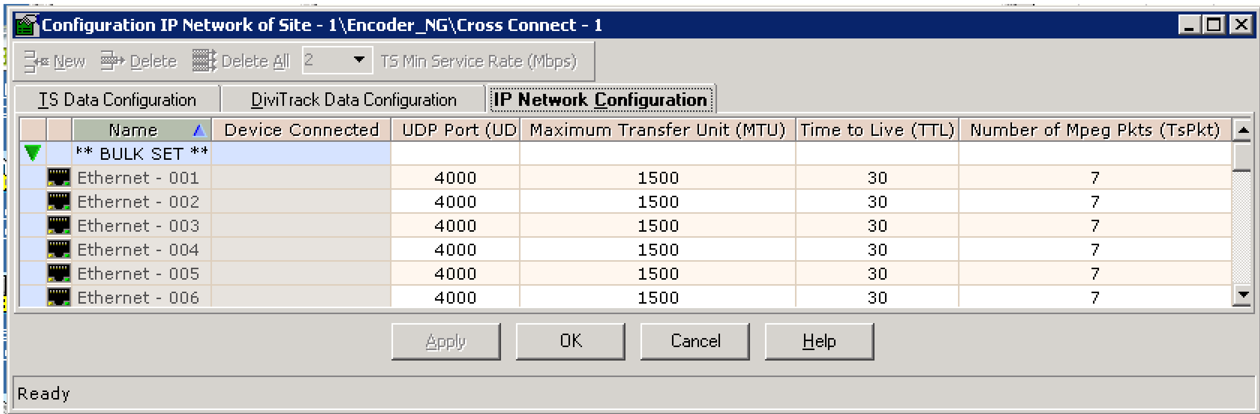
   This example below is for a non-FEC DiviTrackIP 2.0 system, where you need six port addresses per video channel; ports 9990 through 9995 satisfy this requirement. Note that you must start with an even-numbered port. Do not use the so-called “well-known” IETF port numbers that have been already assigned for popular services, like Telnet, SSH, FTP, and the like because this could burden other devices on the network and it will make debugging harder since the Wireshark Ethernet analyzer program tries to interpret packet contents based on the well-known port values.



5. On the DiviTrack Data Configuration tab, set the messaging-related multicast address and ports. Enter one multicast address and port per DiviTrackIP pool. The example should show two ports per line, one port for the old (1.0) format messages, and the second port for the new 2.0 protocol messages, and starting with an even number.



6. In the configure IP Network tab, enter the IP network configuration parameters for all devices specified in this dialog box.

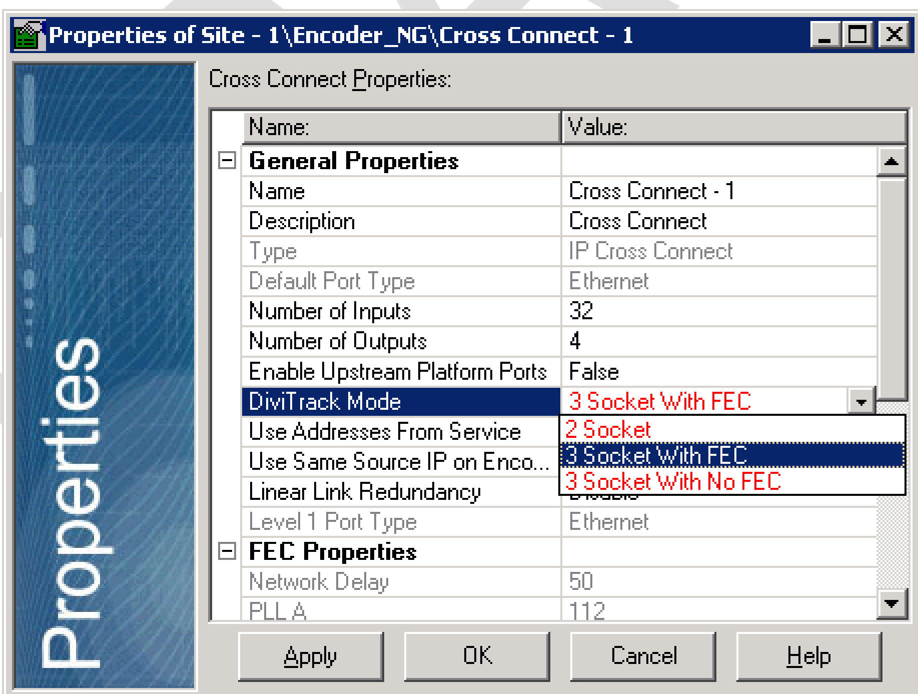


After configuring the dialog boxes, NMX will perform validation to ensure that only multicast addresses are entered for the ranges. It will also ensure that the ranges of multicast addresses and port numbers you entered do not overlap between transport data and DiviTrack messages.

5.4 Configuring the Cross Connect Switch with FEC and IP Addressing

5.4.1 DiviTrack Mode for the IP Cross Connect

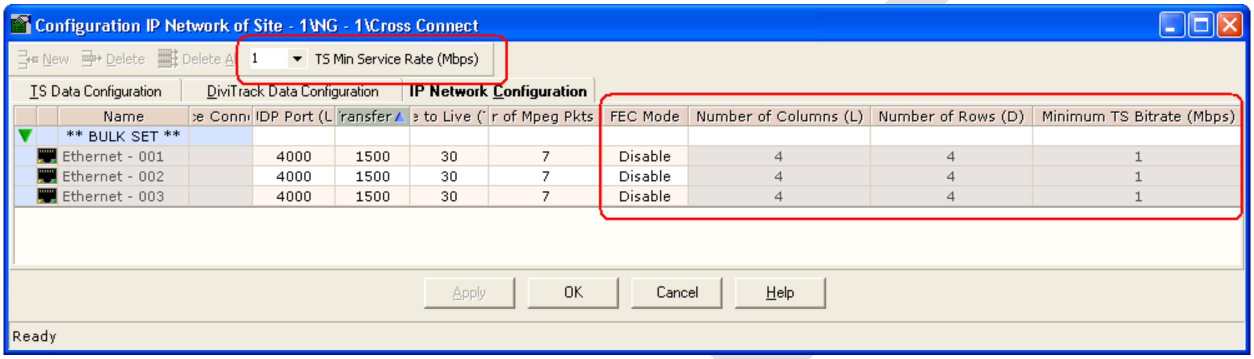
When you choose “With FEC,” the NMX dialog appears as follows:



When “DiviTrack Mode” is set to “3 Socket With FEC”, the FEC columns along with the user selectable FEC parameters L (columns) and D (rows) are shown (see screen shot below).

Note 1: “DiviTrack Mode” is only allowed to change when there are no streams flowing through the IP Cross Connect (i.e., the services must be deactivated.) Therefore if any stream is flowing, the property is shown as “read-only”.

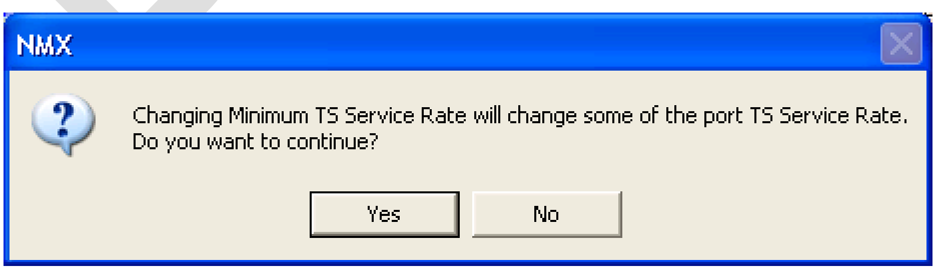
Note 2: When you have selected “With FEC” and subsequently change “DiviTrack Mode” to “Normal”, all values in the FEC related columns remain same as before. For example, NMX will not automatically change the FEC mode column to *Disable* when “DiviTrack Mode” is changed to *Normal*.



By default, the FEC Mode for each input Ethernet port is set to *Disable*. The user can change the mode to *Annex A* or *Annex B*, and then can configure the FEC L and D parameters, and the Minimum TS Bitrate which is set to 2 Mbps by default. Note that Annex A is not supported in NMX 4.5 and later releases. Selection of this option will results in a “not supported” pop-up message.

There is a drop-down list “TS Min Service Rate” at the top of the dialog box. This list allows you to specify the lower bound of the values in the “Minimum TS Bitrate” column. If you increase the lower bound while some values in the “Minimum TS Bitrate” column are smaller than the new lower bound value, an NMX GUI will pop up a message box to ask whether to automatically adjust the values in the “Minimum TS Bitrate” column or not. If “Yes” is selected, the NMX GUI will change those values that are smaller than the new lower bound to the new lower bound value. If “No” is selected, the NMX GUI will cancel the lower bound value change.

Note that this setting is important to the proper operation of DT/IP since this lower bound on bit rate directly impacts the delay through the de-interleaver and error corrector in FEC streams. If set too low, this will cause the ProStream 1000 TS buffers to overflow. The minimum rate should be set at 2 Mbps or higher for HD pools. The required min rate setting is a function of the selected L and D values as well as the minimum video bit rate set for the VBR operations plus the audio and date included in the encoder output TS stream. If you have an SD statmux pool, because of the typically lower VBR min rates used, the percentage of nulls passed between the encoder and mux will be higher if a TS min rate of 2 Mbps is selected.



Note that when the "Minimum TS Bitrate" value is non-zero, NMX will set ELC-family encoders to work in "Minimum TS Bitrate" smoothing mode which means that nulls will be stuffed in the encoder output to maintain the minimum bit rate for the SPTS.

DiviTrackIP and FEC Related Constants

The following DiviTrackIP and FEC related constants are shown on the individual IP cross connect icon.

- Max No of Columns (L)
- Max No of Rows (D)
- Max Product (L x D)

The L and D constants control maximum values that will be allowed on the IP cross connect icon. These values are read-only and shown for information only. Items in grey text in the properties page cannot be edited.

5.4.2 Separate Complexity Message Socket (3-socket mode)

In this release of DiviTrack, all complexity traffic (for other than MV-series encoders) flows on a separate socket from the video, at the next port number higher than the video multicast IP/port base value (N+1, where N, the base port value, is an even number).

Please note that if the NMX IP Cross-Connect icon has the "with FEC" property set, video and audio packets will be delayed by approximately two seconds additional going through the DiviTrack controller to allow for de-interleaving and error correction, even if all individual MPEG streams have the FEC disabled. For low-latency applications, make sure the NMX IP Cross-Connect icon is created without FEC. ("no FEC" mode).

6 Assigning Specific IP Multicast addresses to Services

6.1 IP Address Persistence Feature

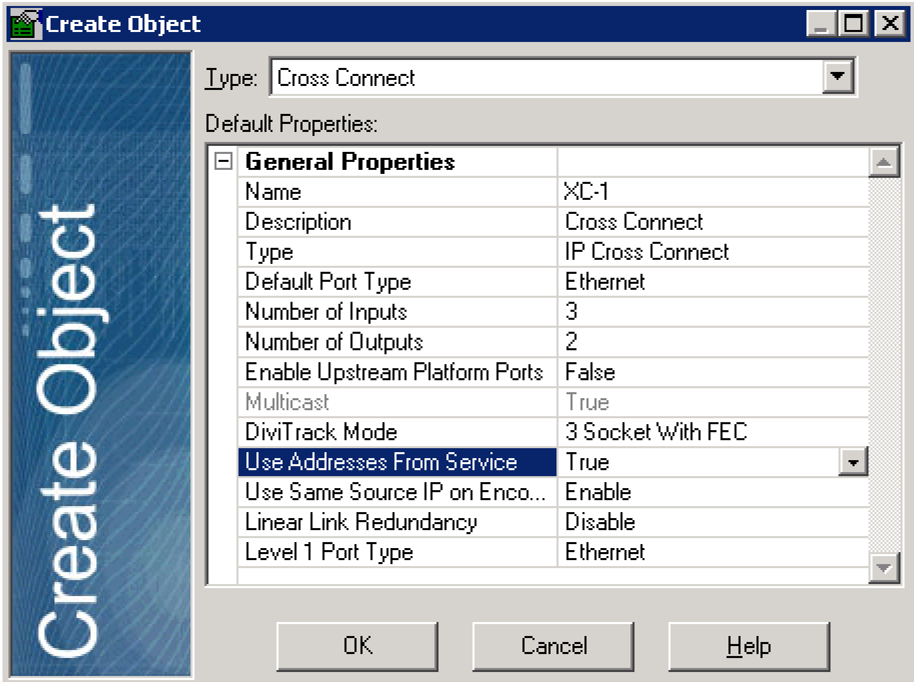
In releases after NMX 4.5 and prior to NMX 4.7, NMX assigned the addresses that encoders would use to send a service to the DiviTrack controller. You might not know this value until after the NMX-chosen value was assigned.

Once an MC address had been allocated to a particular intermediate IP TS between the encoder and mux, it would be maintained the throughout the TS lifecycle, despite a disable/enable operation on the streams, a deactivate/activate operation on the service map, or the shut down and re-start of the Domain Manager of NMX.

This way, once the addresses were known, for monitoring purposes the same address could be selected to check the health of a given service. However, keeping track of the NMX-selected assignments was an extra burden to operators.

Customers requested the ability not only to keep the addresses constant, but also to assign a specific address value to the intermediate IP multicast address from the encoder. Again, this helps with monitoring system health and debugging service trouble. You can now assign a particular value to the intermediate MC address for a service in NMX 4.7 and beyond.

Select this feature in the properties page of the NMX IP Cross-Connect icon dialog page, as shown below. The field, *Use Addresses From Service* set to *True*, enables this. Otherwise, addresses will be assigned in an arbitrary way from the list in the Configure IP Network tab of the NMX IP Cross-Connect.



Different customers have different requirements on how MC addresses should be allocated on the intermediate IP transport streams. Some options are:

1. A fixed block of MC address for each intermediate transport stream.
2. Specific address range per encoder or per encoder group. For example, encoders in City A need address range 1, and encoders in City B need address range 2. All encoders are connected to the same XC, and are routed to the same Muxes.

NMX provides an interface for you to define the desired MC address on the input channel. Since for encoder + XC + Mux setup, the input channel and the intermediate IP TS have a 1:1 relationship, NMX will be able to get the MC address from input channel property and provision the intermediate IP TS accordingly. Note that, for a multi-channel encoder, using a separate transport stream (SPTS) for each channel is important.

6.2 Associating Intermediate TS IP Addresses to Input Channels

The GUI provides a spreadsheet view of the input channel as shown in the table below. You define the Intermediate TS IP address, and the starting IP port number (that must be an even number).

If you have the service configuration property “Intermediate TS FEC enabled” turned on, the GUI automatically fills in the ending port number which is 5 numbers higher than the starting number. (This allows for reservation of the additional ports that FEC requires) The GUI also checks that the next channel’s starting port number is 6 higher than the last one, had the next channel taken the same IP address. This is to support block address allocation for 3-socket DiviTrack. For example, Channel 1 takes IP port 1032 (TS data), 1034(FEC row), 1036(FEC column), and 1033 (complexity), therefore the ending port number for Channel 1 is 1036, and the starting port number for Channel 2 is 1038.   The example is shown below.

Channel Name	Channel ID	Inter. Ts IP address	Inter. Ts IP Starting port	Inter. Ts IP Ending port

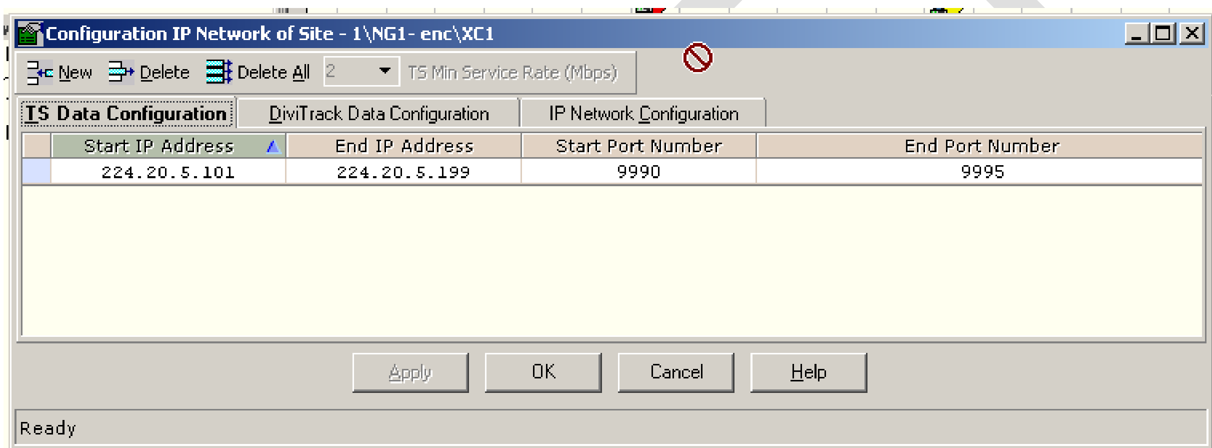
			number	number
Channel 1	1	224.20.5.1	1032	1037
Channel 2	2	224.20.5.1	1038	1043
Channel 3	3	224.20.5.2	1032	1037

For legacy 2-socket mode (DiviTrack Mode=Normal, not valid for DiviTrackIP 2.0), each TS only needed 1 MC IP port.

Note: many customers prefer to use a separate MC address for each service and rather than sharing different ports with the same MC address. This helps in debugging and traffic bandwidth management. NMX lets you choose either way.

6.3 Setting addresses on the Cross-Connect

On the XC, you must allocate a sufficient address range for all the input channels. The GUI is shown below.



When streams are provisioned, if “Use Addresses From Service” property of the Cross-Connect icon is TRUE, the MC address defined on the service will take the MC address from the input channel, and check whether it’s within the range defined on the XC. If it is, NMX assigns it. If the input channel MC address falls out of the range defined on the XC, NMX will assert loss of stream alarm, with the error message that the MC addresses are configured incorrectly.

If on the XC, “Use Addresses From Service” is not checked, NMX will automatically allocate MC addresses from the range defined on the XC (as NMX has done in previous releases).

6.4 STC Pool Multicast Address/Port Address Assignment

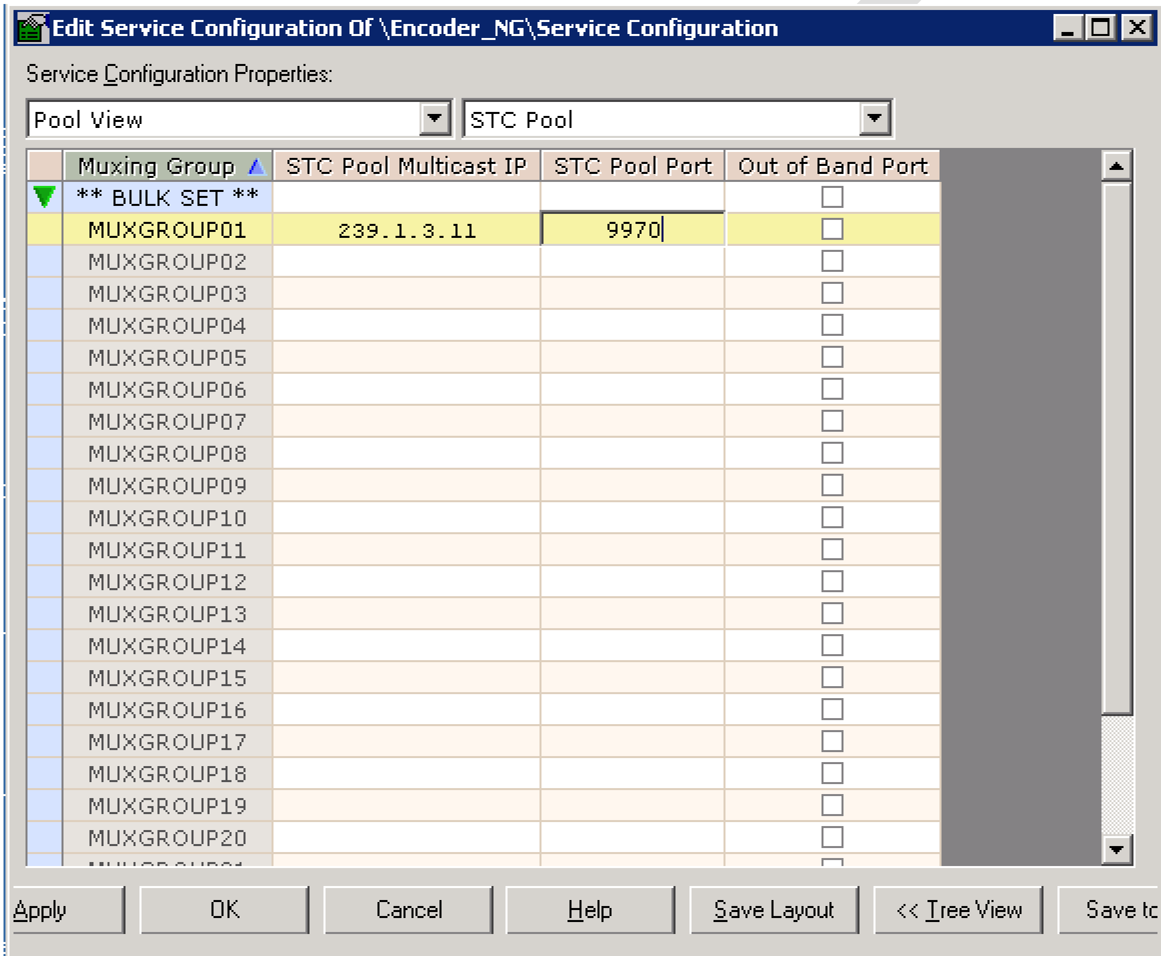
The STC Pool property page (accessed with Edit Service Configuration/Spreadsheet command) shows the STC pool multicast address and port that has been configured by NMX provisioning. Encoders joined with this multiplexer will lock their internal STC to STC messages arriving on this IP address and port via HRTP.

If for some reason these properties are not configured, they will display the default values of 0.0.0.0 and 0 respectively, or blank values. If there is no STC pool, the encoders will not synchronize to the DiviTrackIP controller, and their MPEG packets will be discarded as invalid. The result will be no output from the DiviTrackIP controller and an alarm of “Socket Not Active”.

When encoders are first starting up, or they are running in CBR mode, they listen to the STC pool to synchronize their internal clocks with the DiviTrackIP controller. After an encoder is in an active pool, it uses the rate messages controlling that pool (instead of the STC pool messages) to maintain the timing sync. The encoder doesn't need the STC information again until it either leaves the pool to run in CBR mode, or it needs to start up once more.

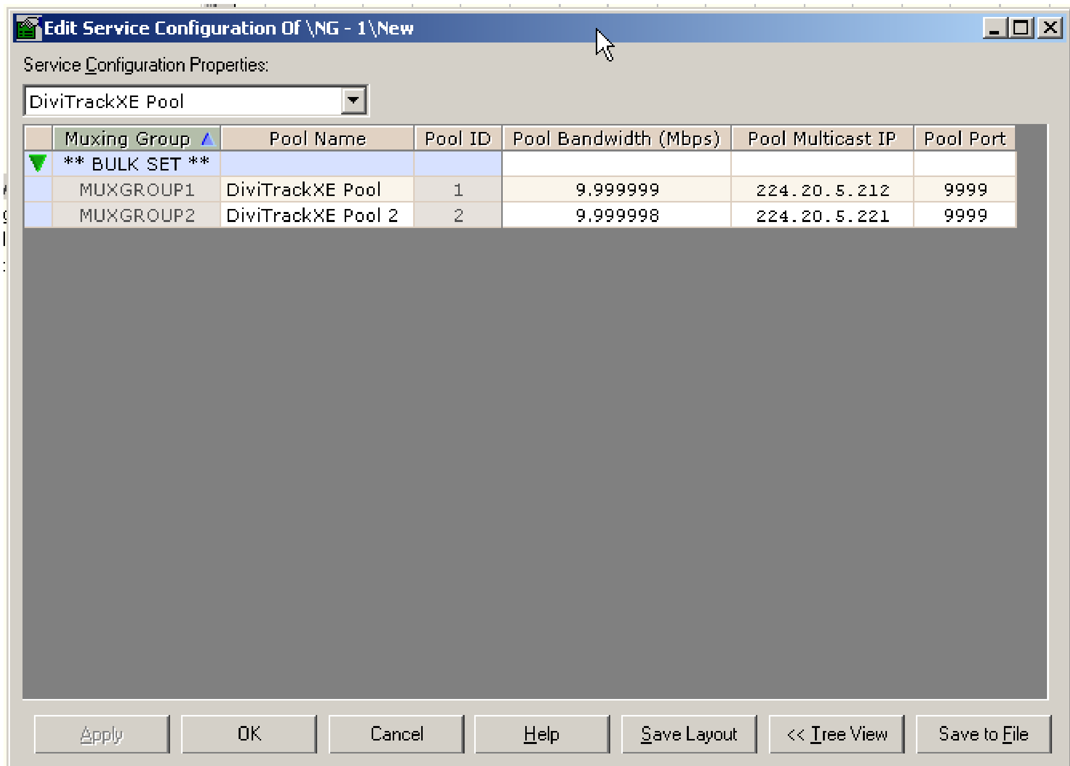
You can choose the MC values you would like to assign to the STC pool. Most customers prefer to use values that are from a different address block than the encoder MC values. You must have space in the NMX IP Cross-Connect reserved ahead of time for the values you assign to the STC pool.

Harmonic recommends to make these port values start on even-numbered ports.



6.5 DiviTrackXE Pool Multicast Address/Port Address Assignment

With the Edit Service Configuration/Spreadsheet command, you set the MC addresses to be used for each DiviTrackIP pool. Remember to also reserve space for these address assignments in the NMX IP Cross-Connect icon by right-clicking the icon and choosing the Configure IP Network command, then picking the DiviTrack Data Configuration tab in the dialog box that opens.

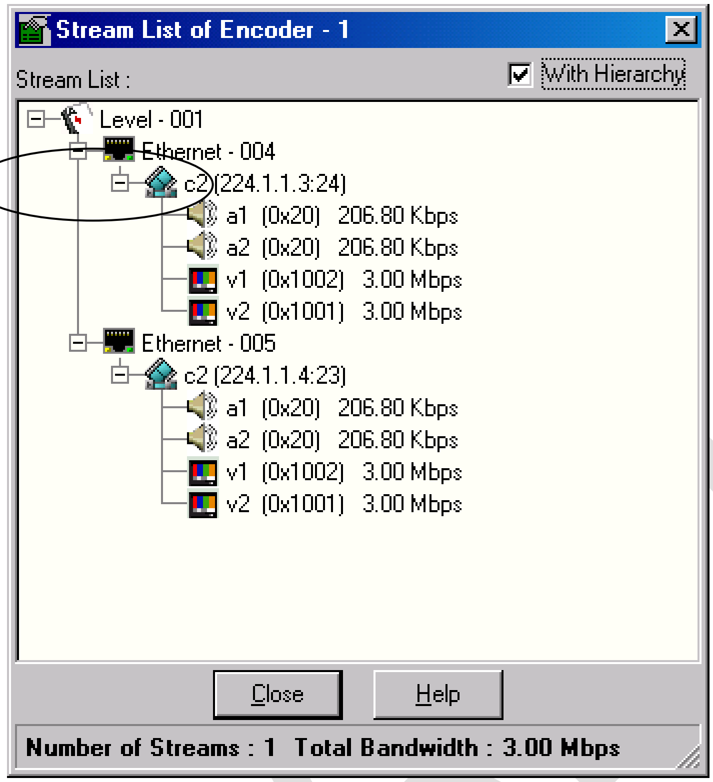


If you use multichannel encoders, be sure that all the channels from an encoder belong to pools in the same DiviTrackIP controller. Each multichannel encoder can receive DiviTrack control messages from only one DiviTrackIP controller (or pair of hot-redundant controllers).

You can split the channels up among pools that are controlled in the same DiviTrackIP controller, because one controller may operate several pools, but you may not split channels between pools that are controlled by different chassis.

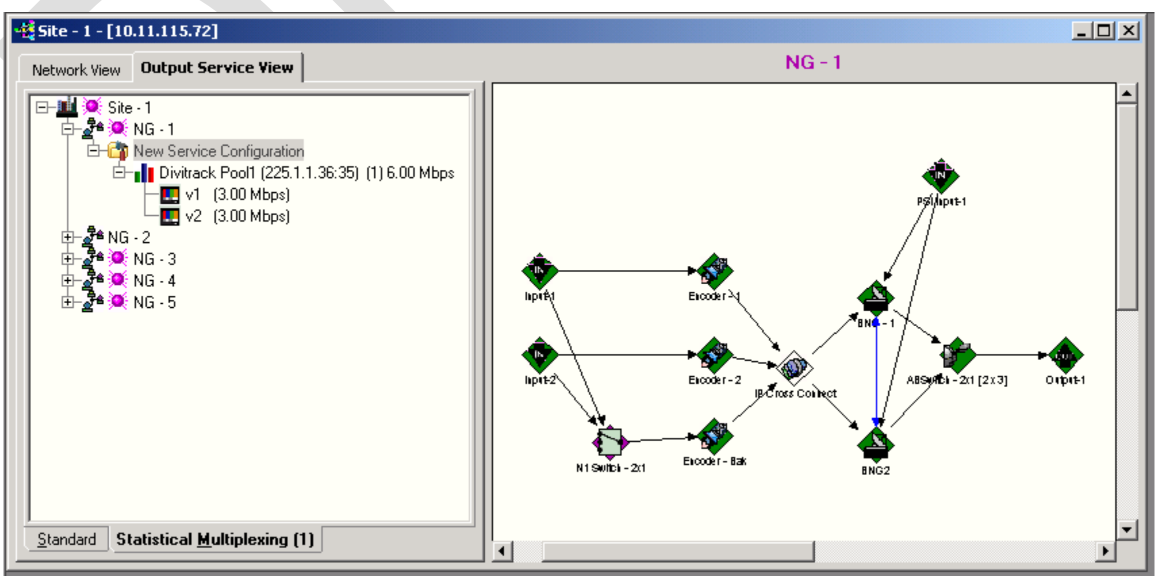
6.6 Stream List Dialog Box

The device Stream List dialog box displays the stream objects and display the corresponding configured multicast IP address/ port numbers used (Address: Port). A single-channel encoder would only have one address listed in the dialog below. The example shown is a multi-channel encoder configuration.



6.7 Stream Editor

For the DiviTrackIP application, the Stream Editor shows the multicast IP address/port configured on the pool object only if the stream map is active. If these properties are not set, they will not be displayed. The multicast address/port number will be displayed as a colon-separated pair in the brackets if these properties are set. For example, Pool1 (Address: Port). Since these are read-only properties, these will not be shown as part of the pool property page.



7 DiviTrackIP Redundancy Considerations

This section is intended to provide enough background on redundancy to allow those installing DiviTrackIP systems to validate proper operation and verify proper connectivity.

7.1 Redundancy Architectural Considerations

On encoder failure, the circuits through the affected encoder are destroyed, and new corresponding circuits are created on a backup encoder. No bandwidth changes take place to any pool, and the backup encoder is assigned to the same pool as the failed encoder.

When the redundant encoder takes over, it starts to stream to the multiplexer using the already assigned socket. The multiplexer does not change and is not aware of the switching.

Multichannel encoders will move *all* their channels to the backup encoder if *any* one channel fails. This will cause momentary interruptions in all services carried by a multichannel encoder.

7.2 Multiplexer Redundancy Switching

As with ASI DiviTrack, each DiviTrackIP controlling multiplexer is provisioned with a “multiplexer priority,” and the multiplexer priority is sent in the DiviTrackIP upstream messages. Each encoder checks all incoming messages’ priorities, but the encoders only use rates from the multiplexer with the highest-multiplexer-priority.

When NMX detects a failure in the “controlling” (for example, the highest-multiplexer-priority) DiviTrack multiplexer, NMX provisions a higher multiplexer priority on the backup multiplexer, if any exists. The encoders then begin to use bit rates from the new controlling (higher priority) multiplexer.

In the case of 1+1 hot-backup multiplexers, this process can be rapid. With N+M cold-backup multiplexers, the multiplexer provisioning process may take some time, and encoders fall back to CBR and operate at their nominal rates during this time.

At startup, the encoder listens on all of its DiviTrackIP rate connections, and it identifies the connection with the highest DiviTrack multiplexer priority. This connection is chosen as the “controlling” DiviTrackIP connection (the one that supplies the bit-rates actually used by the encoder).

During run-time, the encoder keeps track of the multiplexer priority on the controlling connection. It also checks DiviTrackIP upstream messages on the other (backup) connections to see if any of those connections ever has a higher multiplexer priority. If another connection ever does have a higher multiplexer priority, that connection becomes the new controlling connection.

The priority of the controlling connection may change from time to time, upwards or downwards, but as long as that connection has a higher priority than the other connections, it remains the controlling connection. (Support for changing priorities on the controlling connection is required, for example, to support loading of a new NMX map that contains different priorities.)

The encoder caches the most recently received multiplexer priority on the controlling connection. If the controlling connection is dropped (IP failure) or if it has “missing” messages (for example, a gap between STC timestamps larger than 70 milliseconds), the encoder will alarm and begin to output nominal video rate rates. It will not begin to listen to another multiplexer’s DiviTrack connection until that connection has a message with a higher multiplexer priority than the cached priority value. (This prevents multiplexer oversubscription.)

The encoder IP port will have to monitor rate messages from both multiplexers, and when it detects that a redundancy switch has occurred, it must switch its PLL source to start using the new time base and simultaneously change over all queued rate packets to use the new source.

There are two issues that are important to note with respect to this redundancy scheme:

First, at the time when the first DiviTrackIP rate message arrives at the IP port with a higher multiplexer priority, the IP port will switch its time base and flush its rate queue. In some deployments, because of the different network delays between controlling multiplexer and the encoder IP ports at different remote sites, some encoders may be working from a rate message originating at the old primary when other encoders may be listening to the new primary's rate message. For a 50 ms network delay plus jitter and 40 ms PLL offset, with combined local and remote encoders there could be a difference as much as three DiviTrackIP periods between the encoders. This may result in a transient over-subscription at the multiplexer. With the transport stream protection feature, only the remote encoders are at risk for bitrate capping; the local encoders will be running with the new correct rates and will not be clamped.

Second, because the backup multiplexer is using its own internal time base rather than the primary multiplexer's, its STC must be locked to the primary multiplexer's. This underscores the importance of having multicast traffic flowing between the muxes as well as between the encoders and the muxes.

7.3 HHP

HHP is used on the encoders to ensure that more than one encoder per service does not drive the MPEG IP network in the case of communications failure between an active encoder and NMX. Whenever HHP determines that the encoder should enter the MasterBackOff state, no complexity or TS data will be sent. The HHP behavior for DiviTrackIP configurations is identical to that for non-DiviTrackIP systems.

HHP-initiated failover operations on the multiplexer appear to be normal redundancy events for the encoders. This is done by incrementing the multiplexer priority so that the encoders begin to take their rate messages from the appropriate multiplexer.

HHP and IGMPv3 cannot co-exist. At most one of these two features is allowed. IGMPv3 is preferred.

Since IGMPv3 uses the IP Source Address to filter multicast flows, packets from a different source address than the one provisioned can be rejected. This offers the same protection as HHP against the duplicate sender problem. When IGMPv3 is used, HHP must not be used also.

7.4 DiviTrackIP Controller Port Redundancy

The following table summarizes the cases where you can use port redundancy on the DiviTrackIP controller. Of course, port redundancy on all encoder outputs is always supported.

Encoder	ProStream 1000 Port Redundancy
MV-Series	No port redundancy supported
ELC-Series	OK

8 Selecting an IP Switch

8.1 IP aggregation Switches for Encoders

All development and QA testing for DiviTrackIP was all done using Cisco switches (specifically, the Catalyst 2950, 3550, 3650, 3750, and 4948 models). Customer deployments successfully use the larger switches like the 4500, 6500 and 7600 models as well. Switches from Juniper, Extreme Networks, Force10, Raptor and other vendors have also successfully been integrated with DiviTrackIP.

The Cisco switches should not require setup to begin testing, but the default configuration may not be suitable for a production environment. For example, redundancy times may suffer if *portfast* has not been enabled, and multicast flooding may create extra traffic until the IGMP setup is complete.

If you are experiencing problems, you may need to consult with technical support for the IP switch you are using. Any switch used in a DiviTrackIP system must have the following attributes:

- Layer 2 (if it meets the other criteria here and routing is not needed) or Layer 3 switch
- Selectable auto-negotiation of port speed is desirable. Auto may facilitate initial setup (the switch default setting usually is auto-negotiate), but sometimes manual override is needed.
- The switch interfaces must support full duplex operations to prevent video interruption. Hubs and other half-duplex devices will not work for DiviTrackIP applications.
- The switch/router must be multicast capable, should support IGMP, and also should have a mechanism for preventing multicast flooding conditions (flooding can overwhelm the encoder and multiplexer IP ports and results in dropped packets).

All of the Cisco switches tested had 100Base-T ports for connection to the encoder IP ports and 1000Base-T (GbE) ports for connection to the DiviTrackIP controller and customer core network access switch. For connection of Harmonic products with Ethernet outputs to IP networks, see the application note “Network Connections of Harmonic Devices with Ethernet Interfaces,” listed in the references section. This document provides details on connection of Harmonic devices with IP to routers/switches.

Caution: Harmonic recommends separating the MPEG-over-IP aggregation function from other network traffic, such as device management (SNMP) and general workstation connectivity. Failure to make this separation may result in network overflow, and DiviTrackIP may not function correctly.

8.2 Auto-Negotiation vs. Manual Negotiation

For most applications, Harmonic recommends that the switch ports be set to the auto-negotiation mode. Electra (ELC) – series encoders do not have the choice of manual port negotiation. Keep both ends of the link set to the same mode if possible.

The IP ports and the IP switches should initially be set to the auto-negotiation mode. Auto-negotiation is a facility built into the Ethernet physical layer (called the “PHY” for short). Its purpose is to permit switches and routers to automatically match their capabilities to the device being connected. This system is not perfect, so operation is sometimes not graceful for older equipment. Because auto-negotiation operates at the physical layer, it is not well documented for many switch types. If you are having problems at the physical layer that are preventing proper negotiation, contact the switch vendor’s technical support or research their website for troubleshooting tips.

The IP port for MV-series encoders can only operate at 100base-TX Full Duplex. If the IP port is forced to half-duplex, MPEG traffic will have frequent packet losses. Electra-series encoders can communicate at 10 M, 100 M, or 1000 Mbit/s, but they do not offer the choice of manual port negotiation. The 10 Mbit/s selection should be avoided if possible. Past experience with MV-series encoders shows that, with some IP switches, you must set the switch ports to *manual* mode to run correctly. Most of the time, however, auto-negotiation does give the desired result.

You should be aware that some switches may fall back to half-duplex operation mode, even though both the switch port and the IP port configuration have been manually configured for 100 Mbit/s, full-duplex. This behavior is because switch auto-negotiation link detection is still operating even when the switch has been manually configured. This causes duplex inconsistency between the switch port and the device IP port.

8.3 Multicast (IGMP) Considerations (IGMP Version 3 update)

As noted previously, DiviTrackIP requires switches and routers with multicast capability. In addition, DiviTrackIP requires these devices to support IGMP Version 1 at a minimum. IGMP is a Layer 3 protocol, so routers (which are normally Layer 3 devices) should not have any problems with supporting IGMP. Switches, on the other hand, are normally Layer 2 devices. IGMP support is supplied by most switch manufacturers with some important caveats.

The fundamental difference between a router and a Layer 3 switch is that Layer 3 switches have optimized hardware to pass data as fast as Layer 2 switches, yet they make decisions on how to transmit traffic at Layer 3, just like a router would. Many Layer 2 switches employ proprietary mechanisms to permit some support of IGMP. Without IGMP, switches will flood multicast traffic to all of their outputs. This will overwhelm any encoders connected to the switch and will result in the loss of MPEG packets.

Check your technical documentation from the switch or router manufacturer(s) of choice. Network administrators may discover, for example, that IGMP is not enabled by default on their equipment. In such cases, you must enable it manually and possibly configure additional auxiliary equipment. Correctly functioning IGMP is critical to the proper operation of DiviTrackIP with large traffic loads (greater than 40 Mbit/s)

Small systems, like ATSC pools, may not need the flooding protection of IGMP, since their network traffic can be less than 20 Mbit/s in total. Most systems are larger than this and must have IGMP.

Current software releases support IGMPv3 on the ELC5400/7000 encoders and ProStream 1000 multiplexer. If you want to use IGMPv3, you may have to update other equipment connected to your network to handle this protocol. Older equipment may cause a fallback to a non-v3 operating mode.

Older-generation equipment that uses the IPA for multicast output does not support IGMPv3. (MV-series encoder family) Mixing v2 and v3 modes in the same network is not recommended.

8.4 Prevention of Multicast Flooding

Layer 2 switches are required by the IEEE 802.1D standard to deliver all datagrams for which the switch has no entry in its address table to all ports (except the one it was received on). This ensures that the first datagram to be delivered to a previously idle port will reach its destination. This process is called “flooding.”

While this is desirable for unicast operations, it can result in multicast chaos. Different switch manufacturers provide mechanisms for building the address table with multicast operations in action. These mechanisms may be referred to as “IGMP snooping” or “IGMP sniffing” and may cost extra. These mechanisms target IGMP messages specially and place proper entries for each IGMP client into the address table of the switch. Address tables all have age timers, so these entries will be removed unless updated periodically. This update process is done via an IGMP Query message.

A router is normally the IGMP query device. In small systems without a router, either the switch may have the ability to function as the query device or another auxiliary device will supply this function. Without periodic IGMP queries, the address table entries will expire and the switch will flood all multicast datagrams, resulting in packet loss and system failure.

8.5 LAN Switches versus WAN Switches

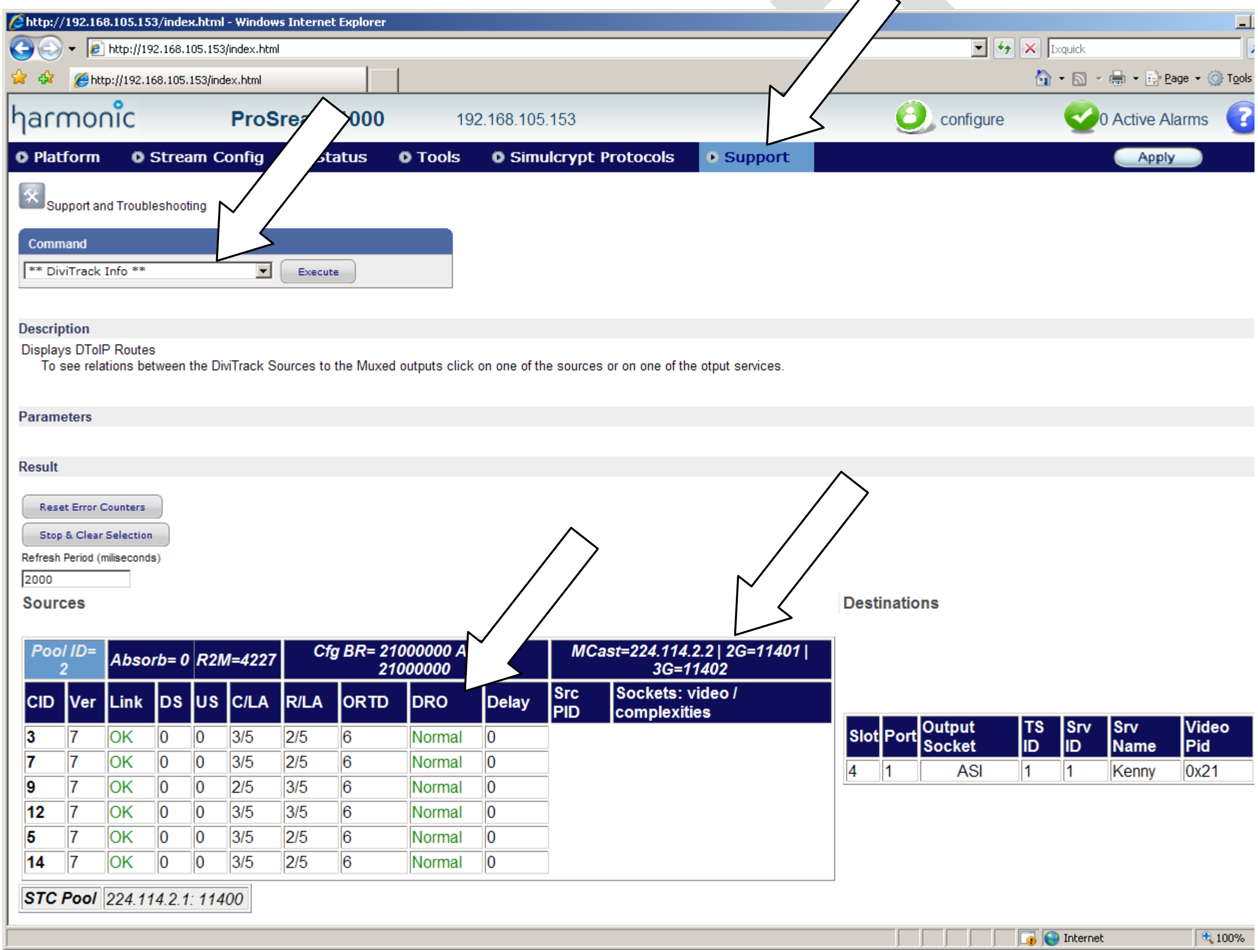
If your network extends beyond your local facility, your switch needs are more complex. Refer to Appendix B for items to consider if you are using a wide-area network and you have limited bandwidth on the long-distance links.

9 Debugging DiviTrackIP 2.0 Systems

You use the stand-alone graphical user interface (SAG) to connect to either the encoder or multiplexor of interest when you're troubleshooting. Open a web browser to the management port address of the device to begin.

9.1 Mux (DiviTrack Controller) Debug Screens

The usual account/password combination for access is *configure/configure.* Select the *Support* tab, then use the pull-down menu to choose the command: ** *DiviTrack Info* **. Press the *Execute* button.

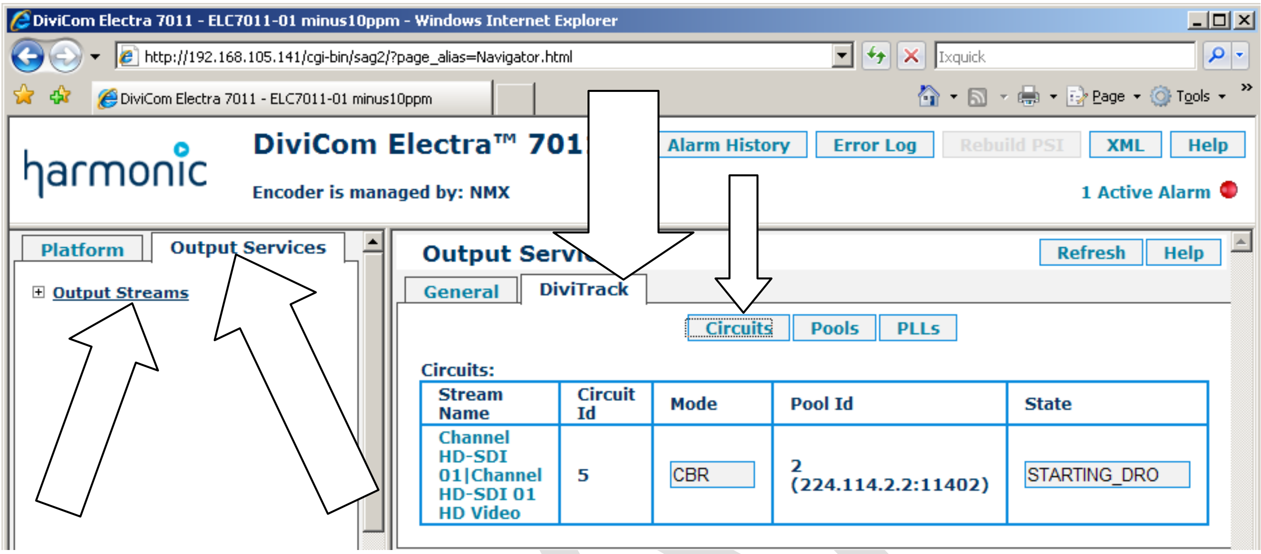


Refer to the screenshot above for the discussion that follows. Notice the column labeled, "*DRO*". This shows the status of each circuit in the pool. When the video is running in variable bit rate (VBR) under control of the DiviTrackIP controller, the status will be "Normal", as shown. Other states you might see are, "Starting" – when the pool is first activated – and "Frozen", if the messages from the mux to the encoder are not being received. This is a good place to look first if something is wrong with the pool.

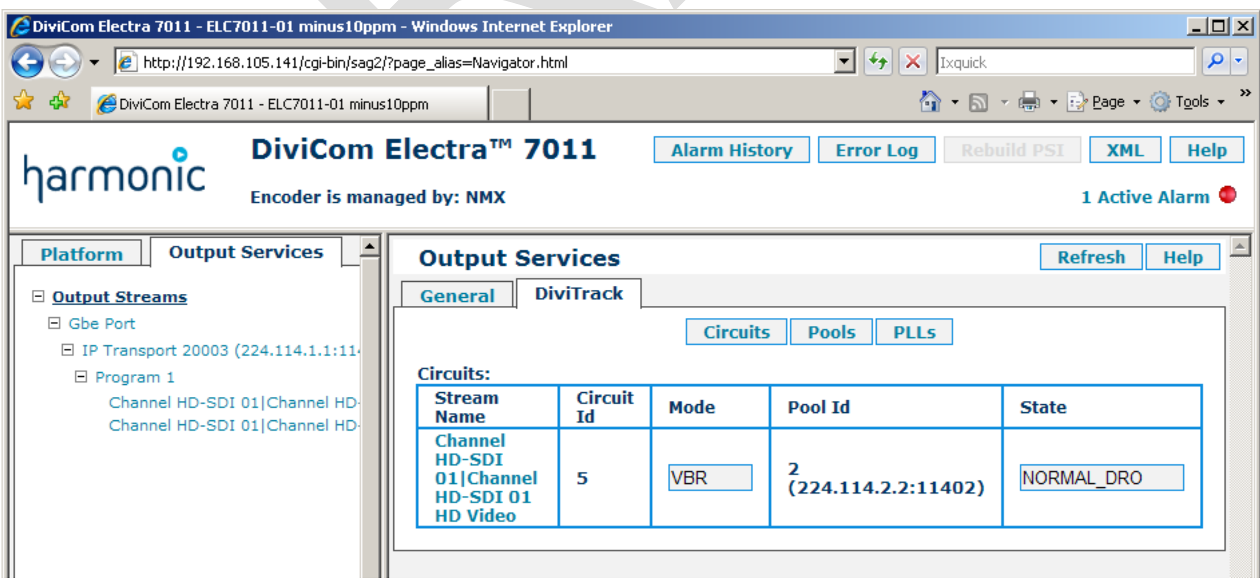
Check the "MCast= …" heading at the right of the table. Does it match what you expect for to see for the pool of interest? Compare the address/port listed here with that used by the encoders, if your encoders are stuck in constant bit rate (CBR) mode. Does the port number here overlap with another one in the system?

9.2 Encoder Debug Screens

Open a web browser to the encoder management address. At the upper left, you will see two tabs, “Platform” and “Output Services”. Select the latter, and a tree view will show in the left pane. Click on “Output Streams”, and observe that the right-hand pane changes to the title “Output Services”. Below that title will appear two tabs, “General” and “DiviTrack”. Select “DiviTrack” to enter the default “Circuits” page.

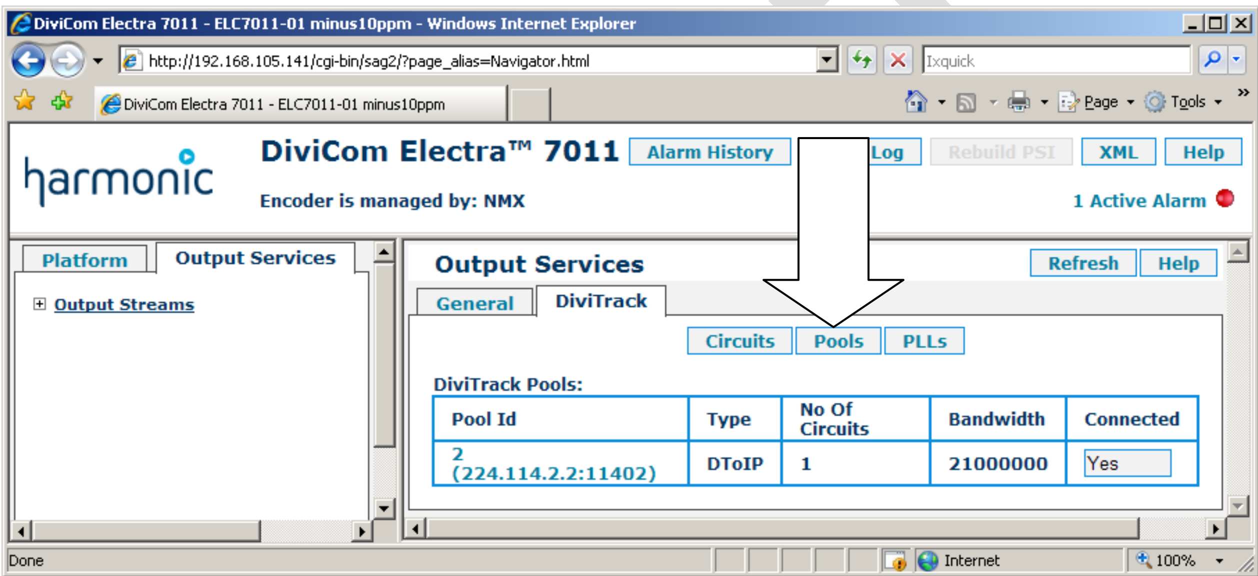


This example shows an encoder that is just starting up. Notice the “Mode” column, the state is CBR. This encoder is not changing its bitrate dynamically just yet. The “State” column shows the reason the encoder is in CBR, due to the “Starting_DRO” state. The encoder has to be communicating with the mux for a few seconds successfully before it will attempt to join the pool, and while it’s testing the connection it will stay in the starting state. The next screen shows what happens a few seconds later, when the encoder has successfully joined the pool. You can see the Mode is VBR, and the state is Normal.

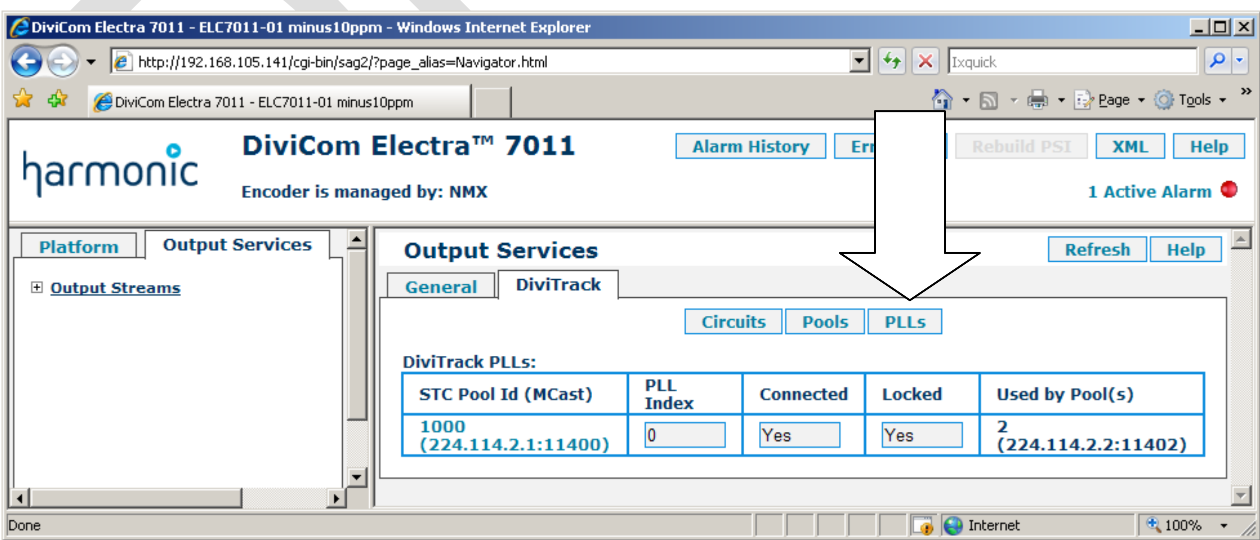


Again, a very important piece of information is the “State” column, showing NORMAL_DRO in this case. This means the circuit is in an active pool, changing its bitrate in response to the controller’s dictates. A multichannel encoder will have several lines in this table, with each line corresponding to on encoded circuit. Note the “Pool Id” column. You can see the value (2) and multicast (224.114.2.2) matches what’s been shown above for the mux. Again, this can assist you tracking down the cause of a stuck encoder or pool.

Click the mouse on “Pools” for the next debug page. This single-channel encoder can only belong to one pool. A multi-channel encoder may have channels that belong to different pools. In that case there will be multiple lines in this display, one line per pool. You can see the multicast that carries the rate change commands along with the port number in the “Pool Id” column, the total bandwidth of the pool (Bandwidth column), and whether the encoder believes that it is properly connected to the mux.



When you select the tab marked “PLL”, the screen shows the state of the encoder timebase that is supposed to slave itself to the timebase of the mux. The “Locked” column is most interesting here.



9.3 Wireshark Captures and Analysis

In the DiviTrack messages between the muxes and encoders that travel on the IP network, there are status fields that can help you debug a system that is misbehaving. The next release of this application note will contain more information about how to use these for debugging.

Wireshark captures of a running network help you confirm the port settings you have selected, and that the IP multicast values for a particular service match your intended plan. The data in the capture also confirms two-way connectivity between the encoders and DiviTrackIP controllers.

10 Troubleshooting Tools

Wireshark (formerly titled Ethereal)
Open Source (free) Network Protocol Analyzer, locally customized with HRTP (Harmonic Real Time Protocol) add-in. Very useful to compare the DiviTrack controller master timestamp (STC) transmission with the encoder's HRTP slave timestamp; if these values differ by more than 20 million (roughly), the encoder is out of sync and you will see no multiplexer output.

TSReader, Professional Edition
This is a low cost program which knows how to read the HRTP MPEG stream over the IP network. It can display thumbnail pictures of an encoder output. It can decode an encoder output stream that has no PAT and PMT by its "Define Manual Channels" feature, where you can specify a video and audio PID by explicit value and no PAT/PMT is required.

TSReader is also valuable to spool an IP video stream into a network for testing, or record a transport stream flowing on a network for later analysis or playback. It checks the MPEG continuity counter so you can see in real-time if you have data loss in your network.
TSReader can also pipe its output to the VLC decoder (below) so you can see live video and audio on your laptop for debugging or confidence monitoring.

The latest version of TSReader will support IGMPv3 and source-specific multicast, making it an extremely valuable aid to troubleshooting on IP networks.

Wlisten
Program to subscribe to a multicast IP address and UDP port, and then count the number of packets received. (IGMPv3 exceptions: routed PIM-SSM won't work)

VLC
Open Source (free) program that can record a transport stream file from an IP multicast source; useful to capture a problematic source for offline analysis. VLC can stream MPEG files like TSReader, but it's more complicated to configure. VLC has a video decoder recently updated to work with Harmonic AVC streams. Older versions cannot decode ELC5400 and ELC7000 video. Get the most recent version (v.0.9.9 or better).

11 Bibliography

Spurgeon, Charles E. 2000, *Ethernet: The Definitive Guide*, Sebastopol, O'Reilly, ISBN: 1-56592-660-9

Hall, Eric A. 2000, *Internet Core Protocols: The Definitive Guide,* Sebastopol, O'Reilly, ISBN: 1-56592-572-6

Both books provide detailed tutorial information regarding network physical and protocol operations. The Spurgeon book devotes an entire chapter to auto-negotiation.

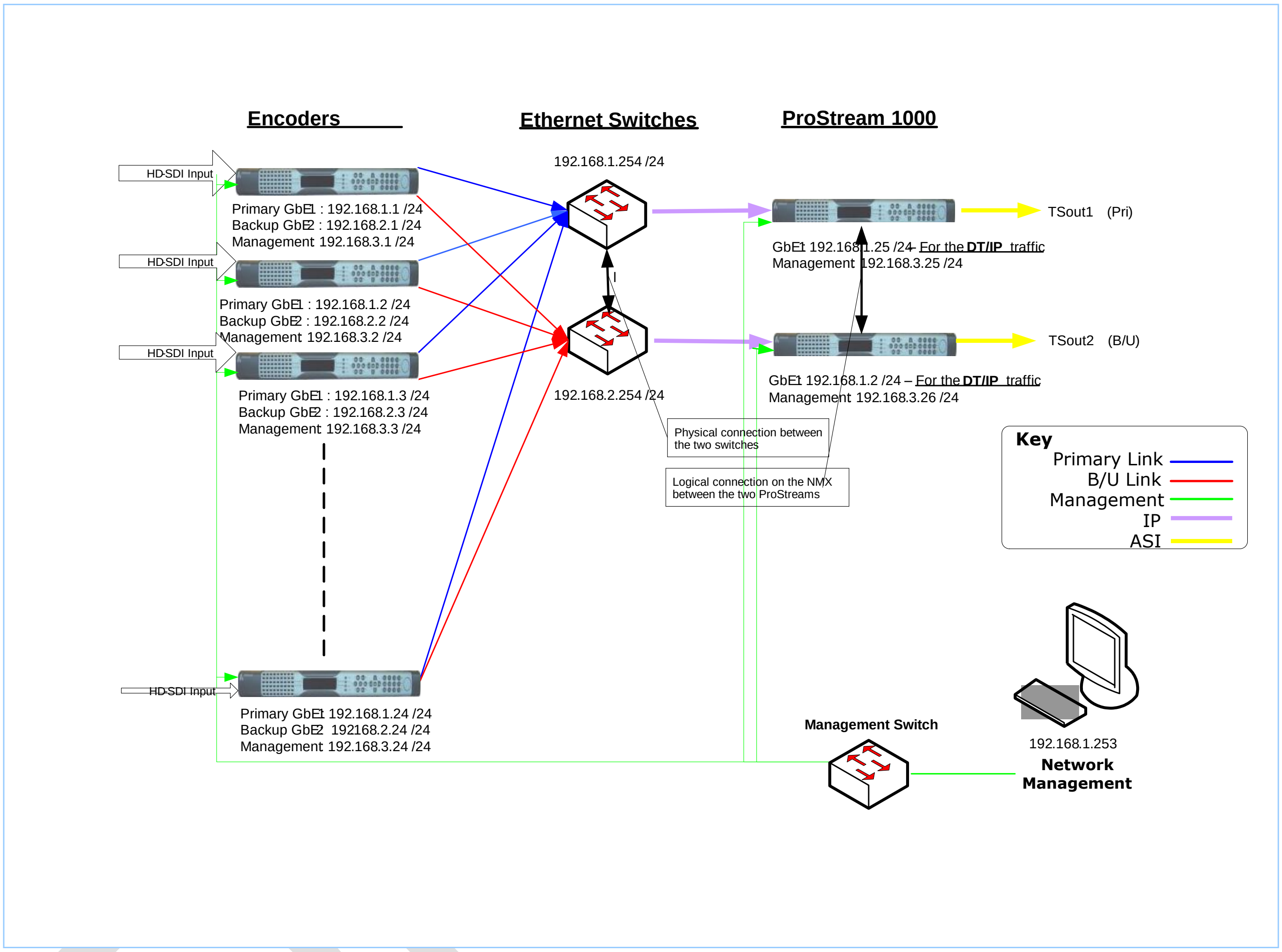
12 Glossary: Acronyms, Initialisms & Abbreviations

AVC	Advanced Video Coding (H.264 MPEG-4 video compression)
BNG	Broadcast Network Gateway: multiplexer and statmux controller
CBR	Constant Bit Rate
DRO	Dynamic Rate Optimization (statistical multiplexing)
DT/IP	DiviTrack statistical multiplexing over IP networks
DTC	DiviTrackIP™ Controller
FAQ	Frequently-Asked Questions
FEC	Forward Error Correction
GBE	Gigabit Ethernet
GIPI	GBE I/O card used by the BNG DiviTrackIP controller and multiplexer
HD	High definition
HHP	Harmonic Hello Protocol: proprietary solution for failsafe redundancy on network failure.
HTTP	Hypertext Transfer Protocol
HRTP	Harmonic Real-time Transport Protocol (extension of RTP that includes proprietary information)
IGMP	Internet Group Membership Protocol
IP	Internet Protocol
IPA	IP Adapter: IP output interface card for MV30/50/100/500 encoders
LAN	Local-Area Network
LOIS	Loss of input sync (cable unplugged or source stops)
LxD	FEC length and depth values for the interleaver/error corrector matrix
MC	Shorthand for multicast IP/port
MPTS	Multi-program transport stream
MV	Media View
NMX	Network management system
PIM	Protocol-Independent Multicast
PLL	Phase Lock Loop
SAG	Stand-Alone Graphical User Interface
SD	Standard Definition
SNMP	Simple Network Management Protocol
SPTS	Single Program Transport Stream
STC	System Time Clock
Statmux	Statistical Multiplexing
PAT	Program Association Table
PMT	Program Map Table
PSI	Program-Specific Information
RFC	Request for Comments
RTP	Real-time Transport Protocol, per RFC 1889
TS	Transport Stream
UDP	User Datagram Protocol
VBR	Variable Bit Rate
VLAN	Virtual Local Area Network
WAN	Wide-Area Network
XC	NMX IP Cross-Connect switch

13 References:

1. Harmonic, *DiviTrackIP FAQs - Rev2.2*
2. Harmonic Application Note, *Redundancy Schemes for IP Headends*
3. Harmonic White Paper, *Understanding DiviTrack Performance*, (0009-A) published February 2000
4. Harmonic Application Note, *Network Connections of Harmonic Devices with Ethernet Interfaces*
5. Harmonic Application Note, *Understanding HHP for Network Administrators*
6. Pro-MPEG Code of Practice #3 release 2, July 2004 (deprecated by SMPTE 2022)
7. Harmonic, *Introduction to DiviTrackIP™*
8. Society of Motion Picture and Television Engineers, SMPTE 2022-1-2007, “Forward Error Correction for Real-Time Video/Audio Transport Over IP Networks”
9. Society of Motion Picture and Television Engineers, SMPTE 2022-2-2007, “Unidirectional Transport of Constant Bit Rate MPEG-2 Transport Streams on IP Networks”

14 Appendix A: Example of DiviTrackIP Network Connections and Addressing



This example network illustrates typical device and encoder link redundancy. Should the primary IP switch fail, MPEG/IP traffic will begin transmitting on the device backup ports. Backup ProStream MPEG input links are also supported[1], although the picture above does not show this option. You may add this link if desired for additional protection.

Note that there is a separate subnet for the primary and backup ports. This is a requirement of the encoder IP output. This example does not use VLANs. You could use a single VLAN if desired for all the MPEG traffic by setting the encoder subnet mask for the primary port smaller than the VLAN subnet mask. The backup port subnet mask would be set similarly. If you would prefer separate VLANs for primary and backup ports, you will need multicast routing on your IP infrastructure to route between the two VLANs, so traffic can flow in the failover case. This is outside the scope of this application note.

[1] Except when using MV100, MV450, or MV500. Only the primary ProStream port is allowed with those.

15 Appendix B: System Bitrate Allocation for Remote Encoder Pools

You should plan for the extra bandwidth (beyond the MPEG-2 TS rate) that is used in sending traffic over IP or ATM-over-IP networks. By understanding each adaptation step, you can provision each layer of the network with confidence to achieve reliable video program transport.

Why do I have more IP bandwidth used than I have for an ASI circuit?

MPEG-2 traffic sent over ASI or a satellite link is sent in 188-byte packets from one sender to a receiver. When we move to an IP network, or an ATM network, additional information is sent along with the MPEG-2 data for IP source address, IP destination address, UDP port values and header checksums, and so on. These additional fields in the datagram count against the IP bandwidth consumed and are not present in a point-to-point ASI link. This overhead is part of the price of using standard IP traffic delivery.

You calculate the increased penalty for adapting the MPEG-2 traffic in an IP UDP stream by the factor of 1408 (length of Ethernet+IP+UDP+MPEG-2 packet) divided by 1316 (seven MPEG-2 TS packets at 188 bytes each). This value is about 1.07, seven percent extra overhead. This factor applies to the usual stream data where the maximum encapsulation efficiency is attained. Some MPEG-2 TS data – DiviTrack complexity information, for example – is only one MPEG 188-byte packet long, and can't be bundled with other traffic, so it has to go in its own IP protocol data unit (PDU). In this case, the 188-byte complexity packet becomes a 274-byte PDU, reducing efficiency further. (Since there are only about 30 packets per second for this traffic, this factor is usually small compared to the MPEG-encoded video payload, and can be safely ignored)

Some applications use a Forward-Error-Correction (FEC) packet stream to help recover lost traffic on a network that may drop or corrupt data. This overhead again counts against bandwidth used on the IP wire, and can be as small as five+ percent. Note that an FEC packet is longer in length than an MPEG video packet by an extra sixteen bytes, so for exact figuring, the 1408 length value of the video traffic has to be replaced by 1424 bytes when accounting for the protection packets. (Again, in practice, this effect is usually in the noise).

IP fudge factor: 1.07 IP headers * 1.05 FEC burden = 1.1235 – call it twelve and a half percent.

Why is my ATM bandwidth so high?

Once traffic has been encapsulated in the IP world, if this traffic has to flow over an ATM network, yet another adaptation layer is applied to the streams with its overhead burden. The first-order effect is to consider the 53-byte ATM cell carrying 48-bytes of user data; this factor is about 1.104 – round it up to 11 percent extra. On top of this "cell tax", not every IP packet ends at a perfect 48-byte boundary, which will apply yet another scale factor. And, there are extra bits to pay for to build up a PDU in for ATM that encapsulates an IP packet.

ATM fudge factor: 11 percent. So far, we have (IP) 1.1235 times (ATM) 1.11 is 1.247 total.

Total correction factor: about twenty-five percent beyond a plain ASI link.

Why is my peak rate higher than my average rate?

When you have multiple encoders wanting to send traffic, there will be some intervals when every device will need to send a packet. In an ASI-only head-end, we have buffers in ASI multiplexers to deal with bursts when we make an ASI transport. With an IP switch, there is no separate multiplexer, so the traffic smoothing has to be done inside the switch. The default configuration on our IP switches is to transmit at the interface line rate. If the WAN link is slower than the Ethernet link – as it usually is – packets could get lost.

In the case of the Cisco 3750 to ASX-200 connection, this link is a 100 Mbit/s Ethernet connection. If there are five encoders at the remote site, each sending a packet at the same time, these five packets will come out in a row (at 100 Mbit/s) from the Cisco link unless we take some action that asks the switch to do something other than default behavior to transmit at full link speed.

This burst of packets – which is normal and expected – only causes trouble if there is insufficient storage space at the other end of the link that is draining packets at the slower WAN rate. Using more encoders will increase the size of these bursts.

What can I do to prevent the burst from overflowing my WAN adapter?

Here is an example for a two-encoder pool setup we have in the lab.

The Cisco 3750/3650 can limit its output rate to a value between ten and ninety percent of its interface line rate by the following: (important line below is the srr-queue bandwidth limit 24, sets output speed to 24 Mbit/s)

```
Current configuration : 2862 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sv3-sw-clab100
!
enable password cisco
!
no aaa new-model
ip subnet-zero
ip routing
!
ip multicast-routing distributed
!
mls qos queue-set output 2 threshold 2 300 350 100 400
mls qos queue-set output 2 buffers 0 100 0 0
mls qos
!
interface GigabitEthernet0/1
 switchport access vlan 10
 load-interval 30
 speed 100
 srr-queue bandwidth shape  0  0  0  0
 srr-queue bandwidth limit 24
 queue-set 2
 no cdp enable
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport access vlan 10
!
interface GigabitEthernet0/3
 switchport access vlan 10
!
interface GigabitEthernet0/4
 switchport access vlan 10
```

Important: the bandwidth limit command has value of "percent of full port speed," so if your port is set to 1000 Mbit/s, the output limit value will be ten times higher than if the port is 100 Mbit/s. This is the reason for the explicit "speed 100" line prior to the limit command.

16 Appendix C: Mixed Encoder Pools

Mixed DiviTrackIP pools are a legacy concept where different encoder types are together in a pool or mixed video compression standards are in the same pool. In DiviTrackIP 2.0, the encoder type or codec type no longer matters. The information below is for legacy (unconverted) pools only and no longer applies to new pools.

Mixed DiviTrackIP (legacy, old pools) are subject to the following restrictions. *These do not apply to new pools in DiviTrackIP 2.0.*

- The ProStream1000 must be the DiviTrackIP controller. BNG is not allowed.
- The MV40, -45, -400, -450 are not allowed to participate in any pool, mixed or not.
- 50 Hz video and 60 Hz video standards cannot both be run simultaneously.
- ELC5000 and MV100 are only supported in MPEG-2 mode.
- Low-delay encoding is not allowed.
- 4:2:2 encoding is not allowed.
- MV100 and MV500 are not allowed to pool with ELC5400 and ELC7000.

As an aside, the AVC encoding mode of the MV100 will not be supported in any pool configuration, mixed or not; only the MPEG-2 encoding on MV100 is allowed to run in DiviTrackIP.

The term “mixed pool” does not apply if all encoders in the pool are the same type. You can have one DiviTrack controller that controls Pool 1 and Pool 2 at the same time, where Pool 1 has all MV100 encoders, and Pool 2 has all ELC7000 encoders.

17 Appendix D: DiviTrackIP Example Basic IP Switch Configuration

The commands below configured a Cisco 3560G switch to operate with a single pool of three encoders and one DiviTrackIP controller. The number of ports, VLANs, etc., would be greater in a real installation, but this simplified example will connect a minimal system together. Only the MPEG traffic ports are shown, as the NMX and device management ports could connect to a separate, unmanaged switch for the setup with a bare minimum of configuration.

```
!
version 12.2
no service pad
no cdp enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3560G
!
enable password cisco
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
ip multicast-routing distributed
ip igmp snooping querier query-interval 50
ip igmp snooping vlan 20 immediate-leave
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet0/1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/3
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/4
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface Vlan1
 no ip address
!
ip classless
no ip http server
!
control-plane
!
banner motd ^C DiviTrackIP Example
^C
!
line con 0
 login
line vty 0 4
 login
```



```
!
end
```

18 Appendix E: IP Switch Detailed Configuration

18.1 Overview

18.1.1 Purpose

The purpose of this document is to describe the basic setup of a Cisco switch for operation in a DToIP environment, as well as some optional features that can be used. It is assumed that the switch is operating as new (out of the box) with no configuration.

18.1.2 Before you begin

Ensure you have the following available before you begin:
Cisco "console" cable
Computer or laptop with an RS-232 connection available
Ethereal or some other network sniffer program installed for basic troubleshooting
System Diagram with port assignments already determined
IP Plan available
Have a basic understand of TCP/IP and the OSI Model and subnetting

18.1.3 Definitions

OSI Model	Open System Interconnection (OSI) reference model was created to help define how network processes function in general, including the various components of the network and transmission of the date. Understanding the structure and purpose of the OSI model is central to understanding how networks operate.
Protocols	Provide the rules and standards by which data is transmitted over a network
TCP	TCP is a connection oriented protocol that provides data reliability between hosts.
UDP	UDP is a connectionless protocol in which a one way datagram is sent to the destination without advance notice to the destination device
MAC Address	48 bit address assigned to the NIC
IP Address	32 bit logical address
Network Address	A reserved address assigned to the network itself.
Broadcast Address	A reserved address used to broadcasting packets to all of the devices on a network.
IGMP Snooping	IGMP snooping allows a switch to snoop or capture information from IGMP packets being sent back and forth between hosts and a router. Based on this information, a switch will add/delete multicast addresses from its address table, thereby enabling/disabling multicast traffic from flowing to the individual host ports.
IGMP Snooping Querier	IGMP snooping querier should be used to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. In a network with IP multicast routing, the IP multicast router acts as the IGMP querier. If the IP-multicast traffic in a VLAN needs to be Layer 2 switched only, an IP-multicast router is not required, but without an IP-multicast router on a VLAN, you must configure another switch as the IGMP querier so that it can send queries. When IGMP snooping querier is enabled, the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from the switch that wants to receive IP multicast traffic. IGMP snooping listens to these IGMP reports

	to establish appropriate forwarding.

18.2 Getting started

- Hook up your Cisco console cable to the "console" port of the Cisco switch and to your RS-232 port on your computer.
  Note: The console port may be located on the front or back of the Cisco switch depending on the model. Refer to the included documentation for questions regarding your specific switch model.
- Open a HyperTerminal session and use the following settings: 9600-8-1-none. Ensure that the scroll lock key is not depressed.
- Press the "enter" key. The switch should respond with a "Switch>" prompt.
  Note: If the switch has been modified the prompt may display a different name (i.e. Cisco> or something else).
- Type "enable" (or "en") to put the switch into privileged user mode. The switch will respond by changing the prompt to "Switch#".
  Note: if the switch has been pre-configured then there may be a password required here. Contact the person responsible for programming the switch for that information.
- You are now ready to start your configuration.

18.3 Basic Commands

Some basic commands that you will need to be familiar with in order to successfully program your Cisco switch. The abbreviation in ( ) below is the shortened version of the command that can be used. There are many other commands available. Refer to the Cisco documentation for a listing of all available commands.

enable (en) – puts the switch into privileged user mode. This is the basic configuration mode
show (sh) – command used to show specific configuration information.
clock – manage the system clock
configure – enter configuration mode
disable – turns off privileged mode
exit – exit from the current user mode
help – displays help
? – displays help. Using the ? after any command will give you the options available for that particular command.
write (wr) – write running configuration to memory, network, or terminal

Some examples of "show":
Switch# **sh running-config** – displays the running configuration of the switch
Switch# **sh startup-config** – displays the switch's startup configuration. This can differ from the running config if changes have been made to the switch after startup.
`Switch#` **`sh vlan`** – displays vlan information
`Switch#` **`sh int vlan 100`** – displays vlan information for vlan 100 only
`Switch#` **`sh interfaces`** – displays interface status and configuration
`Switch#` **`sh int Fa 0/1`** – displays interface information for Fast Ethernet 0/1 only
`Switch#` **`sh version`** – displays system hardware and software status
`Switch#` **`sh ip`** – displays ip information
`Switch#` **`sh history`** – displays the session command history
`Switch#` **`sh arp`** – displays the arp table
`Switch#` **`sh hosts`** – displays the IP domain name, name servers and host table

18.4 Basic Configuration Overview

Several key things must be done at the switch level to ensure a successful DT/IP installation. These include:

- Configuring VLANS
- Configuring interfaces to be members of these VLANs as well as setting these interfaces to access mode.
- Configuring interfaces that will connect to other Cisco switches
- IGMP snooping and IGMP query
- Backing up and restoring configurations
- Resetting your switch to default should you lose your password.

Optional configurations (More on these commands will be addressed later on in this document).

- Configuring passwords for the enable and telnet sessions
- Configuring an IP address for the switch
- Configuring an IP address for a vlan
- Routing commands
- Recovery from a lost password.

18.5 General Configuration

18.5.1 VLAN configuration

Prior to any VLAN configuration the user should have an agreed upon IP plan based on the network design. This mode allows the creation and deletion of VLANS. To put the switch into the VLAN configuration mode, starting from the privileged user mode and type …

```
Switch# vlan database
Switch(vlan)#
```

The switch will respond by changing the cursor to “Switch# (vlan)”.

To create vlan 100 type …

```
Switch(vlan)# vlan 100
Switch(vlan)#
```

(Select any number other than #1 as this is the default/admin vlan and can not be recreated or deleted). Repeat this for all vlans you need to create. To delete vlan 100 type …

```
Switch(vlan)# no vlan 100
Switch(vlan)#
```

To apply the changes made at the vlan prompt you must type “apply” before exiting the vlan prompt. To exit the vlan mode, type “exit”

Example Creating 2 vlans (vlan 100 and vlan 200)

```
Switch# vlan database
Switch(vlan)# vlan 100
Switch(vlan)# vlan 200
Switch(vlan)# apply
Switch(vlan)# exit
Switch#
Switch# conf t
Switch(config)# vlan 100
Switch(config-vlan)# no shutdown (This turns the vlan on)
Switch(config-vlan)# exit
Switch(config)#
Switch(config)# vlan 200
Switch(config-vlan)# no shut
Switch(config-vlan)# exit
Switch(config)#
```

Some optional commands that can be used when configuring your vlan are adding a description, adding an IP address, or changing the name of a vlan.
Adding a description is not necessary, but can be helpful for others when doing troubleshooting.

Optional (adding a description to the vlan, an IP address, and changing the vlan name)

```
Switch(config-vlan)# description TS1 video vlan
Switch(config-vlan)# name video vlan1 (this changes the vlan name)
Switch(config-vlan)# exit
```

18.5.2 Interface Configuration

Each port on a switch should be configured specifically for the device/host that is using that port. Please refer to the Harmonic documentation for each device that describes the Ethernet requirements. Please remember that each RJ45 port is considered an interface, as well as each VLAN. This will vary somewhat according to the type of switch, as Layer 2 Cisco switches will only allow one IP address per switch, thus one IP interface. Layer 3 Cisco switches can accommodate multiple IP interface assignments.

```
Switch# conf t
Switch(config)# interface GigabitEthernet 1/0/1
Switch(config-if)# no shut
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# spanning-tree portfast
```

Optional (Adding a description to the interface and an IP address)

```
Switch(config-if)# description Enc0101
Switch(config-if)# ip address 192.168.10.10 255.255.255.0
Switch(config-if)# exit
Switch(config)#
```


Optional (Using the range command to configure multiple interfaces)
The range command can be used to configure multiple interfaces simultaneously (substitute the port type “FastEthernet” or “GigabitEthernet” based on the switch you are using).

In this example we are setting up gigabit Ethernet ports 1-24 and adding them to vlan 100.

```
Switch(config)# interface range GigabitEthernet 1/0/1 – 24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 100
Switch(config-if-range)# spanning-tree portfast
Switch(config-if-range)# exit
Switch(config-if)# exit
Switch(config)#
```

18.5.3 Interface configuration for Trunking (802.1q)

```
Switch(config)# interface GigabitEthernet 1/0/48
Switch(config-if)# shutdown (this is an optional command)
Switch(config-if)# switchport encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all (optional)
Switch(config-if)# no shut
```

Optional (this will show you the trunking info for this interface. Note that the interface has to be active and have link with another trunk port for this to display the parameters below).

```
Switch# sh interfaces GigabitEthernet 1/0/48 trunk

Port        Mode         Encapsulation  Status       Native vlan
Gi1/0/48    on           802.1q         trunking      1

Port       Vlans allowed on trunk
Gi1/0/48    1-4094

Port        Vlans allowed and active in management domain
Gi1/0/48    1,100,200

Port       Vlans in spanning tree forwarding state and not pruned
Gi1/0/48    none
Switch#
```

18.5.4 IGMP Snooping

DT/IP requires IGMP snooping and an IGMP Query device to be active on the interfaces where the MV encoders and the BNG exchange information in multicast packets. The user should study the IGMP requirements and options in Cisco publications to determine what needs to be configured. **IGMP snooping should already be enabled by default.** Always look at the existing startup configuration to confirm this (using the **sh ru** command at the enable prompt). If you are still unsure you can run the command again.

1. To enable IGMP snooping globally, put the switch into global configuration mode.

```
Switch# conf t
Switch(config)# ip igmp snooping
```

2. To disable global IGMP snooping, again at the global configuration prompt, type:“

```
Switch# conf t
Switch(config)# no ip igmp snooping
```

3. To enable the IGMP snooping on a vlan, at the global configuration prompt, type:

```
Switch# conf t
Switch(config)# ip igmp snooping vlan 100
```

4. If a query device is required and your switch is a Layer 3 switch, you can invoke the query device on one vlan, as it requires the vlan to have an ip address. If you intend to use the BNG as a query device, you can skip this step, but you must enable the query function in the BNG. Refer to the BNG and NMX documentation for more information.
   To enable the query device, from the interface configuration prompt, type the following:

```
Switch# conf t
Switch(config)# interface vlan 123
Switch(config-if)# ip address 192.168.10.10 255.255.255.0
Switch(config-if)# ip pim sparse-dense
Switch(config-if)# exit
Switch(config)#
```

Note: ***Depending on the version of your IOS you may need to run the following in order for the switch querier to work properly***

```
Switch(config)# ip routing
Switch(config)# ip multicast-routing distributed
Switch(config)# ip pim sparse
```
Or
```
Switch(config-if)# ip pim sparse-dense
```
[Avoid using sparse-dense!]

5. To disable the snooping querier, from the interface configuration prompt, type:

```
Switch(config-if)# no ip igmp snooping querier
```

18.6 Optional Switch Configuration Commands

18.6.1 Configuring a switch IP Address

In this example we are setting the switch IP address and subnet mask. This is done by giving an IP address to VLAN 1 (the default or admin vlan).


```
Switch> en
Switch# conf t
Switch(config)# interface vlan1
Switch(config-if)# ip address 192.168.10.100 255.255.255.0
Switch(config-if)# exit
Switch(config)#
```

18.6.2 Configuring a switch with a default gateway

An IP address is assigned to the switch for management purposes. If the switch needs to send traffic to a different IP network, the switch sends traffic to the default gateway. The default gateway is the router IP address. A router is a device used to route traffic between different networks.

```
Switch> en
Switch# conf t
Switch(config)# ip default-gateway 10.10.5.254
Switch(config)# exit
Switch#
```

To remove a default gateway use the **no ip default-gateway** command to delete a configured default gateway.

18.6.3 Setting the "enable" password

The enable command is not password protected by default. It is good security practice to add a password to prevent unauthorized changes to your switch.
In this example we are setting the enable password to "harmonic".

```
Switch> en
Switch# conf t
Switch(config)# enable secret harmonic [
Switch(config)# exit
Switch#
```

18.6.4 Setting a telnet password

If you are using telnet it is good practice to set a password to prevent unauthorized access to your switch. In this example we are setting the telnet password to "harmonic". In order to telnet to a switch you must first set up your switch with an IP address. Refer to section 4.1 for more info.

```
Switch#
Switch# conf t
Switch(config)# line vty 0 4
Switch(config-line)# password harmonic
Switch(config-line)# exit
```



```
Switch(config)# exit
Switch#
```

18.6.5 Saving a running configuration

There are several commands to save a running config.

```
Switch# wr
```

18.6.6 Saving a running config to a startup config

```
Switch# copy run start
```

18.6.7 Copying a startup config to a running config

Procedure for saving a config to a tftp server. Ensure you have ip connectivity (verify by pinging the tftp server) before attempting.

```
Switch# copy start run
```

18.6.8 Saving a configuration to a tftp server

Procedure for saving a config to a tftp server. Your switch must have an IP address assigned to vlan 1 in order to proceed. Refer to section 4.1 for setting up an IP address. Ensure you have ip connectivity (verify by pinging the tftp server) before attempting.

```
Switch# copy run tftp
Address or name of remote host []? (enter the IP of the tftp server)
Destination filename [switch-config] (enter the name you wish to save the config as)(on the switch the config is usually named config.text).
```

18.6.9 Restoring a configuration from a tftp server

Procedure for restoring a config from a tftp server. Your switch must have an IP address assigned to vlan 1 in order to proceed. Refer to section 4.1 for setting up an IP address. Ensure you have ip connectivity (verify by pinging the tftp server) before attempting.

```
Switch# copy tftp start
Address or name of remote host []? (enter the IP of the tftp server)
Destination filename [startup-config] (hit enter)
Switch# reload
```

18.7 Password recovery procedure

Follow the password recovery procedure below if you cannot gain control of the switch.

1. Attach a terminal or PC with terminal emulation (for example, Hyper Terminal) to the console port of the switch.

   Use the following terminal settings:

   - Bits per second (baud): 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow Control: Xon/Xoff

   Note: For additional information on cabling and connecting a terminal to the console port, refer to Connecting a Terminal to the Console Port on Catalyst Switches earlier in this document.

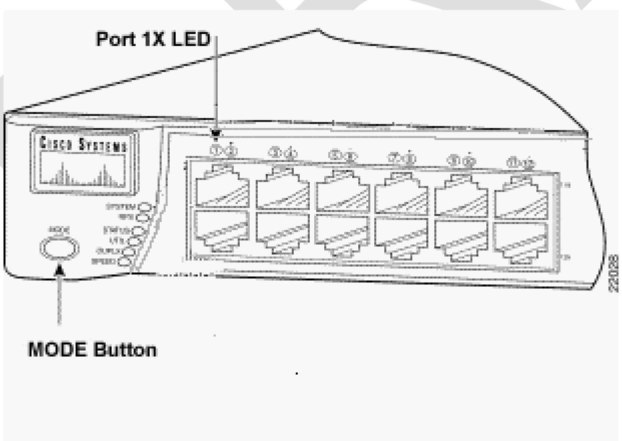
2. Unplug the power cable.

3. Hold down the mode button located on the left side of the front panel, while reconnecting the power cable to the switch.

   For 2900/3500XL and 3550 series switches: Release the mode button after the LED above **Port 1x** goes out.

   Note: LED position may vary slightly depending on the model.

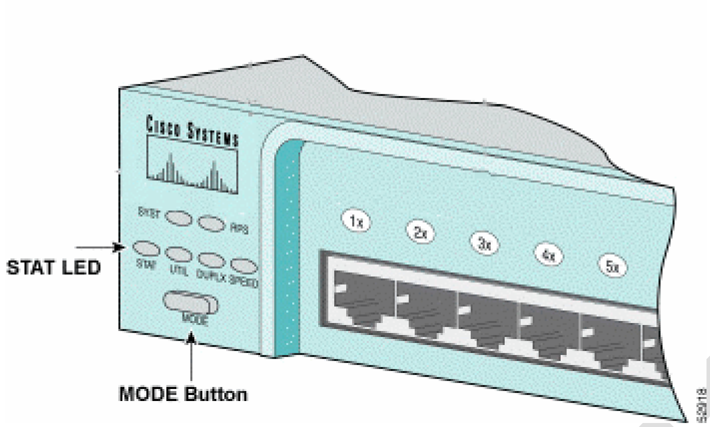
   Catalyst 3524XL



   For 2940 and 2950 series switches: Release the mode button after the **STAT** LED goes out.

   Note: LED position may vary slightly depending on the model.

   Catalyst 2950-24



For 2955 series switches only: The Catalyst 2955 series switches do not use an external mode button for password recovery. Instead the switch boot loader uses the break-key detection to stop the automatic boot sequence for the password recovery purposes. The break sequence is determined by the terminal application and operating system used. Hyperterm running on Windows 2000 uses **Ctrl + Break**. On a workstation running UNIX, **Ctrl-C** is the break key. For more information, refer to Standard Break Key Sequence Combinations During Password Recovery.

The example below uses Hyperterm to break into ***switch:*** mode on a 2955.

```
C2955 Boot Loader (C2955-HBOOT-M) Version 12.1(0.0.514), CISCO
DEVELOPMENT TEST
VERSION
Compiled Fri 13-Dec-02 17:38 by madison
WS-C2955T-12 starting...
Base ethernet MAC Address: 00:0b:be:b6:ee:00
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 19 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 4510720
flashfs[0]: Bytes available: 3230720
flashfs[0]: flashfs fsck took 7 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

*** The system will autoboot in 15 seconds ***
Send break character to prevent autobooting.


!--- Wait until you see this message before
!--- you issue the break sequence.
!--- Ctrl+Break is entered using Hyperterm.

The system has been interrupted prior to initializing the flash
file system to finish loading the operating system software:

flash_init
```

```
load_helper
bootswitch:
```

4. Issue the **flash_init** command.

```
switch: flash_init
Initializing Flash...
flashfs[0]: 143 files, 4 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 2729472
flashfs[0]: Bytes available: 883200
flashfs[0]: flashfs fsck took 86 seconds
....done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
switch:

!--- This output is from a 2900XL switch. Output from a
!--- 3500XL, 3550 or 2950 will vary slightly.
```

5. Issue the **load_helper** command.

```
switch: load_helper
switch:
```

6. Issue the **dir flash:** command.

   Note: Make sure to type a colon ":" after the **dir flash**.

   The switch file system is displayed:

```
switch: dir flash:
Directory of flash:/
2     -rwx  1803357   <date>      c3500xl-c3h2s-mz.120-5.WC7.bin

!--- This is the current version of software.

4     -rwx  1131      <date>                config.text

!--- This is the configuration file.

5     -rwx  109       <date>                info
6     -rwx  389       <date>                env_vars
7     drwx  640       <date>                html
18    -rwx  109       <date>                info.ver
403968 bytes available (3208704 bytes used)
switch:

!--- This output is from a 3500XL switch. Output from a 2900XL,
!--- 2950 or 3550 will vary slightly.
```

7. Type **rename flash:config.text flash:config.old** to rename the configuration file.

```
switch: rename flash:config.text flash:config.old
switch:

!--- The config.text file contains the password
!--- definition.
```

8. Issue the **boot** command to boot the system.

```
switch: boot
Loading "flash:c3500xl-c3h2s-mz.120-
5.WC7.bin"...###############################
##################################################################
##############
##################################################################
####
File "flash:c3500xl-c3h2s-mz.120-5.WC7.bin" uncompressed and
installed, entry po
int: 0x3000
executing...

!--- Output suppressed.
!--- This output is from a 3500XL switch. Output from a 2900XL, !-
-- 2950 or 3550 will vary slightly.
```

9. Enter "**n**" at the prompt to abort the initial configuration dialog.

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]: n

!--- Type "n" for no.

Press RETURN to get started.

!--- Press Return or Enter.

Switch>
```

10. At the switch prompt, type **en** to enter enable mode.

```
Switch>en
Switch#
```

11. Type **rename flash:config.old flash:config.text** to rename the configuration file with its original name.

```
Switch# rename flash:config.old flash:config.text
Destination filename [config.text]

!--- Press Return or Enter.
```

```
Switch#
```

12. Copy the configuration file into memory.

```
Switch# copy flash:config.text system:running-config
Destination filename [running-config]?

!--- Press Return or Enter.

1131 bytes copied in 0.760 secs
Switch#
```

The configuration file is now reloaded.

13. Change the password.

```
Switch# configure terminal
Switch(config)#no enable secret

!--- This step is necessary if the switch had an enable secret
!--- password.

Switch(config)#enable password Cisco
Switch#(config)#^Z

!--- Use Ctrl-Z.
```

14. Write the running configuration to the configuration file with the **write memory** command.

```
Switch# write memory
Building configuration...
[OK]
Switch#
```