Network Divestment Guidelines

**Table of Contents**

[Change Summary 2](#_Toc436744344)

[Introduction 3](#_Toc436744345)

[Purpose 3](#_Toc436744346)

[Scope 3](#_Toc436744347)

[In scope 3](#_Toc436744348)

[Out of scope 3](#_Toc436744349)

[Assumption & Prerequisite 5](#_Toc436744350)

[Pre-Build 5](#_Toc436744351)

[Co-Existence 5](#_Toc436744352)

[Change-in-Control 5](#_Toc436744353)

[IP Addressing (IPv4) 7](#_Toc436744354)

[Network DHCP / DNS Conversion 8](#_Toc436744355)

[Pre-Build 8](#_Toc436744356)

[Co-Existence 9](#_Toc436744357)

[Phase I 9](#_Toc436744358)

[Phase II 10](#_Toc436744359)

[Change-in-Control 10](#_Toc436744360)

[Wireless Conversion (CoWLAN 🡪 Standard) 12](#_Toc436744361)

[Pre-Build 12](#_Toc436744362)

[Co-Existence 12](#_Toc436744363)

[Change-in-Control 13](#_Toc436744364)

[Network Devices Configuration Conversion 18](#_Toc436744365)

[Pre-Build 18](#_Toc436744366)

[Co-Existence 18](#_Toc436744367)

[Change-in-Control 18](#_Toc436744368)

[Voice Conversion – Cisco 19](#_Toc436744369)

[Pre-Build 19](#_Toc436744370)

[Co-Existence 19](#_Toc436744371)

[Change-in-Control 21](#_Toc436744372)

[Voice Gateways 21](#_Toc436744373)

[GVIN (Phase I & II) 22](#_Toc436744374)

[Pre-Build 22](#_Toc436744375)

[Co-Existence 22](#_Toc436744376)

[Change-in-Control 22](#_Toc436744377)

[Non-Cisco Voice Systems Conversion - TDM 22](#_Toc436744378)

[Pre-Build 23](#_Toc436744379)

[Co-Existence 23](#_Toc436744380)

[Change-in-Control 24](#_Toc436744381)

[IBM Cloud services 24](#_Toc436744382)

[Pre-Build 24](#_Toc436744383)

[Co-Existence 25](#_Toc436744384)

[Change-in-Control 25](#_Toc436744385)

# Change Summary

| Version | Date | Change/ Updated by | Summary |
| --- | --- | --- | --- |
| 01 | 09/Jan/2012 | Hung Bui | Initial document |
| 02 | 12/Dec/2014 | Facundo Vives | Document update |
| 03 | 01 Dec 2015 | Marcus Koh | Refresh document (Fix broken links, remove/replace old reference name: Organization, IS catalog, BPs, genesis, PMTS/CMTS.. etc) |
| 04 | 15 Jun 2016 | Marcus Koh | Accepted all tracking changes |
| 05 | 18 Oct 2018 | Roland Hernandez | Full review  Added a reference for Skype Service  Changed all Network and Voice Solutions (NVS) references to Network Solutions (NS)  Changed references from NAS to NMS  Changed references from PCI to WS3/WDS  Changed references from Unix to MRUS |

# Introduction

Divestment projects are by nature high value, and do not always align with all of our current internal processes which drives the need for rapid deployment and effective delivery.

Several different available techniques and solutions have been used and deployed at vary divestment sites. Although each scenario proves to be different and although there’s no single solution to fit them all, not having a standard design solution can lead to labor intensive and inefficient execution of tasks. Therefore, in order to assist divestment teams with consistent and well known network solutions and techniques, guidelines are documented in this guide.

# Purpose

The purpose of this document is to provide a set of guidelines for consistent design and procedure that can be applied to the divestment of network infrastructure. Taking into consideration of following:

* Align with ExxonMobil security and control standard
* Repeatable and robust
* Minimize change effort at Change in Control (CiC)

This document is an integral part of a divestment practices document suite which together provide a comprehensive outlook on a divestment solution.

**Note:** Due to the complexity of divestment projects and nature of guidelines, the final design solution might deviate from the recommendation here presented.

# Scope

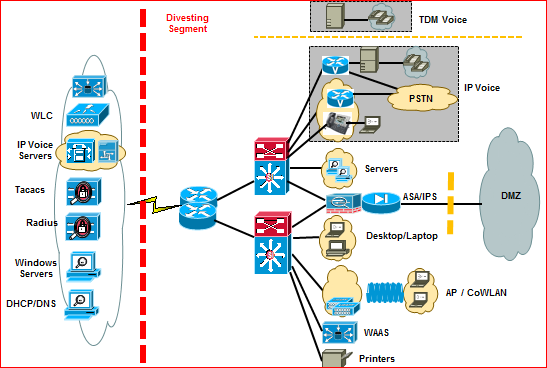
The scope of this guide is based on the common technologies and services that NS supports globally. New technologies and services could be introduced and become standards in the future and between review cycles and might not be listed as in scope.

## In scope

* Wireless CoWLAN
* Network Devices Configuration Conversion
* DHCP/DNS Migration
* Cisco Voice Migration
* Avaya Voice Migration
* Nortel Voice Migration
* Skype Voice Migration – Note: For sites that have Skype for business voice services, the Skype support team should be engaged for guidance if none of the legacy voice services are available at the site

## Out of scope

* Non-network equipment and services
* Non-standard network equipment and services
* Uncommon network solutions (contact center, telecom equipment, etc..)



# Assumption & Prerequisite

As most projects, a divestment one has different stages. The activities that fall into each stage are described in the upcoming sections of this document. It is important to take into consideration the following assumptions and pre-requisites when evaluating the execution of any of the in-scope activities.

## Pre-Build

Divestment agreement has been announced (i.e. it is of public knowledge).

In this stage, the recommended solution is designed and the corresponding network infrastructure is prepared for the Co-Existence stage. Typical implementation activities may include, but are not limited to, the installation of new switches for port capacity expansion, installation and configuration of on-site Call Manager without enabling it and the upgrade or installation of new circuits and the supporting router.

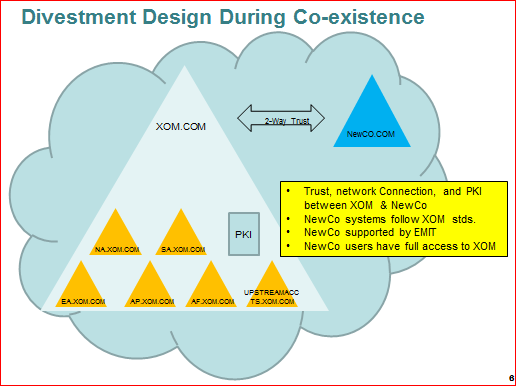
It is strongly recommended to follow NS hardware and software best practices when possible. ExxonMobil Security & Control and practices must be followed. Any need for S&C exceptions should be discussed with NS S&C advisor.

## Co-Existence

This is the period of time between when GME workstations are migrated to the NewCo environment and the Change in Control (CiC) date. Workstations in this state are still fully owned and supported by ExxonMobil. The length of the co-existence period will vary for each divestment project

NewCo, short for New Company, is a term used to represent various aspects of the new environment where users, workstations and servers are migrated to. This new environment counts with its own AD forest\domain and appropriate approved security controls.

During Co-Existence, a trust is established with ExxonMobil existing domains. While the equipment and services reside on this NewCo environment, it is subject to comply with ExxonMobil standard security & control and practices.

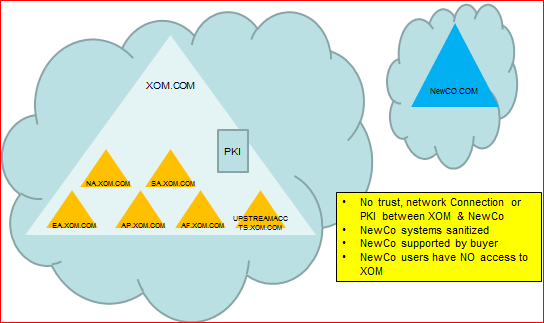


## Change-in-Control

The change in control per se is the date and time at which the Affiliate is handed over to be operated by the buyer. Before this process is completed, any ExxonMobil installs, configuration, intellectual property, etc.. left over in the servers and/or network equipment is removed.

Once this is done and the transition is completed, ExxonMobil security & control and standard practices no longer apply on the divested site. However, MPI guidelines still do.

**Note:** Exceptions may arise depending on the divestment negotiation and technical requirements. These will need to be endorsed and documented.



# IP Addressing (IPv4)

In our network, we make use of both private (RFC1918) and public IP addresses. The latter are public ranges registered and owned by ExxonMobil or an affiliate as could be IOL in Canada. As private addresses can be used by any individual and organization, these can be left configured on the network devices at CiC. However, for the public address space, we have to recover them at CiC.

**Pre-Build**

* No changes

**Co-existence**

* For new subnets requirements, create and assign private RFC1918 subnet(s) and follow current standard IP address request process.
* If existing servers/clients on XOM registered IP space:

1. It’s preferred to convert to RFC1918 private address if technically viable
2. If not possible (e.g. due to conversion complication) to recover XOM registered space before divesting, ensure to document in agreement/SLA so that buyer will treat XOM divested subnets as private and not advertise to Internet.

**Note:** Since XOM registered for the IP space, an ID object associated with XOM information is configured on the ISPs databases. This would potentially prevent other enterprises from accidently advertising the IP space to Internet

1. Divesting XOM registered space completely transferring ownership to the buyer, by following the latest recommended Internet IP registration process. This is a complex process and is highly discouraged.

**Change-in-Control**

* No changes

Network DHCP / DNS Conversion

Production DHCP & DNS services currently run on Infoblox appliances and are supported by Core NMS Team. Within the NewCo environment, another platform may be used such as Microsoft DHCP/DNS.

The guidelines outlined in this section are independent of the chosen platform. Typically though, Microsoft’s DHCP/DNS is used, which is not a standard platform. For such solution, there will be no support model defined.

It is important to notice that Microsoft’s DHCP/DNS run on top of a Microsoft Server OS. An AD service could then run on the same server. However, in order to avoid AD changes affecting DHCP/DNS service and vice-versa, it is strongly recommended by NMS to use a single physical server (stand-alone) for Microsoft DHCP and DNS services.

The divesting infrastructure will initially be supported from the production DHCP \ DNS environment. Once all clients are migrated to the new divesting domain (“NewCo.com”), the DHCP \ DNS services will be migrated off the production environment and into the local environment.

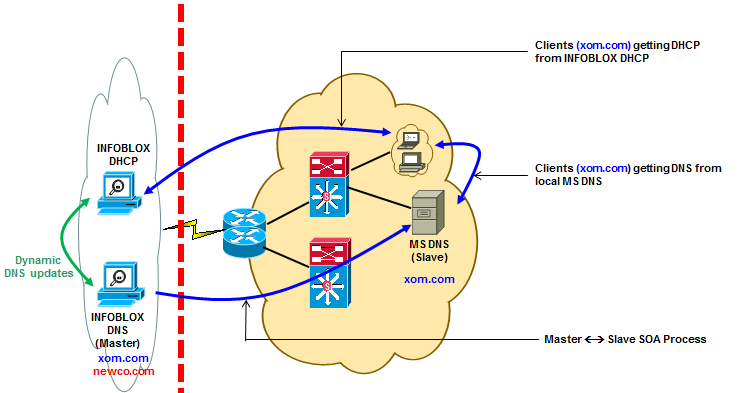
The plan is broken down into Pre-Build, Co-Existence Phase I, Co-Existence Phase II, and CiC

### Pre-Build

There are 3 major activities to be performed during this phase:

1. The production DNS / DHCP services are configured to host the divesting domain (Newco.com).
2. The Local DNS service is configured as “secondary” for Newco.com, pulling the zone data from the production environment
3. The Local DHCP service is configured with all the divesting subnets/ranges, although all are set to “disabled” status.

The diagram below is a high-level representation of these steps



The specific steps are outlined below:

* Define “NewCo.com “ on the production Infoblox environment
* Configure “NewCo.com” as a “dynamic” zone
* Grant Domain Controllers for NewCo.com forest update access to DNS zone
* Configure new Local DNS server as “secondary” for NewCo.com domain, and the corresponding Reverse Zones. Set Masters as production Tier 1 DNS servers.
* Configure existing AD/DNS servers as “secondary” for NewCo.com domain, and the corresponding Reverse Zones. Set Master to the new Local DNS server
* Configure DNS Forwarders on Local DNS: point to production Tier 1 DNS
* Define new DHCP ranges (if any) on the production DHCP service
* Define new DHCP filters on the production DHCP service:
* DIVxxxLAPTOP
* DIVxxxSERVER

xxx = 3-letter code for divestment project

Include T1 and “domain-name” options in each filter

* Define all DHCP ranges on Local DHCP server. Ensure all are in DISABLED state
* Set appropriate DNS settings
* Set appropriate options for COWLAN subnets
* Set appropriate options for Cisco IP-Phones
* Set appropriate options for Avaya IP-Phones
* Set appropriate options for Nortel IP-Phones
* Define new IP-Helpers on the appropriate VLAN interfaces.

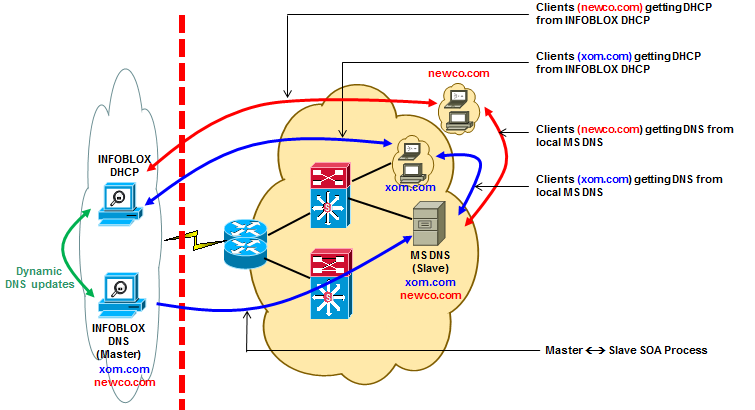
### Co-Existence

#### Phase I

The primary objective of this phase is migrating existing clients (workstations, servers, network devices, etc.) from the ExxonMobil domain to the Newco.com domain.

As clients are migrated, they will continue to receive DNS and DHCP services from the same set of devices as before.

The diagram below is a high-level representation of a migrating environment: current ExxonMobil clients and NewCo.com clients continue to get DHS / DHCP services from the same set of devices.



The specific steps are outlined below:

* WS3/WDS to migrate both Static and DHCP-managed devices
* DHCP-Managed devices to be set with the appropriate DHCP ClassID
* DIVxxxLAPTOP – for both laptops and Desktops
* DIVxxxSERVER – for servers
* Static devices to be set with appropriate DNS and WINS settings
* Coordination with NMS is required so that DNS entries for migrating devices are updated
* MRUS to migrate supported devices
* Devices to be set with appropriate DNS settings
* Coordination with NMS is required so that DNS entries for migrating devices are updated
* NS to migrate :
* Network Devices, updating “name-server”, “domain-list”, “domain-name”
* Coordination with NMS is required so that DNS entries for migrating devices are updated
* COWLAN environment
* Ensure DHCP Option 43 is set appropriately
* Cisco IP-Phones
* Ensure DHCP Option 150 is set appropriately
* Avaya IP-Phones
* Ensure DHCP Options 176 and 242 are set appropriately
* Nortel IP-Phones
* Ensure DHCP Options 144 and 191 are set appropriately
* Ensure that any DHCP Options added between review cycles of this guideline are added

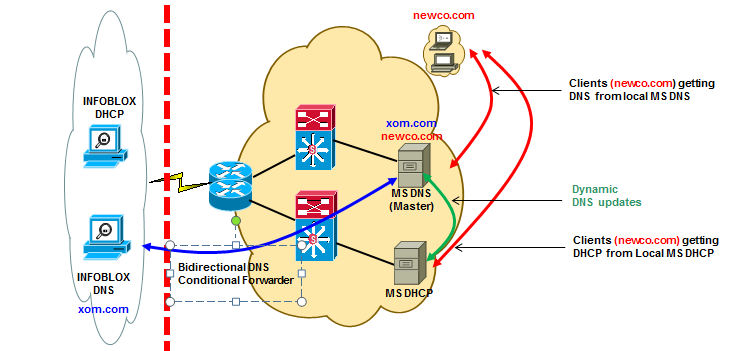
#### Phase II

The primary objective of this phase is to migrate the DNS / DHCP services from the production environment to the “local” DHCP/DNS servers.Close coordination is required to ensure all required workstation and server migrations are completed prior to cutting over from Infoblox to Local DHCP / DNS Servers.

The key activities will be:

1. Transfer SOA role for Newco.com to the Local DNS server
2. Enable the DHCP ranges on the Local DHCP server
3. Enable DDNS updates and set DDNS credentials in Local DHCP server
4. Access Points switch port must be reset to force registration into the new DHCP server – NI Task

The diagram below shows a high-level representation of those steps



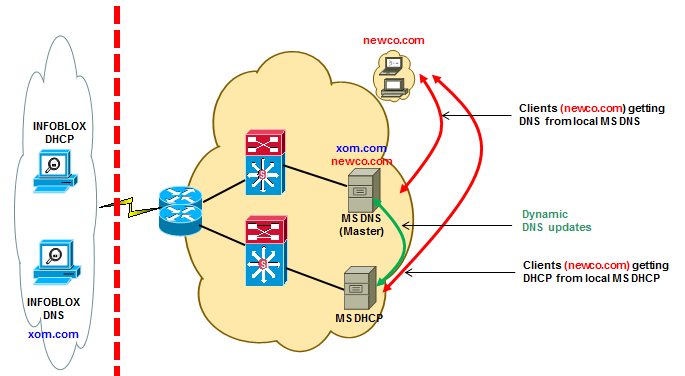
The specific steps are outlined below:

* Lower DHCP lease renewal interval via filters (DIVxxxLAPTOP, DIVxxxServer)
* Change DNS configuration on new Local DNS to become SOA for “NewCo.com” and corresponding Reverse Zones.
* Remove SOA role from production DNS servers for “NewCo.com”
* Create DNS Conditional Forwarders on each production and Local DNS pointing at each other
* Enable DHCP ranges on Local DHCP environment
* Disable DHCP ranges on production DHCP environment

### Change-in-Control

The main objective of this phase is removing the existing DNS bidirectional forwarders. At this point in time, cross-domain resolution between ExxonMobil and the Buyer’s environment will stop.

The diagram below is a high-level representation of this step.



The specific steps are outlined below:

* Change DNS Forwarders on Local DNS to point to Buyer’s DNS environment
* Remove XOM DNS zones from all divesting DNS servers
* Remove DNS Conditional Forwarders from the production and Local DNS environments
* Clean-up XOM environment of divested DDI information

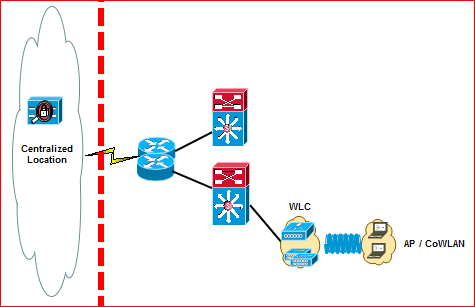
# Wireless Conversion (CoWLAN 🡪 Standard)

For current ExxonMobil CoWLAN deployments, a WLC is collocated with Access Points and different features are enabled such as EAP TLS 802.1x for authentication, WPA/WPA2/TKIP for encryption, etc….

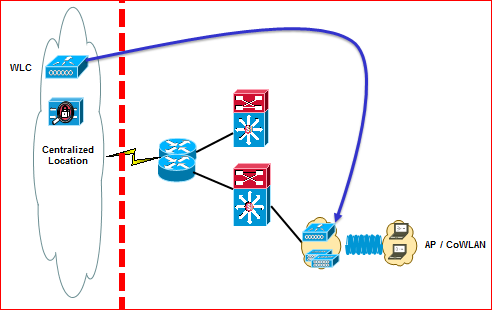
ExxonMobil CoWLAN service at divesting sites will be converted to simple standard wireless configuration (non-ExxonMobil), which will provide wireless access to the divesting company network. Other private services managed by our WLCs, such as GIAS, will not be covered in here as they are typically out of scope.

## Pre-Build

* Divesting site with existing local WLC: No additional build needed at this stage



* Divesting site with centralized WLC: New local WLC with ExxonMobil CoWLAN standard configuration will be installed



* Follow current CoWLAN design & implementation best practices for installing new WLC.

## Co-Existence

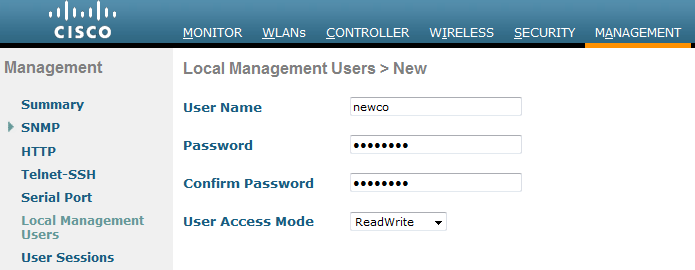
CoWLAN and other services (i.e. GIAS) should continue to be operated under ExxonMobil S&C standards. Some of the changes that could take place at this stage are:

* Activate new local WLC
* Modify/Activate wireless client DHCP scope (option 43) to Re-home local Access Points to new WLC. Because at this stage, there will be a new local Microsoft DHCP server installed, the wireless client DHCP scope/option 43 must be activated on this new server
* Modify/update **ip-helper** on the VLAN interface to point to the new DHCP server

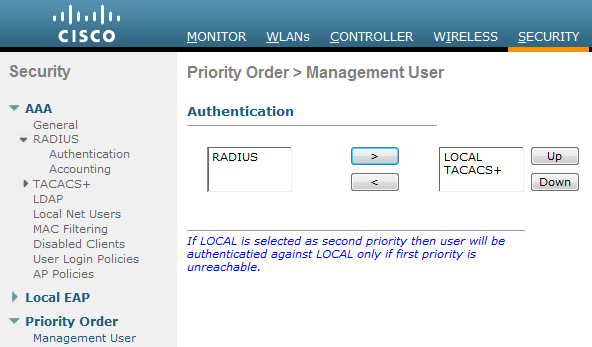
## Change-in-Control

For CiC, the WLC must be configured through the Web Interface. The steps below exemplify how to do this with our current WLC OS version. Should the interface be any different, refer to the WLC implementation practices for an up to date visual reference.

**1. Enable local password authentication**

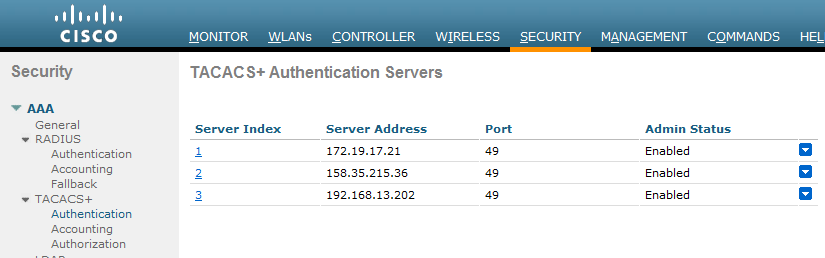
Add a new local administrator login for the WLC. Go to Management > Local Management Users and add a “newco” user with ReadWrite access. Generate a secure password and give it to the Project Manager or Infrastructure Track Lead to be included in the handover package. For the remaining pre-configuration and handover steps, use the newco ID.

Go to Security > Priority Order > Management User and change the authentication order to Local, then TACACS+ or remove TACACS+ from the priority order completely.

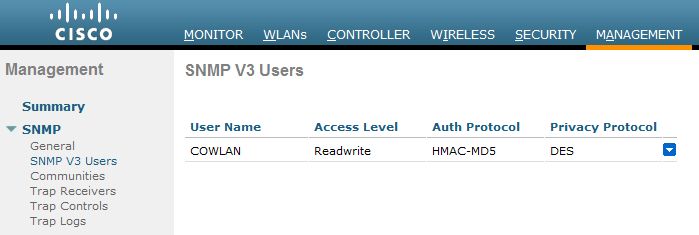


**2. Remove TACACS+/RADIUS authentication**

Go to Security > AAA > TACACS > Authentication and remove the TACACS Authentication servers. Do the same for Accounting and Authorization.



**3. Remove SNMP V3 users**

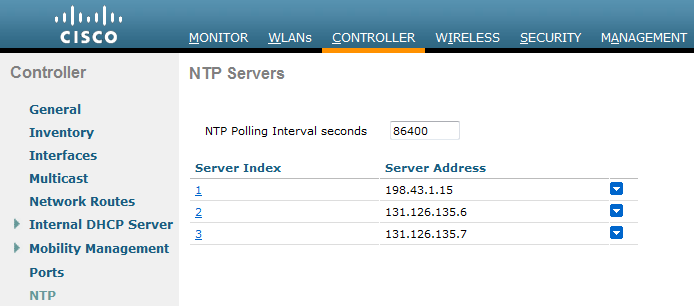
Remove all SNMP V3 users to prevent the WCS (Wireless Control System) from overwriting the configuration with the standard templates.

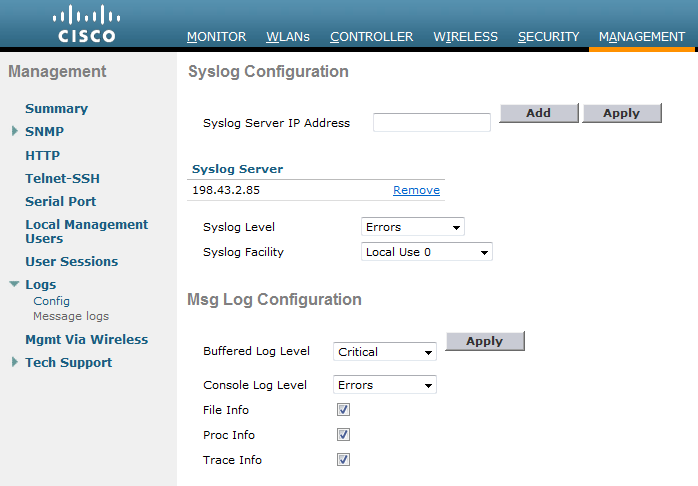
Go to Management > SNMP > SNMP V3 Users and hover over the down- arrow icon and select Remove.

**4. NTP / Syslog Configuration**

Click on Controller > NTP and update the NTP server configuration. Remove the ExxonMobil NTP servers and add a local NTP server IP.

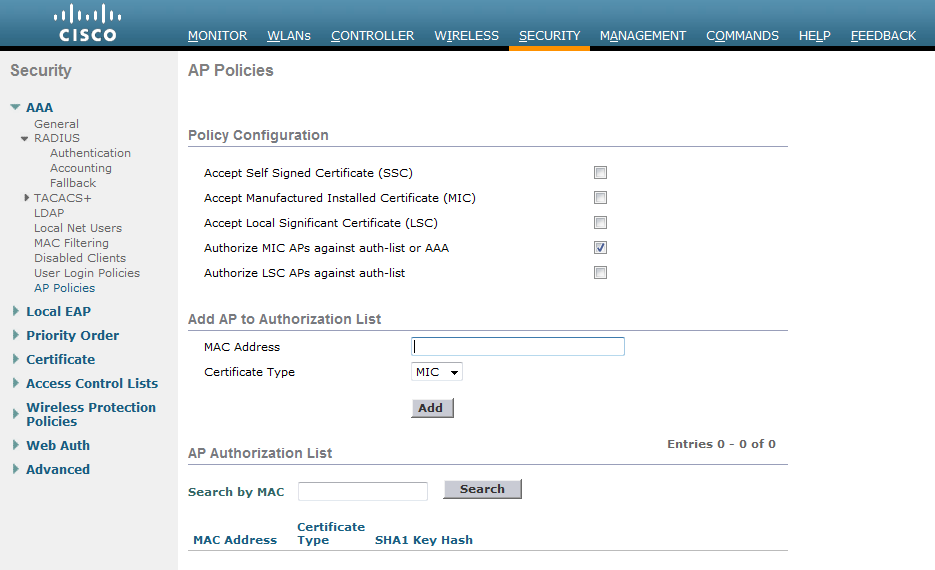
If no NTP server has been set-up, it is recommended to point all NTP clients to the core switch of the hub site, and for it in turn to be relayed to the one of the buyer’s preference.



Click on Management > Logs > Config. Remove the ExxonMobil Syslog server IP and add a local Syslog server (if applicable).

**Authentication (Local MAC)**

Access-points authentication will be converted from RADIUS to local authentication by MAC address.

Go to Security > AAA > AP Policies > Add and enter the MAC Addresses of all the APs.

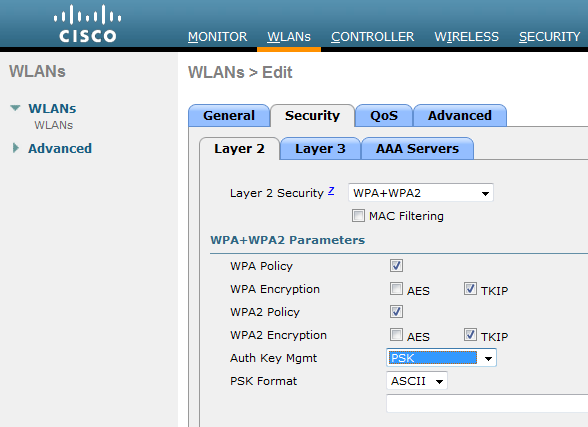
**SSID management**

Assume that SSID will still remain “COWLAN”. However, this subject to change per buyer’s request.

**Wireless Authentication**

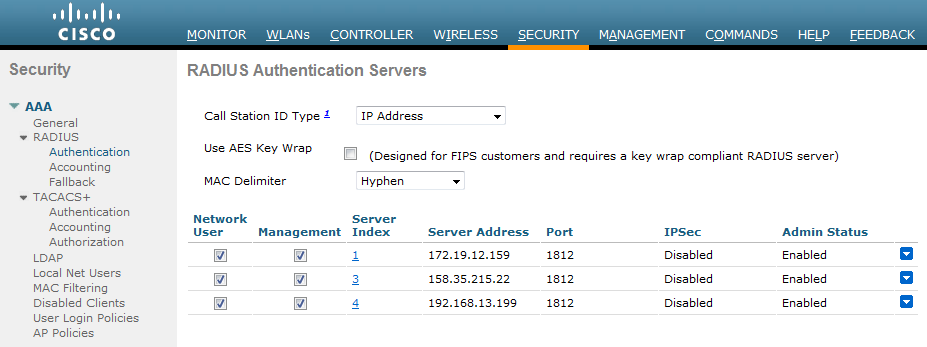
Authentication will be changed from 802.1x to Pre-shared keys. Generate a secure but unambiguous pre-shared key and provide a copy to the Project Manager / INF track lead for handover and for sharing with other team members (i.e. WDS Client Operations) to update the laptop wireless password.

Click on WLAN > COWLAN (1) > Security > Auth Key Management > PSK



Enter the Pre-shared key in ASCII format.

**Remove RADIUS server profiles**

Go to Security > AAA > RADIUS > Authentication and remove the RADIUS Authentication servers. Do the same for Accounting.

**Wireless client management**

Work with server/client team to modify authentication and encryption for CoWLAN SSID appropriately.  
The wireless laptops should be re-configured to use Pre-shared key authentication with WPA/WPA2 security and TKIP encryption.

**Transition support to buyer**  
Wireless SSID and Pre-shared key  
WLC Administration URL, login ID and password

# Network Devices Configuration Conversion

ExxonMobil network devices (such as routers & switches) are configured with ExxonMobil standard configuration practices including TACACS, Quality of Service, Access Control List, 802.1x, etc…These ExxonMobil configuration is recommended to be removed and replaced by non-ExxonMobil configuration (or buyer’s agreed configuration). However, above ExxonMobil configuration may be retained to maintain the service (i.e. QoS for Voice) depending on SLA with buyers.

## Pre-Build

As explained earlier in this document, in this stage new devices are typically installed. These devices must be configured and commissioned according to our standards. It is recommended to submit an automated commissioning request through IT Services. Any new device installed that will be transitioned to the buyer needs to be added to the inventory list that will be handed over to the new company IT Lead

## Co-Existence

During co-existence, network devices will continue to operate per ExxonMobil standards. In some cases, approved exceptions are implemented (e.g., remove 802.1x) and documented accordingly.

Once the CiC date is confirmed, and about 10 days before it, it is recommended to remove TACACS from the non-voice devices except WAN routers, and configure a local admin user and password. These credentials should only be shared among NS members of the project and Infrastructure Track Lead. This configuration will be required to handover administrative control of the equipment to the buyer, but most importantly, to avoid other analysts to access and make changes to the device that may impact the preparation for the CiC. With the removal of TACACS, the support responsibility of the affected devices will fall on the divestment project team.

## Change-in-Control

This stage is crucial in the divestment of a site. Switches provide network access to every host, and routers transport network data from one network to the other, and will eventually connect the divested sites with the buyer’s infrastructure. While the order of activities may vary from one divestment to the other once the command center gives the “go” signal to disconnect, there are some key items that the analyst implementing is strongly encouraged to follow:

* + Before disconnecting from the ExxonMobil network, remove TACACS from those devices that still have it.
  + If the sites are not connected to the buyer through an external connection already, before connecting to them, all network connections to ExxonMobil should be finalized.
  + Non-standard configurations and/or exceptions that were not approved to the moment are not recommended to be implemented until the sites are fully disconnected from the ExxonMobil network.
  + All private/proprietary configuration and/or intellectual property from ExxonMobil that is configured on the network devices should be removed before handing over the network to the buyer.

# Voice Conversion – Cisco

This section provides general guideline to convert ExxonMobil IP Telephony service based on Cisco technology. For complex scenarios, consult Cisco IPT Subject Matter Experts or the corresponding team of Cisco Voice technology stewards’ recommendations.

The set of sites in scope of a divestment project could be comprised of a Campus site, a Hub site, SRST or simply a mix of these. While the objective is in general always the same, to maintain Voice Services if there are any at the divested sites, there are some considerations that are some subtle differences among them for each stage.

Cisco voice technologies may include CallManager servers, Unity Connection servers, Voice Gateways, Analog voice Gateways and endpoints such as IP phones, faxes, etc.. Some of these are only deployed to Hub sites and/or Campus. This applies particularly for the CallManager and Unity Connection servers, which serve various sites and not only the one they are located at.

## Pre-Build

* When there are no Hub sites or Campus, one of the SRST sites needs to evolve to take the Hub role. The election must be done taking into consideration all design requirements such as bandwidth and available network infrastructure to support the voice service. The number of endpoints needed also to be taken into account.
* When there is at least one Hub site or Campus, any of these are candidates to act as Voice hub for any other SRST site. This scenario has two implications
  + All Cisco SRST sites that are not pointing to the elected Hub will need to be re-pointed and the elected Hub confirmed to scale well for adopting new SRST sites.
  + All Cisco SRST sites that are already pointing to the elected Hub, and are not in scope of the divestment, will need to be repointed to a new Voice Hub. However, if they are in scope, there’s nothing to do with them.



*The diagram above shows a possible scenario during this stage*

## Co-Existence

* Existing Cisco IPT services continues to operate under ExxonMobil standards
* When possible, it is strongly recommended to maintain the IP addressing for existing CCM, CUX servers, gateways, and IP phones
* If required to implement a new Hub, any installations of a new CCM/CUX servers should happen during this stage. This includes the implementation of an ICT (inter cluster trunk) between the new Hub and the regional gatekeeper.
* Re-register phones that need to point to a new Hub in this stage. This effort can take a several weeks depending on the number of endpoints and available bandwidth between the cluster and the SRST sites. Hence, it is recommended to plan to finish the repointing of all the phones no later than 2 weeks before CiC. If bouncing the switch ports that connect to IP phones fails for them to learn the new DHCP/TFTP servers, then a factory reset of the phones will be required to force them to update the TFTP address as per the DHCP options settings.
* If there are new subnets with an associated IP phone DHCP scope then they must be activated on the new DHCP servers
* The IP phone DHCP ranges defined on the NewCo DHCP server must contain the correct values for option 150. Depending on specific cases, those values may stay the same as what is defined in production, but in others they will change.  The correct values must be provided to NMS so that the NewCo DHCP range is configured properly
* Update ip-helpers to direct to new DHCP servers
* Transition of TDM circuits and billings ownership

Follow similar general guideline divesting campus in addition to identify all remote SRST sites and start re-homing them to new hub cluster of reference.

Note: This would require significant planning effort including:

* Bandwidth sizing
* CCM and CUX cluster sizing
* Export/Import of devices and voicemail from existing hub to new hub cluster etc…
* Replicating the divested hub’s configuration to the new Hub
* Point the SRST voice GW to new hub

. 

*The diagram above shows a possible scenario during coexistence*

## Change-in-Control

**CCM & CUX management**

* Remove ICT trunk configuration
* Remove Gatekeeper configuration
* Remove LDAP integration
* Enable local authentication
* Reset all local admin accounts and provide buyer with updated information (i.e. CUCMadmin, CUCMApp, etc…)
* In case of an agreement with the buyer for the phones to connect to a buyer CUCM/CUC cluster at CIC, bounce the switch ports that connect to IP phones so that they learn of the new DHCP/TFTP servers. It is common for this to fail on some phones which will not register to the new servers because it won’t update the TFTP address as per the DHCP options settings, thus requiring a factory reset (personnel on site).
* Notify asset management that equipment has been divested

## Voice Gateways

* Follow past section’s guidelines on device configuration conversion to remove any ExxonMobil proprietary information on voice gateways
* Configure the voice gateways to point to the new CCM/CUX servers.



*The diagram above shows a possible scenario after change in control*

# GVIN (Phase I & II)

Since the PBX in GVIN sites has not reached end of life, divesting GVIN phase I requires the voice gateway to be removed, and GVIN phase II sites will only require the migration of the TDM circuits from voice gateways to the TDM PBX.

## Pre-Build

* System continues to operate under ExxonMobil standards

## Co-Existence

* Transition of TDM circuits and billings ownership

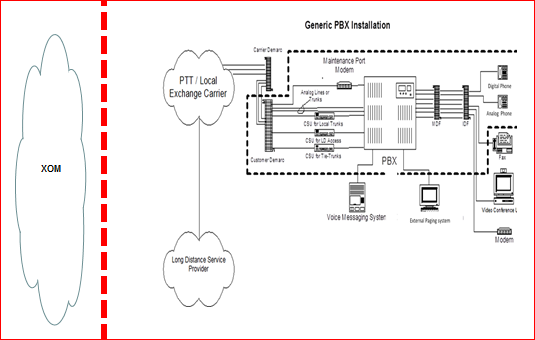
## Change-in-Control

* Migrate the TDM circuits from the voice gateway to the TDM PBX
* Follow above Device configuration conversion guideline to remove any ExxonMobil proprietary information on voice gateways, etc…
* Transition privileged IDs (i.e. default or new password) for TDM PBX
* Notify asset management that equipment has been divested

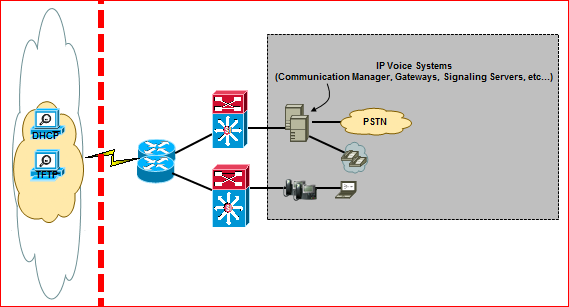
# Non-Cisco Voice Systems Conversion - TDM

There are many non-Cisco voice systems that exist today in ExxonMobil voice network. This document provides general guidelines for the divestment of Avaya and Nortel voice systems. Solution guidelines for other systems such as Ericson, AT&T, etc. will be not be covered in this document.

The following diagrams describes a generic TDM topology



In this case the below, an Avaya/Nortel system. Optionally, the TFTP server could be local



Although the stages’ descriptions are generic, they are applicable only to TDM, IP Non-Cisco Avaya and Nortel Voice systems.

## Pre-Build

* System continues to operate under ExxonMobil standards

## Co-Existence

* Voice system should continue to operate under ExxonMobil standards and controls. However, preparation for transition should be conducted at this stage.
* With existing ExxonMobil Avaya/Nortel IP system deployments, these are stand alone, and there are no remote sites.
* Refer to **Voice system Decommissioning Best Practice** for additional guidelines.
* New circuits may be installed (PRI / Central Office Trunks, business lines (DSL). Existing ones will need to be transitioned at CiC, requiring transitioning/decommissioning paperwork to be started a few weeks before that.
* Additional steps are required for Nortel and Avaya systems
  + Create DHCP scope on NewCo DHCP server. The Avaya and Nortel  DHCP ranges defined on the NewCo DHCP server must contain the correct DHCP options values.  For reference, the DHCP options used are:

**Avaya Phone DHCP Options**

|  |  |  |
| --- | --- | --- |
| Phone Type | Scope Option | Syntax |
| 46XX | 176 | MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719, TFTPSRVR=yyy.yyy.yyy.yyy |
| 96XX & 16XX | 242 | MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719, TFTPSRVR= yyy.yyy.yyy.yyy  xxx.xxx.xxx.xxx = PBX CLAN IP for phone registration  yyy.yyy.yyy.yyy = TFTP IP address where phone firmware is located |

* + Note: If there is no access to the Avaya PBX, the lease time on the DHCP server must be reduced to force the phones onto the new DHCP server. The physical reset of the phones will not work.

**Nortel Phone DHCP Options**

Note: Only Wireless and Conference IP phones use TFTP servers for firmware, all others receive firmware from the signaling server (PBX).

|  |  |  |
| --- | --- | --- |
| Phone Type | Scope Option | Syntax |
| All | *144* | |  |  | | --- | --- | | |  | | --- | | Nortel-i2004-A,iii.iii.iii.iii:ppppp(4100),aaa(1),rrr(5);iii.iii.iii.iii: (4100),aaa(1),rrr(5). | |   •“iii.iii.iii.iii” = the IP Address of the Call Server (S1 or S2)  •“ppppp” = port number for the Call Server  •“aaa” = the Action for the Server  •“rrr” = the Retry Count for the Server  Note: The IP Address must be separated from the port number by a colon (:). The parameters for the Primary (S1) and the Secondary (S2) Call Servers are separated by a semicolon (;). The string must end a period |
| All | 191 | VLAN-A:XXX.  (XXX = data VLAN |

* + Depending on specific cases, the option values may stay the same as defined in production, but it may change in others. Regardless, the correct values must be provided to NMS so that the NewCo DHCP ranges for Avaya and Nortel are configured properly.

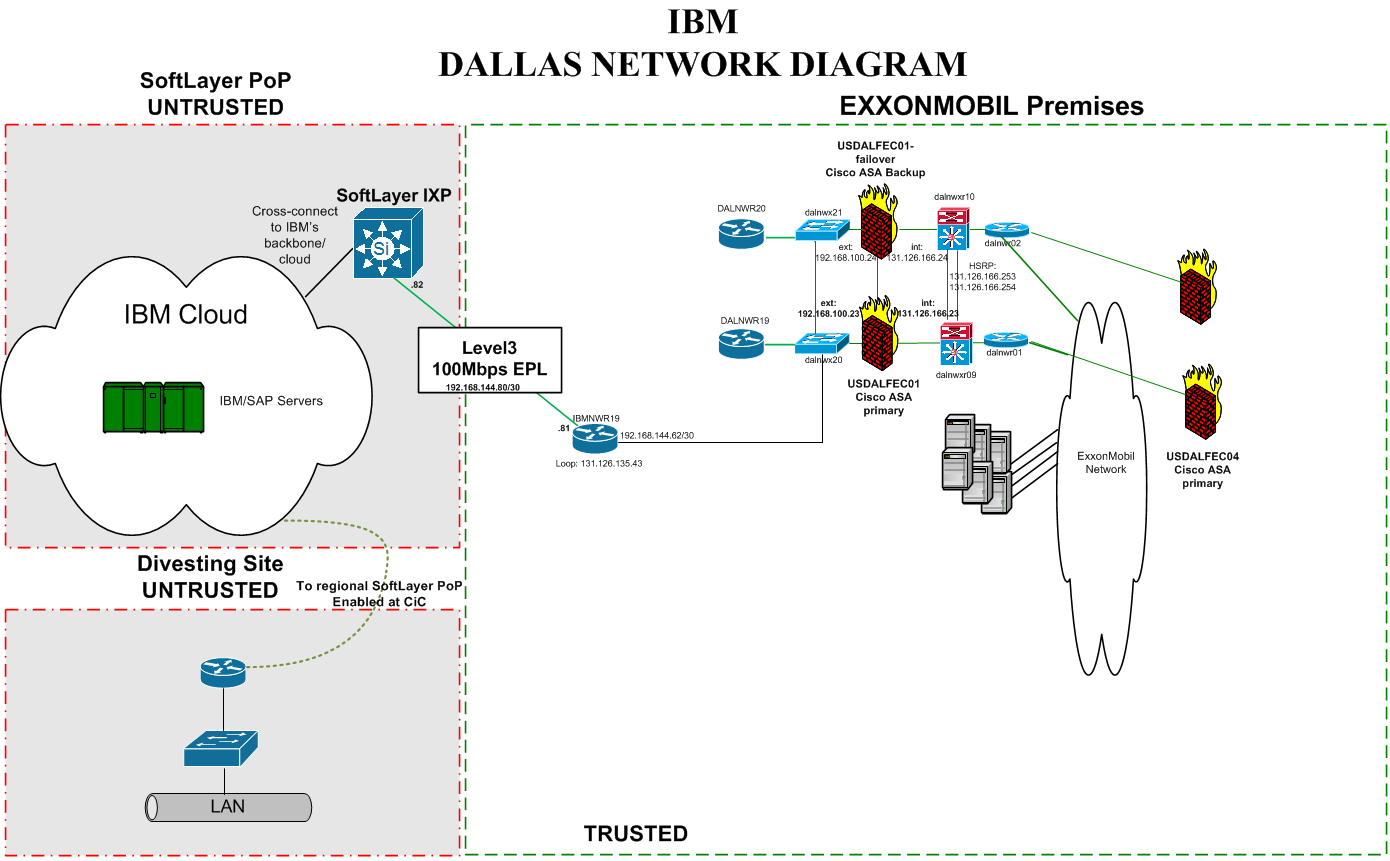
## Change-in-Control

* The following steps must be followed to complete the handover of the system to buyer:

# IBM Cloud services

In support of Downstream divestment projects, IBM is engaged to provide an IT systems platform, including any underlying infrastructure, operating systems, and database software, to host an SAP system based upon a reconfigured ("carved-out") ExxonMobil SAP system, typically STRIPES, that can be fully transferred to the buyer in a divestment and can continue to operate independently of ExxonMobil at the conclusion (Change in Control) of a divestment project.

A network connection between EM Dallas and SoftLayer’s (IBM) PoP is used during divestment project transition activities. At the PoP, a cross-connect gives access to IBM cloud services. This facilitates systems and data copies (SLO process) to the IBM SAP system.



## Pre-Build

No changes. Base connectivity has already been established. This set-up does not change between divestments.

## Co-Existence

Firewall rules need to be updated by NetSec to allow traffic from selected SAP servers in the Dallas internal network that contain data of the divesting sites to the servers in IBM’s cloud.

## Change-in-Control

During change in control, all production data hosted in Dallas SAP servers is transferred to the cloud by the Applications team. Once the data transfer is completed, the Dallas network will continue to connect to SoftLayer, but the firewall rules that were put in place for this divestment will need to be removed by the NetSec analyst.