S

Hicom 150 H, V1.0 Update

(Formerly known as the Hicom 150 E, R3.0)

SVU46 Prerequisite Reading Material

Revision November 15, 2000

Revision Schedule

Date	Name	Revision
6/8/2000	Andy Brown	Begin first draft
10/12/00	Andy Brown	Complete first draft for preliminary
11/15/00	Andy Brown	Final copy from review comments

Attention

This document was produced solely for training purposes and should not be used for field reference. Database examples used in this educational document may cause software conflicts with customer applications and should not be used as models.

Printed copies of this material may contain information that is not current. For the most current information refer to the on-line documents on the TAC Advisor web site.
External address: http://www.tac.siemenscom.com, Internal Address: http://tac.fld.rolm.com

Table of Contents

1 Introduction

The R3.0 changes for the Hicom 150E are not as abundant as in R2.2. However, what may be considered as lacking in the quantity of changes, is more than made up for in their quality. The 2 most notable enhancements to R3.0 are the addition of "Multiple Line Appearances" also known as MULAPs and the LAN based connectivity and administration support of the system. These new features are brand new to the Hicom 150 E, for R3.0. Oh! Did I say "Hicom 150 E"?

There is another change that you should know about concerning the system name. This name change reflects the overall Siemens communication's family known as "HiPath". The new product name is now the "Hicom 150 H, V1.0". When referencing this product the V (for Version) must be uppercase. The "H" stands for "HiPath Enabled". The rest of this document will refer to the Hicom 150 E, R3.0 as the new name "Hicom 150 H, V1.0".

There are several new features available as well as enhancements to existing features. Following, is some helpful information about what the features are, how to implement them, and some programming information as needed. The programming information, as written, is based on the requirement that you are already experienced on R1.0 and R2.2 system programming.

The V1.0 information that follows will be broken down into 3 categories: hardware, features, and service related changes. Each topic within the 3 categories will be presented in the following manner.

- **What's New:** A brief introduction of the new feature or enhancement.
- **Feature Operation:** How the new feature will be implemented by the user.
- **Programming Note:** How the new feature or enhancement will be installed, or reprogrammed.
- **Delta:** If applicable, how the new feature or enhancement differs from Release 2.2.

2 Hardware

There are only 2 pieces of hardware that are new for the Hicom 150H, V1.0. There is a new CBMOD that is required for the OfficePro operation. There is also a new V.24E interface card for system access that replaces the V.24 circuit card on the OfficeCom and OfficePoint systems. The HG 1500 is not new just for V1.0, but is mentioned in this document because the 150 H administration feature requires V1.0 software to be functional.

2.1 CBMOD (Control Board, Modular)

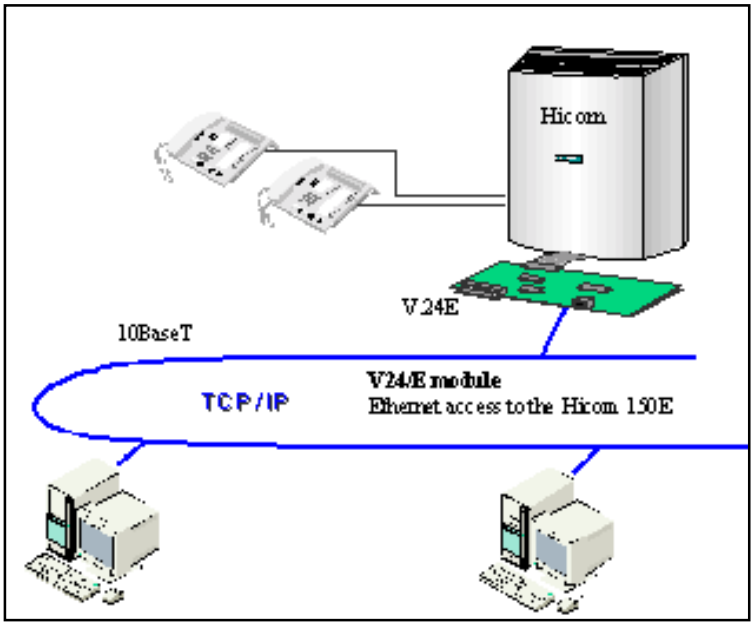
What's New: The new CBMOD for the OfficePro has the on-board memory expanded from 2MB to 4MB. This card will be shipped with any new OfficePro for V1.0.It will be required for any OfficePro that is upgraded from R1.0 or R2.2 to V1.0 software. The new CBMOD can be identified by the modified Siemens part number of Q2960-X200.

Programming Note: No CBMOD specific programming changes are necessary.

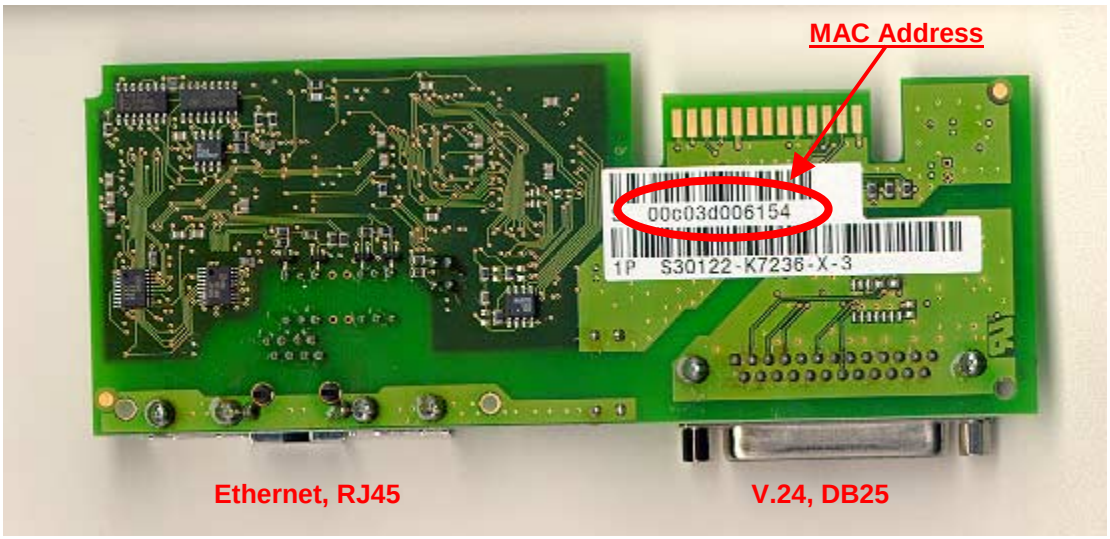
Delta: The new CBMOD is downward compatible to R1.0 and R2.2 systems if replacement as a spare is necessary. The CBMOD with 2MB of memory (X100) for R1.0 and R2.2 is not supported by the V1.0 (R3.0) software and will not boot up. Any upgrades to V1.0 software will require that the CBMOD be upgraded as well.

2.2 V.24E Administration Interface Card

What's New: New OfficeCom and OfficePoint systems will be shipped with the V.24E serial/Ethernet interface board. The new V.24E incorporates the standard RS232, DB25 connector as serial port 2. Serial port number 1 has been replaced by an RJ45, 10BaseT, Ethernet connector for integration into the customer's LAN environment. This will allow the system to be administered over the LAN as a TCP/IP supported interface. It is important to note, however, that while LAN access is supported, the V.24E still only supports a maximum speed of 19.2 Kbps on either interface.



The V.24E interface is not supported by the OfficePro. The OfficePro will rely on the HiPath HG1500 (formerly known as Xpress@LAN) interface card for all LAN integration features.



Front view of the V.24E card with the LAN connection on the left and the V.24 on the right.

Programming Note: The V.24E IP information is programmed in the Network area as indicated by the Assistant E toolbar illustration on the right. The actual programming will be covered in more detail in section 5.1 of this document.

Delta: This feature is not supported on R1.0 or R2.2 software versions of the OfficeCom and OfficePoint systems.

2.3 HXGM and HXGS circuit cards for HG1500 (formerly Xpress@LAN)

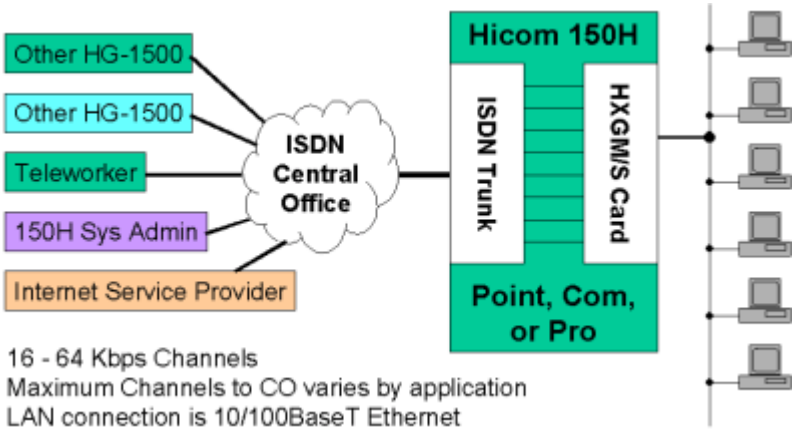
What's new: The HXGM and HXGS circuit cards allow the Hicom 150H V1.0 system to be integrated into an Ethernet LAN environment. These cards provide a means for LAN based IP administration at 10/100 Mbps Fast Ethernet, and also serve as an IP/IPX to ISDN converter for non-dedicated dial-up LAN connections over PRI, BRI, CorNet. These dial-up connections can be from 150H to 150H to link 2 normally unassociated LANs. They can provide multi-user access to a digital ISP with a common single account. Also supported is VoIP (Voice over IP) with the Siemens OptiClient 130™ soft phone running under WindowsNT™ or with Microsoft® NetMeeting™.

The Hicom Xpress Gateway, Medium (HXGM) card (Q2930-X) is a full size card for the OfficePro only. Since the V.24E card is not supported by the OfficePro, the HXGM is the only means to integrate the Pro into the LAN environment for IP based system administration. Also, since the OfficePro never supported the Siemens® LANBridge™, this allows the Pro to take advantage of all the great features of the HG1500.

The Hicom Xpress Gateway, Small (HXGS) card (Q2931-X) is a half size card for the OfficeCom and OfficePoint. It provides the same basic functions as the HXGM, only with fewer data channels.

You may think that the HG 1500 sounds a lot like the LANBridge application. Well, you'd be right. Except that the HG1500 application is much more robust than its LANBridge predecessor.

The illustration at left shows the high level overview of the HG 1500 in the 150 H system. As mentioned previously, it allows IP traffic on the LAN at the far right to be sent out of the system over ISDN and is then converted back to IP at the far end.



Programming Note: The programming of the HXGM and HXGS will not be covered in this document. For HiPath HG 1500 training you will need to enroll in the Siemens ICN Education course. Look on the Siemens ICN Education on-line registration for more information on the "HG 1500 Installation and Maintenance" course, code TE95.

Delta: The HXGM and HXGS circuit boards are not supported by the R1.0 software version. They are supported only by the R2.2 and V1.0 (R3.0) versions of software.

3 Station Features

3.1 Multilevel Feature Key Programming on Optisets

What's New: Optiset key programming now supports multilevel key buttons. Each user programmable button is capable of supporting 2 features as long as one of those features is an external repdial number. A "shift" key is used to differentiate between the 2 levels (the 2 different features) of the key assignment. The external repdial key must always be set for level-2 of the key button.

Feature Operation: Any time a feature key button is pressed the system will automatically activate the feature that is set to level-1. In order to use the external repdial feature on level-2, press the shift key first, then press the feature key button.

Programming Note: The external speed dial must be programmed as the level-2 feature. The level-1 feature can be any LED (Light Emitting Diode) supported feature on the base Optiset or the attached KEU module. The multilevel key programming is NOT supported on the 90 button Busy Lamp Field (BLF) module. Assistant E provides a new check box to program the level 1 or level 2 feature button. It is located at **Settings → Configure Station → Feature Key Programming**. Labels will print with both levels on each key except for the bottom key on each column, which will only print level 1.

Delta: This is a new feature and is not supported on R1.0 or R2.2 software versions.

3.2 Mobile PIN (a.k.a. Mobile Authorization)

What's New: The "Mobile PIN" feature allows a subscriber to use a remote (passive) phone in the 150 H system to make an internal or external call based upon the toll restriction COS entitlement of the subscriber's own (active) phone. The COS information is linked to the user's own station number and private PIN code. When "Mobile PIN" is activated at a remote phone, the subscriber overrides the remote telephone's COS. Any CDR information will reflect the station number that is linked to the subscriber and their private PIN number. The PIN number will not be printed on the CDR report.

Feature Operation: First, the subscriber must reprograms the private 6 digit PIN code at his/her assigned telephone (active) with the access of code *93. The default PIN code is "0 0 0 0 0 0" and must be changed to another code sequence. Now the subscriber may go to any phone in the system, dial *508 (Mobile PIN access code) + the home (active) station number +the new PIN code + the desired phone number. The call will be either allowed or restricted, based on that subscriber's normal COS. The feature can also be activated by means of the Optiset call service menu or by a Mobile PIN programmed key button.

As long as this feature is activated, the remote (passive) station cannot be reached by its actual station number. Do-not-disturb is activated on the remote phone.

Programming Note: No additional system programming is required.

Delta: This is a new feature and is not supported on R1.0 or R2.2 software versions.

3.3 Flexible Hunt Group Membership

What's New: Subscribers assigned to groups can join or leave specific or multiple groups as required. These groups may be hunt groups or ringing groups.

Feature Operation: By dialing #85 and the group call number, a subscriber can leave a hunt group. When the hunt group is called, the specific subscriber will not be alerted. By dialing *85 and the group call number, the subscriber can rejoin the hunt group. To leave all groups the access code is #85# and to rejoin all groups the code is *85*. Feature buttons are also available for activation and deactivation.

Programming Note: The subscriber must be an assigned member of a hunt group or ringing group in order to leave or rejoin that group. Assignments to hunt groups are the same as in previous releases of software.

Delta: This is a new feature and is not supported on R1.0 or R2.2 software versions.

3.4 Directory Enhancement

What's new: The internal directory now supports the display of system groups. This is necessary to dial MULAP groups from the directory.

Feature Operation: Press the internal directory key button and use the OptiGuide scroll keys to navigate and select the desired phone number to be dialed. The directory access code may also be used.

Programming Note: The option to show a call number in the internal directory is activated in 2 different programming areas. For standard stations the option is turned on in the **Settings → Setup Stations → Station → Param → Flags** screen. Activate the feature "Entry in Telephone Directory".

For MULAP groups, the option is activated in the screen for **Settings → Incoming Calls → Groups/Hunt Groups → Group**. Any group with an "X" showing in the "Tel. Directory" column will display in the OptiGuide internal directory. You may have to scroll the screen window to the far right to see this option. If you want only the MULAP to appear in the directory, then you will need to turn off the standard directory feature in the station features. Otherwise, they will both be visible.

Delta: This enhancement is not available in R1.0 or R2.2 versions of software.

3.5 Attendant P

What's new: The BLF screen in Attendant P now displays station numbers or names. There is a maximum of 240 buttons for the BLF. At 800 x 600 screen resolution, the BLF will display 4 screens of 60 buttons each. At 1024 x 768, the BLF will display 2 screens of 120 each. Station busy indications may be color coded for internal or external destinations. The BLF will also display the busy status of S0 devices.

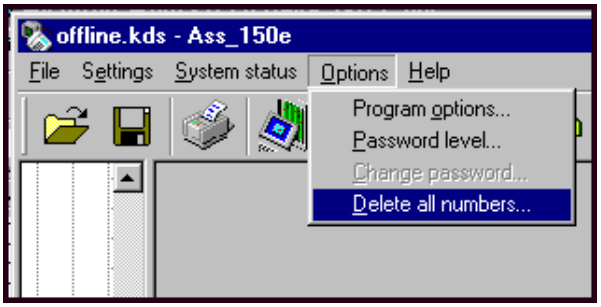
Delta: These new features are not available in previous releases of Attendant P.

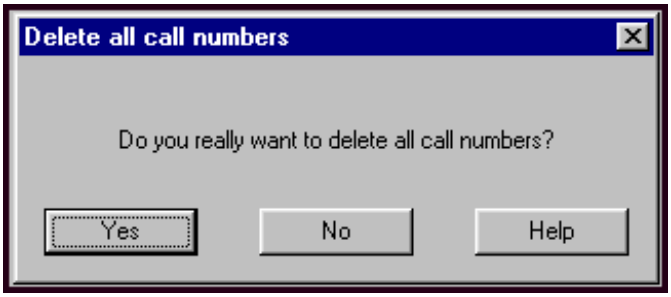
4 System Features

4.1 Delete All System Call Numbers

What's new: As a programming aid to simplify non standard numbering plans, a new feature to delete all call numbers has been added. This feature will delete call numbers and DID numbers of all stations and hunt groups, trunk service codes, trunk group route codes, modem numbers, and the internal attendant code of 0. This will not delete the substitution codes for * and #, service access codes or the access code of 9 for trunk group 1.

Programming Note: To delete all system call numbers use the menu path **Options → Delete all numbers**. Then a confirmation dialogue box will appear and you should click on next. Remember, there is not an "undo" feature. If you delete the call numbers by accident, the only way to get them back is to close the KDS without saving the database.





Delta: This feature is not available in R1.0 or R2.2 versions of Assistant E.

4.2 Freeze Trace

What's new: It's now possible for an Optiset to dial an access code and stop, or freeze, a call processing trace that has been started by the service center, in order to isolate a specific event.

Feature Operation: In general, the trace is started by development, the SSSC, or on-site personnel. The real time call processing data enters and exits a small buffer on a FIFO (First In, First Out) basis. When the specific event occurs, a party on site can freeze the information in the buffer by dialing the freeze trace access code of *509. With the trace stopped, the buffer information can be retrieved by service support personnel.

Programming Note: The access code *509 is the default access code.

Delta: This feature is not available in R1.0 or R2.2 Hicom 150 E operating systems.

4.3 Open Interfaces for TAPI and CSTA

What's new: V1.0 now supports the 1st Party TAPI expansion to display the forwarded-to call number of a called subscriber if call forwarding is active. This is provided from the addition of 2 new parameters of redirect information, the redirected party name and number.

The system also supports 3rd party CTI (Computer Telephony Integration) applications that are phase II and phase III CSTA compliant. A PC based software telephone is a good example of a 3rd party CTI application.

Feature Operation: The Optiset display will now show the "Called Party Number" to be the destination number instead of the dialed number. This allows the TAPI application to know both dialed and destination numbers and react as programmed.

Programming Note: This feature requires Windows 2000™ and the version 3 TAPI drivers.

4.4 Multiple Line Appearances (MULAP)

What's new: It's all new. Multiple line appearances allow a subscriber's extension to appear on another Optiset's key button as a line appearance. That line appearance (MULAP) has a call number that is unique to the specific subscriber. When that MULAP's call number is dialed, every Optiset with that MULAP appearance will be signaled. It will be signaled visually with the LED and optionally with an audible ring. As an added note, each Optiset that has a specific MULAP as an appearance is considered to be in a group of that MULAP. Therefore, a MULAP group has a specific call number and has 1 or more Optisets assigned to it.

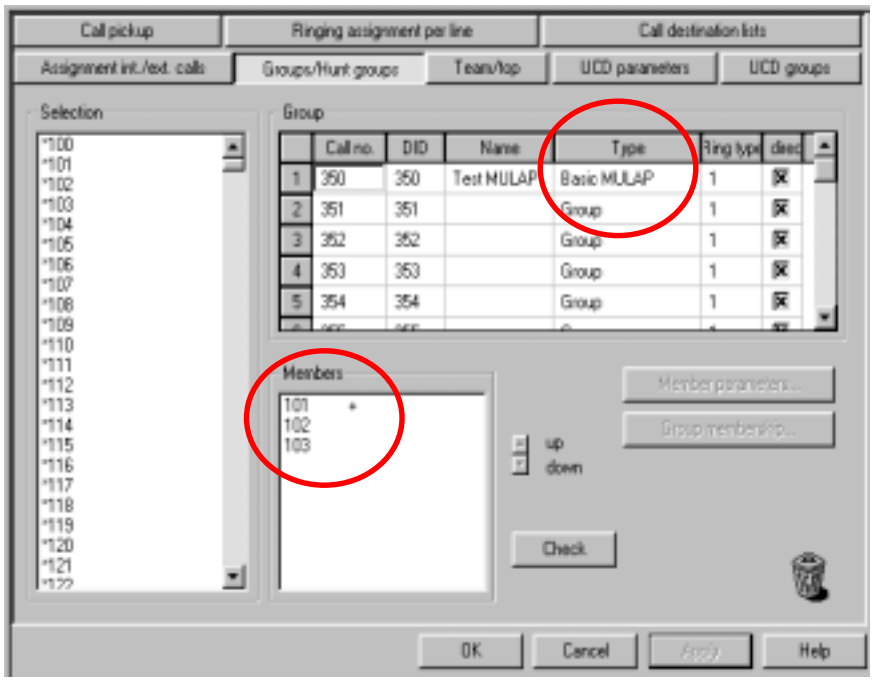
Programming Note: All MULAP groups are programmed in the **Incoming Calls → Groups/Hunt Groups** or the **Incoming Calls → Team/Top** screen of Assistant E. Some previous versions of Assistant E called this the "Call Management" screen.

A MULAP group can be created and assigned in 3 different ways. It can be created as an individual basic group for simple applications. A MULAP group can be assigned as a "team" for those situation where each member of the team must have the line appearances of all other team members on their phone. Lastly, a MULAP group can be assigned as a "top" which is the replacement programming for the "Executive/Secretary group". Under normal conditions, only members of the "top" group are allowed to directly call the executive member.

The overall concept of assigning a MULAP is a 3 step logical process.

1. Create a MULAP basic group, team, or top.
2. Assign specific Optisets to the group or team.
3. Assign that specific MULAP group key appearance on each Optiset in the group. A phone must be in the MULAP group to have a button appearance of that MULAP group.

1: As a basic MULAP:



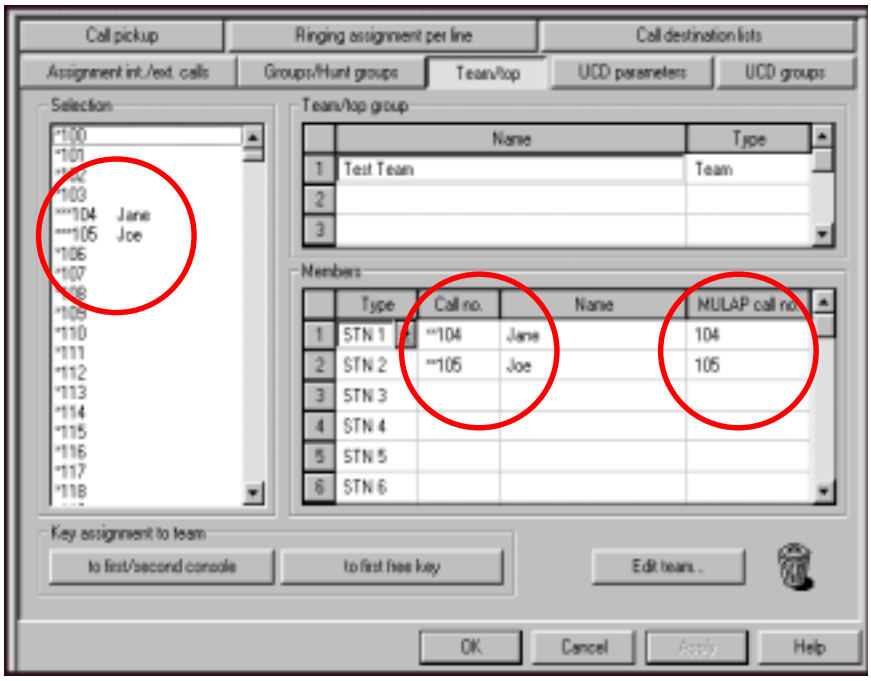
The "basic" MULAP is created "manually" in the **Incoming Calls → Groups/Hunt Groups** screen. This is very much like assigning a hunt group except that the group type is set as **Basic MULAP**. Then each Optiset device that will have a MULAP appearance can be dragged or double-clicked into the basic MULAP group. Then the MULAP appearance key button must be assigned on each Optiset.

This presents a couple of challenges. First off, The call number of the MULAP group is in the 350 to 499 numbering plan range. It is not in the 100 to 349 range that the customer may currently be using. Ok, so you just change the numbers, right? It is possible to change the call numbers of the basic MULAP group to the normal station number. However, you must now change the call numbers of the stations to something else. You can't just delete them. You'll need those station call numbers when you try to add the MULAP key to an Optiset. In the **Setup Station → Key Programming** screen the only stations that appear as valid station hardware are those with call numbers. Even if you don't need them.

In this example, a basic MULAP group has been created and stations 101, 102, and 103 are members of that group. The plus sign (+) by station 101 in the "Members" window shows that 101 is the master member of the group. The master flag is only significant to certain features. The most significant of these is message waiting. Message waiting will be signaled only to the master member of a MULAP group. In this example, if you were the primary owner of this MULAP with a call number of 350, then you would be the master member.

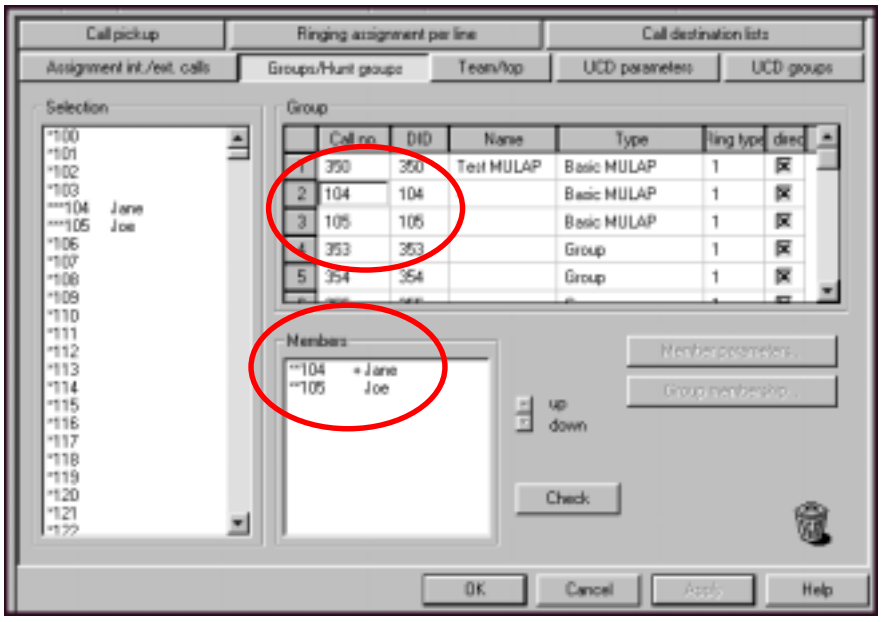
Also an (x) in the "Telephone Directory" Column indicates that the MULAP call number will be included in the system's internal directory that is available through the OptiGuide or feature button.

2. As a MULAP team:



This is an alternative to the basic MULAP but with a unique twist that circumvents the numbering plan challenges that are posed by basic MULAP programming. For this type of assignment you must navigate to the **Incoming Calls → Team/Top** screen. In the "Team/Top Group" window, assign the name of the Team with a group type of "Team". From the "Selection" window, drag or double-click the stations that will be a member of the group. For this example I have added Jane, 104 and Joe,105 to the group.

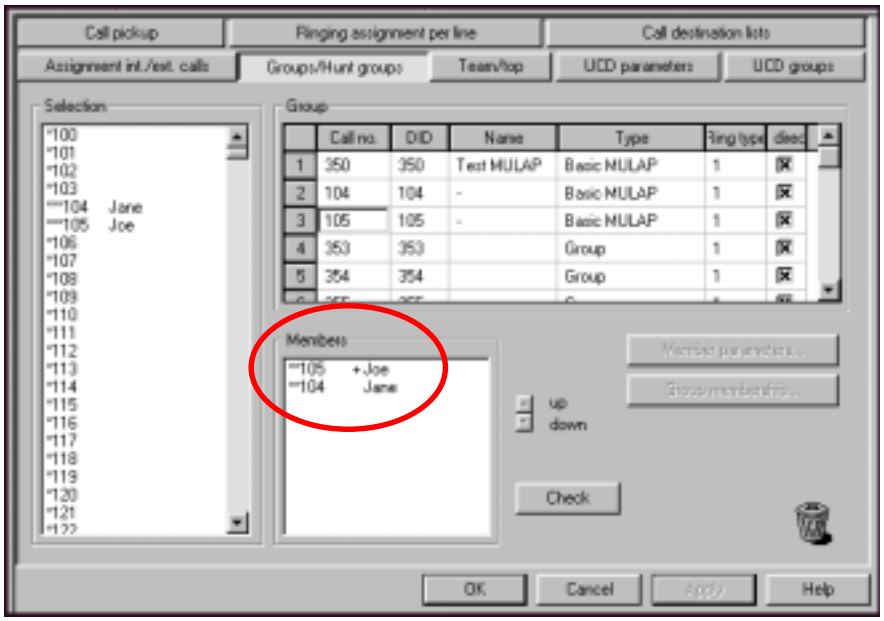
Notice what happens to the station numbers after they are added to the team group. The call number of each station added to the team, is now preceded by double stars (**). In the example you will see three stars in the "Selection" window because this is an offline database and the 3rd star indicates that the station is not active. Also notice that the MULAP call number in the "Members" window, above, is now the same number of what the original Optiset device call number used to be, 104 and 105.



Now, if you look back at the hunt groups screen at the right, you'll see something really special. The call numbers of the next available hunt groups, 351 and 352 for this example, were changed to Jane's and Joe's personal call number 104 and 105. In this screen shot, Group-2 is selected and we see in the "Selection" window that **104 belongs to Jane. In the "Members window, you can see that Jane is the

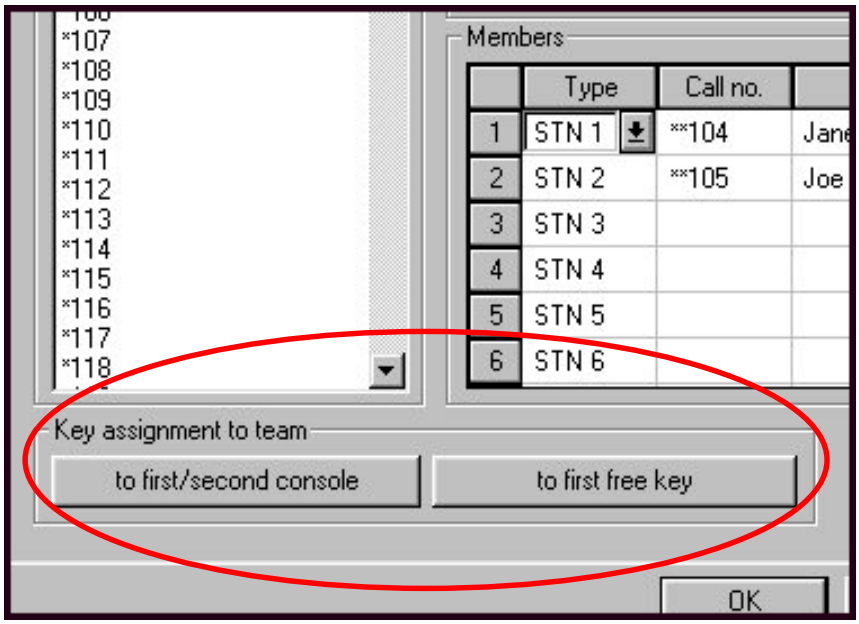
master member of this group because of the plus sign (+) by her name. Remember, this means that if you send a message waiting to 104, then only Jane will receive the message waiting indication.

If you were to select group-3 (105), as on the right, then the "Members" window will reflect that Joe is the master member of that group.



When assigning MULAPs as a team, most of the renumbering work is done for you. Another nice feature of team assignments is the actual key assignments to the Optisets. Keep in mind, however, that these key assignments are team based. When you click on either one of the key assignment buttons, all Optisets on the team receive all MULAP keys on the team. The previous examples show Jane and Joe to be on a MULAP team. When the MULAP key buttons are automatically assigned, Jane will have her own MULAP as well as Joe's. Joe will also have both MULAPs. In addition, each member of the team will automatically receive a DSS (Internal Repdial) key for all other team members. When assigned as "First/Second Console" a "Leave/Join Hunt Group" key will also be assigned.

As the "Key assignment to team" buttons imply there are two ways to assign the MULAP keys on the Optisets.



- **To first/second console:** This will assign the MULAPs to the 1st or 2nd KEU as in the following table. Keys will not be assigned to the base Optiset. This example reflects a team with members 104, 105, 106 and 107. The tables represent the 4, 2-column KEUs that that had all vacant keys to start with.

KEU for 104	
MULAP 104	Leave/Join HG
MULAP 105	DSS to 105
MULAP 106	DSS to 106
MULAP 107	DSS to 107

KEU for 105	
MULAP 105	Leave/Join HG
MULAP 104	DSS to 104
MULAP 106	DSS to 106
MULAP 107	DSS to 107

KEU for 106	
MULAP 106	Leave/Join HG
MULAP 104	DSS to 104
MULAP 105	DSS to 105
MULAP 107	DSS to 107

KEU for 107	
MULAP 107	Leave/Join HG
MULAP 104	DSS to 104
MULAP 105	DSS to 105
MULAP 106	DSS to 106

- **To first free key:** This will assign the MULAPs to the 1st free (vacant) key available on either the Optiset or any attached KEU. The tables represent the 8 feature keys in the right column on the 4 Optisets. If the base Optisets already have keys assigned, then the MULAP keys will be assigned to the KEU if one exists.

STN 104
MULAP 104
MULAP 105
DSS to 105
MULAP 106
DSS to 106
MULAP 107
DSS to 107
Release

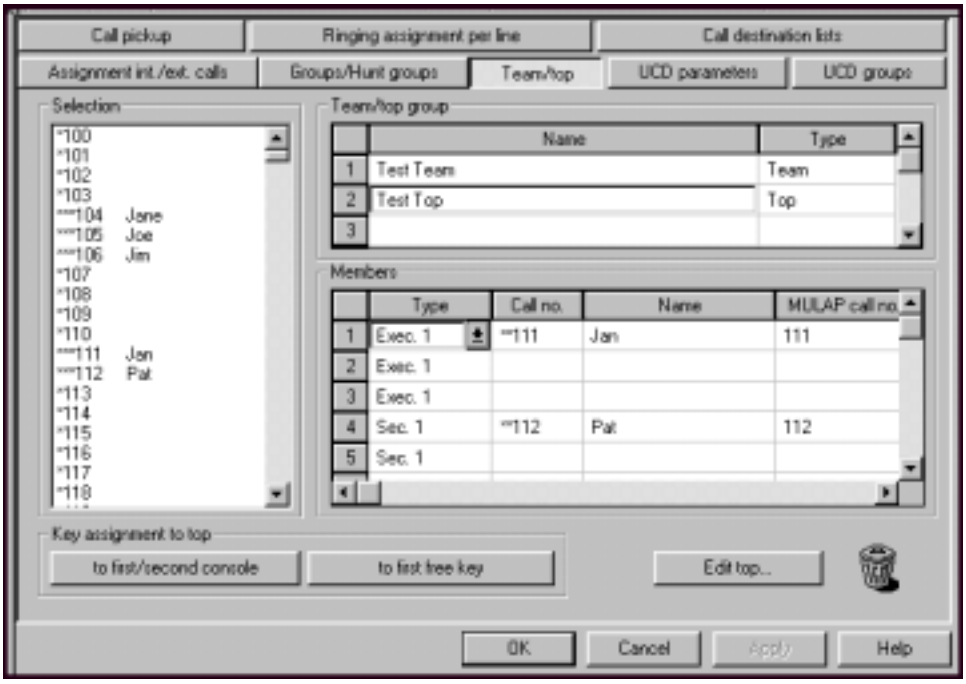
STN 105
MULAP 105
MULAP 104
DSS to 104
MULAP 106
DSS to 106
MULAP 107
DSS to 107
Release

STN 106
MULAP 106
MULAP 104
DSS to 104
MULAP 105
DSS to 105
MULAP 107
DSS to 107
Release

STN 107
MULAP 107
MULAP 104
DSS to 104
MULAP 105
DSS to 105
MULAP 106
DSS to 106
Release

3: As a "Top" Team:

The assignment of a "Top" team is, in general, the assignment of what was previously known as "Executive / Secretary Groups". By looking at the screen capture below, you should be able to see that the executive and secretary nomenclature is still in use with the actual group members. In the example, you see that Jan and Pat, extensions 111 and 112, have been added as a Top team. Jan is the executive and Pat is the secretary. Just as a MULAP team, the original station numbers have been changed to **111 and **112. The call numbers are now 111 and 112.

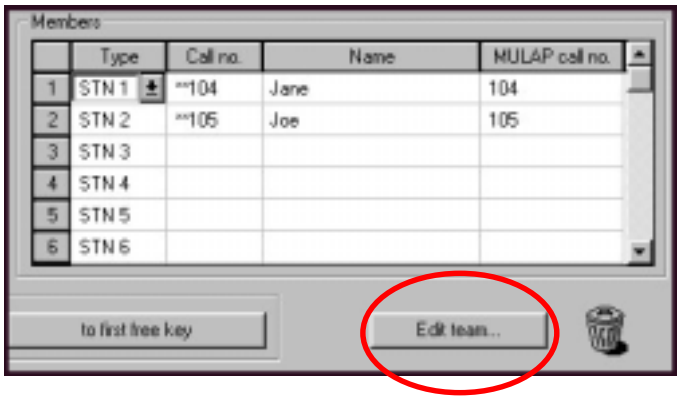


This Top group takes on the same properties of previous the release's executive/secretary groups in that only the team members are allowed to directly call the executive. In addition the automatic key assignment buttons will assign the Top specific feature keys like the Ring Transfer and DSS.

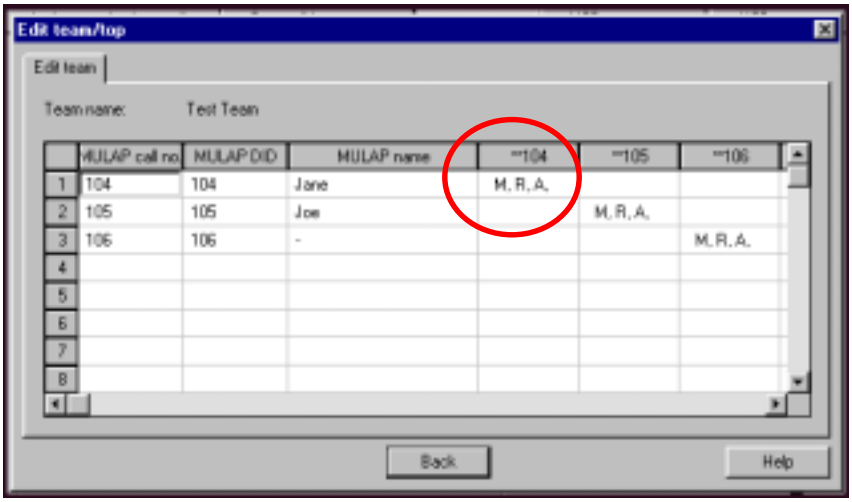
Recap: Ok, now you know the 3 ways to create and assign MULAPs. First, as a basic MULAP, then as a Team and finally as a Top. Each method has its own unique characteristics. Its up to you as to how you apply them to your specific customer database. But this is only the basic assignment of the MULAPs. If you need to "fine tune" any of the MULAP appearances, follow the guidelines in the next section, "Editing the Team".

Editing the Team:

When you are in the "Team/Top" screen there is one more button that you need to be familiar with. That button is the "Edit Team…" button. If you're making an executive / secretary group then the button will be labeled as "Edit Top…".



By clicking on this edit button you can set certain parameters of the MULAP such as the master status, ringer on or off, and incoming / outgoing seizure information.

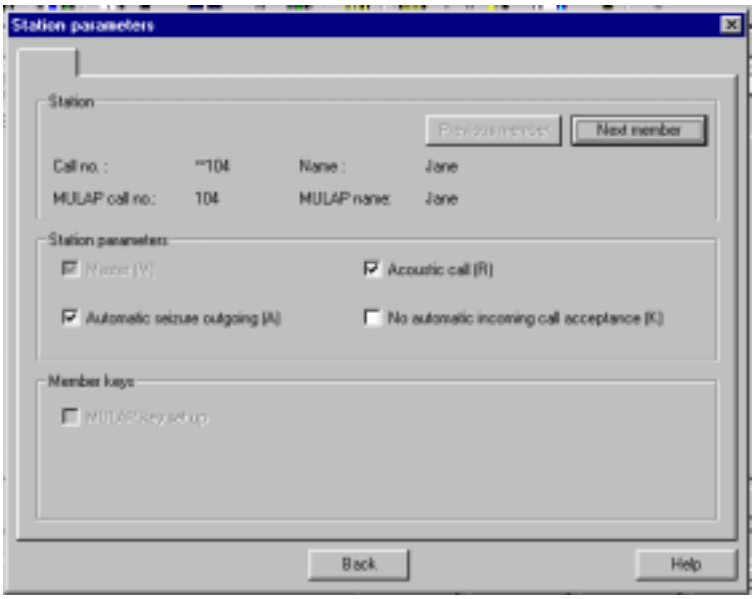


The edit button will bring you to this particular screen. This information is valid only for the 1 team that you have selected. In this example you see the team of Jane and Joe and another unnamed member with extension 106. Notice that the MULAP also has a DID number assigned. This was part of the automatic renumbering of the team assignment. If you were to look back at the station screen, you would see that the DID numbers have been removed for all newly created MULAPs. It is also possible to change the name of the MULAP in this window.

There is some other information on this screen that you may have noticed. For the team there are columns identified by the call number of the physical Optiset. You can tell that it's the physical Optiset by the fact that the call number is preceded by the (**). Ok, how does this work? As an example for one key appearance, look a the column for **104. This is Jane's actual Optiset device. On this Optiset, appear the MULAPs of Jane (104) and of the other team members, 105 and 106. The square at the intersection of the row for MULAP 104 and the **104 column will identify the operating parameters of the individual MULAP key on that Optiset. In this case, that key is identified as the (M)aster, the button will (R)ing, and that line will be seized

(A)utomatically for outgoing. What if you want to change these parameters? Double click on the square and you will see another window like the one on below.

In this screen you can change the parameters as required. If you turn off the "Automatic Seizure Outgoing" then the user will be forced to select an outgoing key before dialing. If you turn off "Acoustic Call" then the line will not ring when called. By default the feature "No Automatic incoming call acceptance" is turned off. This means that if this line receives an incoming call the line will be answered if the handset is lifted. If you want the user to first select the line key in order to answer the call, then turn this feature on by clicking a check mark in the box. Remember it this way… No check mark is automatic.



The other MULAP appearances on the same Optiset can be set as desired just like this line was. The "Next Member" and "Previous Member" buttons will advance and return to the other Optisets while the programming is for the same MULAP.

Additional MULAP Information:

MULAP related maximums:

Description	Point	Com	Pro
Maximum BASIC MULAP groups in the system	10	50	150
Maximum device members per BASIC MULAP Group	8	20	20
Maximum device members per MULAP Team	8	10	10

A MULAP cannot be a member of a "Ringing group" or a "UCD group".

If a MULAP is a member of a hunt group, and all member devices are set for no ringing, the MULAP will be removed from the hunt group.

A MULAP must be forwarded with the "Forward Line" feature. The default access code is set in the system as *501 to activate forwarding an #501 to deactivate forwarding.

A MULAP team can have only one master per Optiset. It cannot be changed The only way to have multiple master MULAPs on one Optiset is to assign the appearances as basic MULAPs

and reset the master statuses manually. This is done in the **Groups / Hunt groups** screen with the button “Member parameters”. Remember, in this case the call numbers will also have to be changed manually.

By default every station device is programmed to be included in the internal directory. When the MULAP is assigned you would typically want the MULAP to be in the directory and not the physical device. Especially if the device call number has been changed to "**something". To remove the call number of the device make sure you go to the screen, **Setup stations → Station → Param** and disable (uncheck) the feature “Entry in telephone directory”.

When a MULAP is assigned by the team method, more than just the call numbers are changed. Following is a list of other system references that are reassigned in the process. This will apply to upgrades as well as new installations. **Important: These changes are NOT canceled if a team or a member of a team is deleted.**

- destinations of call forwarding keys and call forwarding MULAP keys
- destinations of call number keys
- destinations of night service keys
- destinations of send info keys
- call assignment of MSI lines
- call diversion destinations (Call Management)
- intercept position day/night
- destination door phone of door systems
- members of a hunt group

A short, low volume, notification ring is available to Optisets when a call rings in while a MULAP on that phone is busy. The normal ring cadence may also be used. Use the path **Settings → System Parameters → System Settings → Advisory Call** to make this change.

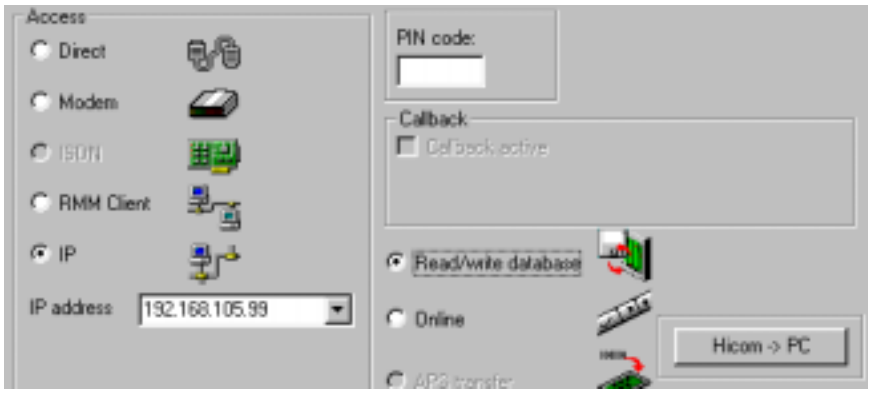
When a call on a MULAP is placed on hold, 1 of 2 things can happen. If the call is placed on hold on a basic or team MULAP, and the user goes on-hook, then the call is on common hold. The call may be picked up on another phone by pressing that subscriber's MULAP key. If the user places the call on hold from a top MULAP, then goes on-hook, then the call is on exclusive hold and can be picked up only by the party that placed it on hold.

Delta: MULAPs are new for R3.0 and not available in R1.0 or R2.2 Hicom 150 E software versions.

5 Service And Administration

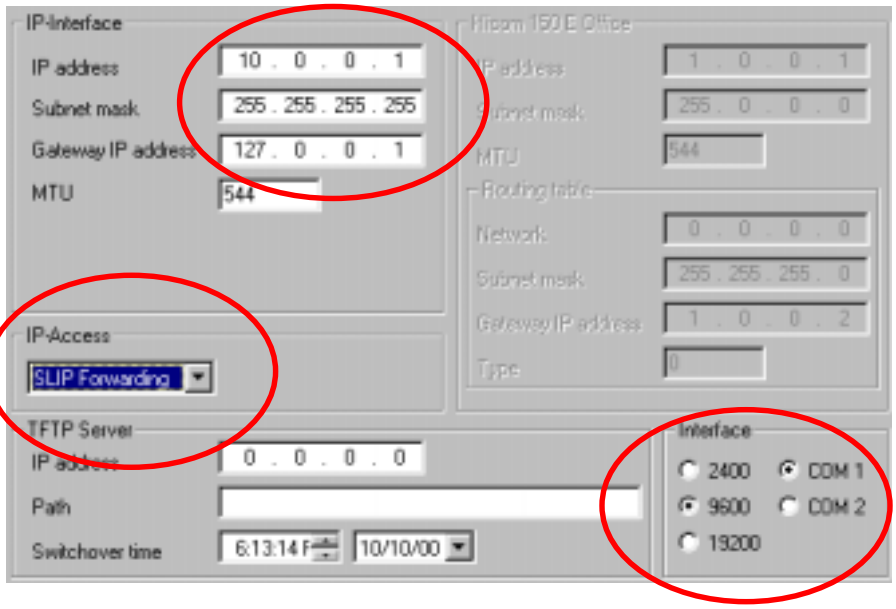
5.1 LAN Based 150 H Administration

What's new: Upload and download the 150 H KDS file over the LAN? Its new for V1.0. Whether you connect the 150 H to the LAN with the V.24E or the HG 1500 hardware, you can communicate with the 150 H over with your PC on the network. You still have to have Assistant E installed on the PC, but you're no longer required to be tethered to the switch with the V.24 serial cable. There is some setup required, however.



Feature Operation: When uploading and downloading the KDS using TCP/IP protocol over the LAN, you only need to identify the system by IP instead of "Direct". The 150 H will have its own IP address.

Programming Note: As previously mentioned there are 2 ways to connect to the LAN. With the V.24E ComServer or with the HG 1500 cards. We'll start with the V.24E card.

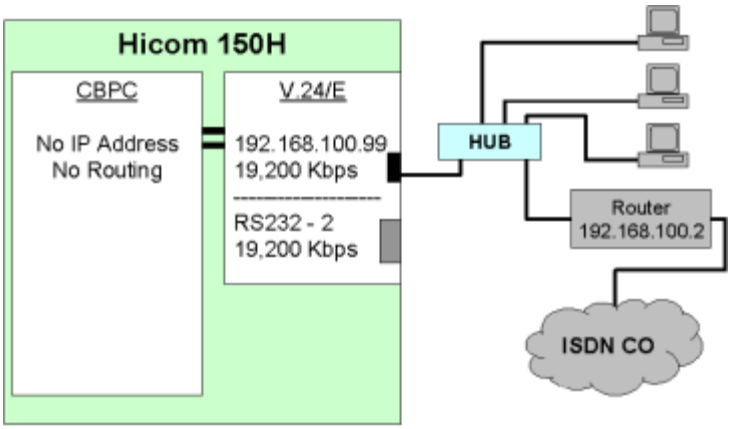


V.24E: The V.24E is actually a System to SLIP (Serial Line Internet Protocol) converter. The V.24E takes the place of the old V.24 card so the 150 just plugs right in and communicates with the card. The card, however, connects directly with the LAN over the system's "serial port" 1 and communicates with the LAN using IP. The V.24E is restricted to a maximum serial speed of 19.2 Kbps. Program its operation by activating the "SLIP Forwarding" IP access and assigning the proper IP information. Above is a screen shot of the default data from the **Settings → Network.. → IP Address** screen.

Notice that the default information provides for an IP address of 10.0.0.1 and an Interface speed of 9600 bps. The subnet mask is set for 255.255.255.255 and must be changed to match that of the customer's network. The "Gateway IP address", 127.0.0.1 is a default "local host" IP and can be left alone if no external router is used. The MTU (Maximum Transmit Units) can also be left as default.

Here's a screen shot of a sample customer database. Remember this is only an example. An actual system will be tailored to the customer's requirements. The IP address that this customer has chosen is a Class-C address of 192.168.105.99 and the subnet mask will be 255.255.255.0. Of course you'll want to set the interface for the maximum speed of 19.2 Kbps.

Now the V.24E will respond to the IP address of 192.168.105.99 over the RJ45 LAN port. The following illustration shows how the SLIP Forwarding is incorporated into a network.



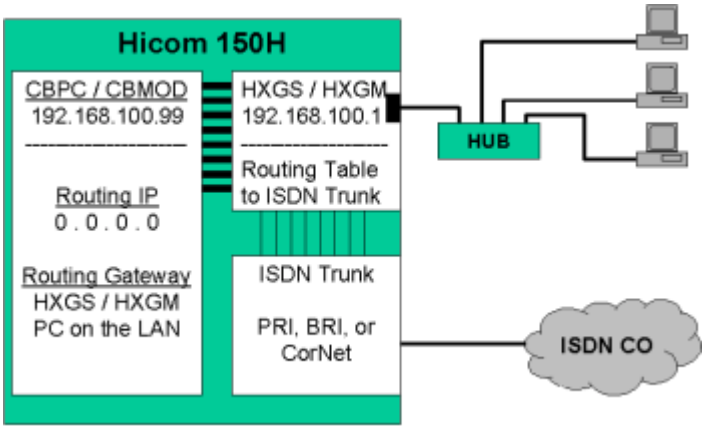
Note how the IP address is actually assigned to the V.24E card. When connected to the network, it forwards all data transmitted to that IP to the system. Since the link from the V.24E to the CBPC is the same as the old dual serial card, it's speed is still only a maximum of 19.2 Kbps. Note that all IP addresses shown are only examples and will vary with your customer's installation.

HG 1500 hardware: Now we can get into some high speed networking. By using the HG 1500 hardware the 150 H can be connected to the LAN using 10/100 Fast Ethernet technology. No more 19.2 Kbps speed limit. The method that the 150 H uses is called HIP Forwarding. HIP stands for Hicom Internet Protocol. This will allow a setup that can utilize the routing table that is built into the HG 1500 hardware, the HXGM and HXGS cards. Even with that, there is an available assignment in the 150 H for one routing IP address. This can be used to send all remote IP address calls to either the HXG card or to an external router. This will be illustrated shortly.

This would be a good time to mention that this document will not delve into the programming of the HG 1500. I can say that this 150 H programming requires that the HXG card already be installed and programmed and you will need to know the following information.

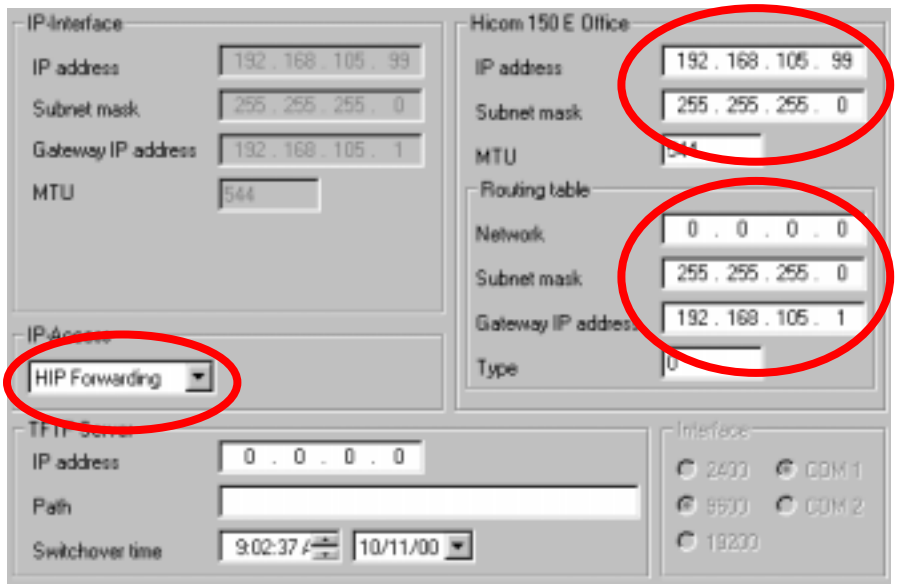
- The IP address that will be assigned to the 150 H (customer provided)
- The "LAN interface" IP address of the HXG card that is already programmed
- The IP address of the external ISDN router if used by the customer

If you're interested in learning how to install and program the HG 1500, there is a Siemens course available. Look on the Siemens ICN Education on-line registration for more information on the "HG 1500 Installation and Maintenance" course, code TE95.

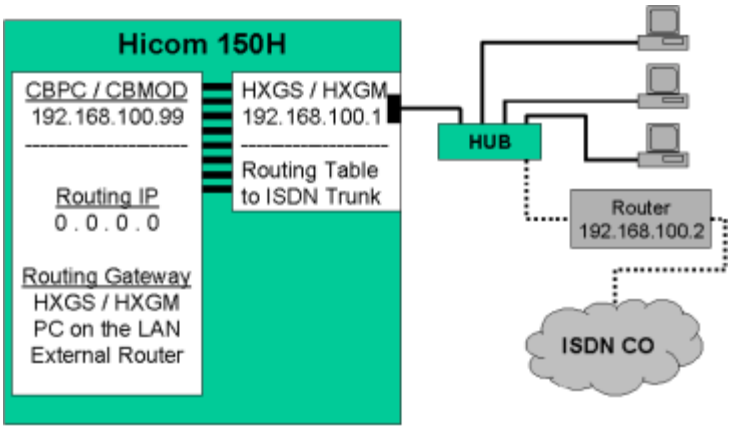


This illustration shows the first layout that will be programmed. The 150 H has its own ISDN trunks and does not rely on an external ISDN router. The 150 H IP is 192.168.105.99. The HXG LAN IP is 192.168.105.1. This will be the gateway for the 150 H. The routing IP of the 150 H is 0.0.0.0. This allows the routing of any IP call that is not on the local network. These calls will go to the gateway that is the HXG card and will utilize that routing table to determine how the IP call will get to its intended remote destination, whether it be over ISDN or an external router on the LAN.

The box heading of "Hicom 150 E Office" indicates the area for the IP and subnet mask of the switch. The box heading of "Routing Table indicates the area for the routing and gateway information. Notice that the gateway is the IP address of the HXG card on the LAN. As previously mentioned, this will allow any IP calls by the switch to be sent out over ISDN. This could include system error messages, status messages, and CDR over IP.



Maybe your customer is not using 150 H internal ISDN trunks but, instead, using an external router to place the ISDN calls over their own lines. In this case you would change the "Gateway



IP Address" to reflect that of the external router. This illustration shows the typical layout. Again, remember that the IP information is only an example.

There is one other item that needs to be mentioned. To upload and download the customer database KDS file, use the IP access in the transfer screen and use the IP address assigned to the Hicom 150 H.

Delta: This feature is not available in R1.0 or R2.2 software versions.

5.2 SNMP Administration

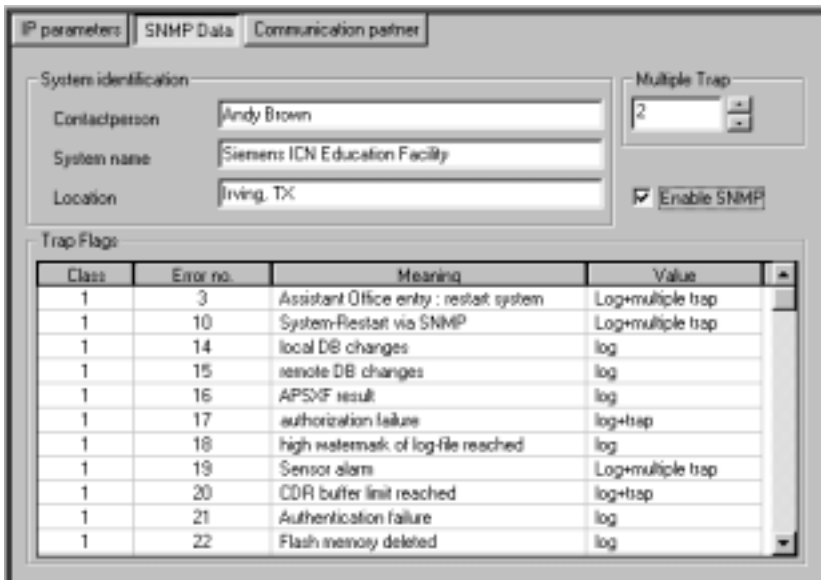
What's new: SNMP… Simple Network Management Protocol. A standardized protocol that is used to access and administer servers, routers, bridges, hubs, and other network devices. In the 150 H it is used to allow the transfer of critical system information to an administrative server running 3rd party software such as HP® Openview™. This allows an administrator to request status information or to review information that was sent automatically by the 150 H system. This type of setup designates the administration server side as the manager and the 150 H side as the agent.

Examples of the type of status information include, but are not limited to, error history, early warning error trap alerts, system-up time, authentication failures, CDR thresholds, and APS transfer results. The administrator can also perform certain functions such as system restarts, delete log and CDR buffers, upload and download the KDS, and set the system time and date. It should be noted that the actual transfer of complete files falls under the heading of another kind of protocol known as TFTP, Trivial File Transfer Protocol. The request for that file, however, was sent by SNMP.

There is also a provision for a firewall to allow specific IP address to access certain areas of administration such as APS transfers, KDS downloads, CDR data, Assistant E access, and Telnet access.

Programming Note: First off, the programming of SNMP administration requires that the 150 H already has access to the LAN with either the V.24E module or with the HG 1500 hardware. Secondly, we'll start with the programming to send SNMP error traps to an administration manager server.

This illustration shows the areas of programming that must be assigned. The first thing to do is to activate or "Enable SNMP" by placing a check mark in the box provided.



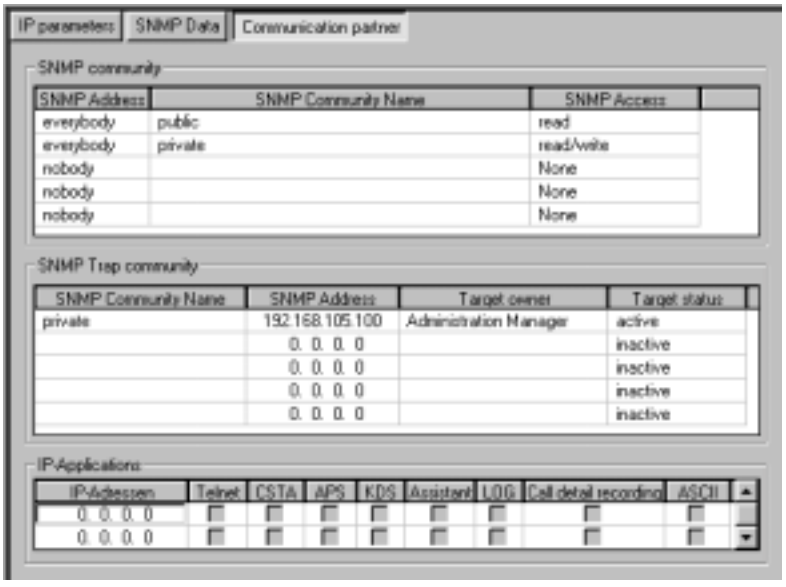
The "System Identification" box contains the plain text information about the 150 H site. You can even add a phone number in this area if desired. The contact person is usually the customer's communications manager of the site.

The "multiple trap" assignment should be considered since part of the SNMP protocol does not require any message receipt confirmation. If the trap information IP packet never makes it to its destination, there is no way for the 150 H to know this. Therefore it's a prudent move to enable multiple traps so that the message will be sent more than once as a precaution.

The "Trap Flags" are preset to automatically log an entry in the error history and this cannot be turned off. There are two other options that will allow a trap to be sent in addition to the log entry. One option is to send a single trap and the other is to send multiple traps. Multiple traps will, of course, use the multiple trap quantity previously assigned.

In the example screen above, you see certain action items turned on to send SNMP traps. These were chosen only as examples and your customer will most assuredly require something different. Now that we have enabled the traps, we must tell the system how to get the SNMP information to the proper destination.

In the example at the right, you can see that the re are two default "communities". These communities dictate the general read only or read/write privileges of any parties with access. It is typical to see the public and private communities in a lot of default SNMP applications. These may be changed as required or new communities may be added. The communities may be assigned as "everybody", "nobody", or may also be IP specific.



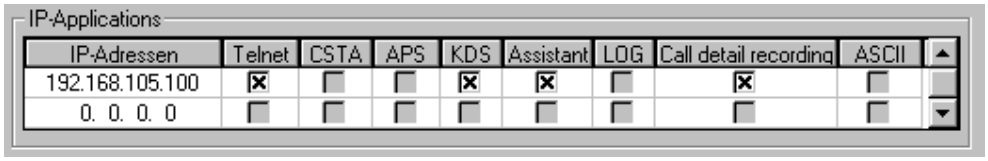
The "SNMP Trap Community" must be a community that is already assigned in the top table. This entry is case sensitive. This is the community that will determine the rights of the trap administrator. In the example, you see that the administration manager has the IP address of 192.168.105.100. and the "target status" is active. This is the destination IP that will receive and process any SNMP traps that occur in this 150 H system.

Normally, the customer will have the administration management software to perform all these functions. When you install these features you may be required to test your applications with an SNMP utility installed on your service PC and connected to the LAN. This utility must monitor UDP port 162 and watch for SNMP traps that occur on the network. There is a variety of these utilities on the internet. There are no specific recommendations but one that is available is the "SNMP Trap Watcher" from BTT Software® (web site unknown).

Now that your customer can send SNMP traps to an administrator they may want to also allow the administrator to perform certain IP based applications. These applications may include downloading the KDS file, CDR buffer, administration log file, the ASCII hardware map, or even use Telnet as an Assistant T device. All this over the network using TCP/IP and the protocol that I mentioned previously, TFTP.

The "IP applications" box is the area in which this is programmed. In the screen shown above the "IP applications" box is default. In its default state all users have Assistant E access to the system. Even though all the check boxes, including "Assistant" are left blank, this function is available. This is only a temporary measure if the IP applications will be used. As soon as any one or several of the other boxes are checked, the "Assistant" E access will be disabled unless it is also checked. Just an important FYI (For Your Information).

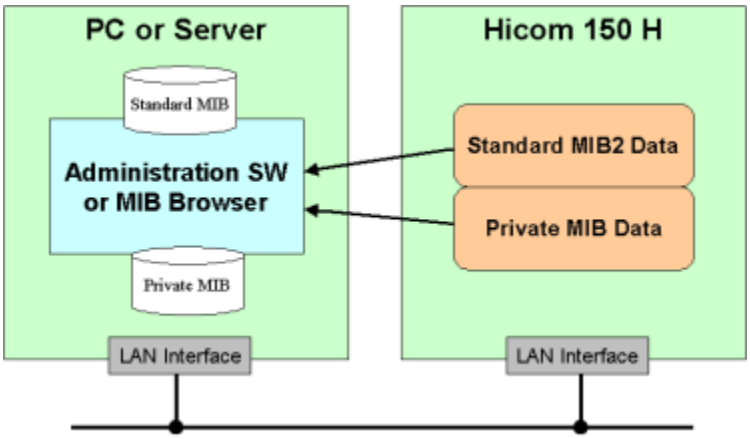
In the following screen shot you can see that we have allowed the administration manager at 192.168.105.100 to have access to Telnet, KDS download with TFTP, CDR, and Assistant E access.



KDS download with TFTP? Why not just use Assistant E? Here is one of those special functions of the 3rd party administration software. The manager can send a TFTP request for the KDS file and transfer the database to the server without Assistant E. There are TFTP client/server tools available on the internet to test this and other similar functions. A 30 day demo application of TFTP Turbo™ is available from Weird Solutions® at www.weird-solutions.com . These applications have specific file names in the150 H.

- KDS over TFTP hicom.kds
- CDR call data gel.txt
- Administration log file log.arc
- System HW map ascii.txt
- 150 APS file [filename].fli (upload to system only)

These SNMP and TFTP commands can be important for testing purposes with the SNMP, TFTP monitoring software. The 3rd party administration software will have all of these commands built in or will have access to special Siemens script files called "private MIB files" to accomplish these special tasks. There is another test tool that I haven't mentioned yet. Its called a MIB browser. MIB is an acronym for "Management Information Base". It uses these MIB files or script files to read and write certain data information to the switch over the network with TCP/IP protocol. One popular MIB browser is from AdventNet® (www.adventnet.com).



This illustration shows the typical usage of MIB files. The industry standard and private (Siemens) MIB files are installed on the server or MIB browser. These script files are used to interrogate and command the 150 H system as required.

Delta: This feature is not available in R1.0 or R2.2 versions of software.

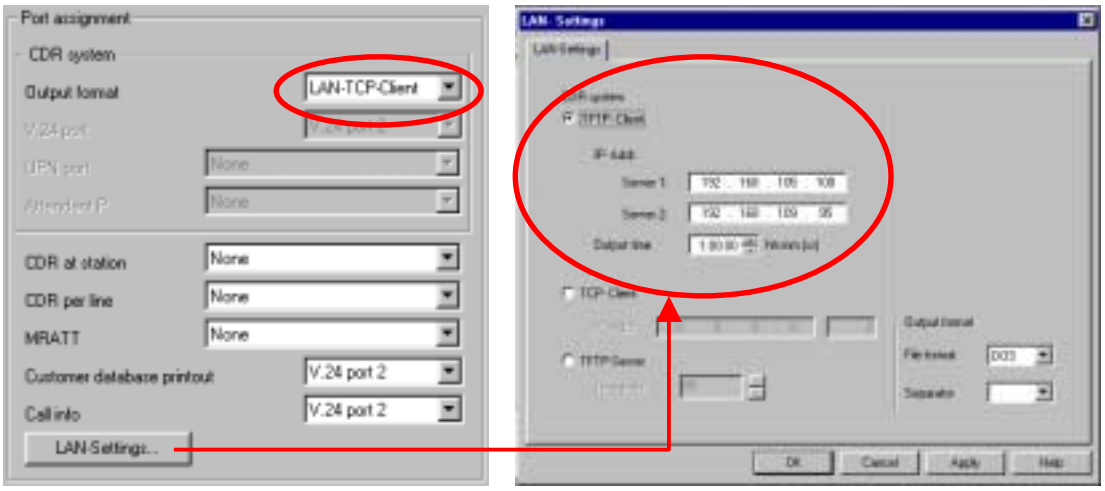
5.3 CDR over IP

What's New: CDR information can now be transmitted from the system to a server over the LAN with TCP/ IP protocol. This will allow CDR to be collected by a LAN based server.

Programming Note: There are three possible delivery methods for the CDR over IP. Each relies on a server / client relationship. Depending on which of the 3 delivery methods is used, The 150H may be the client or it may be the server. The CDR data will be sent over the LAN to an administrator PC which may be designated as a client or server. This administrator PC will typically be running a software application to collect, store, and report the CDR information. Two such applications that are available are the HP® Openview™ and IBM® Tivoli™. It is also possible to utilize certain TFTP (Trivial File Transfer Protocol) test tools on a PC to verify that the CDR over IP programming on the 150 H is operating properly.

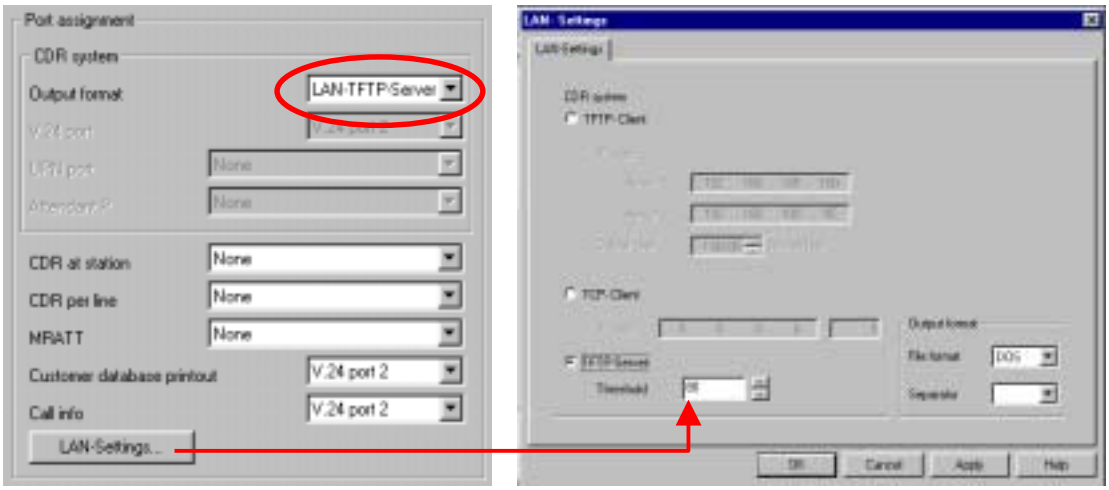
Two of the options are based on the TFTP protocol. This protocol is a very simple means of communications. The information is sent using UDP (Universal Datagram Protocol) packets over IP. UDP port 69 is used for this purpose.

LAN-TFTP Client: This choice assigns the 150 H as the TFTP client. Call charge data is sent to an external application server by the switch. Transmission is controlled by a timer. A connection to the TFTP server is set up at the appropriate time. All existing call charge data is transmitted in a file and the connection is then terminated. If the server connection cannot be set up, an alternative server may be addressed. Each data transfer session is actually sending an ASCII text file that contains the CDR information. A new file name is used for each transmit session. The IP addresses of both primary and alternate servers and the timer can be configured here. The UDP port is fixed as port 69 and cannot be changed.



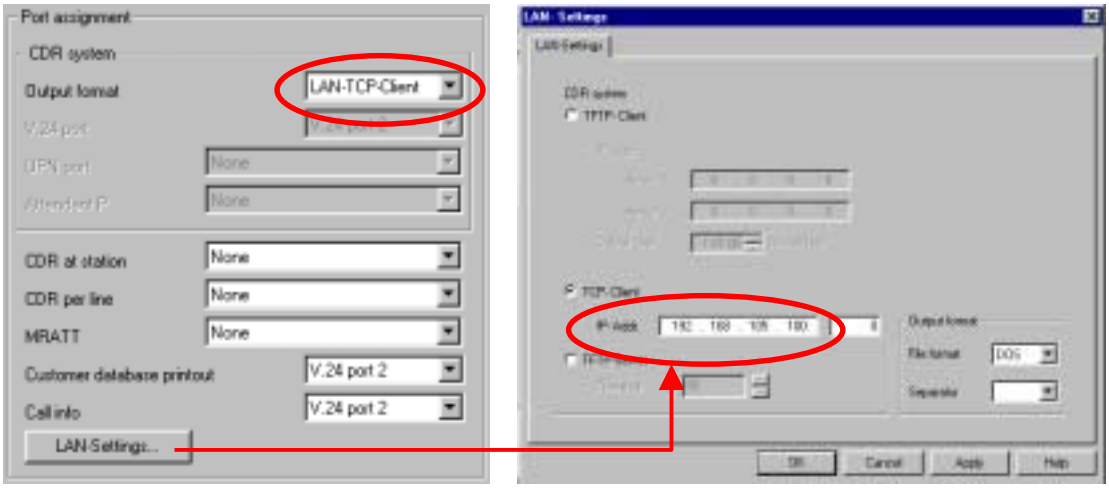
This illustrates the programming as a LAN-TFTP Client to send data to 2 different servers each hour

LAN-TFTP Server: This choice assigns the 150 H as the TFTP server. The remote application requests the output of call charge data from the 150 H. In order to do this, the remote application must set up an SNMP connection and request the call charge data. All existing call charge data is then transmitted as an ASCII text file and the connection is terminated. The application can request the call charge data either independently or when triggered by an SNMP trap, a signal from the 150 H that the CDR buffer threshold has been reached. The actual threshold of the buffer is defined in the LAN settings screen below. The IP addresses of authorized clients can be configured in the network firewall data of the 150 H.



This view indicates the option of LAN-TFTP Server being used with the default threshold value of 80%.

LAN-TCP Client: This choice assigns the 150 H as the TCP client. When a single call charge has been incurred, a TCP/IP connection to an external call charge server (external application) is initiated by the switch. When the connection has been set up, the individual call charge data is transmitted. The connection remains permanently open, and any other charges that occur are transmitted. Each data record is transmitted individually.



This view indicates the option of LAN-TCP Client sending all data to the server as individual records.

Delta: CDR over IP is a new feature and is not supported in R1.0 or R2.2 versions of software.

6 System Upgrade

Service changes include new upgrade and logon procedures. Remember, always refer to the Upgrade procedures on the TAC Advisor before attempting an upgrade. The following information applies to upgrade of all R1.0 and R2.2 versions of software to V1.0 (R3.0) unless otherwise indicated.

6.1 General Upgrade Information

6.1.1 Office Pro

What's New: OfficePro upgrades require that the V1.0 SW be installed on a replacement FMC8 or FMC10, and the new CBMOD (Q2960-X200) must be installed in the cabinet before upload.

6.1.2 OfficeCom

What's New: Unlike R2.2, there is only 1 version of the V1.0 software for the OfficeCom. It can be installed only on a R2.2 hardware chassis with a full variant CBPC. It is not possible to upgrade any of the R1.0 hardware to V1.0 software.

The SW for the V1.0 HW has a digit 2 as the 3rd character to designate the R2.2 hardware as in this example. **cw2d468l.b01** This indicates that R2.2 hardware must be used. Upgrades require the V1.0 software installed on a replacement FMC8 or FMC10.

6.1.3 OfficePoint

What's New: OfficePoint upgrades to V1.0 require that a partial variant CBPC be installed in the system and that the V1.0 software be installed on replacement FMC8 or FMC10. There is only one version of R2.2 SW for the OfficePoint.

6.1.4 Software Conversion

What's New: It is still necessary to convert the down level customer KDS file to V1.0 as in previous upgrades. However, unlike the R2.2 upgrades, this conversion is only 1 step directly to V1.0 regardless of which version it is being upgraded from.

6.1.5 General Upgrade Notes

Following are some important points to remember when starting an upgrade.

- Analog trunk circuits must never be connected to the system when the TMGL card is not plugged in. Permanent damage to the system could result.
- There is no procedure to convert from one hardware platform to another. If you need to replace an OfficePoint with an OfficeCom or replace and OfficeCom with an OfficePro then the upgrade must be handled as a new installation.
- The APS transfer whether remote or over the V.24 port is not possible when upgrading to V1.0 from any down level software version. An FMC replacement is required.

- Be sure that the FMC has the appropriate software version for the upgrade that you are attempting.
- When you install the V1.0 Assistant E, be sure to answer YES to the prompt of "Overwrite INI file?" All Assistant E versions use the same ASS_150E.INI file location in the C:\WINDOWS folder. The new version will have additional configuration data.
- The chart below outlines the requirements for upgrade from the various levels of hardware and software for each system type.

System Hardware Type	Upgrade from R1.0 SW	To Upgrade from R2.2 SW
OfficePoint, All systems	CBPC, partial or full variant V1.0 software	CBPC partial or full variant V1.0 software
OfficeCom with R1.0 hardware	Replace with R2.2 chassis, CBPC full variant V1.0 software Relocate TMST1 card	Replace with R2.2 chassis, CBPC full variant V1.0 software
OfficeCom with R2.2 hardware	Not Applicable	V1.0 software only
OfficePro All Systems	CBMOD (2960-X200) V1.0 software	CBMOD (2960-X200) V1.0 software

6.2 Upgrade Procedures

The upgrade procedure that follows is a condensed "lab exercise" version of what an actual field upgrade would entail. The fully documented upgrade procedure will be available on the "TAC Advisor" in time for the actual V1.0 release. Since the on-line procedures are continuously updated, It is very important that you use them when conducting a field upgrade.

1) Install and start the V1.0 Assistant E. Set the baud rate and transfer the KDS in the down level system to the PC. If downloading a R1.0 database be sure to log on to Assistant E with the R1.0 password and no User Name. R2.2 systems require the user name and password of 31994. After the download is completed, save the KDS as **ORIGINAL.KDS** from the FILE menu.
2) Make notes of, and then delete, any Executive/Secretary groups that exist. They will be reassigned as "Top" groups after the software upgrade conversion.
3) Make notes of, and then delete any Executive/Secretary key layouts that exist. They will be reassigned automatically when the new "Top" groups are assigned.
4) (R1.0 Only) Delete, any Executive/Secretary groups destination lists that exist. The destination list entries for Executive/Secretary groups will not be required in V1.0.

5) (R1.0 Only) Make notes of, any system timer changes that are site specific. The upgrade will take all R1.0 software timers back to default values. All R2.2 system timers will remain intact.
6) Now, save the KDS as **MODIFIED.KDS.** Close the database from the FILE menu.
7) Convert the MODIFIED.KDS file to release V1.0 as follows.
   a) From the FILE menu, click on "Convert customer database…".
   b) Select the KDS file to convert and click on OK.
   c) Select the version "Release 3.0" and pick the appropriate system type and country version (USA). Click NEXT. If you see the Assistant E Warning "Offline generated database! No user rights checked.", click OK.
8) Notice that the KDS file name is now **OFFLINE.KDS**. This was changed as part of the conversion process.
9) Reassign any Executive/Secretary groups as the new "Top" MULAP groups and assign the key layouts as required.
10) Now, save the database as **UPGRADED.KDS.**
11) Disconnect the analog trunks from the system.
12) Power down the system and remove the FMC with the down level software version.
13) Install the FMC with the V1.0 software.
14) Power up the system and immediately default the system back to the German language with the reset switch.
15) Set the country identification to USA and the "Fixed Password".
16) Make sure the system has booted up to the English language.
17) Set the system's baud rate to 19,200, and reset the time and date.
18) Upload the entire V1.0 upgraded KDS file into the system.
19) Reset the system.
20) When the system boots up, make sure that it is operational
21) Download a fresh KDS file from the system to the PC. This will be necessary for any delta uploads. By default this will be the **LASTLOAD.KDS**.
22) Save the KDS as **FINAL.KDS**. This is your backup.

7 Service Support

Note: The following information concerning the TAC Advisor pertains only to those that are authorized to have access to Siemens' TAC Advisor. Your company's contract may or may not provide this authorization.

Just a reminder that the TAC advisor is still your central location for all Hicom 150 H, V1.0 technical updates, troubleshooting tips, software release information, and product alerts. The TAC Advisor also has, error code information, frequently asked questions (FAQ) and most importantly, the latest Assistant E and system software downloads.

The Technical Assistance Center (TAC) is available to take your calls. All calls are processed on a "highest priority, earliest received" basis. Help them better help you by doing everything you can before calling. Check your facts and the documentation first. Try the TAC Advisor to find the information you need. Its quick, its easy, and it beats waiting in queue. The TAC is working hard to keep your waiting time to a minimum.