Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
*** * ***
Université du 7 novembre à Carthage
*** * ***
Institut National des Sciences Appliquées et de Technologie

Project of end of studies

For the obtaining of

Diplôme Universitaire Technologique

Pathway: Information Networks and Telecommunication

Subject:

Installation and administration of a management platform for the MSAN equipment under Windows 2003 Server

Realized by: **Bayrem JRIDI**

Hosting enterprise:

Nokia Siemens Networks

Sustained on 21/06/2010

Jury's president : Dr. Emir Damerji
Examinator : Dr. Mohammed Daass
Enterprise supervisor: Mr. Abdelaziz BEN MANSOUR
INSAT's supervisor: Dr. Kamel KAROUI

Academic year: 2009/2010

Introduction

Being supplier of solutions of access and connectivity for the stationary and converged Networks, Nokia Siemens Networks, with its varied range of products, wish to be the partner of Tunisia Telecom for the development of its network (MSAN and NGN).

Taking into consideration the future needs and extensions of the network, and in order to migrate to networks of new generation (NGN), Nokia Siemens proposes its Platform IP Multiservice (Multi Service Access Node): hiX56xx. Meanwhile, Tunisia Telecom aims, by the present project, at achieving the following :

- Satisfaction of needs in service POTS and xDSLs in the new zones.
- Extension in terms of capacity POTS and xDSL in the existing network.
- Progressive replacement of the central of obsolete commutations.
- Coming closer most possible to end-users via IP MSAN Outdoor solution offering services of very high debit.
- Improvement of the maintenance while using a centralized and unified system of management for services POTS and xDSL. Nokia Siemens Networks, with its MSAN portfolio and its large local staff expertise, makes it possible to reach the objectives of Tunisia telecom thanks to a set of advantages of which one can mention:
- The MSAN approach which aims at reducing the network complexity by the migration from a multiple network to a simple network offering multiple services (ADSL, ADSL2, ADSL2+, VDSL2, SHDSL, POTS).
- The Flexibility to launch new services based on tendencies of the market is another asset in the development strategy of the network infrastructure. So the Flexibility of layer ACCESS in terms of connectivity interfaces will increase Tunisia Telecom's ability to offer new services such as Voices (VoIP), Triple Play for the residential subscribers and Videoconferencing and IP CENTREX for Enterprises.
- Solution-Completed and Proofed End-to-End "Carrier Ethernet" for easy integration within the network of Tunisia Telecom.

The goal of the practicum is to understand the MSAN technology and the installation of its platform of management using, first, the CLI model then the graphic model via the management system of ACI-E.

Therefore, I will present the NSN Company and then study its new project MSAN alongside with the configuration and the administration of the equipment of the IP MSAN platform via the centralized management system called ACI (Access Integrator). But first, it's sensible to start by explaining the difference between the existing architecture and the solution provided by NSN, and then I will proceed

by installing the new centralized management platform to get in the end to configure the Network Elements of the new telecommunication infrastructure.

Presentation of the company [1]:

NOKIA SIEMENS NETWORK (NSN) is a company formed by the fusion of Nokia and of Siemens. It does several activities in the field of the telecommunications including the manufacture of telephonic devices. NSN is one of the principal companies charged to supply telephonic operators with the necessary technology to accomplish their functions. It is assigned to provide, to program and to install the different devices to operators and to ensure the follow-up of these materials. To achieve its projects, NSN follows a precise work organization allowing it a long-lasting better contribution output. Engineers are organized into small groups according to their specialty and their field of expertise. Each group takes a part of the project. With more than 60,000 employees in over 150 countries, Nokia Siemens Networks is one of the largest telecommunications hardware, software and services companies in the world. It is committed to innovation and sustainability and offers a complete portfolio of mobile, fixed and converged network technologies as well as professional services including consulting and systems integration, network implementation, maintenance and care, and management services. NSN serve more than 600 customers around the world – Communications Service Providers (CSPs) who face a multitude of challenges as they focus on capturing greater value through business model innovation, reducing the complexity within their businesses and networks, growing their customer base and minimizing subscriber churn. Nokia Siemens Networks is the leading telecommunications solution provider in the Middle East and Africa region, which is one of the most strategically important markets for its fixed and mobile businesses.

[1] See list of references p: 79

Chapter 1

State of the art

1. State of the art

In this chapter I will be depicting the existing architecture and the reasons for the migration to the MSAN solution.

1.1. Presentation of the existing architecture[2]:

The following figure shows the existing architecture of an xDSL network with different components on the subscriber side and those on the operator side.

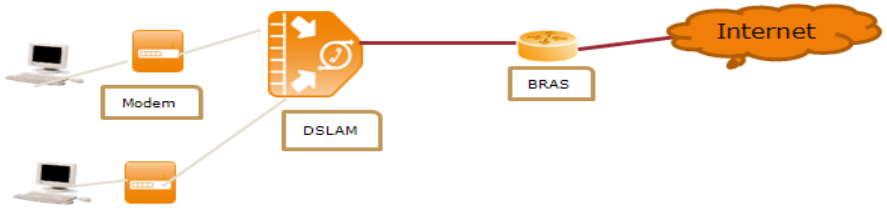

Figure 1.1: existing network architecture

1.1.1. The customer's equipment:

To be connected, the subscriber must have an analog phone line within the coverage area of the ADSL line (4 to 6 Kms from the dispatcher to the Operator). In addition, he must have a filter and a modem.

• Filter: a box located on the phone jack which separates the Internet data (digital broadband) from voice (low frequency): telephone calls.

• Modem: The modem is the device used to transfer information between several computers (2 at the base) through telephone lines. It is the acronym for a modulator / demodulator.

[2] See list of references p: 79

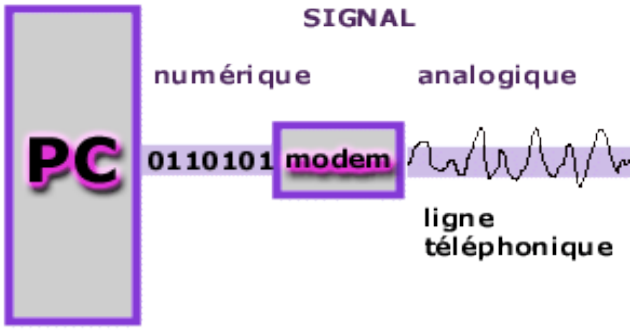

Figure 1.2: Positioning of a modem

1.1.2. The operator's equipment:

The network architecture is built through different equipment from the operator's point of view in order to provide the services to the customer.

a. DSLAM: Digital Subscriber Line Access Multiplexer:

In the telephone exchange, all modems and filters are concentrated at the DSLAM (DSL Access Multiplexers). Each DSLAM covers a number of ADSL lines which are located in the area covered by the exchange. The DSLAM collects data transmitted by users. Lines of customers arrive on a splitter, which allows the user to connect to the telephone switch and DSLAM if a DSL subscription is available. The DSLAM is itself connected to a hub. The DSLAM is an element of ATM concentration that is limited in the afforded bandwidth, the complexity of the technology offered by ATM.

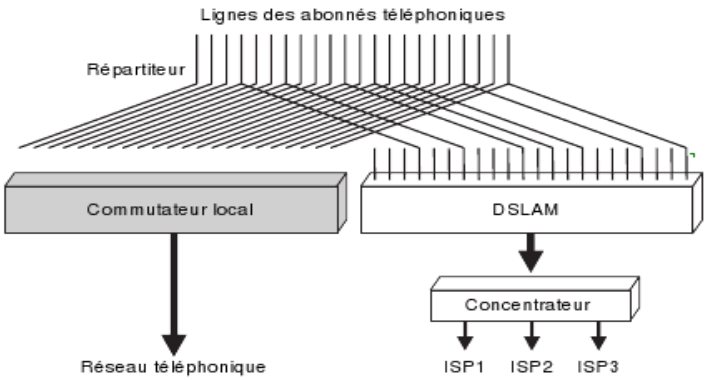

Figure 1.3: Positioning of a DSLAM

b. BRAS: Broadband Remote Access Server:

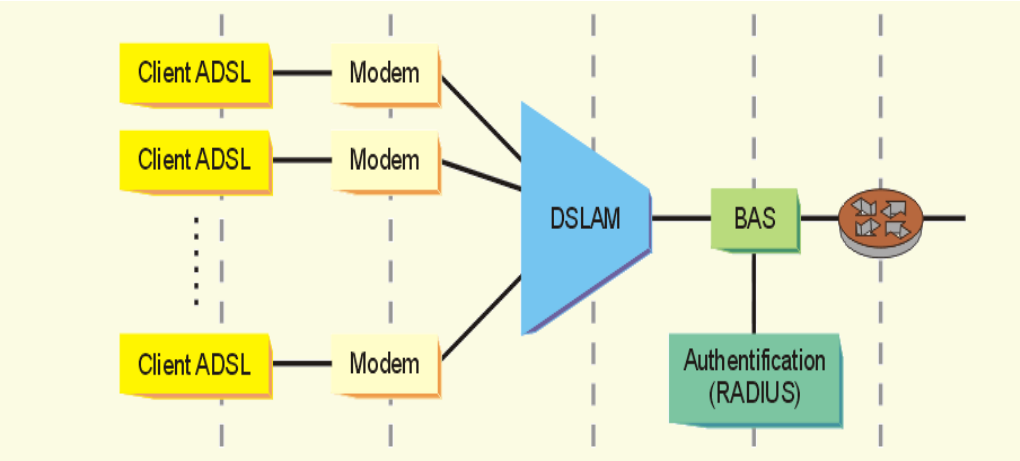

Figure 1.4: Positioning of a BRAS

The BAS is a server whose function is to manage the data. Data transportation is performed between the modem and the BAS which ends the PPP sessions. The broadband network using a device playing the same role as that of BAS is called BRAS, which in turn interacts with the radius server.

c. RADIUS: Remote Authentication Dial–In User Server:

The identification of a username and password is managed by a RADIUS. The RADIUS AAA protocol (Authentication, Authorization, Accounting), can make the connection between the needs of identification and the user base. The transaction authentication is initiated by a client of RADIUS, which may be a modem or remote access client application. The server processes it if necessary by accessing an external database: SQL database / oracle ..., user accounts or domain machine.
Authentication: identifying subscribers.
Authorization: The granting of access rights and profiles of subscribers.
Accounting: the preparation of diagnostic (date of connection, sites visited, billing ...)

Chapter 2

NSN's solution: MSAN

2. NSN's solution: MSAN

In this chapter I will describe the MSAN solution provided by NSN, the subject of my training, focusing on the system components and its functionalities.

2.1. System Overview[3]:

The hiX 56xx is a shelf based modular Ethernet/IP-DSLAM that terminates the ATM and Ethernet traffic coming from the subscriber lines and consolidates it on one or more Fast/Gigabit Ethernet towards the Metropolitan Area. The PVCs (Permanent Virtual Connections) of the ATM layer are terminated on the interface unit and translated to Ethernet to be transported through an Ethernet/IP environment. The multiple PVCs/VLANs are usually mapped into one or more VLANs and forwarded to the right destination with the appropriate CoS. DSL is the ideal solution for the bottleneck of the last mile, providing voice, data, and video solutions.
The following DSL technologies are used:

– VDSL2

– ADSL2+/ADSL2/ADSL

– SHDSL

Its high speed interfaces are suitable for asymmetrical and symmetrical applications such as high-speed Internet access, teleworking, video conferences, virtual private networking and streaming multimedia content and video. Additionally, POTS interfaces for Voice over IP (VoIP) are provided. With the introduction of the hiX56xx Multi-Service Access Node (MSAN), the next generation broadband access (xDSL/Ethernet) and narrowband VoIP (POTS/ISDN) service can be provided. On the other hand, PSTN substitution by IMS/FMC comprises also the migration of conservative POTS subscribers who are not disposed to move to new SIP based home infrastructure. Session Initiation Protocol (SIP) AGW can satisfy this demand and does not change the Service Level Agreement (SLA) to those types of subscribers. Additionally, voice and data (fax and modem) transmissions over IP will be supported. The CXU is the central unit of hiX 5625/hiX 5630 and hiX 5635; it plays the important role of switching the traffic, managing all components and providing the network interfaces. There are various types of central units for different shelves:

[3] See list of references p: 79

Product Name	Shelf	CXU
hiX 5635	M1200	CXU_B
hiX 5635	M1100	CXU_B1/CXU_B2/CXU_B21/CXU_B3
hiX 5635	G1100	CXU_B1/CXU_B2/CXU_B21/CXU_B3
hiX 5630	M600	CXU_C/CXU_C2/CXU_B3
hiX 5625	M400	CXU_C/CXU_C2/CXU_B3
hiX 5625	G400	CXU_C/CXU_C2/CXU_B3
hiX 5625	G400R	CXU_C/CXU_C2/CXU_B3

Table 2.1: CXU for hiX 56xx

The CXU_B/CXU_B1/CXU_C contain 4 fixed electrical GE interfaces and 4 interfaces for optical GE uplinks. The CXU_B2/CXU_C2/CXU_B3/CXU_B21 have 4 optical/electrical GE interfaces. A maximum of 4 of these 8 possible uplinks can be used. The uplinks can be used as uplink towards the core network or they are used either to cascade other DSLAMs or to connect to a collocated switch. A typical configuration can be e.g.: 2 optical GB uplinks and 2 electrical GB links towards a cascaded/collocated DSLAM/switch. In order to be able to use the optical uplinks, separate pluggable modules (SFPs) have to be delivered for these slots. The maximum line capacity of hiX 56xx is dependent on the equipment configuration; the following table lists the maximum line capacity of hiX 5635:

Shelf	CXU	Plug-in Units	Maximum Line Capacity
M1200	One CXU_B	24 port VDSL	24 x 16 = 384
		48 port ADSL	48 x 16 = 768
		72 port ADSL	72 x 16 = 1152
		48 port SHDSL	48 x 16 = 768
		72 port VPLU	72 x 16 = 1152
	Two CXU_Bs	24 port VDSL	24 x 15 = 360
		48 port ADSL	48 x 15 = 720
		72 port ADSL	72 x 15 = 1080
		48 port SHDSL	48 x 15 = 720
		72 port VPLU	72 x 15 = 1080
M1100	One CXU	24 port VDSL	24 x 15 = 360
		72 port ADSL	72 x 15 = 1080
		48 port SHDSL	48 x 15 = 720
		72 port VPLU	72 x 15 = 1080
G1100	One CXU	24 port VDSL	24 x 14 = 336
		72 port ADSL	72 x 14 = 1008
		48 port SHDSL	48 x 14 = 672
		72 port VPLU	72 x 14 = 1008
M1100/G1100	Two CXUs	24 port VDSL	24 x 14 = 336
		72 port ADSL	72 x 14 = 1008
		48 port SHDSL	48 x 14 = 672
		72 port VPLU	72 x 14 = 1008

Table 2.2: Maximum Line Capacity of hiX5635

The equipment used in our project consists in the M400 for the hiX 5625, the M600 for the hiX 5630 and M1100 for the hiX 5635.

2.1.1. SURPASS hiX 56xx as Part of Carrier Ethernet Solutions:

The hiX 56xx is a network element which includes the necessary service adaptation functions to support the delivery of all types of applications over Ethernet/IP networks. The main components of the next generation broadband network are: the DSL customer premises equipment, IP/Ethernet DSLAM, Ethernet aggregation layers multi-service edge routers, broadband remote access servers (BRAS) and home entertainment network (video and content delivery solution). The hiX 56xx is one element of this end-to-end solution; however Nokia Siemens Networks is able to provide the complete next generation broadband network and video integration solution where full interoperability is ensured.

The hiX 56xx DSLAM operates as a multiplexer which consolidates the traffic originating from a number of subscriber lines to a feeder interface connected to the Ethernet/IP network. The subscriber lines can be ADSL/ADSL2/ADSL2+/VDSL2 and SHDSL lines. With unit VPLU, the hiX 56xx operates as an interface between the IP network and the legacy PSTN. Equipped with voice-processing units that are called analog gateway line units (AGLU), by using SIP, hiX 56xx can establish, modify and terminate internet telephony calls and, more generally, multimedia sessions or conferences. Access Integrator Ethernet (ACI-E) is the management system for all pieces of the solution. It enables the operators to benefit from the whole feature set supported by the products. ACI-E EM (Element Manager) GX supports FCAPS-functionality (fault management, configuration management, accounting management, security management and performance management). Mass provisioning tables, topological maps and wide network alarm tables are further value-added services that facilitates operators daily work.

ACI-E can also be integrated into any existing network management platform via SNMP or CORBA Northbound interface, providing the wide feature set offered by the element manager.

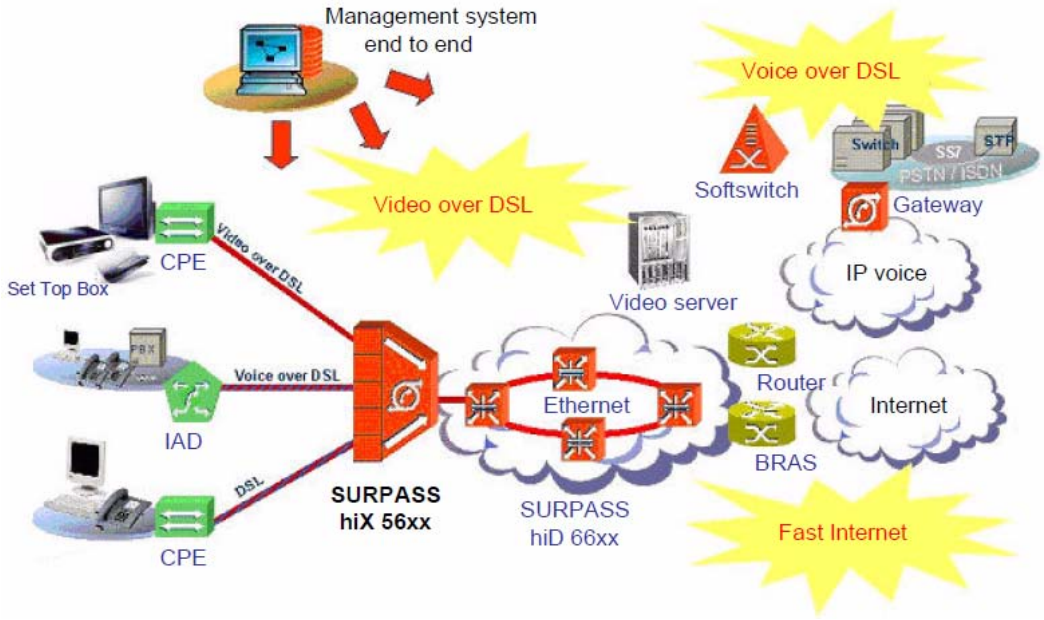

Figure 2.1: Network Architecture with hiX 56xx

2.1.2. System Architecture:

As seen in the previous section the NE HiX 56xx contains three different types of material the HiX 5635, HiX 5630 and HiX 5625. In our case, we are working on the HiX 5635 and the following figure shows the architecture of the hiX 5635 on shelf M1100:

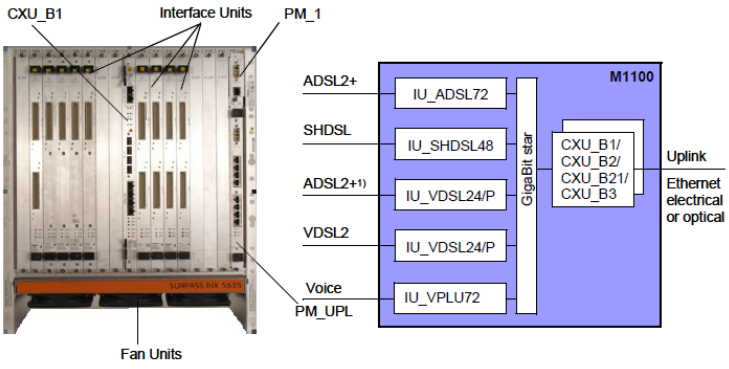

Figure 2.2: hiX 5635 System Architecture (M1100)

2.2. System functionalities:

The hiX 56xx provides the following functionalities:

- Voice over IP

- Line test (ILTF)
- Link aggregation acc. to 802.3ad based on MAC or IP
- Spanning tree (STP, RSTP and MSTP)
- Ethernet ring protection (ERP)
- Cascading based on electrical and optical Fast and Gigabit Ethernet interfaces
- Enhanced L2 functionalities
- Carrier Ethernet Border Switch (CEBS)
  - N: 1 MAC address translation
  - MAC address translation 1:1
- Multicast capabilities (IGMP v1/v2, IGMP Proxy, termination, filtering)
- 1 k Multicast Groups
- PPPoE support, DHCP relay agent, DHCP simplified relay agent and filtering
- PPPoA support
- PPPoA to PPPoE translation
- Ingress policer per CoS
- Performance management
- Access control lists based on port, MAC, Ethertype, L4 info
- IEEE 802.1Q tagged frame supporting 4 k VLANs
- VLAN single/double tagging
- Double tagging for in-band management and ANCP
- Routing between in-band management channel and out-of-band Interface
- VLAN translation
- VLAN mapping acc. to port, ATM VC, IP SA/DA
- Any L2 mode (tagged and untagged traffic per port)
- MAC/IP anti-spoofing
- Single/double ended line testing (SELT/DELT)
- Broadcast storm control.
- Clock synchronization
- Alarm history

2.2.1. VoIP Function:

Hix 56xx R2.7M is the first release that converged H.248 [1] and SIP in one voice line,

(1) See annex p: 80

though H.248 and SIP are built into different software images. The DSL part of R2.7M is based on R2.7 while the VoIP part merges from R2.0M and R2.6S. Besides the old CXUs(B/B1/C), R2.7M also supports the next generation CXUs (B2/C2/B21/B3).

2.2.2. DATA Function:

The hiX 56xx provides various data functions below are the most important ones that are needed through the project:

a. Bridging:

The hiX 5625/30/35 IP-DSLAM uses an advanced carrier mode bridging technique supporting suitable features for telecommunication environment. Bridging provides secure and efficient network environment between DSL subscribers and the IP-DSLAM. Within the same VLAN, port isolation is guaranteed in upstream direction.

With carrier mode bridging in downstream direction, the IP-DSLAM compares the destination MAC address of unicast Ethernet frames with a MAC table. Then the frame is forwarded to the appropriate subscriber port. Frames with a so far unknown destination address are discarded.

This is in contrast to standard IEEE 802.1D Ethernet bridges which would request flooding to every port (i.e. DSL line) which is not secure in case of unicast flooding. It will also congest the available DSL capacity with unsolicited data. With the bridging technique, ports of users which may never have requested any broadcast traffic are blocked. With IPDSLAM, bridging of Ethernet frames to a DSL port is only possible after a user has sent an Ethernet frame towards the network and made his MAC address known to the IPDSLAM in this way.

b. VLAN Tagging:

In legacy versions, the IU was able to add one tag while the CXU could add another tag, thereby achieving double tagging. As for the current mechanism, all tagging is per bridge port, i.e., the CXU does no longer add any outer or s-tag.

Tagging is controlled by four parameters:

– A system setting “Tagging Mode” on the CXU

– A per bridge port setting “VLAN Mode”

– An outer tag PVID per bridge port (oPVID)

– An inner tag PVID per bridge port (iPVID)

(Used only when adding two tags at the same time).

Based on these settings, the IU adds no, one or two tags to a frame, or removes tags accordingly in downstream direction. The CXU, in any case, does not add or remove any tags.

Both PVID values of a bridge port are always configured by the CXU while the inner tag may be unused when a single-tagged frame is the result of the tagging mode settings.

Inner PVID value is set to '1' per default, while default outer PVID is (slot*100+port). The

Ethertype ID of the inner tag is always 0x8100 while it is a system adjustable setting for the outer tag and defaults to 0x88A8, which is consistent with IEEE 802.1ad "Provider Bridges". The following table summarizes the options and their effects (U = untagged, T = tagged, D = double-tagged).

VLAN tagging mode (see Figure below)	VLAN mode IU port	Tagging mode CXU	DSL line	Uplink interface
(a)	Stacking	Double	U	T
(b)	Stacking	Double	T	D
(c)	Stacking	Single	U	T
(d)	Stacking	Single	T	T
(e)	Double	Double	U	D
(f)	Double	Double	T	dropped
	Double	Single	n/a	n/a

Table 2.5: Tagging Modes of IP-DSLAM

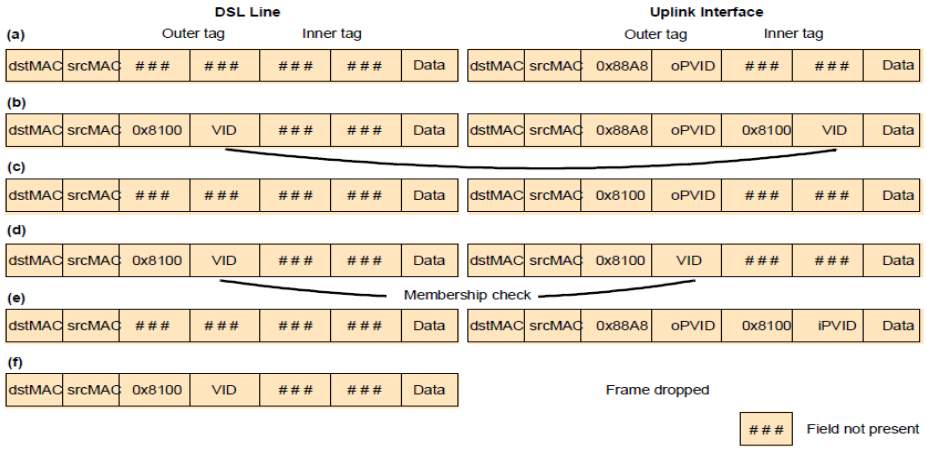

Figure 2.3: Tagging Modes of IP-DSLAM

c. Security:

Different levels of security are provided by the MSAN such as:

- ✓ Access Control List
- ✓ Denial of service
- ✓ IP Anti-Spoofing

- **Access Control Lists:**

Access Control Lists are rules that can be configured in network elements to allow or deny the forwarding of specific traffic. The hiX 5625/30/35 supports ACLs which can be configured based on different parameters:

- Port
- MAC Address (list, range)
- Ethertype
- IP destination and source address

- **Denial of Service (DOS) Prevention:**

To avoid DOS attacks and MAC spoofing the following mechanisms are implemented:

- Limiting of the number of MAC addresses per port
- Storm control
- Suppression of broadcast and multicast frames
- Port isolation (i.e. avoids connectivity between subscriber ports)

- **IP Anti-Spoofing:**

Many computer viruses or worms attack the target system using DoS or scan the network. In this case, that software usually changes its source IP address to hide itself. Sometimes, hack software tries to change its source IP address to pretend being the target system.

In order to prevent IP spoofing, reliable information about IP address of a subscriber is needed. This information can be acquired by:

- using DHCP information
- static configuration

The existing DHCP relay software stores port identification information as well as MAC address of the host. This information is used for ARP reply agent also. With that, the bound IP address can be managed. Each entry is aged out after the lease time and the lease time is updated by each DHCP_ACK packet. But, this action is performed by DHCP relay software which sends events to the IP anti-spoofing component. The following events can be provided by the DHCP relay software:

- New entry (port identification, IP address)
- Delete entry (triggered by aged-out or DHCP Leave/Decline message)

2.3. Presentation of the solution:

With the introduction of the hiX56xx Multi-service Access Node (MSAN), it's possible to combine more effectively the delivery and operation of different services within a common access platform as well as a common aggregation network. This solution contributes to an optimization of the costs and expands the reach of the provider in terms of the services offered. With this approach, Data Broadband Access (xDSL/Ethernet) and narrowband voice services (using VoIP both for POTS and ISDN) can be provided to the final customer. In summary, the main function of the VoIP feature within the IP DSLAM hiX5625/30/35 is to enable the IP DSLAM to do the mediation between legacy TDM telephone lines (POTS or ISDN) and the emerging next generation IP packet networks by converting voice streams originating from the TDM line to media streams for IP networks and vice versa. In addition to the voice over IP functionality, other bearer types such as Fax and ISDN over IP are also supported. The VoIP feature in the hiX5625/30/35 will ensure seamless interworking with any Soft switch using either the MEGACO or SIP protocols. Existing hiX5625/30/35 installed equipment will have the option to become a Multiservice AGW by simply adding the VoIP card into the system and performing a software upgrade in order to activate the new functionalities.

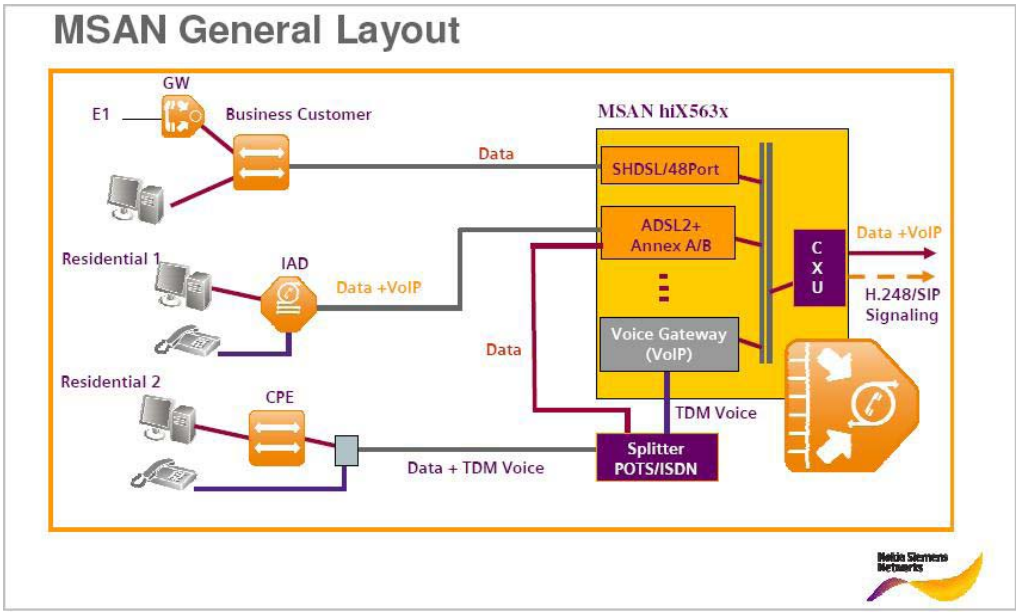

Figure 2.4: MSAN general layout (Costumer's view)

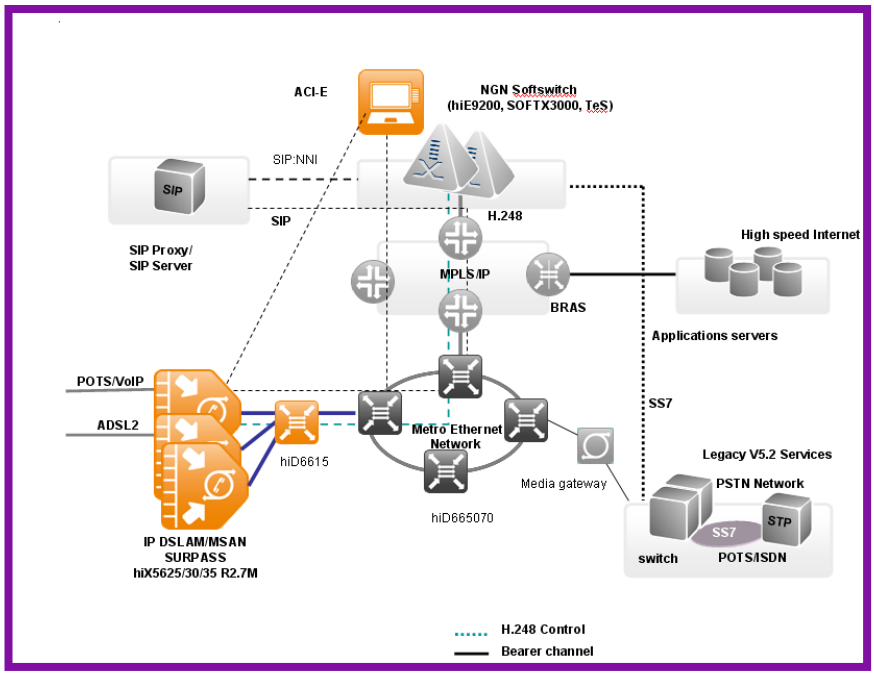

Figure 2.5: MSAN general layout (Operator's view)

In an NGN scenario, the subscribers' traffics entering into the IP DSLAM comprise data, VoIP and TDM voice. Business customers normally will have only data traffic and will enter the network via G.SHDSL line card directly, including VoIP traffic which has been generated within their networks.

The same holds for residential users who subscribe to data and VoIP services, where their IADs or home gateways packetize the voice traffic before forwarding it to the DSLAMs. The VoIP card will play its role whenever there is a subscriber who has data and PSTN services. The voice traffic coming from these subscribers will be TDM voice (POTS/ISDN) and therefore will have to be converted to VoIP. Traditionally, the TDM voice traffic can either be offloaded to a local TDM exchange as it is or carried over a carrier grade IP network. The voice conversion process begins when the TDM voice reaches the CO and is directed from the MDF to the splitter units. The POTS/ISDN splitters will separate the narrowband TDM voice from the broadband data traffic and then forward both to the different boards on the MSAN that are prepared to handle the two specific services.

Packetizing the TDM voice becomes an essential part of the solution and this task is held inside the voice gateway board. This board is responsible for performing all necessary voice encoding steps to packetize the original TDM traffic. After the VoIP packets are created, they are forwarded via the internal bus to the controller unit that forwards them to the IP network. Both RTP and Signaling traffic have to be sent from the MSAN to allow a successful VoIP scenario.

To ensure that this solution is capable of getting into the POTS/ISDN-to-VOIP market as early as possible and in order to position our solution competitively, we have planned our new VOIP Line Card for the IP DSLAM SURPASS hiX563x to be available (B600) in a 3-step timeline:

Step1)

- 72-port POTS voice line card with H.248.
- To be supported only in hiX5630v chassis.
- "Single Service" AGW support for POTS only VoIP (no xDSL broadband services in the same chassis).

Step 2)

- Uses the same hardware (voice line card, CXU, chassis) with a new software upgrade.
- Supported in hiX5625, hix5630 and hiX5635 chassis.
- Multi-Service AGW support for xDSL, Ethernet & Voice H.248.
- Integration test with hiE9200 S3.1 and Alcatel Softswitch.

Step 3)

- 32-port ISDN BRI (2B1Q & 4B3T) voice card with H.248/ SIP.

Chapter 3

Installing the ACI: the MSAN administration platform

3. Installing the ACI: the MSAN administration platform

The administration of our platform is made by a centralized management system which is composed of three servers and their redundant and that makes a total of six servers as in the figure below.

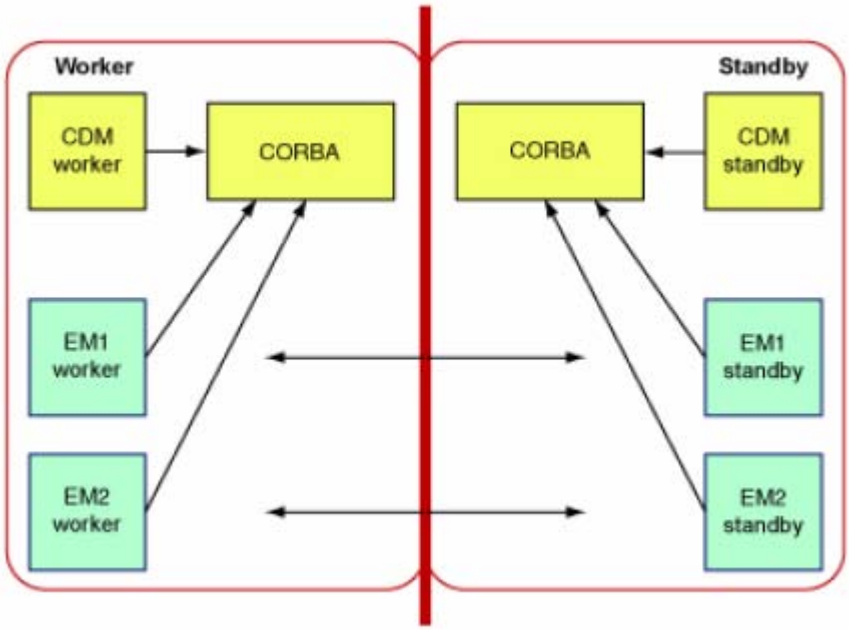

Figure 3.1: Centralized management system

Now I will proceed by the installation of each server and its functions in this system and afterwards I will manage the geo-redundancy and the other administration tasks handled by the ACI administration system.

All servers must be either on "Windows 2003 Server" which is our case or else on "Solaris".

- The first server is an RMC server for "Remote Management Controller" whose role is to manage the Geo-Redundancy.
- The second server is an ACI-EM GX which is the server responsible of managing the hiX equipment.
- The third is an ACI-EM DX responsible of managing the hiD equipment.

Now we will start by the SW that must be installed in each server and they are "Windows 2003 sever" and the "ACI Core".

3.1. Installation of Windows 2003 Server:

Windows 2003 server is our Operating System, that's why we will start by installing it. In this section figures the essential steps of Windows 2003 Server to the project.

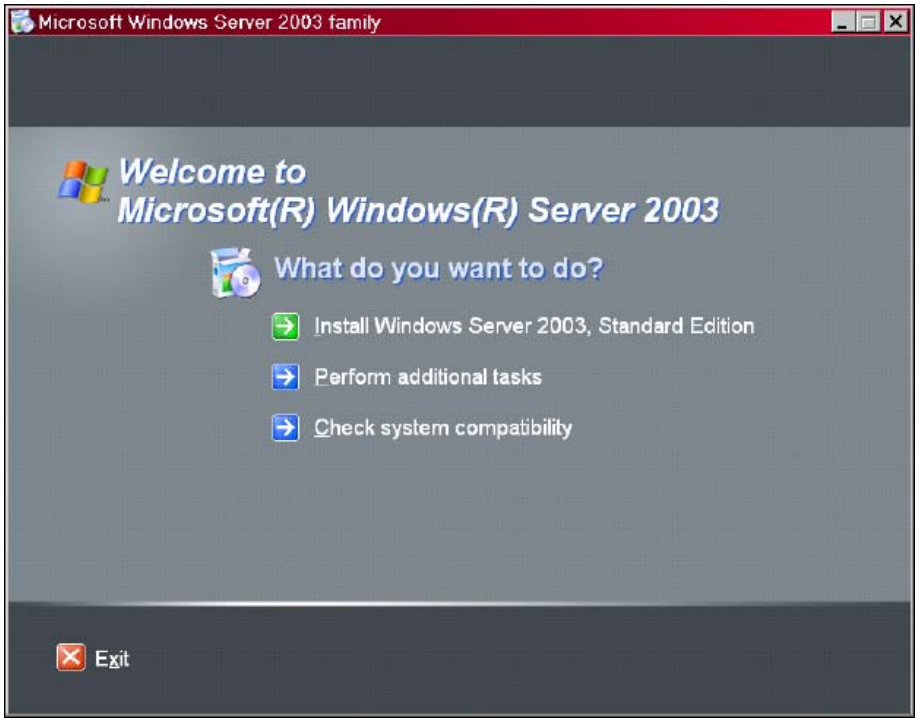

Figure 3.2: Win 2003 Server Installation window

The above screenshot is one alternative to start installing from the computer's hard drive but we can also install it from the CD by Changing the BIOS boot sequence to boot from a CD-ROM drive, by pressing the F2 button during startup of the PC and going to the appropriate menu in the BIOS. Then after rebooting the machine we can start the installation following the instructions provided.

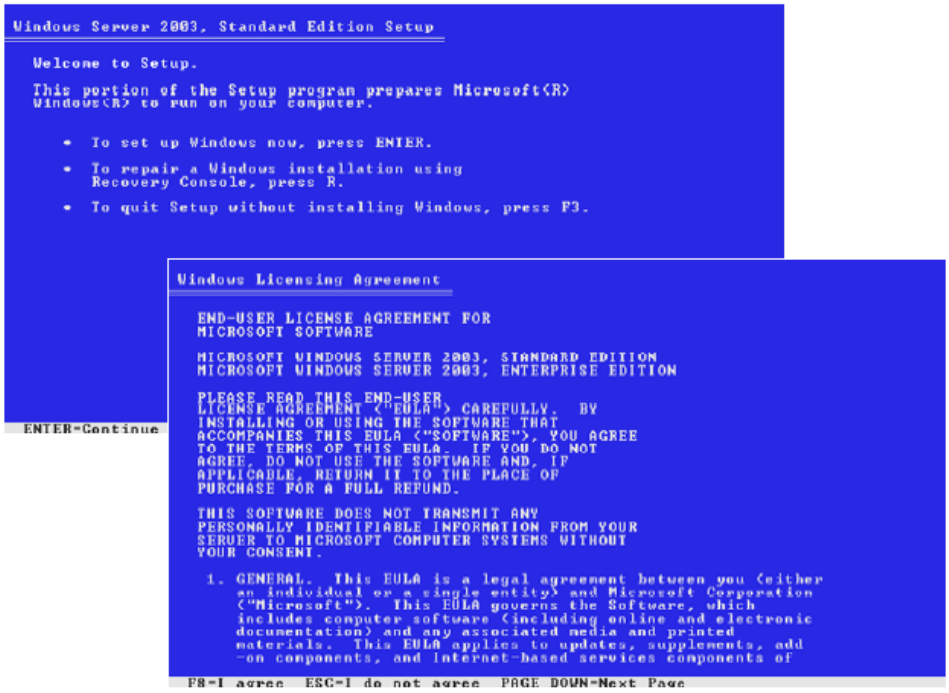

Figure 3.3: Win 2003 Server Installation start up

After selecting the set up options, we choose the right partitioning we need in our architecture, then we proceed by formatting our partition using the needed file system-Windows uses NTFS file system.

After formatting the partition the installation wizard starts copying the setup files:

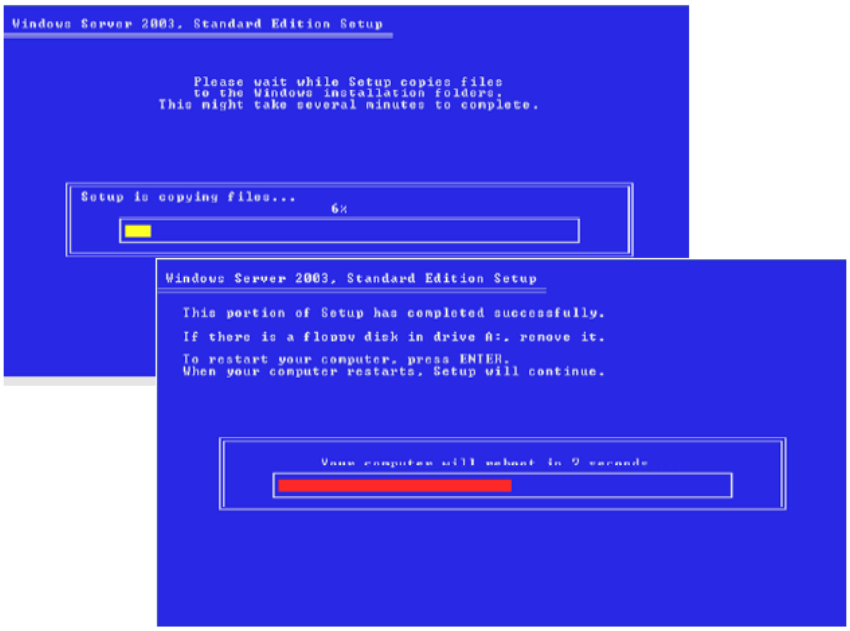

Figure 3.4: Copying setup files

The installation can take from fifteen to thirty minutes according to the server's capacities. Setting the computer name and the time setting is an important step in our work because the computer name will be used in further configuration and administration roles:

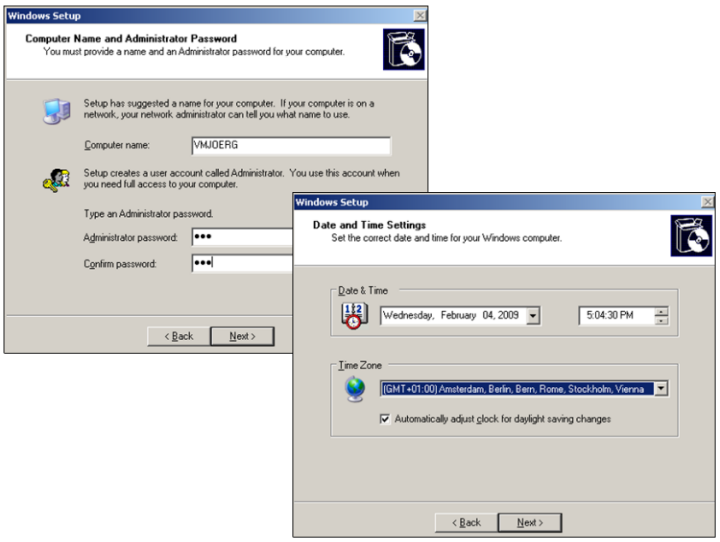

Figure 3.5: Computer name and time setting

The most important step in the installation is to set the server's IP address:

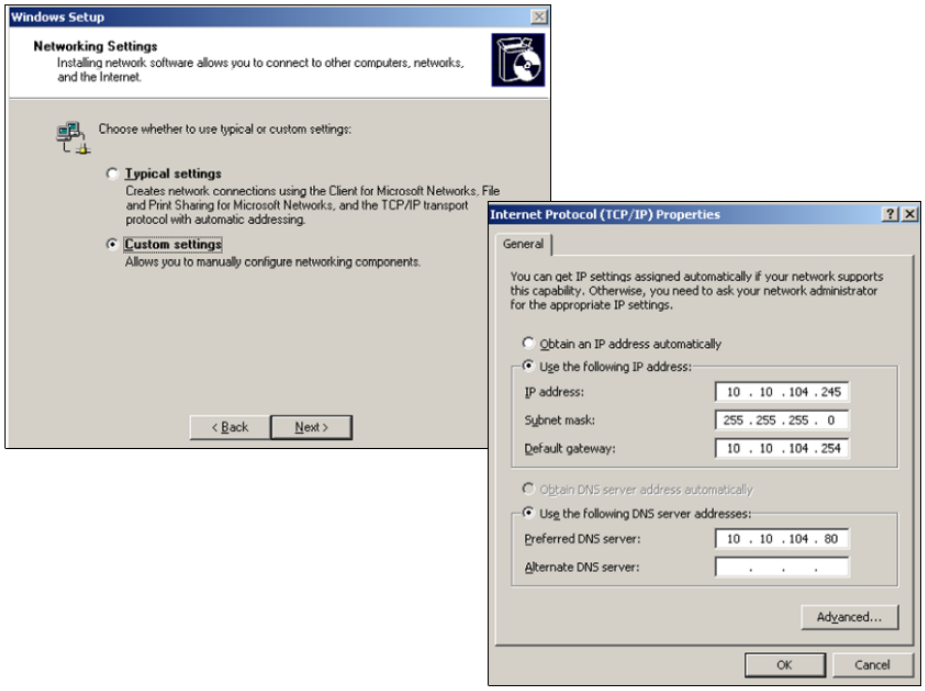

Figure 3.6: IP setting

It is highly recommended after installing windows to install the ACI components in a partition different from the one containing the Operating System. That's why we should create a new partition. This can be done with the Windows Disk Management:

'Settings' -> 'Control Panel' -> 'Administrative Tools' -> 'Computer Management'

In the "Computer Management" window, double click on directory:

'Storage'->'Disk Management'

To create a new Partition:

• Highlight the unallocated space.

• Right click and -> 'Create Partition'. The Create Partition Wizard will start.

While creating the partition Windows 2003 server provides the possibility to create either a primary partition or an extended partition.

- ✓ Primary Partition: is a volume created using the free space on a basic disk.
  Windows 2003 and other operating systems can start from a primary partition. Up to four primary partitions on a basic disk can be created, or up to three primary partitions and an extended partition.
- ✓ Extended Partition: An extended partition is a portion of a basic disk that can contain logical drives. Use an extended partition if you want to have more than four volumes on your basic disk.

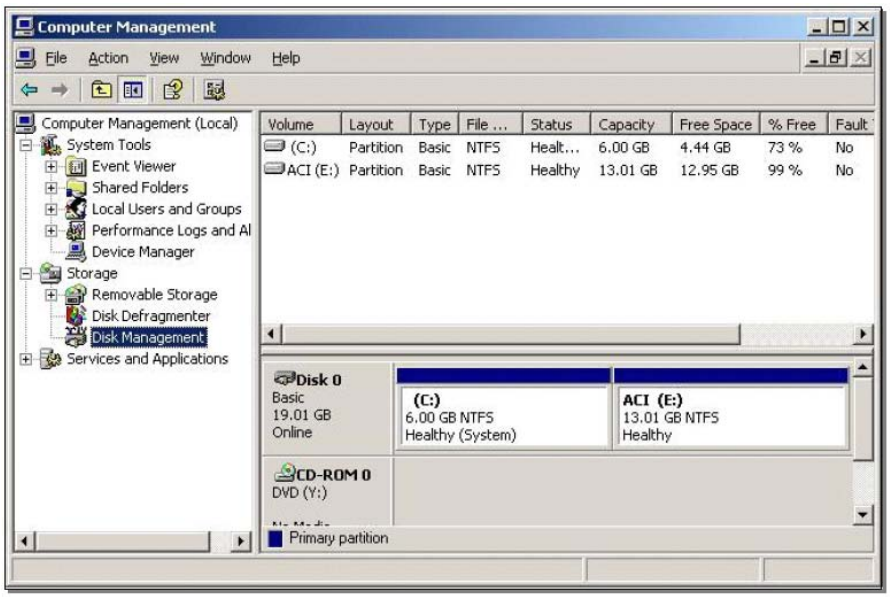

Figure 3.7: Windows 2003 Disk Management

The used file system should be NTFS.

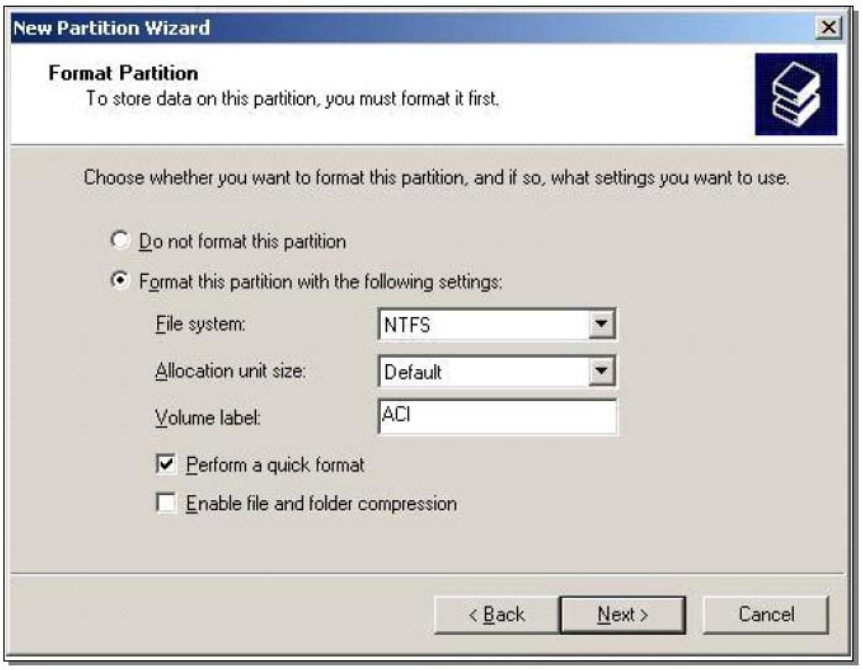

Figure 3.8: Windows 2003 formatting tool

For the Access Integrator to function correctly, a few Windows 2003 standard settings have to be modified after the installation.

The following configurations have to be carried out:

- Expanding the virtual memory and optimizing the performance
- Deactivating the screen saver
- Configuring the log in the event viewer

To expand the virtual memory we can proceed this way:

- Select the menu:

•"Start" ->"Settings" ->"Control Panel"

From the Control Panel, open the "System" -> "Advanced" -> click on "Performance Options…"

- In the "Virtual Memory" box click:"Change"

Enter the new values for the Virtual memory size:

"Initial size (MB)"= 512 (double the RAM size)

"Maximum size (MB)"=512 (at least double the RAM size)

- Press"Set" and then"OK" button

And after that of course it is recommended to reboot the PC.

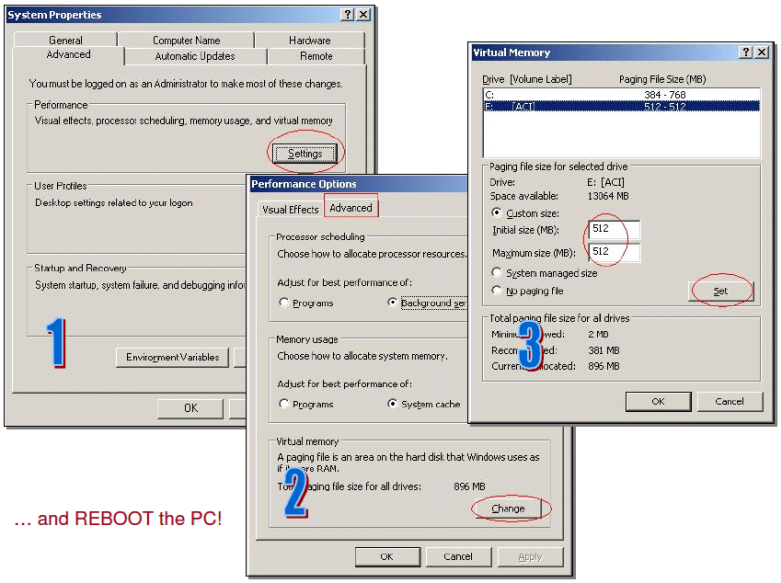

Figure 3.9: Performance of the ACI Server PC

The screen saver of an ACI server must be shutdown because it slows the computing speed of the PC. The events in ACI can be supervised by using the Windows 2003 application "Event Viewer". This application log, by Windows 2003 default settings, is set to overwrite entries older than 7 days when the log is full. This is insufficient for ACI, and there is a chance that the log runs full before the 7 days causing ACI inability to write to the log file. Warning messages will appear frequently due to this case. To prevent this, the setting for the log has to be changed:

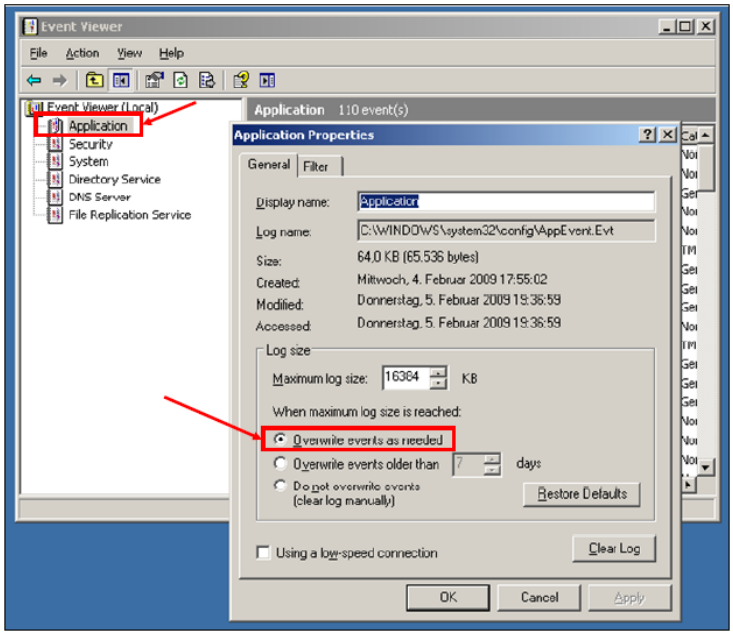

Figure 3.10: Event Viewer settings

3.2. Installation of ACI Core:

The ACI Core components must be installed in all the ACI servers. The installation package of the ACI Core / ACI-OAM contains other SW installation packages which are:

- ✓ UDP Router: must set the IP address of the domain controller.
- ✓ JRE: must be installed as the application is developed under JAVA.
- ✓ TAO: is a freely available, open-source, and standards-compliant real-time C++ implementation of CORBA based upon the Adaptive Communication Environment (ACE).
- ✓ Versant: is the SW that creates the object-oriented database for an ACI.
- ✓ Jacorb: is an Open Source Java implementation of the Corba standard.
- ✓ Licensing server: is needed for all kinds of ACIs
- ✓ Security server: is the SW that provides the access list control and that attributes permissions to the users.
- ✓ Tomcat: Tomcat implements the servlet and the Java Server Pages (JSP) specifications from Sun Microsystems, providing an environment for Java code to run in cooperation with a web server. It adds tools for configuration and management but can also be configured by editing configuration files that are normally XML-formatted.

The diagram below lists the steps of the ACI Core installation:

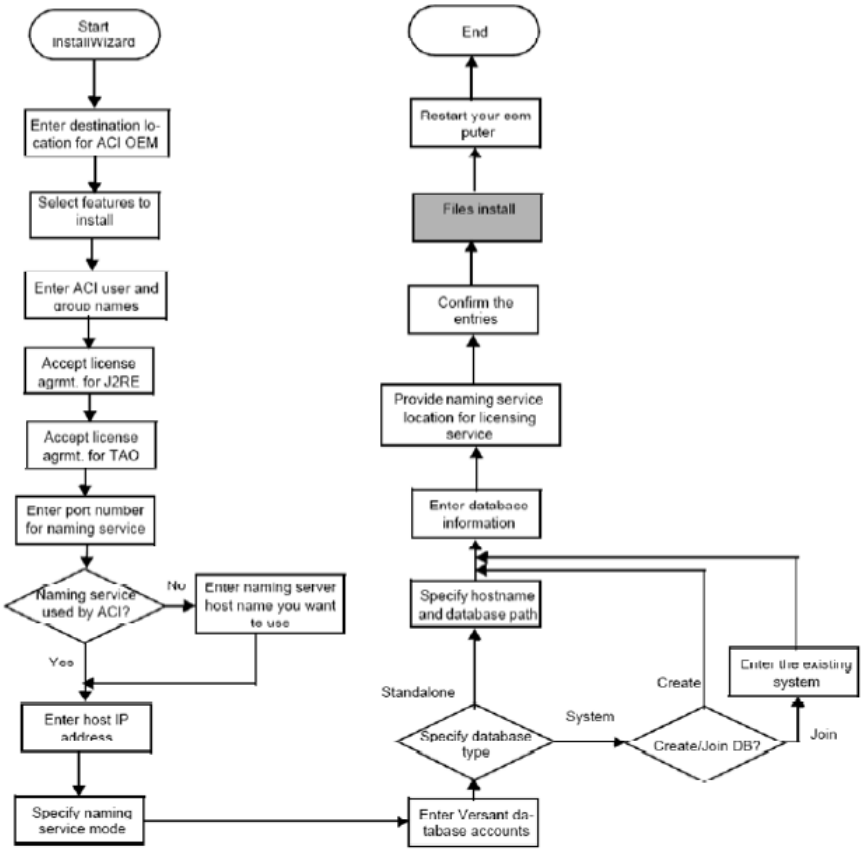

Figure 3.11: Installing the ACI Core diagram

The following screenshots display a "quick" Core installation, performing the whole installation in one step, followed by a single reboot:

The Core installation launches the installation of the required SW.

The JRE is a must for the SW to function because it's a JAVA based SW, this is the reason behind the JRE being the first component to install by the Core.

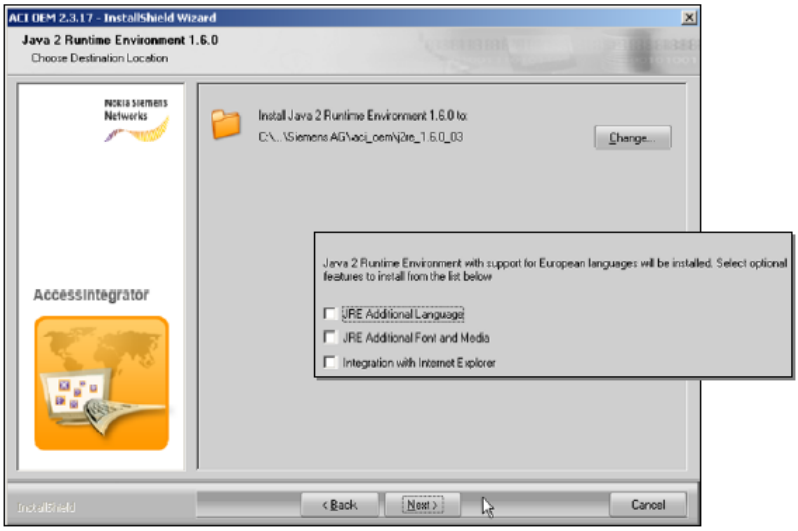

Figure 3.12: Java Runtime Environment

The JACORB is also required to provide the interaction between the different SWs that constitutes the ACI/OEM.

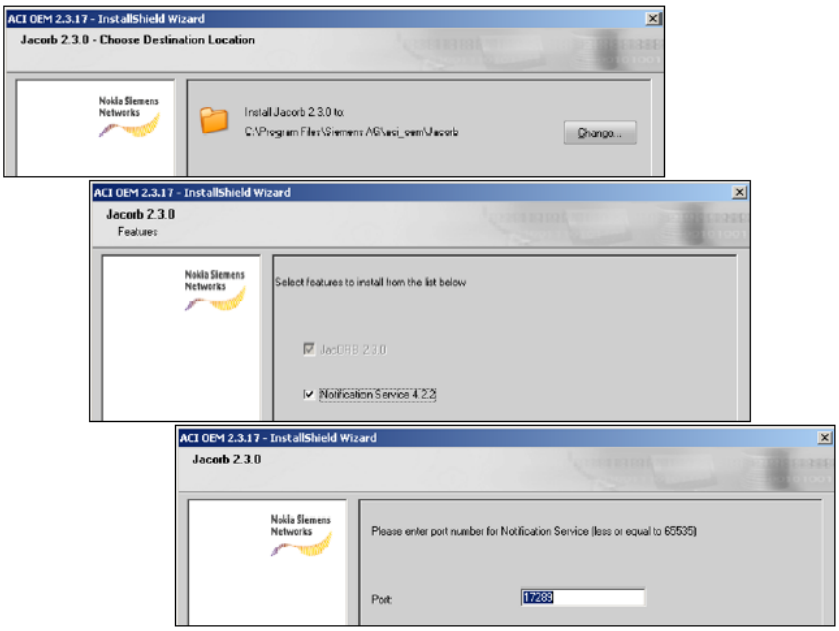

Figure 3.13: JACORB Installation

The TAO is the SW that provides the naming service of our administration platform and it must be installed in a single PC of the network whose IP address should be indicated.

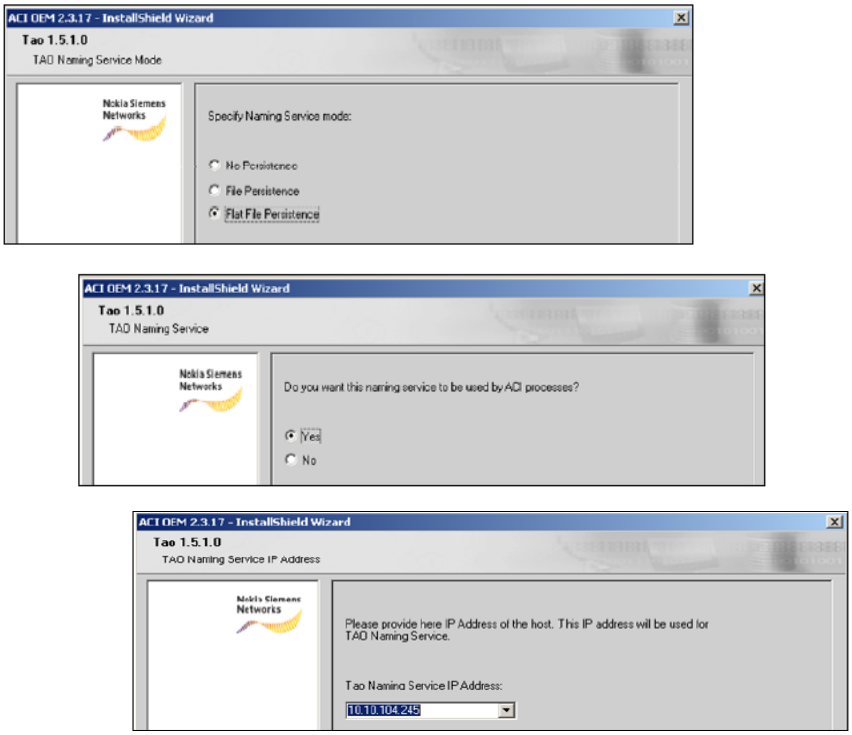

Figure 3.14: TAO Installation

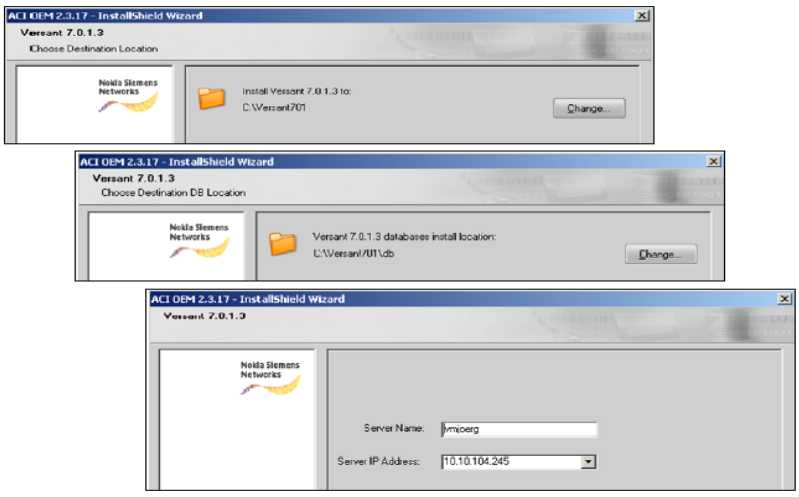

Figure 3.15: Versant Installation

The licensing server figured below is related to the versant data base figured above (see *Figure 3.15*) for this reason once the versant installed we must not change any of the values of DB in the LS installation.

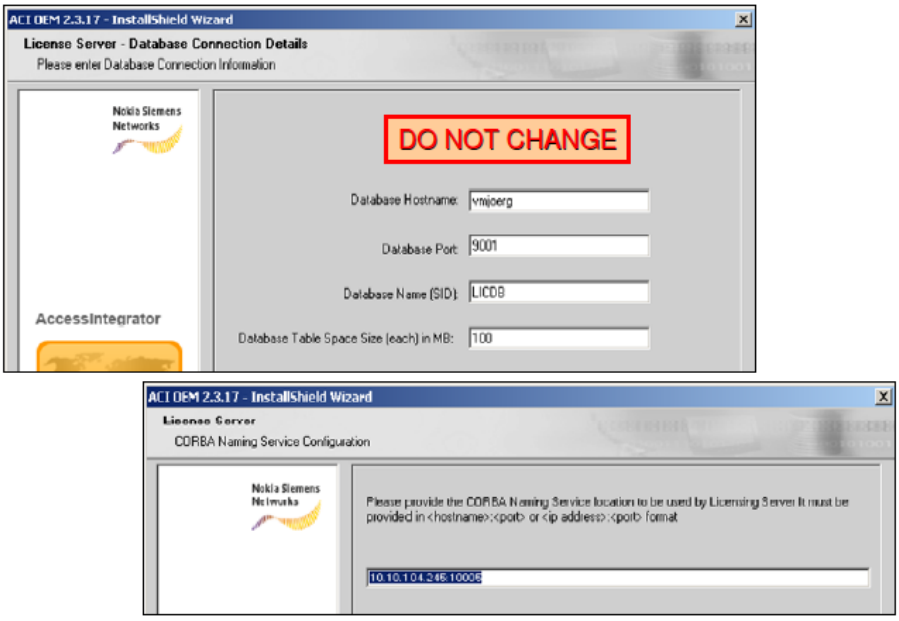

Figure 3.16: Licensing server Installation

The security server is the SW that provides the access management as well as the administrators' and the users' creation.

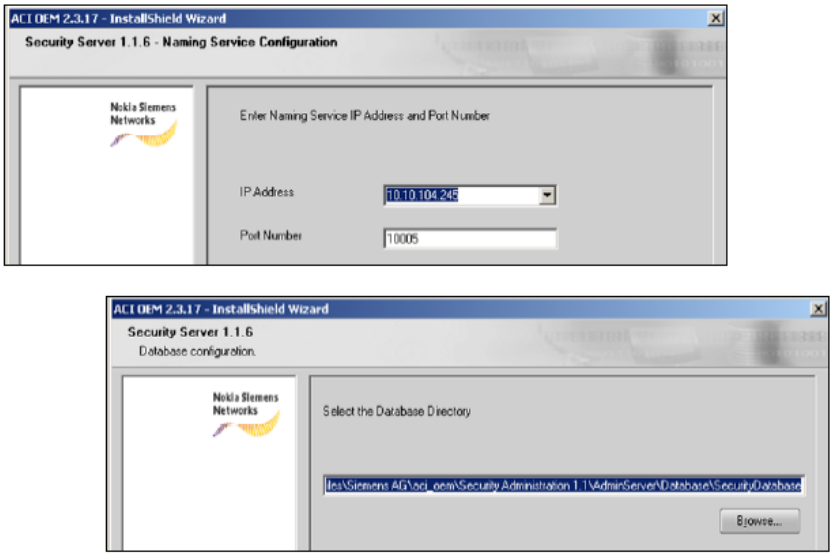

Figure 3.17: Security server Installation

3.3. Installation of servers' specifications:

In this section we will install each server's specific SW. Our platform contains the following architecture:

Server's Name	Functionalities	Installed Software	Properties
RMC1	- Primary domain controller - RMC Server	- RMC Client - RMC Server - Client EMGX Worker - EMGX Client Stand by - CDM client worker - CDM client Stand by	Hostname : RMC1 IP Address: 172.16.27.3 Mask 255.255.255.224
GX1	- EMGX primary Server for the hix supervision	- OEM - EMGX Server - Admin server - Admin Client - RMC Agent - FTP server 1 - Licensing server 1	Hostname :GX1 IP Address: 172.26.27.5 Mask: 255.255.255.224
GX2	- EMGX Secondary Server for the hix supervision	- OEM - EMGX Server - Admin server - Admin Client - RMC Agent - Licensing server 2	Hostname :GX1 IP Address: 172.26.27.7 Mask: 255.255.255.224
RMC2	- Secondary domain controller - RMC Server	- RMC Client - RMC Server - EMDX Client Worker - EMDX Client Stand by - CDM client worker - CDM client Stand by - FTP server 2	Hostname : RMC1 IP Address: 172.16.27.9 Mask: 255.255.255.224
DX1	- EMDX primary Server for the hiD supervision	- OEM - EMDX Server - RMC Agent - CDM server	Hostname :GX1 IP Address: 172.26.27.11 Mask: 255.255.255.224
DX2	- EMDX Secondary Server for the hiD supervision	- OEM - EMDX Server - RMC Agent - CDM server	Hostname :GX1 IP Address: 172.26.27.13 Mask: 255.255.255.224

Table 3.1: Administration platform

3.3.1. RMC1:

This server is designed as the primary domain controller so it needs to be configured as such by following these steps:

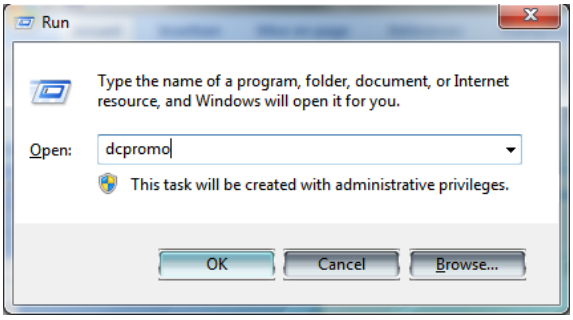

Figure 3.18: Domain controller promotion

Start Active Directory Wizard	**Go to "Start" → "Run" and type in : dcpromo (= domain controller promote)**
Active Directory Wizard Welcome screen	**Click NEXT**
Domain Controller type	Domain Controller for a new domain (DC)
Create a New Domain Tree	
Create a New Forest	
Full DNS (Domain Name)	Enter the DNS name for the new Domain **Full DNS name** : e.g. ACI.com
NetBIOS Domain Name, the name other users will use to identify the new domain.	Confirm the NetBIOS Domain Name. **NetBIOS Domain Name** : e.g. ACI
Database Location and Log Location	Recommended to use the **default path**
Shared System Volume	Recommended to use the **default path**
If a DNS Server is not installed, a message will appear	Confirm and install the DNS server on the PC
Permissions	Select whether to allow permissions to non-Windows 2000 or strictly only to Windows 2000 servers.
Administrator password for Directory Services Restore Mode	**Administrator password :**
Confirm the Summary information	Click **NEXT**
Active Directory Wizard is configuring the installation	Have the Windows 2003 CD ready in the CD-ROM drive
Installation Completed	Click **FINISH** and **Restart the PC.**

Table 3.2: Primary Domain Controller creation

a. RMC Server/Client:

The RMC (Remote Management Console) is the geo-redundancy administration SW. The RMC installation is dependent on the ACI/OEM. ACI/OEM must be installed in one of the domain machines. RMC requires Versant DB that's why we should indicate the Versant path in the machine where the ACI/OEM is installed:

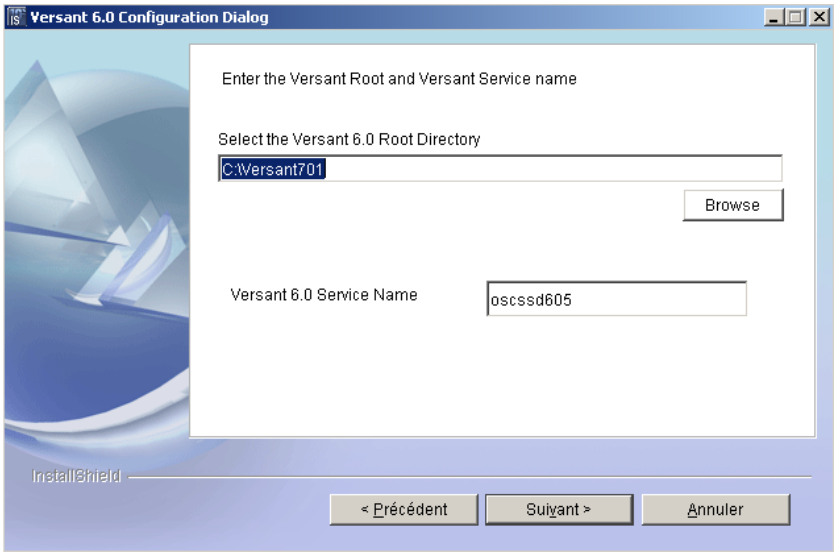

Figure 3.19: Versant path indication

Then we should set the users that are illegible to connect to RMC server as figured below:

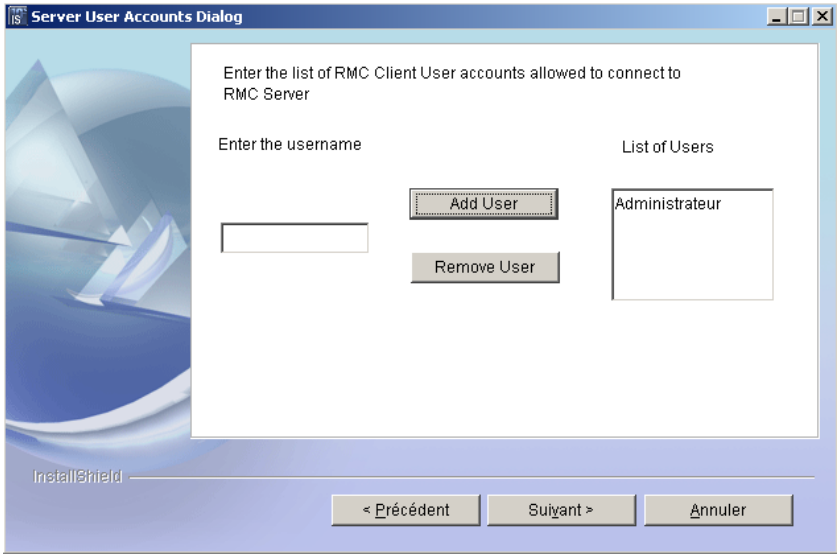

Figure 3.20: Users' authentication

After the install Shield finalizes the installation a system reboot is required.

When the installation is done, we can see that all the services are down; they will be loaded when we start the geo-redundancy.

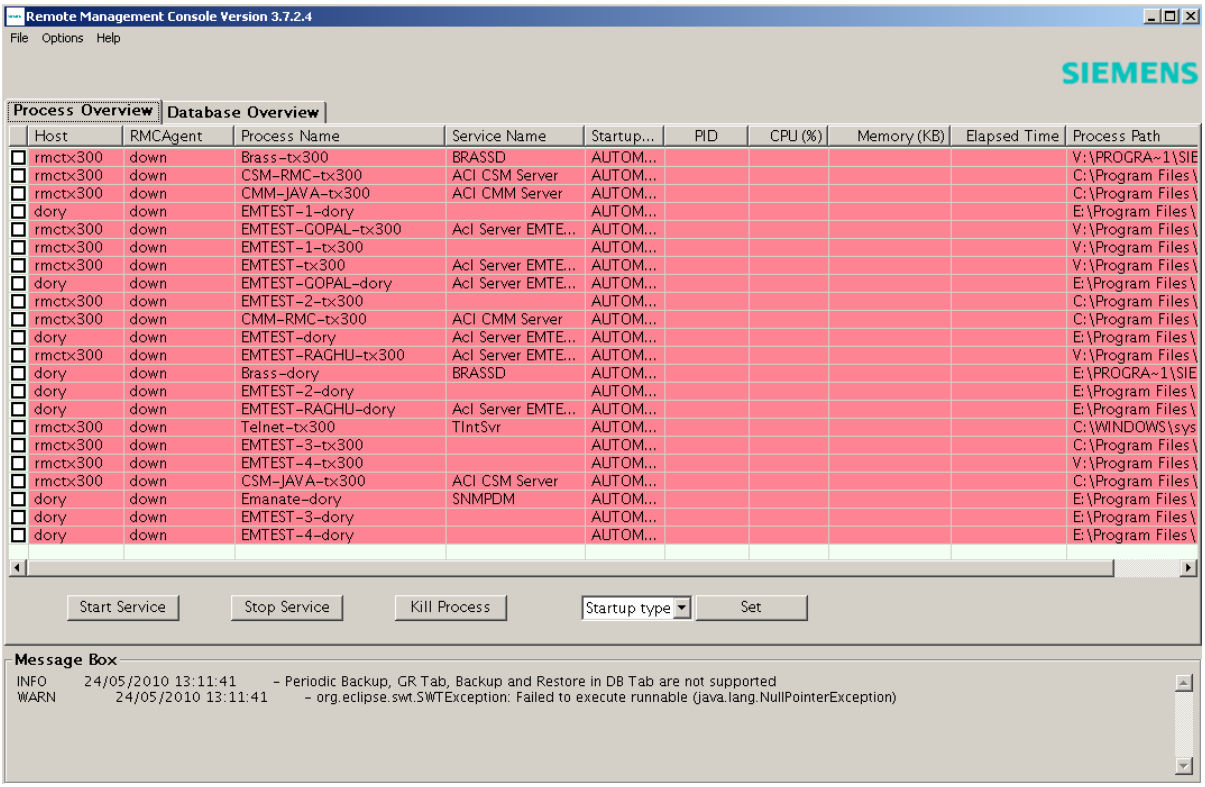

Figure 3.21: RMC SW

b. ACI/EM-GX Clients:

This RMC server ensures the geo-redundancy of the ACI/EM-GX which manages the HiX equipment, for this reason we installed two clients of the EM-GX one in a worker mode and the other in a standby mode.

During the installation the naming service machine's IP address should be verified carefully because once it's introduced it can't be changed unless we reinstall everything.

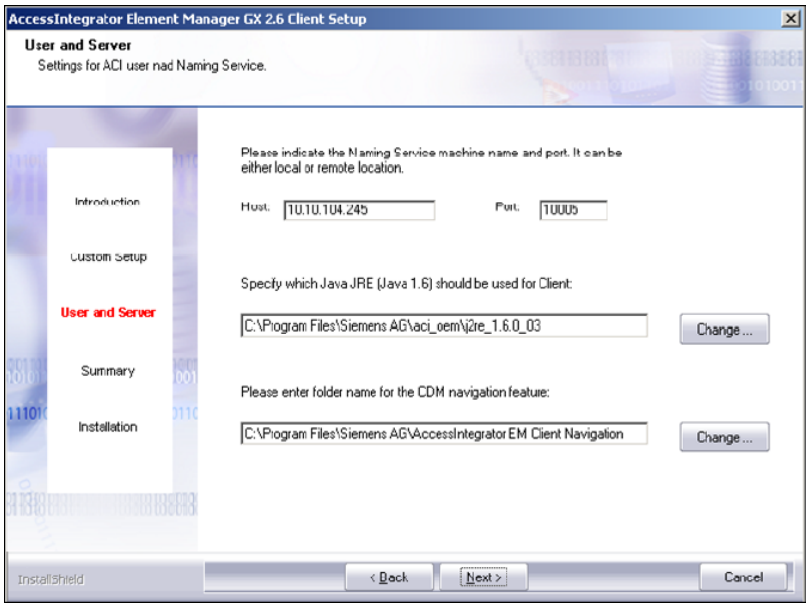

Figure 3.22: Corba naming service verification

We can see in the following figure that the EMGX server's IP address is indicated in the login panel. The difference between the worker client and the standby client is that the worker client is linked to the worker server's IP address and the standby client to the standby server.

Figure 3.23: EMGX login

3.3.2. RMC2:

The RMC2 machine contains the same Software as the RMC1 except for EMGX, instead there is EMDX which is the controller for the HiD equipment and the installation procedure is typically the same. We should also verify the IP addresses for the worker and the standby clients.

The RMC2 is also the secondary DC of our domain. The secondary DC installation isn't much different from the primary; the only difference is instead of creating a new forest we just add our server to an existing forest:

Start Active Directory Wizard	Go to "Start" → "Run" and type in : **dcpromo** (= **d**omain **c**ontroller **promo**te)
Active Directory Wizard Welcome screen	Click **NEXT**
Domain Controller type	Domain Controller for an **existing domain**
Join Forest	**Join Forest** (if the Forest is already created)
Network Credentials	Authorization to administer Forest **Admin Username :** **Password :** **Domain :**
Full DNS (Domain Name)	Enter the DNS name for the new Domain Tree **Full DNS name :** e.g. ACI.com
NetBIOS Domain Name, the name other users will use to identify the new domain.	Confirm the NetBIOS Domain Name. **NetBIOS Domain Name :** e.g. ACI
Database Location and Log Location	Recommended to use the **default path**
Shared System Volume	Recommended to use the **default path**
If a DNS Server is not installed, a message will appear	Confirm and install the DNS server on the PC
Permissions	Select whether to allow permissions to non-Windows 2000 or strictly only to Windows 2003 servers.
Administrator password for Directory Services Restore Mode	**Administrator password :**
Confirm the Summary information	**Click NEXT**
Active Directory Wizard is configuring the installation	Have the Windows 2003 CD ready in the CD-ROM drive
Installation Completed	Click **FINISH** and **Restart the PC.**

Table 3.3: Secondary Domain Controller creation

We must provide the primary server's permission to this server to join the existing domain:

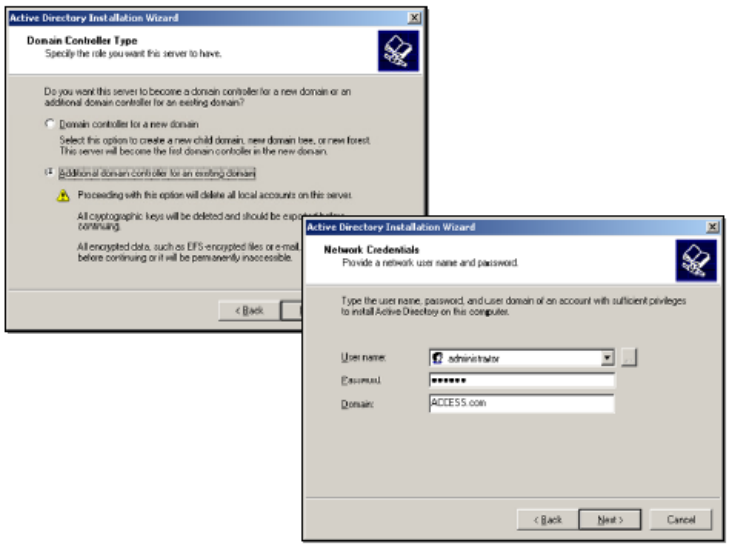

Figure 3.24: Obtaining the DC's permission to join the Domain

3.3.3. GX1 and GX2:

In addition to the installation of the OEM, the administration server and the licensing server previously seen in the Core installation section, the EMGX server has to be installed here.

The EMGX server works in three modes: work station, network mode which is our case or a custom installation where we can provide our necessities:

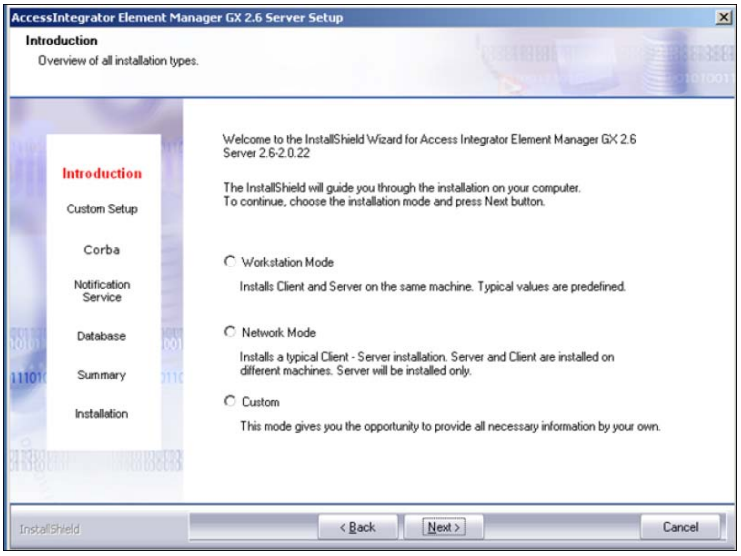

Figure 3.25: EMGX installation mode

Then we specify the naming service machine which allows the other machines to connect to the server as the domain controller or in our case the RMC1.

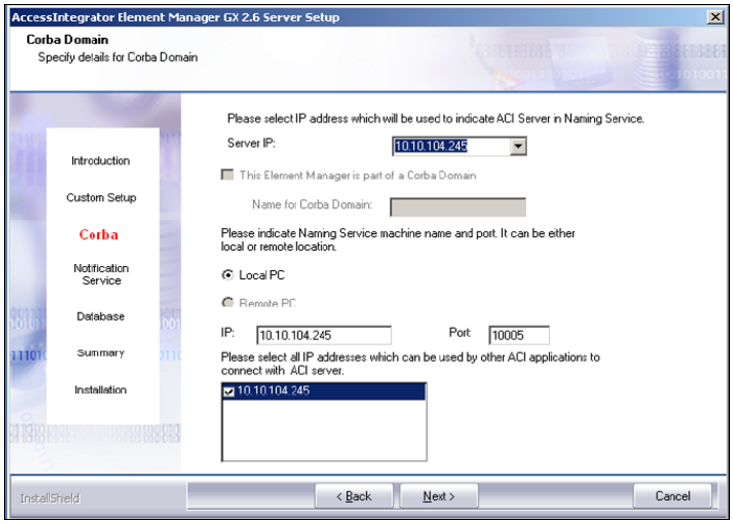

Figure 3.26: CORBA naming service verification

The last step is to install the DB and to choose its backup directory.
The GX2 server is basically a clone of the GX1 server but its services are in a standby mode.

3.3.4. DX1 and DX2:

The DX servers are similar to the GX in their functionalities and their SW installation where we find the OEM and EMDX installation of which is similar to EMGX installation. The only difference is that there is no need to install the licensing and the admin servers as we need only one server of each SW per domain. However, we add the CDM (Cross Domain Manager) server to the OEM, RMC agent and the EMDX.
The Cross Domain Manager is used as an additional operational support for the management of large networks of multiple NE types.
This way we are able to see all network elements in the Graphical User Interface (GUI) of the Cross Domain Manager. Network tasks such as alarm handling via a central alarm list or drawing of network maps are possible.
For operational tasks on the network elements level an ACI EM client session is opened and the operator is able to configure, in dependency of the security management, the network elements. Implemented in the ACI, Cross Domain Manager is the Security Management based on functionality and a selection of network elements (security domaining). The installation of the CDM server is similar to the other ACI-EM servers.

3.4. Geo-redundancy:

The basic concepts of the Geo-redundancy are:

- To each host on worker site there is a second host on a standby site.
- There are multiple worker/standby sites possible.
- Only the applications on one site are up and running, e.g. on worker site. This site has the master role.
- On the alternative site, e.g. standby, the database is kept up to date by a replication mechanism (replication channel), but all applications on this site are stopped, except the RMC agent and the database server. This site has the replica role.
- In case of a disaster strike, i.e. the master site becomes unavailable and then the alternative site, e.g. the standby site, will start up the applications. After such a switchover the roles are changed, the standby site is then in either standalone or in master role.
- A switchover can be carried out in two ways:
  - Manually (by the operator)
  - Automatically (based on rules by the RMC manager)

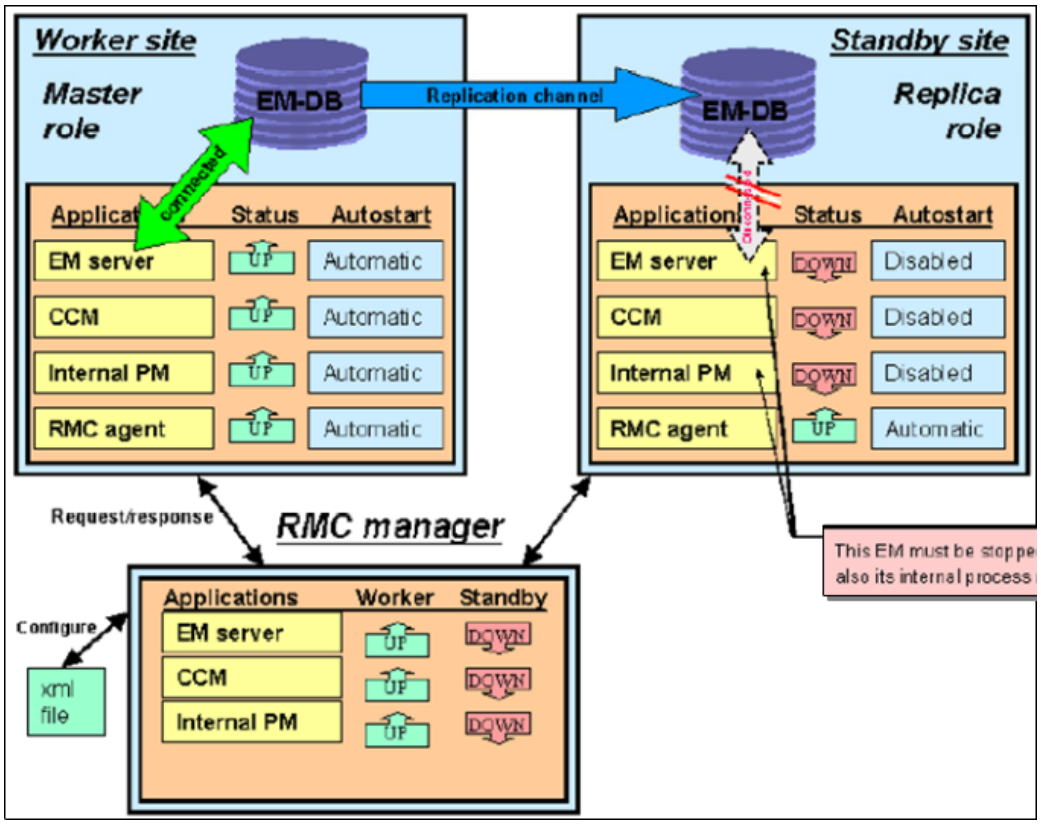

Figure 3.27: Geo-Redundancy

3.4.1. Concept:

The worker and standby sites are assigned per configuration in **RMC_Config.xml** file to a server pair where one server does actively send replication information and the other server passively receives database replication information. Typically, the site which has the initial master role will be the worker site.

TIP: In case of a Geo-Redundancy switchover the site names are not changed, but the roles are changed.

Roles:

• Master

This is the active side. The EM server is up and running. Changes to the database are sent to the replication channel.

• Replica

This is the passive side. The EM server is initially stopped. Only the database process is running. Changes made in the master database are received from the replication channel and entered into the database so that the replica database has the same content as the master database.

• Standalone

This can be an active side, with the EM up and running. Changes to the database are not replicated (neither transmitted nor received). The roles can be assigned and changed via the RMC manager in the “Geo Redundancy” tab.

3.4.2. Automatic Switchover Mechanism:

In RMC Geo Redundancy solution, processes are ensured high availability in a Geo Redundancy site, using automatic switchover for a pre-defined set of use cases. A Geo-Redundancy site contains two machines called worker and standby, as mentioned earlier. The RMC manager supports management of multiple Geo-Redundancy sites at a time. Each Geo-Redundancy site is managed independently. Each Geo-Redundancy site can enable or disable the automatic switchover feature from the RMC manager. Any number of Geo-Redundancy sites can have automatic switchover enabled at the same time, from one RMC manager.

As the automatic switchover is performed by RMC manager, manager must be running all the time.

TIP: Automatic switchover for a Geo-Redundancy site is enabled only by double clicking the Geo-Redundancy site in the “GR Sites” table and clicking on "Enable" button. Single click on Geo-Redundancy site in the “GR Sites” table will not enable automatic switchover.

TIP: When automatic switchover is enabled and all the monitored processes in master site and replica site are down but then RMC manager will bring all processes up in the master site.
If one or a few processes go down in master site, the processes in replica site are brought up and processes in master site will be brought down by RMC manager.

In a Geo-Redundancy site, the status of processes is constantly monitored by the RMC manager. If the processes use Versant database, replication feature can be integrated into the Geo-Redundancy solution by specifying it in the RMC_config.xml configuration file. Also, if a process becomes unavailable in a Geo-Redundancy site, RMC manager takes care of making it available in either worker machine, or standby machine, based on automatic switchover algorithm.
When there is a failure in one machine then all the monitored processes are automatically switched over to the other machine by the RMC manager. This step involves bringing down all the monitored processes in the failing machine and starting all the monitored process in the other one.
RMC supports the local process monitors for the processes participating in Geo-Redundancy. If a local process monitor is present, automatic process restart is available for the process.
In Windows and Solaris, certain ACI servers install their own local process monitors, for the ACI EMs to configure the local process monitors in a Geo-Redundancy site.
The RMC manager can manage Windows Geo-Redundancy sites and Solaris Geo Redundancy sites at the same time. The Geo-Redundancy sites to be managed are defined in the RMC manager configuration file.
Automatic switchover feature is disabled on manager startup. The operator has to enable it manually. This is for a safety reason, when multiple managers have the configuration file to manage the same Geo-Redundancy site. The operator will ensure that automatic switchover is enabled only in one manager for this particular Geo Redundancy site. If two different managers send conflicting commands to the same Geo-Redundancy site, the system behavior is undefined.

TIP: Startup type of services should be either manual or automatic in Windows and automatic only in Solaris if automatic switchover is to be supported. RMC manager will not start the service if the startup type is disabled.

3.4.3. Geo-Redundancy types:

In networks with CDM installed on top of EMs there will be two alternatives for the Geo-Redundancy configuration:

- EM redundancy
- Full redundancy

In our case we use the full redundancy type which consists of replicating the entire worker site to the standby site:

- Redundancy for EMs and CDM and CORBA naming service.
- A switch over is only possible for the entire site.

In this setup the EMs and the CORBA naming service and the CDM are doubled up geo redundantly. This scenario has the advantage that CDM and naming service are also redundant. The disadvantage is that a switchover of only one EM or only the CDM is not possible; a switchover has always to be made for the entire site, i.e. for all EMs and naming service and CDM.

The CDM worker communicates only to the worker EMs.

The CDM standby communicates only to the standby EMs.

The CDMs will never communicate to a mixture of worker/standby EMs.

The “Geo-Redundancy” tab in the RMC Console monitors and controls the status of the Versant Asynchronous Replication (VAR). VAR enables Versant databases to be replicated automatically. The worker and standby servers of a Geo Redundant pair of servers are in a master/replicant relationship, where the master is the transmitting site and a replica is the receiving site.

Fields:

Field Name	Description
GR Sites	Several pairs of Geo Redundant hosts may be configured in the `RMC_config.xml` file. Each pair is displayed in the list of “GR Sites”. Selection of a pair of hosts is done by left mouse double click. The pair of hosts which is selected is displayed in color blue. The tables for “Worker” and “Standby” and “Application Details” will display the applications of the selected pair of hosts. Enabling automatic Geo Redundant switchover for a pair of hosts is done by the “Enable” and “Disable” buttons below the “GR Sites” list of hosts. When automatic Geo Redundant switchover is enabled, then button left to the pair of hosts will be colored in green. When automatic Geo Redundant switchover is not enabled, then button left to the pair of hosts will be colored in blue.
Worker	The worker part of a Geo Redundancy site as configured in this `RMC_config.xml` file
Standby	The standby part of a Geo Redundancy site as configured in this `RMC_config.xml`
App ID	Application ID as configured in the `RMC_Config.xml` file. It is a placeholder for the configured process name, service name and database. Any alphanumeric string can be chosen and assigned. Please refer to hints in chapter 3.1 "Monitoring and Control of Processes and Services" and 4 "Geo Redundancy"
Role	Replication role (master, replica, standalone)
Channel fill-state	Number of outstanding updates to the replica database
Host	Host where the application resides
RMC Server	Status of the RMC agent
Process Name	Process name of the given application
Service Name	Service name of the given application
Startup type	Startup type of the service (automatic, manual, disabled), see also 3.1.3 "Startup Types"
Database name	Database name

Table 3.4: RMC fields

Buttons:

Button	Description
Enable	Enable automatic switchover surveillance
Disable	Disable automatic switchover surveillance
Refresh	Manual refresh of the "Geo Redundancy" tab (not of any other tab)
Start service	The service of the selected application ID will be started.
Stop service	The service of the selected application ID will be stopped.
Set	Set the selected startup type for the selected application ID.
Configure standalone	A master or replica database is set back to a standalone role (it will no longer transmit nor receive replication information).
Configure master	A database is configured to a master role in the replication scenario. This is normally done form the status standalone.
Configure replica	A database is configured to a replica in the replication scenario. This is normally done from the status standalone.
Start channel	Start the VAR channel (which transports the messages on changes in the master database to the replica database).
Stop channel	Stop the VAR channel.

Table 3.5: RMC Buttons list

The figure below shows the Geo-Redundancy tab and the options available in it.

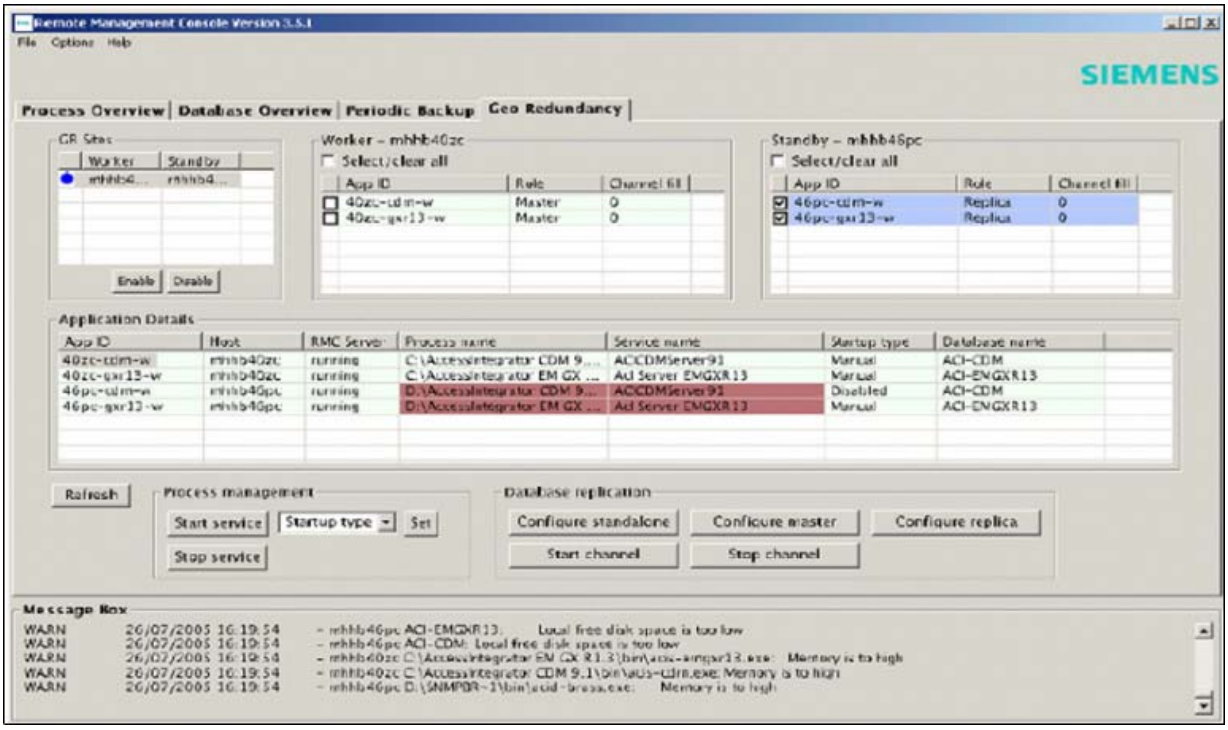

Figure 3.28: RMC Geo-Redundancy

3.4.4. Configuration:

The RMC manager holds little configuration information:

- RMC manager configuration (in **RMC_Config.xml** file)
- Configuration properties (in **rmcclientconfig.properties** file)
- Geo Redundant replication properties (in **replication.properties** file)

Generic Remarks

The RMC manager holds most of the configuration information in RMC_Config.xml file, e.g.:

- Which processes/services are to be supervised on which server.
- Their executable and service names
- The thresholds which are to be supervised
- The association of hosts to a Geo-Redundant pair of hosts, etc.

After a change of the **RMC_Config.xml** file, it will have to be reloaded in order to become effective in the RMC manager. This is done via RMC manager menu:
“File” -> “Reload XML-file”.

3.5. SW maintenance:

The operator has the possibility of maintaining the SW using either the CLI or ACI and this is one of the advantages of the centralized management system.

3.5.1. SW management using CLI:

The operator has the possibility to use the Command Line Interface to perform the Software Management tasks. If a backup of a configuration file or an upgrade of the software of the NE is needed they can be performed directly through a console cable. It's also possible to connect through a telnet session to the management interface of the CXU board.
For the console connection, a SW that can read and write from the COM port is needed (e.g. HyperTerminal). For the telnet session the operator has first of all to configure the management interface inside the equipment (with a given IP address) and only after that can he establish a telnet session to the NE.
On what follows we will see some of the functions that the user should apply while performing the Software Management tasks on the hiX 56xx using the Command Line Interface.

a. Checking the NE configuration:

The user has some commands available on the CLI which allow him to check if the configuration of the NE is correct before the backup is performed. It's possible to see the complete configuration of the element or see only a specific set of parameters like SNMP settings, VLAN configurations or Interfaces. The next table shows the most common commands used to check the current configurations and some of their variants.

Command	Mode	Function
Show running-config	All	Shows the complete system configuration
show running-config { arp bridge | dns | full | hostname | login | qos | rmon | router | rule | snmp | syslog | time-zone | time_out }		Shows a configuration of the system with the specific option
show running-config **interface** interface name	Privileged Global	
show running-config { adsl | atm | erp | lacp | mac | max-hosts | shdsl | stp | trunk | vlan }		

Table 3.6: CLI commands for the NE maintenance

As an example, the next pictures display an extract of actual results obtained after performing some of the commands listed above. Those commands were performed using the remote telnet session.

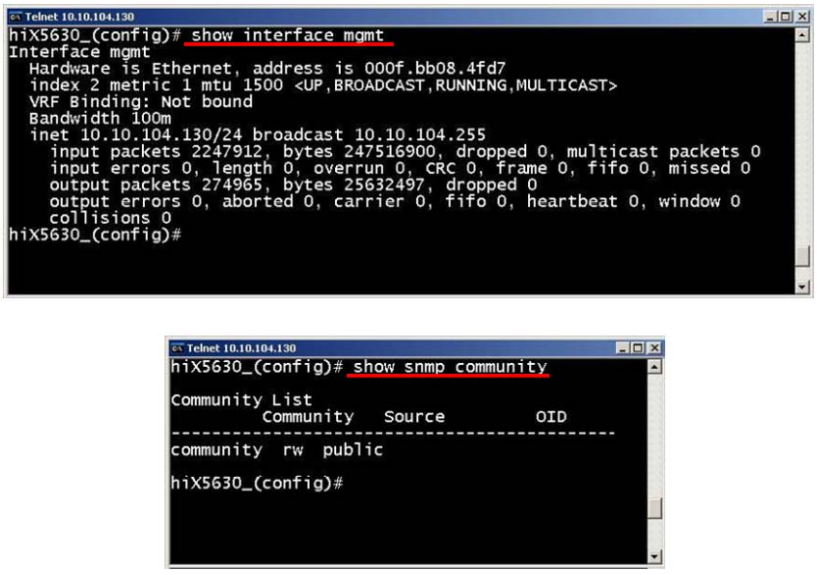

Figure 3.29: Examples of different "show" commands using telnet session

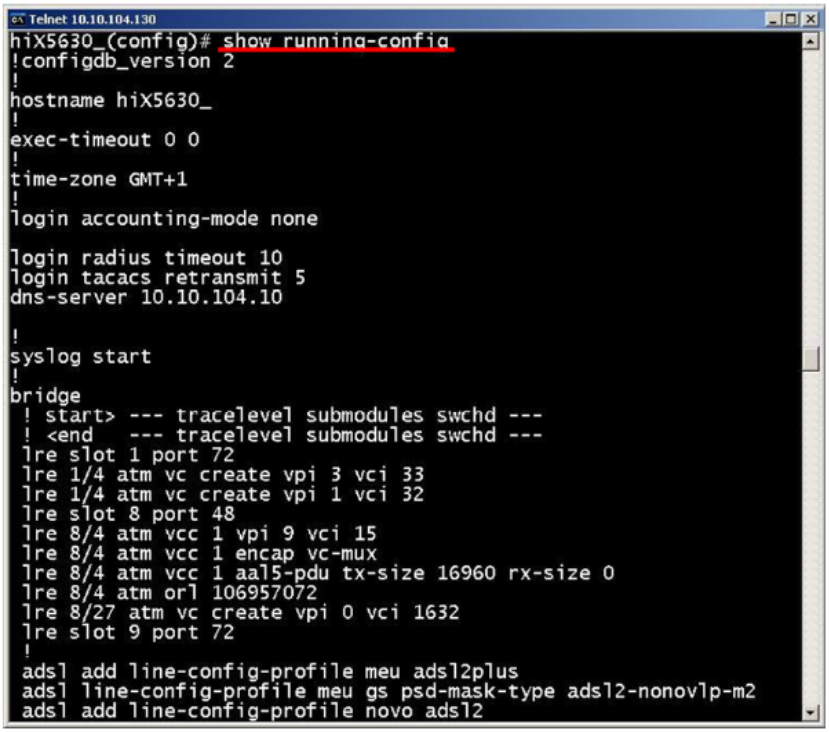

Figure 3.30: "Show Running-Config" command and extract of the information returned

b. Saving System configuration:

After the configuration files are changed, the operator should save the changes in the flash memory, or else the configuration file will be lost in case of system rebooting, resulting in all unsaved configurations to be lost.

To save the system configuration we use the following command:

Command	Mode	Function
write memory [destination]	All	Saves changed configurations in the flash memory.
write [file | terminal]	Privileged	Destination: configuration file name Terminal: current terminal (same as show running-config)

Table 3.7: CLI commands for saving system config

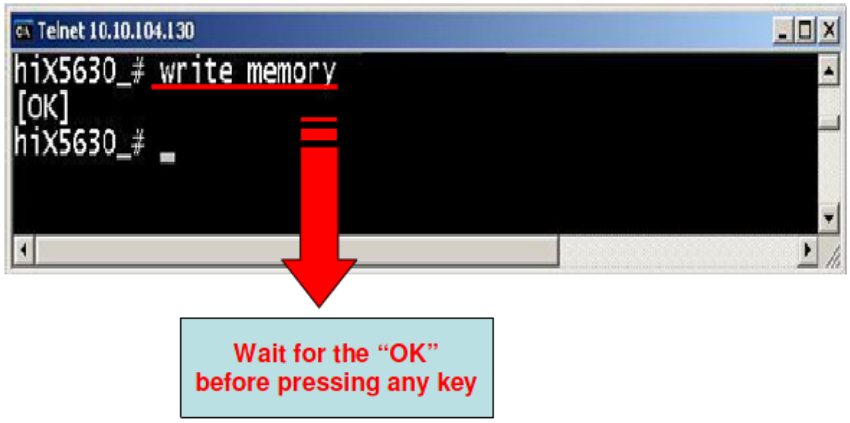

Figure 3.31: "Write memory" command

c. Managing system config files:

It's possible for the operator to create and save configuration files inside the hiX56xx.

The operator can choose to backup the current running configuration or the startup configuration and then create a new local config file. The operator can later restore a saved config file back to the startup configuration and reboot the system with the new configuration. He can also decide to perform the backup using a remote server where a designated configuration file, previously saved inside the hiX, will be transferred via FTP to the remote location.

To use the backup capabilities of the NE use the following commands: Note that variable "filename" showed in the next commands represents a filename that can be configured by the operator.

Command	Mode	Function
copy running-config {filename/startup-config}	Global	Copies the running configurations to a config file or to the startup-config.
copy startup-config filename		Copies the startup configuration to a config file specified by the operator.
copy filename1 filename2		Copies a config file with a different name.
copy filename startup-config		Copies a designated config file to the startup configuration.

Table 3.8: Commands for the config files management

To check the current status of the configuration files it is possible to consult the list of all files created.

Command	Mode	Function
show config-list	Privileged / Global	Lists all configuration files inside the NE. These files are created with the copy commands in the table above.
erase filename		Deletes a designated configuration file.

Table 3.9: Commands for current status check

The next images will help illustrate some of the commands we have just seen for managing the configuration files inside the hiX system.

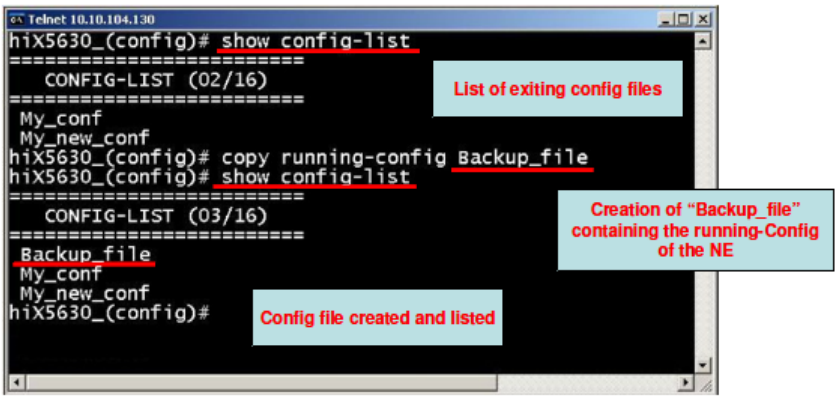

Table 3.32: Example of storing the running configuration to a local config file

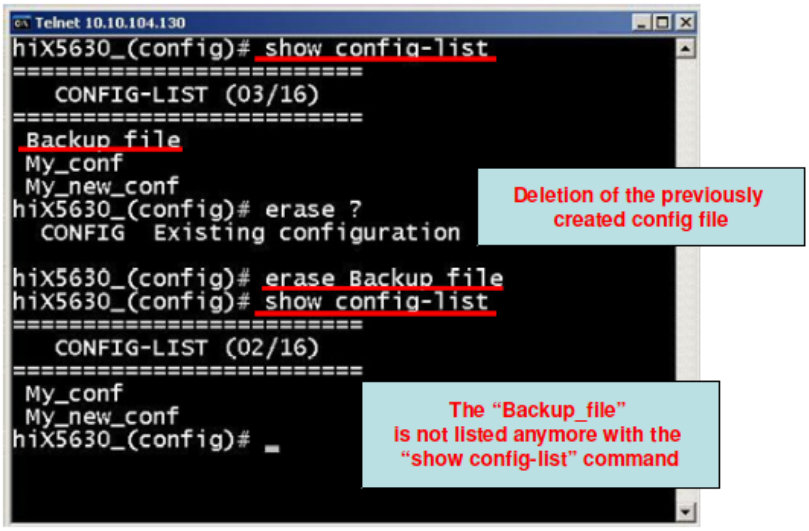

Figure 3.33: Erasing a Config file

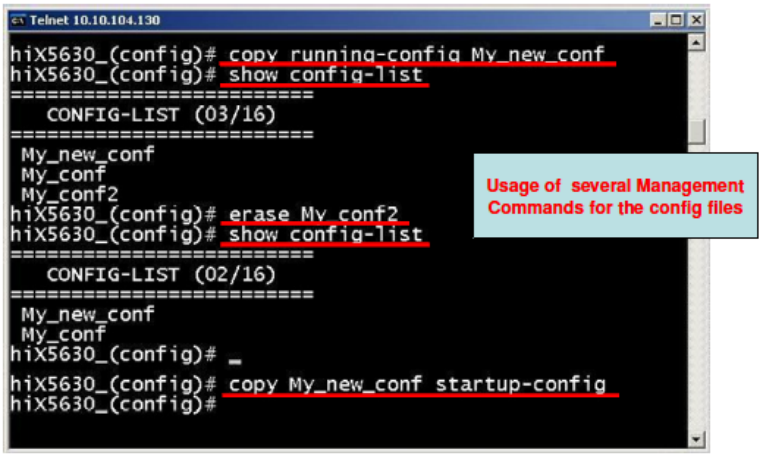

Figure 3.34: Config File Management

d. Restoring the defaults configuration:

The operator can delete or change the configurations one by one but he also has the possibility to reload the complete configurations of the NE with the default settings.

To restore the default configurations of the system the operator should use the following commands:

Command	Mode	Function
restore factory-defaults	Global	Restores the factory default configuration.
restore layer2-defaults		Restores the layer 2 default configurations.
restore layer3-defaults		Restores the layer 3 default configurations.

Table 3.10: Commands for default configuration restore

Remember that after the restore of the factory defaults it is still necessary to reboot the system for the new configurations restart. To reboot the switch the operator should use the following command:

Command	Mode	Function
reset { all | card | type}	Enable	Reloads the NE to boot with the new configuration.

Table 3.11: Commands for the card reload

At any time the operator can check the status of the two OS images inside the NE (The NE contains two OS images one is set to be a default and the other a rescue image which is backed up occasionally from the default OS.

To do so he should use the following command:

Command	Mode	Function
show flash	Enable	Displays the current OS information including the size and the version of each OS image.

Table 3.12: Commands for OS status check

The following screenshots show some of the commands previously used:

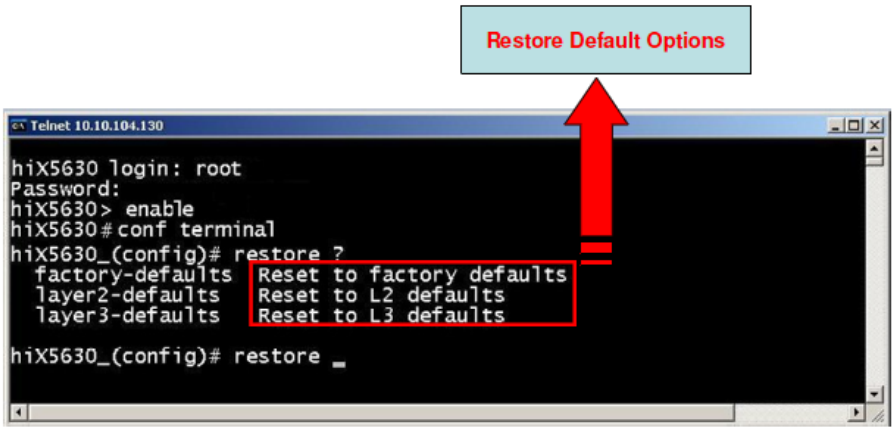

Figure 3.35: Restore Default options

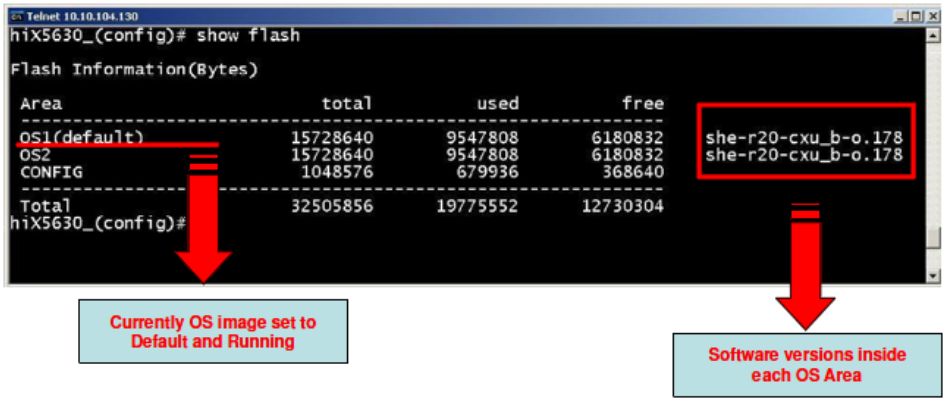

Figure 3.36: "show flash" command and returned information

3.5.2. SW management using ACI:

The ACI-E offers a set of tools especially designed to handle the Software inside the hiX5600 system. These tools allow the management of both configuration files and operating system software. The user can, for instance, upgrade the OS image or restore a designated configuration file in case of need.

These tools belong to the Software Management functionality and can be found under "NE Maintenance" inside the "Maintenance" menu in the main window of the ACI-E.
We will now take a closer look at some of these functionalities and focus on the Software Management capabilities of the hiX5600 IP DSLAM.

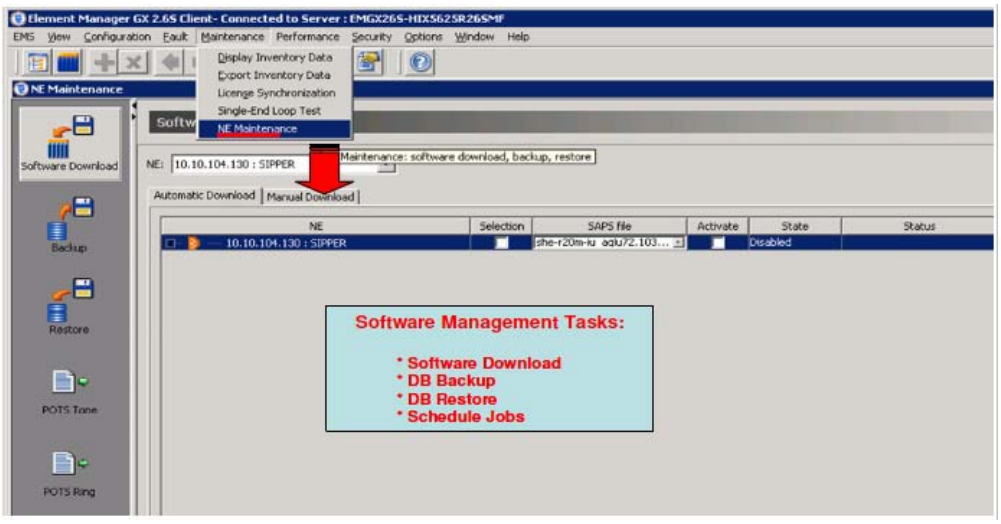

Figure 3.37 "NE Maintenance" in the "Maintenance" menu

a. FTP Information:

Before performing any of the Software Management tasks, like downloading the system's software, it is necessary to check if the FTP information is properly configured in the NE. This information is entered when the NE is added to the SNMP DCN Tree in the ACI-E and is essential to access the FTP server and perform the data transfer.
This information includes the FTP server address, the user authentication (login and password) and the name of the directory inside the FTP root. To specify the directory only the relative path inside the FTP root is necessary and the "\" must be changed to "/" on the path!
To check or change this information about the FTP server the operator should go to "SNMP Settings" by right clicking on the desired NE. Then on the "User Settings" tab it is possible to read or change the configured values. Remember that if this window doesn't contain the right information about the FTP server no tasks that involve the data transfer to or from the FTP will be possible.
This is a slightly different method from the one used in the previous hiX5300 ATM DSLAM, where the information about the FTP server (IP address, authentication and name of the directory) was sent to the NE by the DHCP server during the startup procedure. Now this information should be configured by the operator when a new NE is added on the ACI-E.

The FTP server stores not only the software loads for the individual boards (CXU and IUs) but is also used as a repository for the backed up configuration files and for the uploaded log files.

b. Upgrade of the NE:

To perform a software upgrade, a backup or restore on the hiX56600 the user should open the "NE Maintenance" window and go to the "Software Download" tab.

In case of a software upgrade, the existing software version continues working in RAM memory. Only after activation is the new load transferred to the RAM overwriting the previous version. The activation requires a reboot of the plug-in unit.

If the software upgrade results in a new NE version, the change is noted automatically in the SNMP-DCN view provided that the "System Upgrade" option is enabled during the software update. If this option is not selected, it is necessary to delete and reinsert the NE from the DCN tree so that the system recognizes the new version.

In this window it is possible to access all available loads stored in the software directory on the FTP server. The different lists show the affected NEs or Plug-In Units, the current running software and the stored software loads. The user can choose between the different loads through a drop-down list.

The next image illustrates the "Software Download" window in ACI-E.

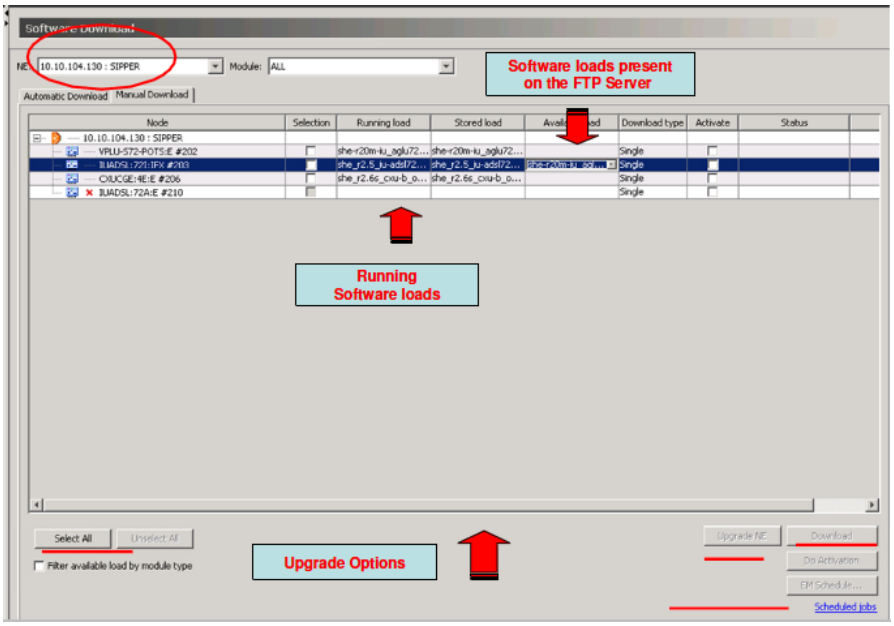

Figure 3.38: Configuration backup options in ACI-E

A normal procedure for a software download will be as follows:

Select a single NE or a group of NEs and open the "Maintenance" ➔ "NE Maintenance" from the main menu. Choose between the download options available or press the "Download" button for an immediate start of the download procedure. Between the download options we can find for example "Activation after Download" that will reset the unit as soon as the download is complete, forcing this way a reload of the Plug-In Unit with the new software.
Enable "All of Type" to update all PIUs of the same type on the NE to the selected software.

c. Backup and restore of the NE:

To configure the Backup and Restore of the database inside the hiX5600, the user should open the "Maintenance"➔ "NE Maintenance" window from the main menu.
On the left hand side there will be available the Backup and Restore options for the NE.
These options allow the safe storage of the Database and of all the configured parameters on a remote FTP server, where this information can be later accessed whenever necessary.
The database should be backed-up regularly in order to ensure a safe storage of the configurations of each NE. The database backups can be done at any time manually, or they can be configured as a time schedule job, in a way like we have seen before in case of the software download procedure.
The operator can with these options backup the configuration file to a location designated for data recovery. If the actual configuration file gets corrupted it is possible to restore the baked up file.
After configuring the NE the data must be saved or else all configurations will be lost if a reboot of the NE occurs. That's why the backup and restore procedures are fundamental tasks in managing the network elements, adding an important security level in terms of security and safety of the system's information.

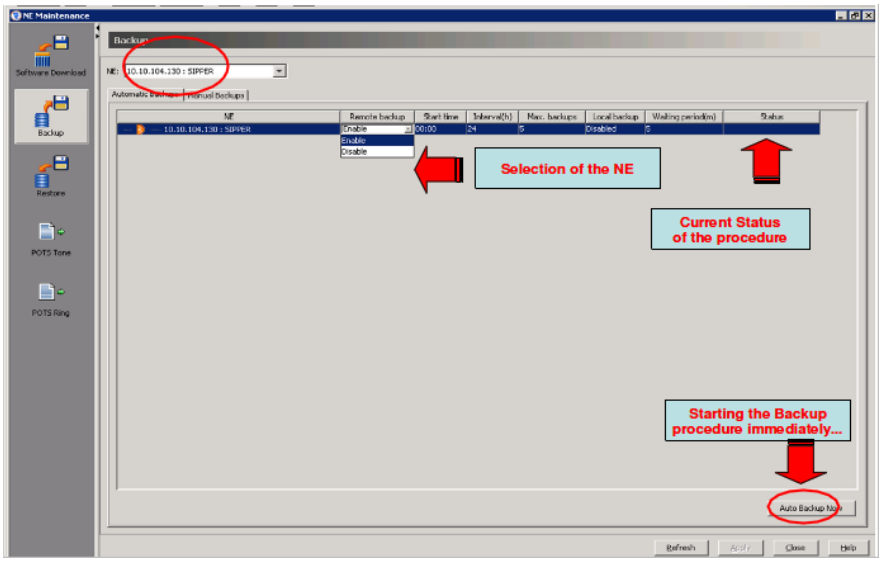

Figure 3.39: Database Backup with ACI-E

d. Restoring a NE DB:

The Restore function is intended for a download of a previously backed up database to the NE. During this procedure the latest (or one of the latest databases) stored in the FTP server is transferred back to the selected network element. The available databases are accessed via a drop-down list on the "Restore" tab inside the "NE Maintenance" window. So basically the Restore procedure transfers the remotely stored database from the FTP server to the NE. The FTP server must be available to the NE and there must be some stored files which include the name, the IP address of the NE and the date and time when the file was backed up. These files have **.data** extension.

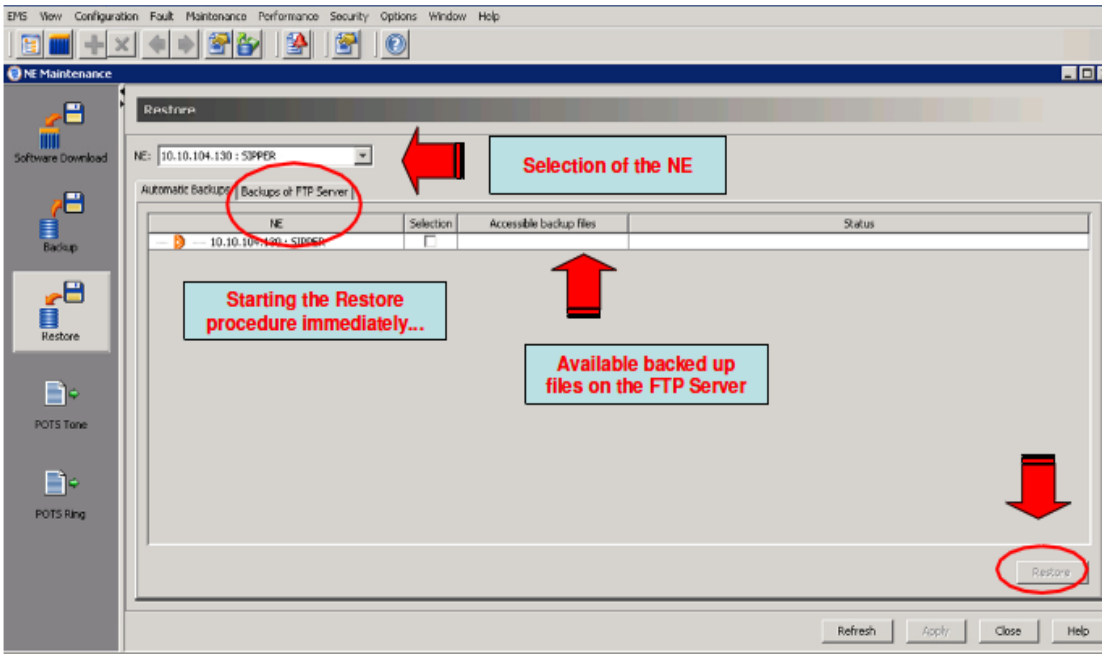

Figure 3.40: Restore procedure with ACI-E

Chapter 4

Installation and configuration of the equipment

4. Chapter 4: Installation and configuration of the equipment

After connecting all the equipment we proceed by the configuration starting with our main NE: the DSLAM which is composed of the hiX 56xx and the hiD.

4.1. DSLAM configuration:

The configuration could be made either with the CLI by connecting to the equipment via the telnet through a serial port (see figure below)

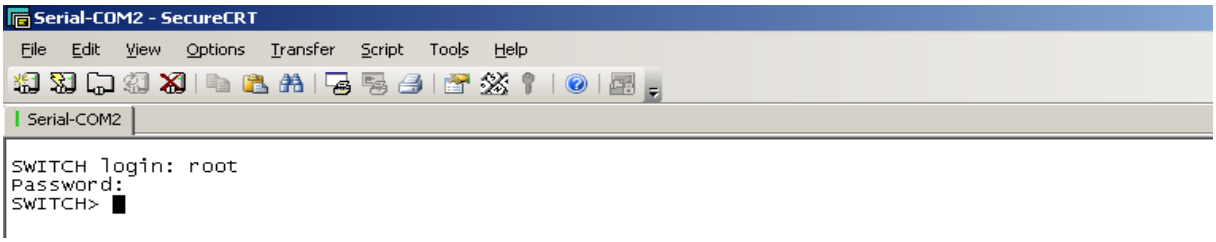

Figure 4.1: Connecting to the DSLAM via serial port

or with the ACI-EM (see *Figure 3.24*) which is our management software that we have already installed as in the administration and the management chapter, through a graphic interface. The DSLAM configuration consists in two scenarios:

- Single tagging
- Double tagging

4.1.1. Single tagging scenario:

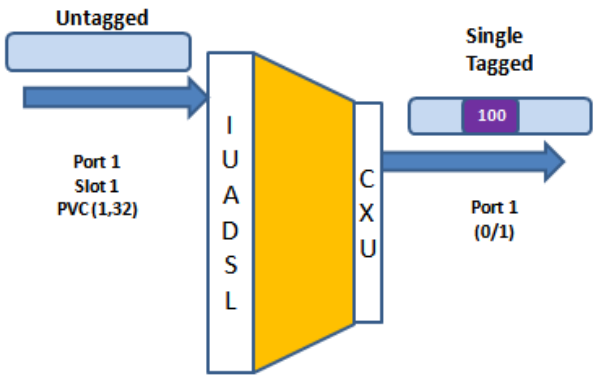

Figure 4.2: Single tagging scenario

The traffic received from the user at the port 1/1/1 is a traffic without VLAN tag. The DSLAM tags the traffic with a VLAN ID 100 and then sends it to the uplink via port 0 / 1 of CXU card.

a. Creating and configuring the VLANs:

✓ **CLI configurations:**

To create a VLAN we should connect to the equipment in a bridge mode and use the following configuration lines:

- HiX5635(bridge)# vlan create 100
- HiX5635(bridge)# lre 1/1 atm vc create vpi 0 vci 35
- HiX5635(bridge)# lre atm vcc 1 vpi 8 vci 35

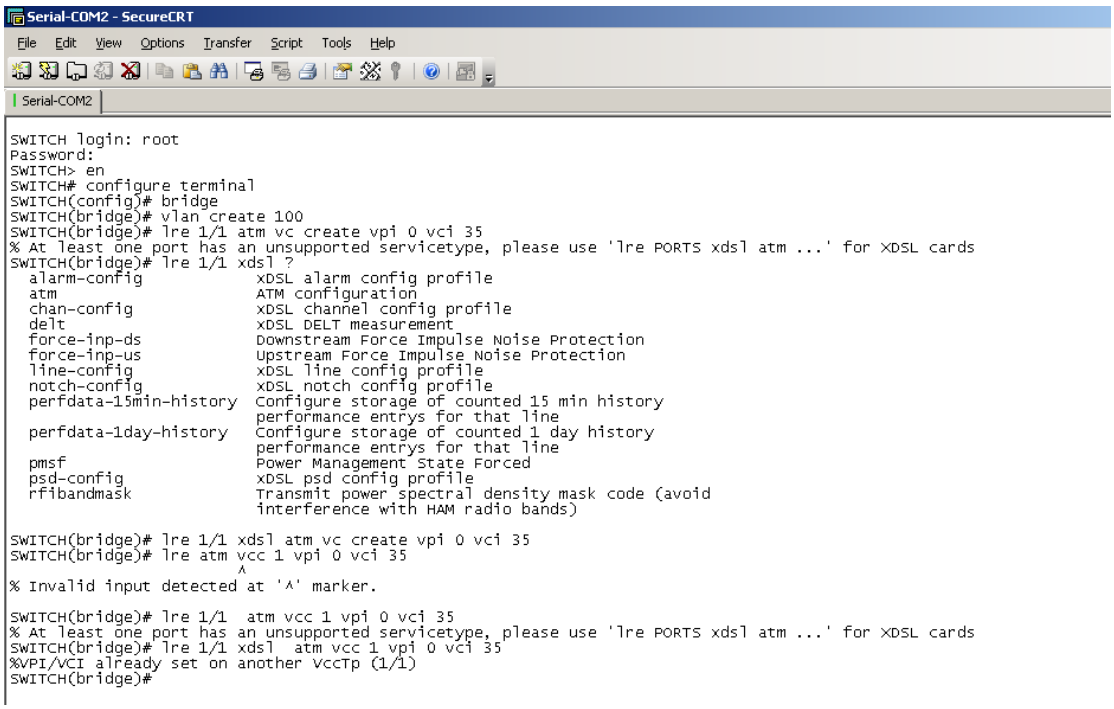

Figure 4.3: VLAN creation with CLI

✓ **ACI configurations:**

With the ACI we use the VLAN menu to create a new VLAN and provide its specifications.

To create a new VLAN

1) Select the NE in the Network view.

2) Click “Configuration” -> “Equipment Configuration” from the main menu. Select "Bridge" under the desired NE and inside choose the "VLAN" option in the navigation pane.

3) Open the “Overview” tab. This tab lists all created VLANs.

4) Click “New” and choose the VID.

5) Click “OK”.

This will create a new VLAN inside the system with configured VLAN ID. The range of valid VLANs is from 0 to 4095, although inside the system some VLANs are already reserved and are not intended for normal user application.

The next image illustrates the VLAN Configuration dialog inside the Global Bridge Configuration window.

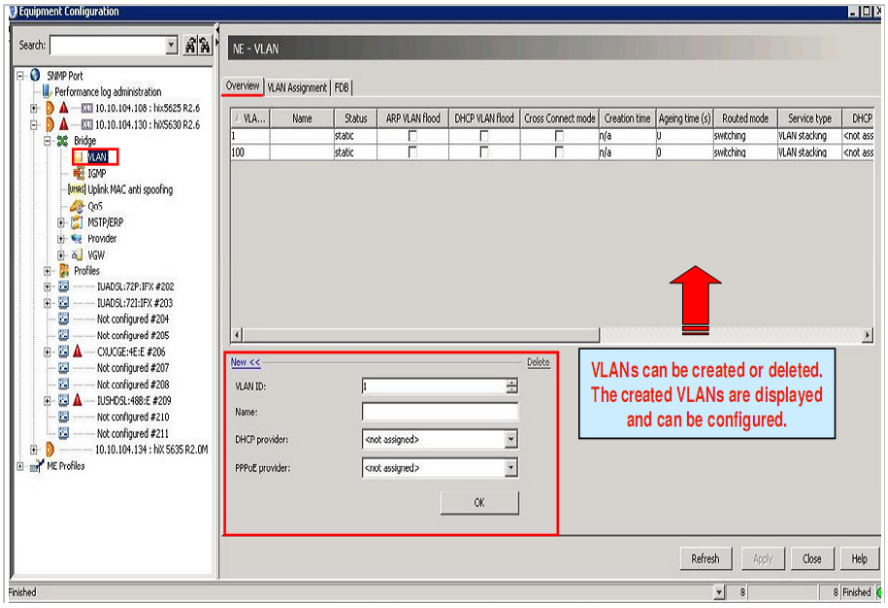

Figure 4.4: VLAN creation with ACI

b. Bridgeport configuration:

After creating the VLANs we must configure the bridgeports as well as their tagging mode.

✓ CLI configuration:

- HiX5635(bridge)# port lre 1/1 disabled

The port must be disabled before configuring it; we can't perform any action on an active port.

- HiX5635(bridge)# bridgeport 1/1 taggingmode untagged

To configure a port it must be set to an untagged mode because it is useless to configure it while it is tagged.

✓ **ACI configuration:**

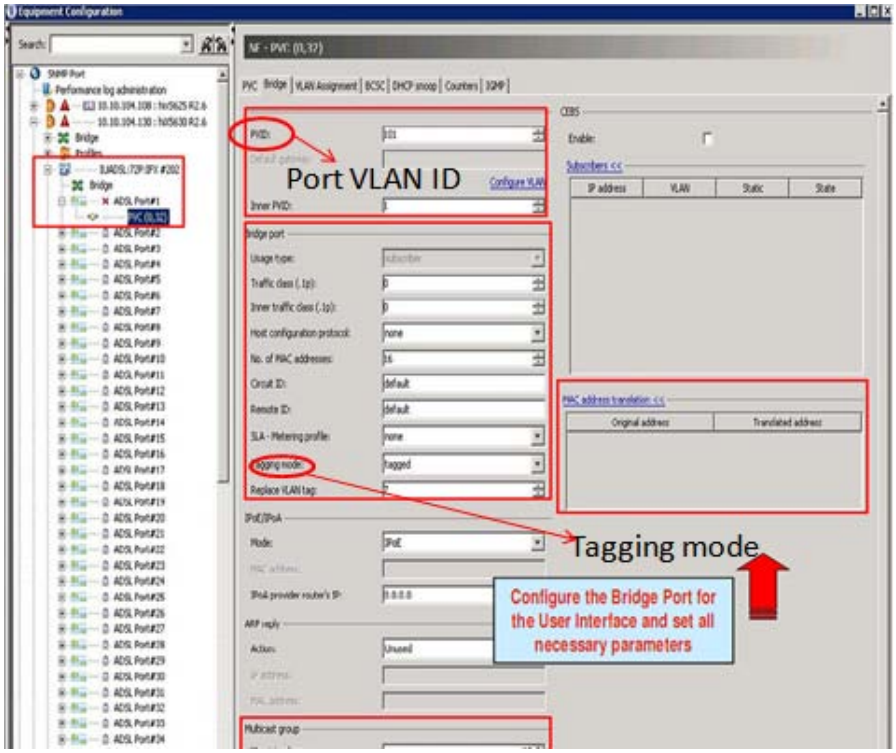

Figure 4.5: Bridgeport configuration with ACI

c. Adding VLAN to the port:

After creating both the VLAN and the Port we add the VLAN to the port:

✓ **CLI configuration:**

The followihg command adds the VLAN 100 to both input and output ports 0/1 and 1/1/1 respectively.

```
HiX5635(bridge)# vlan add 100 1/1/1 untagged
HiX5635(bridge)# vlan add 100 0/1 tagged
```

Figure 4.6: Adding VLAN to ports with CLI

✓ **ACI configuration:**

To add a VLAN to a port using ACI we choose the Port in the left list and then add the desired VLAN in the right list using the appropriate tagging mode (tagged/untagged).

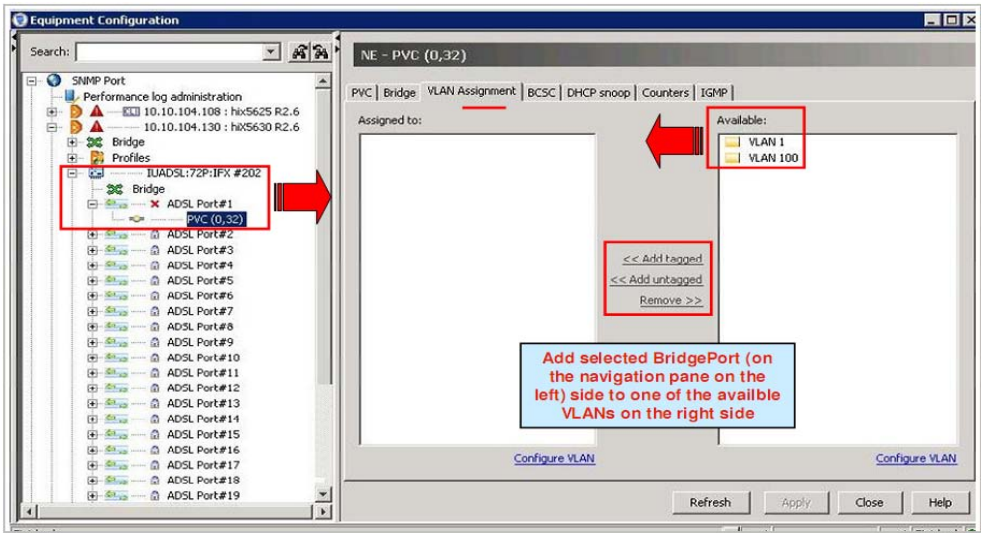

Figure 4.7: Adding VLAN to ports with ACI first alternative

We can also perform this action by assigning the VLAN from the global Bridge configuration.

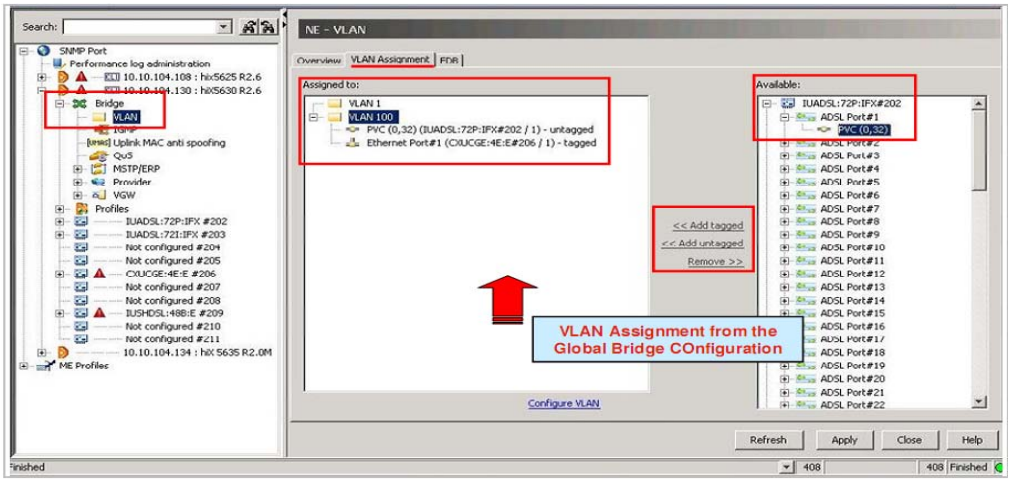

Figure 4.8: Adding VLAN to ports with ACI second alternative

4.1.2. Double tagging scenario:

The traffic received from the user at the port 1/1/1 is a traffic without VLAN tag. The DSLAM tags the traffic with a VLAN ID 100 and 200 then it is sent to the uplink via port 0 / 1 of CXU card.

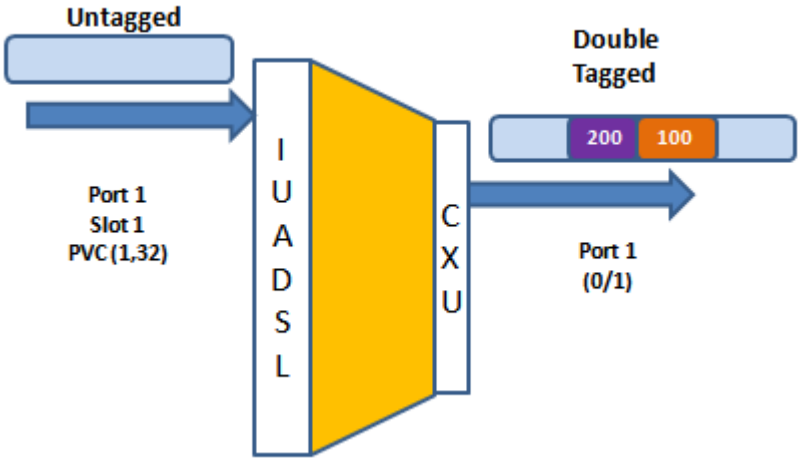

Figure 4.9: Double tagging scenario

a. CLI configuration:

The following commands are those used to configure the double tagging scenario. As proceeded in the single tagging scenario, we have to create our VLANs and then assign them to the port we want to use making one of them as the main PVID and the other one as the "inner-pvid" as shown in the figure below.

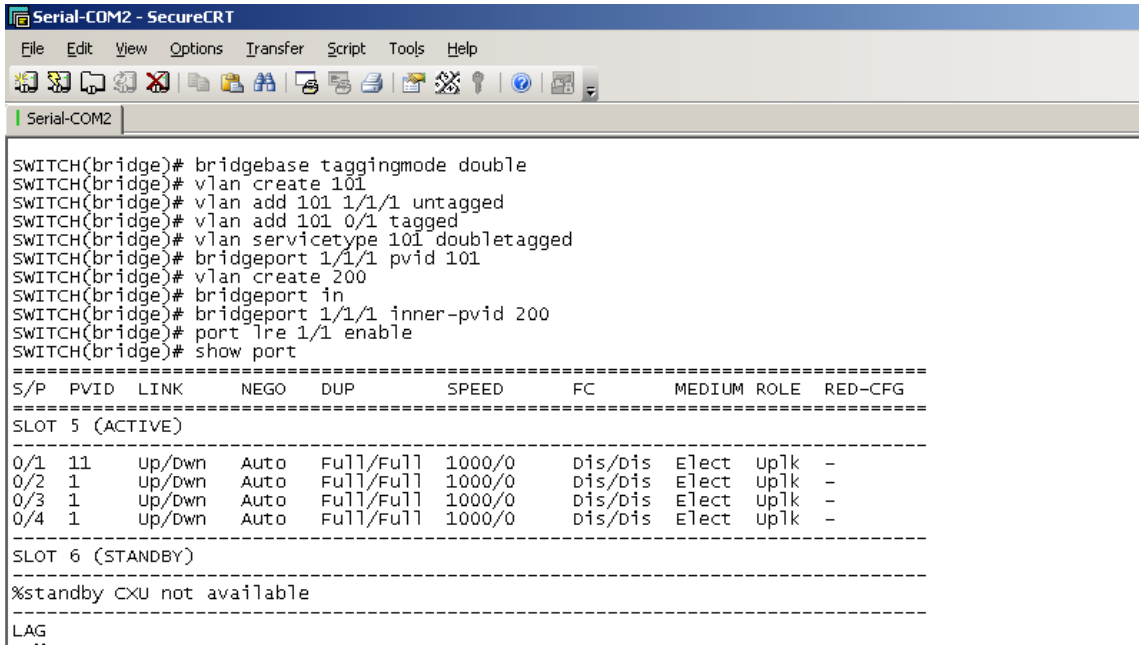

Figure 4.10: Double tagging scenario

b. ACI configuration:

The first step is creating the Bridgeport and the VLAN then setting their configuration.

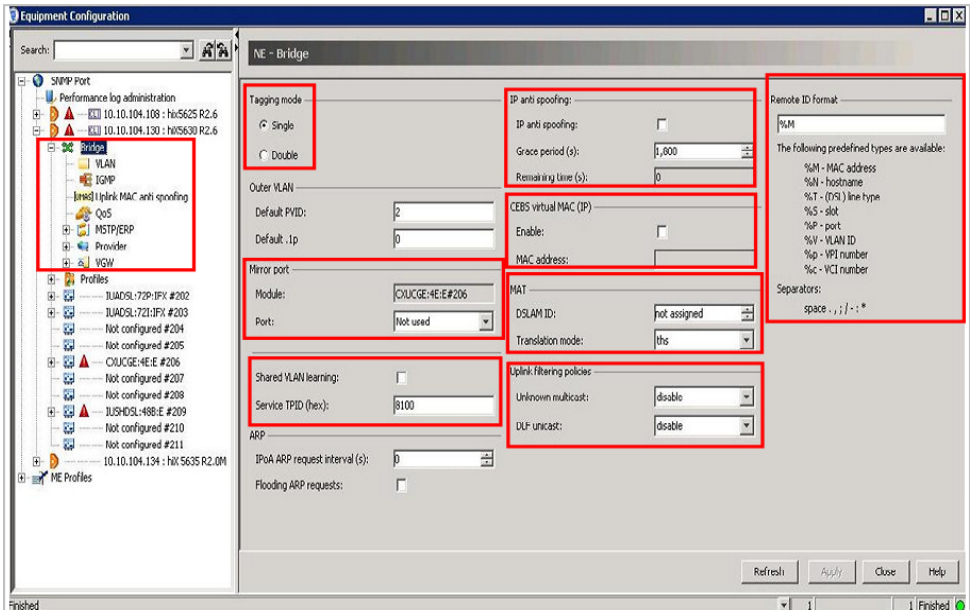

Figure 4.11: Bridgeport creation and configuration

The second step is to set the double tagging scenario by configuring the port for the user interface.

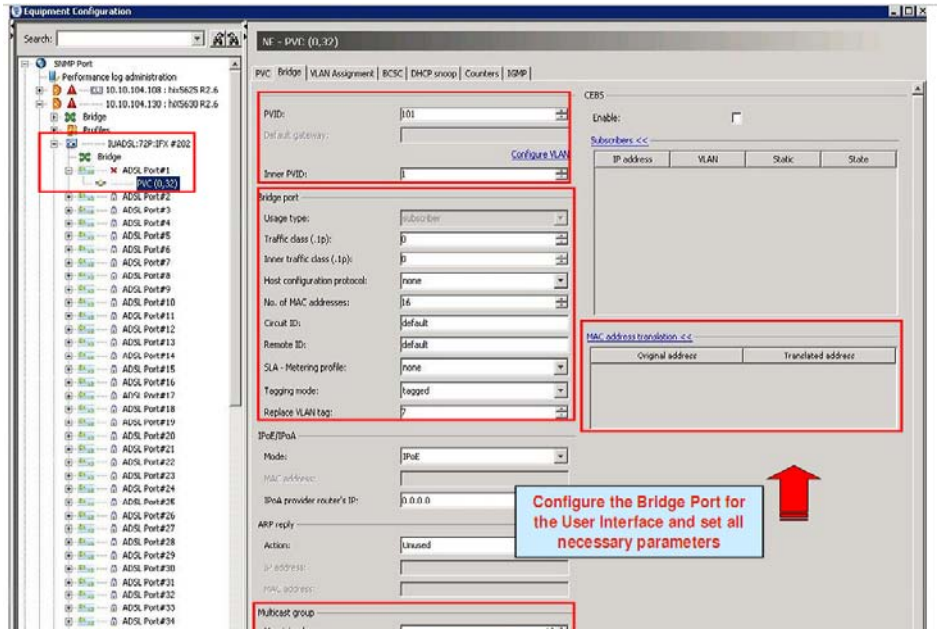

Figure 4.12: Double tagging scenario configuration

4.2. BRAS configuration:

To make the configuration of the BRAS, several steps and several scenarios are to consider.

4.2.1. Global Configuration of the BRAS :

Below are a few samples of the configuration of a BRAS with all possible scenarios:

*Scenario for tagged VLAN (s) static.

*Scenario for tagged VLAN (s) dynamics.

*Scenario untagged.

In global configuration, there are some command lines that are repeated in each scenario and others are specific for a well-defined scenario. Therefore, we will treat each command line in the different scenario mentioned and its role.

```
aaa domain-map « simens.com »
auth-router-name RouteurV
ip-router-name RouteurV
ipv6-router-name RouteurV
```

Figure 4.13: configuration step 1

The above command allows:

- ✓ To assign subscribers to the domain "simens.com" to a virtual router which in this example is named Router V.
- ✓ To authenticate subscribers.
- ✓ Establish an IP port to the subscriber.
- ✓ To create a port for the IP version6 subscriber.

```
aaa local database “auth-db ”
aaa local username X@simens.com database “auth-db”
password hello
ip-address 123.123.123.123
```

Figure 4.14: configuration step 2

These command lines are responsible for:

- ✓ Authentication at the local database named "auth-db" to say that local authentication is done without connecting to a RADIUS server.
- ✓ Creating the users with a password and an IP address.

In this example the name of the database is "auth-db", the user's ID is X@simens.com, the password is 'hello' and the IP address is 123.123.123.123.

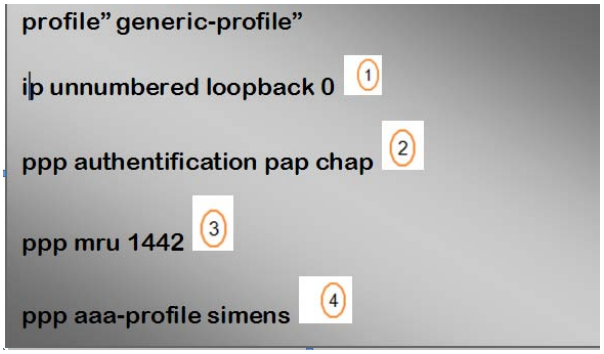

Figure 4.15: configuration step 3

The above commands:

1) Configure the profile "generic-profile":

① This is a default gateway assigned to subscribers, not an IP address.

② Interface for permanent router.

③ This command line limits the maximum number of units received (Max. e.g. 1442 units).

④ Call Siemens profile.

2) Set the profile "svlan-prof" to create a VLAN dynamically, we consider this case in the scenario "tagged" for svlan dynamic.

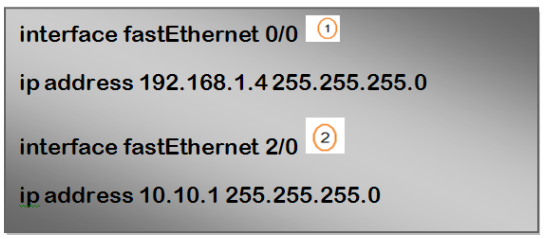

Figure 4.16: configuration step 4

① Creates an interface to the RADIUS server.

② Creates an interface to the web server.

In this step, the command line to look for the configuration of a PPPoE interface simple. This interface has no vlan. This configuration will be studied in the scenario "untagged".
Then, we will study the configuration of a dynamic svlan, we will detail in the scenario "tagged" a dynamic svlan.
Afterwards, we will discuss the configuration of a static svlan in detail in the scenario of a tagged svlan static.

Figure 4.17: configuration step 5

This command defines the set of 11 IP addresses assigned to subscribers based on their authentication.

Figure 4.18: configuration step 6

① Statement by the radius server, which has the IP address 192.168.1.22 and password 'juniper'.

② Source Address requests for authentication.

The commands discussed in the overall configuration remain unchangeable and follow the same order.
Following, is a detailed view of the command lines specific to the scenarios mentioned above.

4.2.2. Setting up an "untagged" scenario:

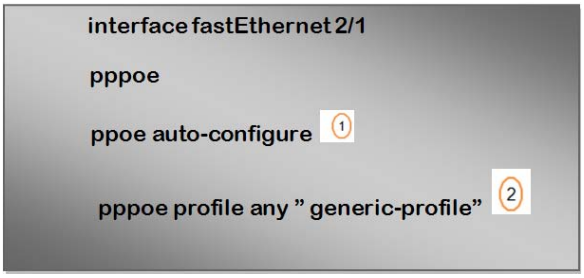

Figure 4.19: Untagged scenario setting

1 To say that the interfaces are dynamic.

2 This is the profile used for dynamic interfaces

4.2.3. Setting up a "tagged" scenario for a static svlan:

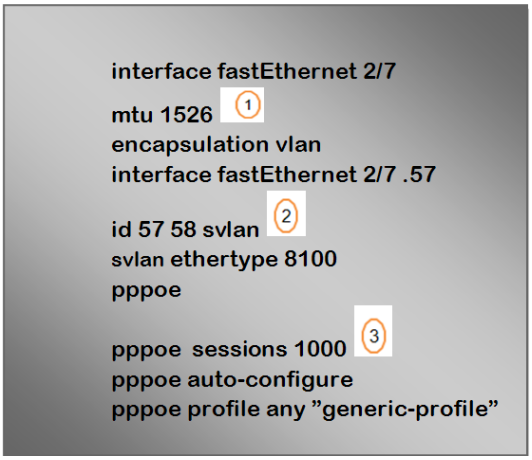

Figure 4.20: Static tagged scenario setting

1 It is a command line to limit the maximum number of units in issue (Max. e.g. 1526 units).

2 The identifier of svlan(s).

3 The session connection pppoe number 1000.

4.2.4. Setting up a "tagged" scenario for a dynamic svlan:

The following command creates a vlan dynamic in profile "svlan-prof"

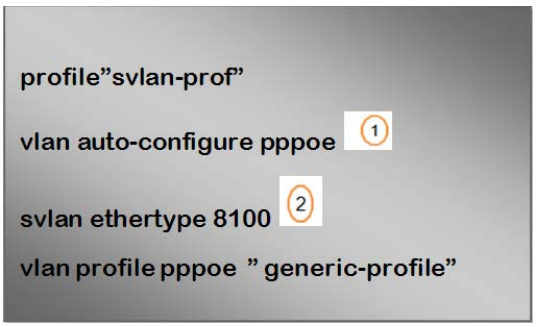

Figure 4.21: Dynamic tagged scenario setting step 1

1 Dynamic creation of a VLAN.

2 The default type Ethernet 8100.

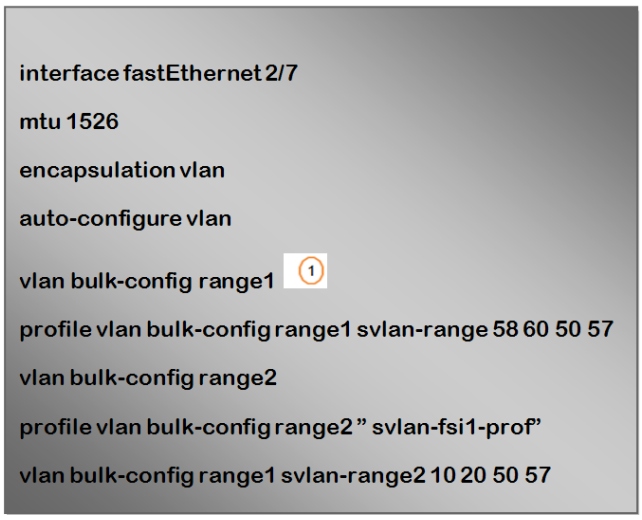

Figure 4.22: Dynamic tagged scenario setting step 2

1 The declaration of vlan(s) dynamic.

2 The svlan(s) are arranged in the order determined above.

4.3. VoIP Configuration:

As we said before one of the advantages of the MSAN system is that we will nomore use the PSTN "Public Switched Telephone Network" that is in French RTCP "Réseau Téléphonique Commuté Public". All the voice calls now are managed throw VoIP.

4.3.1. CLI configuration:

The configuration of Voice over IP requires several steps in order to operate. In the configuration of this case, it is assumed that the caller and called are in the same site, the test is therefore local. The *Figure 4.23* shows in detail the operation architecture of the voice through an IP-MSAN.

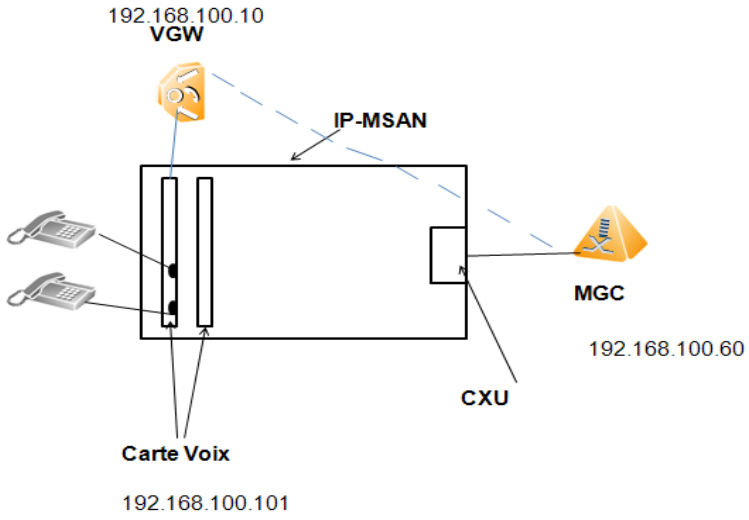

Figure 4.23: Voice function architecture

- ✓ The card IP-MSAN voice acts as a gateway, Access Gateway (AGW)
- ✓ An AGW can share multiple Virtual Gateways (VGW).
- ✓ Each VGW is controlled by a single Media Gateway Controller (MGC).
- ✓ The functionality of the signaling and the control run at the motherboard CXU.
- ✓ IP-MSAN voice cards are Media Gateways.
- ✓ Currently, the signaling protocol used is H.248 support; the implementation of the SIP protocol is underway.
- ✓ The signal can be separated using the VLAN(s).

The process described above has created a single VLAN the role of which is to ship the H.248 stream. The VLAN(s) for signaling and for voice traffic can be the same. To achieve the smoothest functioning of VoIP, several steps are necessary.

a. The installation of an MGC:

In this step, we installed the "OpenMGC(1)" which is an MGC simulator. It plays the same role of the soft switch. The simulator includes a configurable file *(Figure 4.24*) called **mgc.cfg** in which it assigns IP addresses of the Media Gateway and Media Gateway Controller. In this case, the simulator will play the role of MG and MGC as the test is local. A common address is assigned both to MGC and MG. Thus, the MGC operates to ensure correct signalization. The simulator also contains an executable file through which we test the proper operation of the simulator.

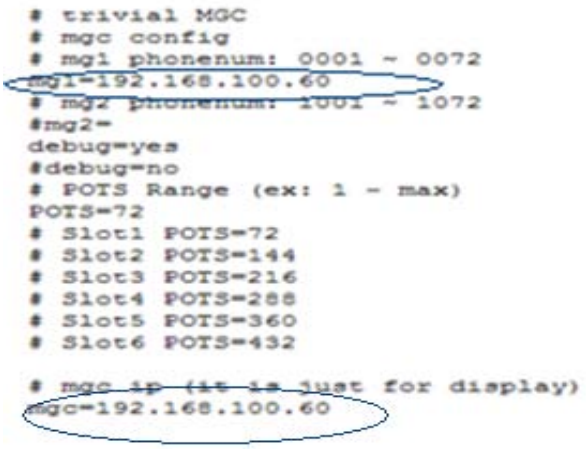

Figure 4.24: configuration file of the simulator

To test the operation of the OpenMGC, we ran the executable file and it verified the existence of the IP address that was introduced at the file 'mgc.cfg'.

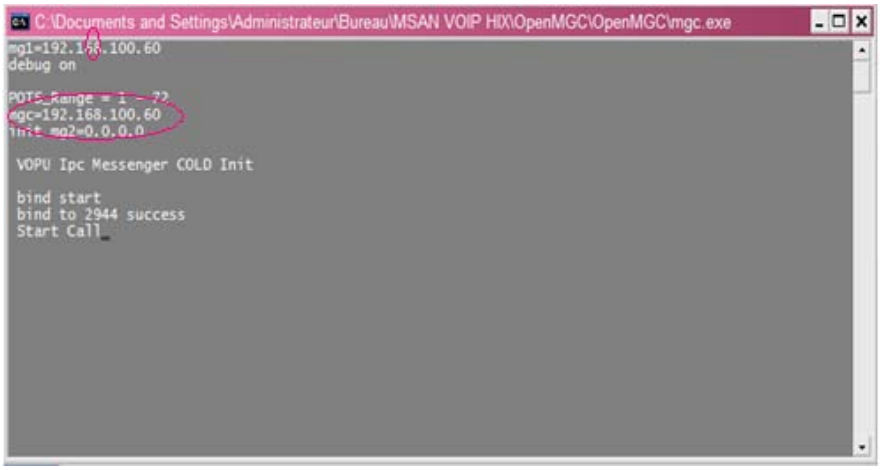

Figure 4.25: The simulator's test

(1) See annex p: 81

b. The configuration steps:

Step 1

Creating a VLAN with ID 10, the vlan is not tagged. It is attributed to port 0 / 1 card and the card CXU voice number 7 (s7).

```
SWITCH(bridge)# vlan create 10
SWITCH(bridge)# vlan add 10 0/1 untagged
SWITCH(bridge)# vlan add 10 s7  untagged
```

Figure 4.26: Creating a VLAN

Step 2

Assigning an identifier to the port VLAN (PVID) with the command (Bridgeport 0 / 1 PVID 10).

```
SWITCH(bridge)# bridgeport 0/1 pvid 10
SWITCH(bridge)# show port
```

Figure 4.27: Identification of the VLAN's port

```
S/P PVID LINK   NEGO  DUP     SPEED    FC     MEDIUM ROLE RED-CFG
SLOT 5 (ACTIVE)
0/1  10  Up/Up  Auto  Full/Full 1000/100  Dis/Dis Elect Uplk -
0/2  1   Up/Dwn Auto  Full/Full 1000/0    Dis/Dis Elect Uplk -
0/3  1   Up/Dwn Auto  Full/Full 1000/0    Dis/Dis Elect Uplk -
0/4  1   Up/Dwn Auto  Full/Full 1000/0    Dis/Dis Elect Uplk -
```

Figure 4.28: The port's status

The identifier 10 is assigned to the active port (UP / UP) 0 / 1 card CXU.

Step 3

This action switches the voice VOIP command. It specifies the command described in *Figure 4.23* for inbound and outbound. In this case, the incoming connection to IP-MSAN which has as IP address (192,168,100,101) is transferred to GC (192,168 .100.60).

```
SWITCH(config)# voip
% voip-mode
SWITCH(voip)# iphostprofile create 2 testp no 192.168.100.101/24 192.168.100.60
```

Figure 4.29: The iphost profile configuration

This profile is set to index number 2 and has the name testp.

Step 4

It creates an interface with the address 192.168.100.200, called br11.

```
SWITCH(config)# netdevice 192.168.100.200/24 h248 10
SWITCH(config)# interface br11
SWITCH(config-if)# no shutdown
SWITCH(config)# show interface
```

Figure 4.30: The creation of an interface

Step5

Under the H248 mode, we configure the profile of the media gateway controller (MGC) giving an index (e.g. 8), a profile name (IP8). The IP address of MGC (192.168.100.60) and port 20005 have already been configured for the simulator.

```
SWITCH(voip)# h248
% h248-mode
SWITCH(h248)# mgcprofile create 8 ip8 mgc 192.168.100.60 20005
```

Figure 4.31: The creation of the MGC profile

Step 6

After configuring the MGC, we applied the profile "iphost" index 2 to the card or slot, in this case we worked on the card number 7 (s7).

```
SWITCH(h248)# voicectp s7 iphostprofileid 2
```

Figure 4.32: Allocation of iphost to voice card

At this stage, we create a profile VGW by associating a name (in this case the name is vgwtest) and an index (in this case 2). The VGW's role is to interconnect the simulator and to map MGC voice (s7) which is added to the Virtual Gateway in the card number 7. It also specifies the IP address of the simulator (192.168.100.60) and the port number 20005.

```
SWITCH(h248)# vgw create 2 vgwtest
SWITCH(h248)# vgw 2 add slots s7
SWITCH(h248)# vgw 2 midip 192.168.100.60 midport 20005
SWITCH(h248)# vgw 2 start
SWITCH(h248)#show vgw
```

Figure 4.33: The configuration of VGW

With the command (show VGW), the list of VGW(s) appears.

VGW List

Index	Name	AdminStatus	OperStatus	Protocol	MidIp	MidPort	MgProfileID	MgcProfileID	priorityprofileID	DomainName
2	vgwtest	up	down	h248	192.168.100.60	20005	1	1	0	

Figure 4.34: The list of VGW(s)

The table above displays the list of bridges that have been created: The VGW which was created as (vgwtest) and having index 2 is active (UP).

4.3.2. ACI configuration:

The ACI configuration is made by the EM-GX. To configure the VOIP we should follow these steps using GUI "Graphic User Interface".

a. Configuring the L2/L3 infrastructure:

Required configurations are:

- ✓ Create IP hosts
- ✓ Assign port-to-vlan membership and, if required, pvids
- ✓ Define routes for voice and signaling

The figures below show how to create an IP host

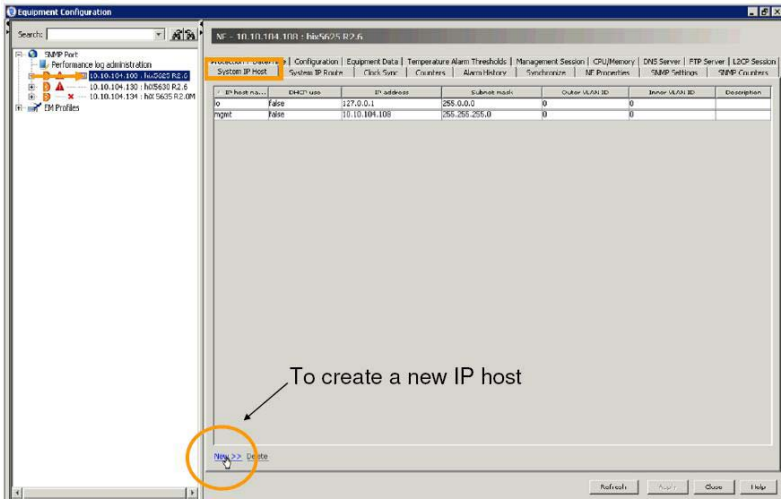

Figure 4.35: List of IP hosts

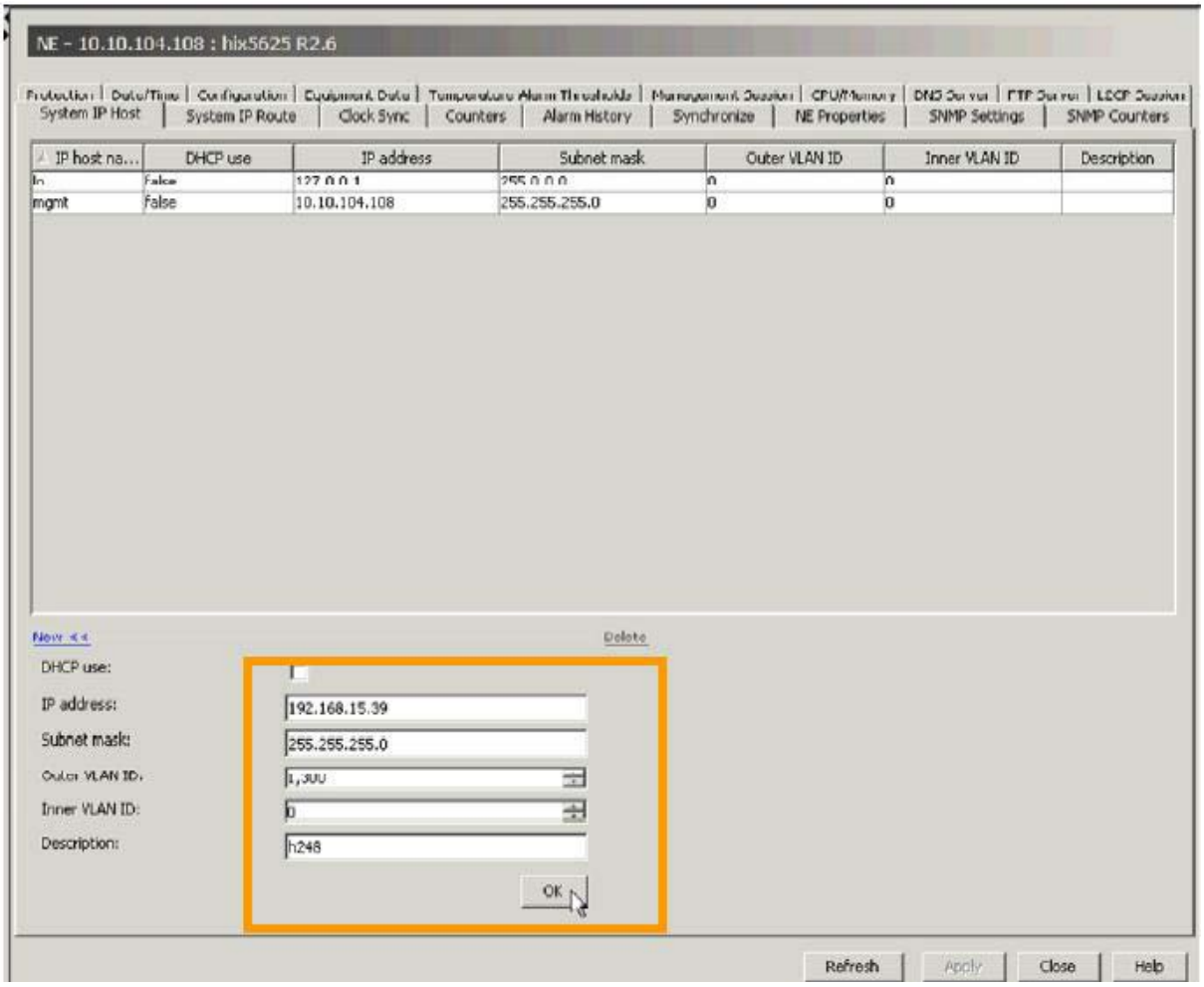

Figure 4.36: Create the IP host for H.248

Now we include the relevant ports into the VLANs for VoIP following the same procedure as in the data (DSL) configuration: see (*Figure 4.7* and *Figure 4.8*).

b. Configuration of Voice Gateways:

Multiple voice gateways can be configured on the MSAN, e.g. to communicate with different MGCs as would be the case if they belong to different providers. The following figure shows how to create a voice gate way and the different options to provide e.g (name, IP address, protocol version, etc…)

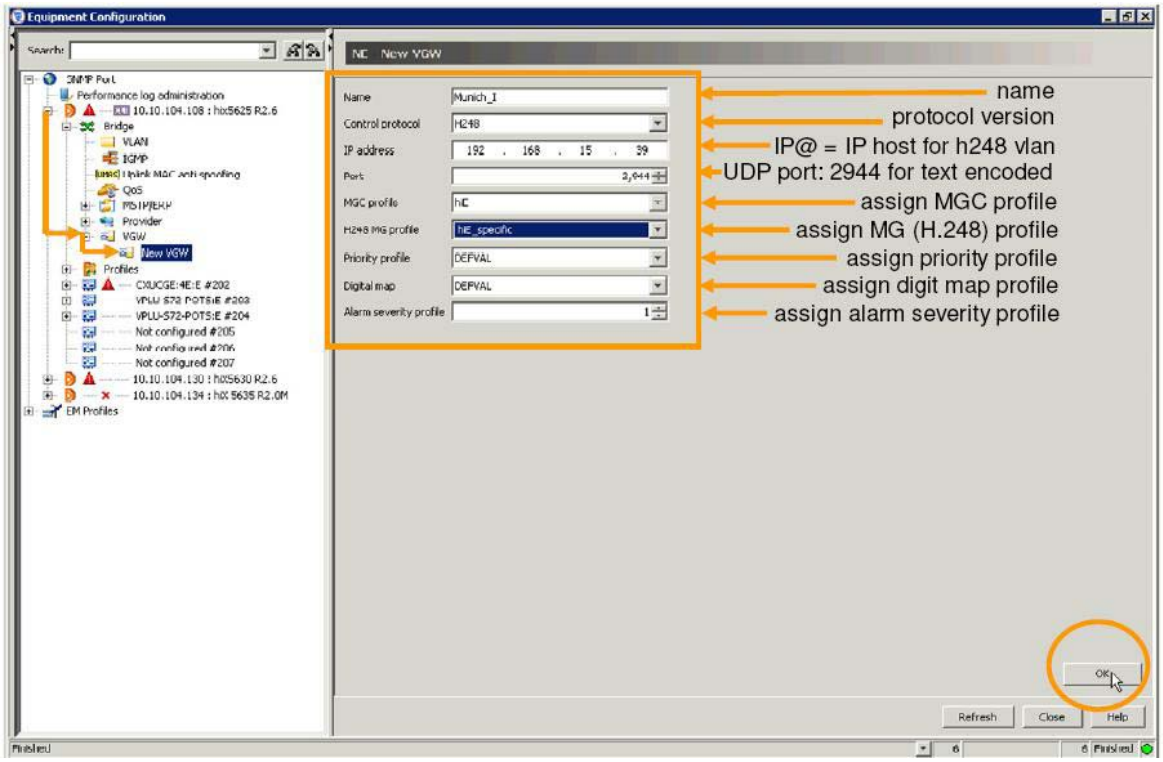

Figure 4.38: Create a voice gateway

The voice connection termination point can be configured in one step per VPLU card. The specifications are:

- ✓ IP host profile
- ✓ RTCP profile
- ✓ RTP port base
- ✓ Media codec
- ✓ Media jitter buffer
- ✓ Media fax
- ✓ RTP stream mark TOS

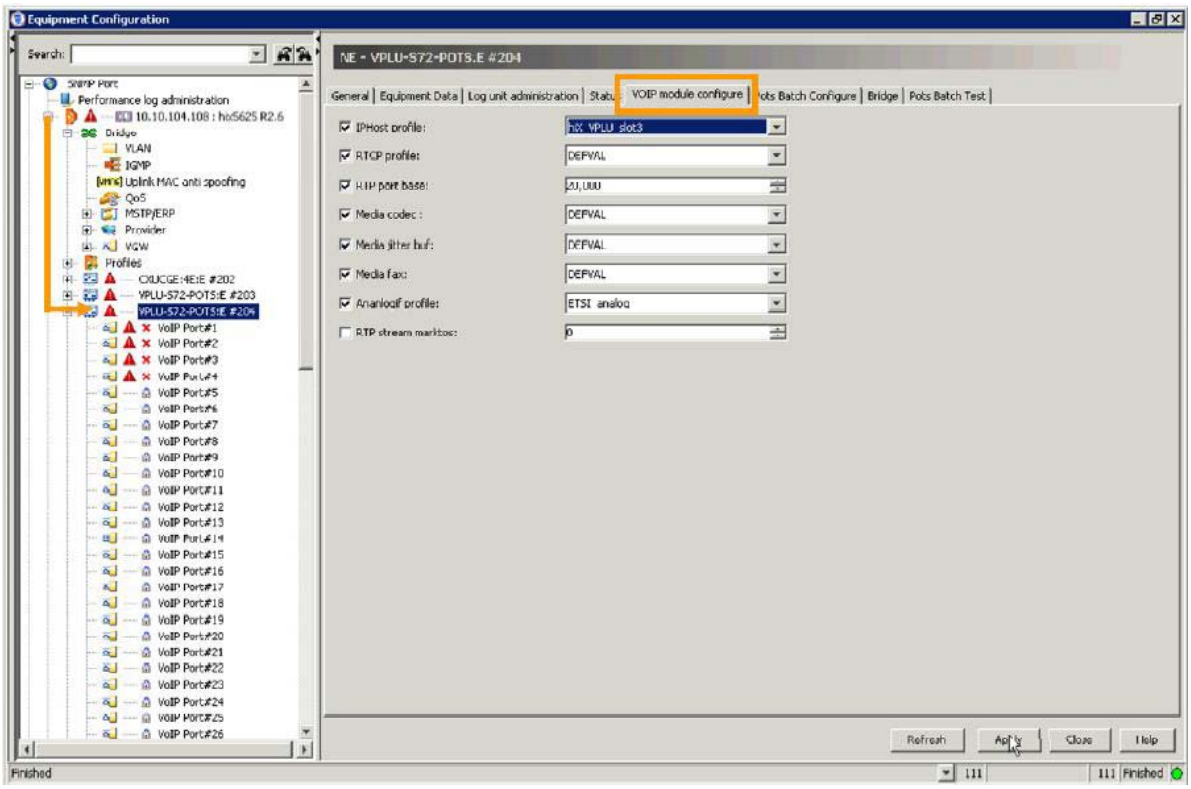

Figure 4.39: Configure Voice Connection Termination Point

Having done with this step, our configuration is finalized and we can start performing voice calls.

Conclusion

During this training I managed to install the new telecommunication infrastructure of Tunisie Telecom consisting in one of the NGN projects which is the IP MSAN provided by my host enterprise NSN. I proceeded by mounting the equipment needed and configuring it in two different methods: by using the CLI and by the GUI thus putting in focus the advantage of the new centralized management system "ACI" (a real-time management platform composed of three servers and their redundant ensuring the Geo-Redundancy and other administration tasks to the system). This project is meant to guarantee a perfect QoS to an increasing number of connected customers by migrating to the VoIP technology which provides a better quality of voice call and reduces the risk of line interruption and loss. Besides the centralized management platform provides a real-time management opportunity in an easy way by using the GUI with the ACI Software instead of the CLI that demands a specific knowledge of the network's engineering environment.

This project can be also subject for further improvements specially by integrating the 3G technology and by using additional new technologies, notably the introduction of the Video over IP platform to enable video conversations between the customers.

List of Abbreviations

A

ACI: Access Integrator

AGW: Access Gateway

ANCP: Access Node Control Protocol

ATM: Asynchronous Transfer Mode

B

BRAS: Broadband Remote Access Server

C

CD: Compact Disk

CDM: Cross Domain Manager

CLI: Command Line Interface

CONFIG: Configuration

CORBA: Common Object Request Broker Architecture

CoS: Class of Service

CPE: Customer Premises Equipment

CXU: Central switching Unit

D

DB: Database

DoS: Denial of Service

DSLAM: DSL Access Multiplexers

E

EM: Element Manager

F

FTP: File Transfer Protocol

G

GUI: Graphic User Interface

I

IP: Internet Protocol

ISDN: Integrated Service Digital Network

IU: Interface Unit

J

JSP: Java Server Page

L

LAN: Local Area Network

LRE: Long Rich Ethernet

L2: Layer 2

L3: Layer 3

M

MDF: Main Distribution Frame

MGC: Media Gateway Controller

MSAN: Multi Service Access Node

N

NE: Network Element

NGN: Next Generation Network

NSN: Nokia Siemens Networks

O

OS: Operating System

P

PC: Personal Computer

PSTN: Public Switched Telephone Network

PVID: Port Virtual ID

R

RADIUS: Remote Authentication Dial –In User Server

RAM: Random Access Memory

RMC: Remote Management Console

RTP: Real Time Protocol

S

SLA: Service Level Agreement

SW: Software

T

TAO: Telephony Application Object

TDM: Time Division Multiplexing

V

VAR: Versant Asynchronous Replication

VGW: Virtual Gateway

VLAN: Virtual LAN

VoIP: Voice over IP

VPLU: VoIP line Unit

3G: Third Generation

List of references

[1]: Nokia Siemens Networks Tunisia/ Tunisie Telecom Market agreement

[2] [3]: syd_hix5625_30_35_r28

Annex

H.248:

H.248 protocol is developed for real time multimedia data communication on IP. MEGACO standard is regulated by IETF and ITU. It is for outer call agent with MGCP, that is, for interface between MGC (Media Gateway Controller) and MG (Media Gateway).

It has same structure with MGCP. Even if it was developed after MGCP, MEGACO is enough for MGCP function and supports additional function with rapid growth.

The below is components for H.248 (MEGACO)

- Signaling Gateway: overall calling and hanging up function
- Access Gateway: transmits voice and computer data by packet.
- Call Agent: receives signal from SG, manages bandwidth and provides server by choosing MG

Hix56xx R2.7M support H.248 version 2. Some packages or event/signal belongs to H248 version 3. The following features are newly introduced in R2.7M:

- H.248.1 Generic
- H.248.16 Extended DTMF Detection (xdd)

This package provides an extended DTMF digit map completion event, incorporating detailed reporting of timeouts, digit buffering control, and reporting and control of processing of extra events.

- H.248.14 inactivity Timer (it)

The package provides support for MGs detecting the failure of MGCs by messagesilence and is only used on the ROOT termination.

A MGC that support this package may detect whether or not a MG supports the package by auditing it. A MGC may choose to set the inactivity timer event containing the maximum silence period or "maximum inactivity time" on the ROOT termination.

The MGC should then ensure that the time between messages sent to that MG never exceeds this period. The MGC ensures this by sending any message as a test or keep-alive message (such as the empty Audit of ROOT) whenever no other message is needed within the period.

Hix uses MODIFY with it/ito event as keep-alive message to implement heartbeat mechanism between a VGW and MGC.

- ServiceState in complicance with H.248 v3

The "serviceStates" parameter of "TerminationState" descriptor is supported in compliance with procedures described in H.248 v3.

The "Out of service" "serviceState" is used as the test state, when the Termination is under test as a result of a management request on MG. The "test" service state may be used by MGC, when MGC order test calls.

To implement the "ServiceState" in compliance with H.248 v3, Hix does the adaptations below:

– "ServiceState" parameter support ("InService", "OutOfService", Test)

– Reply "Out of service" when the Termination is under test as a result of a management request on MG.

– In case a termination failure or recovery, HiX will send "ServiceChange" with Reason code 904/900 to MGC.

– When a termination goes into line test state, HiX will send "ServiceChange" with Reason code 905 to MGC.

• Support of Keepactive

Keepactive intends to be supported only for signal amet/mpb. When an amet/mpb with keepactive flag is coming, if there is no old amet/mpb been played, this new one will be discarded according to H.248.1 (g/sc). If there is amet/mpb been played now, the new signal will be played rightly after the old signal finishes.

• Support of error code 533

In case of UDP transport and if transaction reply exceeds IP MTU value an Error 533 "Response exceeds maximum transport PDU size" shall be generated in reply to MGC.

• Support of maximum 5 Signals in signal list

Hix can support maximum of 5 signals in a signal list.

MGC:

A **Media Gateway Controller** (MGC) is a system used in certain Voice over IP telephony architectures. An MGC controls a number of dumb terminals, the Media Gateways. The MGC receives signalling information (like dialed digits) from the Media Gateway and can instruct it to alert the called party, to send and receive voice data etc. There are several protocols which can be used between MGC and Media Gateway: SGCP, IPDC, MGCP and Megaco (also known as H.248). The MGC receives also the term **Call Agent** when referred in the context of MGCP.

Some MGCs can interface with other signaling protocols, like SS7 (for interconnection with the traditional telephone system), H.323 and SIP.

A VoIP architecture using an MGC is sometimes called softswitch architecture. Advantages of the softswitch architecture are that the Media Gateways are easy to maintain and that the softswitch operator retains full control. On the downside, softswitch architectures tend to be inflexible. Highly available MGCs are expensive to implement, as an MGC needs to be stateful. Source: "*http://en.wikipedia.org/wiki/Media_Gateway_Controller*"