Cisco главное руководство по развертыванию NCS 1.1

Содержание

Введение

Система управления сетью (NCS) Cisco Prime представляет собой следующее поколение платформы управления сетями Cisco. Система разработана для управления проводными и беспроводными сетями доступа.

Управление жизненным циклом WLAN: Всестороннее управление жизненным циклом WLAN включает полный диапазон планирования, развертываний, мониторинга и устранения проблем, исправления и оптимизации.

- При планировании — Встроенные программные средства планирования и проектирования упрощают размещение точки доступа определения и покрытие. Кроме того, информация от сторонних программных средств обзора узла может быть импортирована в Cisco NCS для способствования Проектированию WLAN и развертываниям.
- Развертывания — широкий набор интегрированного контроллера и шаблонов настройки точки доступа отправляет быстрые и экономически эффективные развертывания. Сетевой контроль поддерживается для эффективного управления конфигурацией. NCS также предоставляет программные средства для способствования мониторингу, обновлению и миграции Cisco Aironet автономные (автономные) точки доступа, чтобы действовать в качестве облегченных точек доступа и выполнить CAPWAP. Основанное на роли управление доступом предоставляет гибкость для сегментации беспроводной сети в один или несколько действительных доменов, управляемых одиночной Cisco платформа NCS.
- При мониторинге и Устранении проблем — Централизованный мониторинг всего WLAN помогает поддерживать устойчивую производительность WLAN и оптимальный беспроводной опыт. Cisco CleanAir предоставляет подробные сведения о событиях радиочастотной помехи, качестве воздуха, и интерференционных угрозах безопасности,

чтобы помочь более эффективно оценивать, расположить по приоритетам и управлять проблемами радиочастотной помехи. Простые в использовании графические дисплеи служат отправной точкой для обслуживания, безопасности, устранения проблем и будущего планирования мощности. Графики, диаграммы и таблицы являются интерактивными для быстрой настройки и изменения конфигурации. Иерархические деревья сопоставления, цветовое кодирование и значки поддерживают быструю визуализацию и оценки статуса сети, устройств и качества воздуха. Вездесущая сводка аварийных сигналов предоставляет устойчивый отказ, событие и Управление сигналами тревоги. Персистентный инструмент поиска упрощает перекрестный доступ к сети к непосредственной и исторической информации об устройствах и активах, расположенных где угодно в доступе к сети, включая оконечную точку и атрибуты сеанса, историю ассоциации, расположение оконечной точки, производительность RF, статистику, управление радиоресурсами (RRM) и качество воздуха. Встроенный Инструмент диагностики клиентов предоставляет пошаговый метод для анализа проблем для всех соединенных проводом и беспроводные клиентские устройства. Этот устойчивый инструмент диагностики клиентов помогает уменьшать текущие расходы путем ускорения разрешения ярлыков проблемы для множества типов устройства клиента Wi-Fi.

Роль NCS в сети

Этот рисунок изображает сетевую архитектуру беспроводной связи Cisco с Cisco Главный NCS. Взаимодействия между различными сетевыми элементами, которые являются контроллером беспроводной локальной сети, AP, коммутатором Cisco Catalyst, Cisco Mobility Services Engine, Системой управления сетью, станцией управления клиентской сети и сторонним приложением.

Порты, используемые NCS

Поддержка устройств и версии программного обеспечения

Тип устройства	Версия поддерживаемого программного обеспечения*
Cisco Catalyst коммутаторы серии 2000: 2960, 2975	Независимый от выпуска программного обеспечения Cisco IOS
Cisco Catalyst 3000 Series Switches: 3560, 3750-E, 3750-X	Независимый от Cisco IOS Software Release
Cisco Catalyst 4500 Series Switches	Независимый от Cisco IOS Software Release
Cisco Catalyst 6000 Series Switches	Независимый от Cisco IOS Software Release
Контроллеры беспроводной локальной сети Cisco 2x00, 4x00,	4.2.x, 6.x, 7. x

5500 Интегрированный WLAN (WLCM, WiSM, WiSM2)	
Cisco Aironet автономные AP	Программное обеспечение Cisco IOS версии 12.3 (7) JA и позже

* - поддерживаемые выпуски ПО контроллера перечислены в Комментариях к выпуску NCS.

NCS имеет два параметра развертывания:

1. совместимость оборудования
2. виртуальное устройство

Виртуальное устройство является файлом OVA, который может быть развернут на VMware ESX/ESXi 4.x и 5.0. Эта таблица предоставляет номера масштаба для устройств, которыми управляет NCS.

Платформенные весы				
	Унифицированный AP	AP AIO	Коммутаторы	Контроллеры беспроводных LAN
Маленькое виртуальное устройство	3,000	1,000	1,000	240
Среднее виртуальное устройство	7,500	2,500	2,500	600
Большое виртуальное устройство	15,000	5,000	5,000	1,200

Примечание: Номера платформенных весов для контроллеров беспроводной локальной сети (WLC; s) максимальный масштаб. WLC не говорят против количества лицензии NCS.

Эта таблица приводит требования к оборудованию для виртуального устройства на основе проводного/беспроводного масштаба.

Виртуальное устройство – требования к оборудованию			
	Процессор	DRAM	Жесткий диск

Маленькое виртуальное устройство	2 ядра 2.93 ГГц	8 ГБ	200 ГБ
Среднее виртуальное устройство	4 ядра 2.93 ГГц	12 ГБ	300 ГБ
Большое виртуальное устройство	8 ядер 2.93 ГГц	16 ГБ	400 ГБ

Домашняя страница NCS

NCS 1.1 предоставляет способность контролировать клиентов IPv6. Новая домашняя страница dashlet, Клиентское количество Типом IP-адреса, предоставляет визуальный индикатор клиентов на основе Типа IP-адреса. `Not detected` обращается к клиентам, IP-адрес которых не может быть определен; как правило, проводные клиенты в случаях, где отслеживание IPv6 не доступно/поддерживаемо на устройстве.

Поддержка обозревателя

NCS 1.1 поддерживает эти браузеры:

- 3.6 и позднее Firefox
- Google Chrome 12.0.742. x
- Microsoft Internet Explorer с плагином Chrome**Примечание:** Собственный Internet Explorer не поддерживается.

Этот документ предоставляет архитектурное понимание и руководство по проектированию для развертываний NCS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco Главный NCS 1.1.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Установка

Физическое устройство: установка ISO

NCS доступен и как медосмотр и как виртуальное устройство. Этот раздел предоставляет шаги для установки образа ISO на физическом устройстве.

1. Загрузите и запишите ISO к DVD. ISO зарегистрирован на программном обеспечении Загрузки (только зарегистрированные клиенты). Используйте свое имя пользователя и пароль Cisco.com.
2. Установите ISO. Машина перезагрузки с ISO вставлена. Будет отображено следующее диалоговое окно. Выберите опцию 1 или 2, которая зависит от того, как вы связаны с устройством
3. Установка занимает приблизительно 30 минут для завершения. После того, как образ ISO установлен, перезагрузки сервера. После ваших перезагрузок устройства перейдите к Физическому Разделу настройки / Разделу настройки Виртуального устройства.

Виртуальное устройство: VMware установка OVA

Выполните эти шаги в этом разделе для развертывания OVA в VMware ESX/ESXi 4. x. После того, как OVA был установлен, продолжите Физический Раздел настройки / Раздел настройки Виртуального устройства. Время, которое требуется для развертывания, варьируется основанное на скорости сетевого подключения к хосту ESX.

Разверните Файл OVA. OVA Зарегистрирован на программном обеспечении Загрузки (только зарегистрированные клиенты). Загрузите соответствующий OVA на основе количества устройств, которым управляет этот сервер NCS.

Используйте vSphere Клиента для установки OVA

Выполните следующие действия:

1. Запустите Клиента VMware vSphere. Выберите **File> Deploy OVF Template**.NCS образ VMware упакован как OVA (открытый архив виртуализации) файл. Элемент меню в предыдущем снимке экрана для шаблона OVF. OVA является набором элементов в одиночном архиве. Эти элементы, как правило, состоят из файла описания виртуальной машины (*.ova), файл манифеста (*.mf), и файла виртуального жесткого диска (*.vmdk).
2. Выберите **Browse** и найдите файл OVA NCS. **Нажмите кнопку Next.**
3. После того, как файл OVA выбран, VMware, ESX/ESXi читает атрибуты файла OVA. Продолжите посредством шагов, чтобы к выбрал файл OVA, который вы хотите установить в ESX/ESXi. На странице Disk Format выберите опцию **Толстого выделенного формата**.
4. Сводная страница перечисляет опции, которые были выбраны. **Нажмите кнопку Next**. Перезагрузки NCS. После того, как виртуальная машина была создана, это появляется на левой стороне окна. Для запуска виртуальной машины выберите ее из левого меню, которое перечисляет установленные виртуальные машины, и нажмите **открытый**

консольный значок. На этом этапе NCS установлен как виртуальная машина. Остаток шагов настройки идентичен для физической и виртуальной машины.

Физическое Обновление / Обновление Виртуального устройства

Выполните следующие действия:

1. Получите URL расположения файла, где образ обновления NCS сохранен на сервере. Выполните эти команды для обновления установки NCS:`ncs1/admin# ncs stop`
```
Stopping Network Control System...
This may take a few minutes...
Network Control System successfully shutdown.
```
2. Как только NCS был остановлен, вводит режим конфигурации и размещает URL расположения файла в репозиторий:`ncs1/admin# conf t`
```
Enter configuration commands, one per line.  End with CNTL/Z.
ncs1/admin(config)# repository NCS58
ncs1/admin(config-Repository)# url http://xxxx/sanity/1.X.X.10/wcs-cars-appbundle/
ncs1/admin(config-Repository)# exit
ncs1/admin(config)# exit
```
3. Проверьте, что доступы к репозиторию файл задали с URL ранее:`ncs1/admin# show repository NCS58`
```
ncs-upgrade-bundle-1.1.0.58.tar.gz
```
4. Выполните эти команды для инициирования процесса обновления от репозитория.`ncs1/admin# application upgrade ncs-upgrade-bundle-1.1.0.58.tar.gz NCS58`
```
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
```
5. Сообщение должно появиться, который указывает, что процесс обновления теперь завершен.

Начало NCS

После перезагрузок сервера войдите в систему как в admin, использующий пароль, который вы предоставили как часть шага настройки. После того, как вы войдете в сервер, запустите сервер NCS с команды `admin@ncs-server opt]# ncs start`.

Когда NCS работает, консольные сообщения указывают. Войдите в свой сервер NCS через web-браузер как пользователь `root` с паролем, который вы выбрали во время установки. Пароль при загрузке может быть изменен после того, как вы войдете в NCS посредством входа в систему браузера.

Миграция от WCS до NCS

Необходимо обновить их сервер Cisco WCS к одним из этих версий, прежде чем вы попытаетесь выполнить процесс переноса к NCS 1.1. x. x.

- 7.0.164.3
- 7.0.172.0
- 7.0.220.0

Этот раздел предоставляет инструкции для того, как переместить WCS или на Windows или на сервере Linux к NCS. Выпуск NCS является основным релизом для обеспечения

установившегося управления проводных и беспроводных устройств и увеличенной масштабируемости. Платформа NCS основывается на Linux 64 бита ОС, и база данных бэкэнда является DBMS Oracle. Существующие платформы WCS являются или Windows или Linux, 32 бита и база данных бэкэнда являются Существенным DB.

Переход данных от WCS

Данные экспорта от WCS

Данные экспорта от WCS 7.x через CLI. **Экспорт userdata** команда CLI доступен в Выпуске 7.x WCS и позже, который создает файл .zip, который содержит файл данных WCS. CLI не предоставляет возможности настраивать то, что может быть экспортировано; экспортируются все неглобальные определяемые пользователем элементы. Выполните эти шаги для экспортирования данных WCS:

1. Остановите сервер WCS.
2. Выполните команду **экспорта** через файл сценария и предоставьте путь и экспортируйте имя файла, когда предложено.
3. Для Linux выполните export.sh вся/data/wcs.zip команда. Для Windows выполните export.bat вся \data\wcs.zip команда.

Миграция данных WCS к NCS

Выполните эти шаги для миграции данных WCS:

1. Разместите файл .zip экспорта WCS (например, wcs.zip) в репозитории или папке (например, репозиториях).
2. Войдите как пользователь с правами администратора и остановите сервер NCS путем ввода **команды ncs stop**. Настройте репозиторий FTP на устройстве NCS с командой **репозитория**:`ncs-appliance/admin#configure ncs-appliance/admin(config)# repository ncs-ftp-repo ncs-appliance/admin(config-Repository)# url ftp://209.165.200.227// ncs-appliance/admin(config-Repository)# user ftp-user password plain ftp-user`
   Примечание: Удостоверьтесь, что заархивированный файл доступен с **командой show repository repositoryname**.
3. Введите **команду ncs migrate** для восстановления базы данных WCS.`ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo`
4. По умолчанию никакие события WCS не перемещены. Введите **команду ncs start** для начала сервера NCS после того, как завершено обновление. Войдите к интерфейсу пользователя NCS с входом в систему в качестве root и паролем при загрузке.Эти данные не перемещены от WCS до NCS:Подмножество отчётов — Предварительная загрузка Образа AP, Статус Профиля AP, Сводка AP, Клиентское количество, Клиентская Сводка, Трафик клиента, Отчёт о PCI, Подробное Соответствие PCI и Сводные отчеты, Предпочтительный Сводный отчет Сети Вызова, Посторонние AP, Оперативные Жулики, Новые Оперативные Жулики и Сводные отчеты Безопасности.Кастомизация информационной панелиСтатистические данные Станции клиента не заполнены со старыми данными WCS в диаграммах клиентов, клиентской подробной странице, информационных панелях и отчётах.Клиентская историческая информация о сеанса действительно становится обновленной.История событий, сохраненная в базе данных WCS, не перемещена на NCS.IP - сервер RADIUS/TACACS

и учетные данные не перемещены и должны быть добавлены снова после того, как миграция завершена. Необходимо скопировать последние настраиваемые атрибуты с NCS и включать их в AAA-сервер для проверки подлинности пользователя / авторизация в TACACS +/RADIUS.**Примечание:** Удостоверьтесь, что сервер RADIUS/TACACS включен как режим AAA на странице Administration> AAA> AAA Mode Settings.Только сигналы тревоги с Корневым виртуальным доменом перемещены от Выпуска 7.0 до NCS.Пароль при загрузке не перемещен от Выпуска 7.0.164.3 или 7.0.172.0 до Выпуска 1.1 NCS. x. x. Пользователь должен изменить пароль при загрузке во время установки приложения. Пользователи маршрута non и их учетные данные перемещены во время миграции.Категории аварийных сигналов и подкатегории не восстановлены после миграции Сводке аварийных сигналов NCS.

Обновите NCS от NCS 1.0.x к 1.1

Можно обновить от Версий 1.0.0.96, 1.0.1.4, 1.0.2.28 NCS, и 1.0.2.29 к NCS 1.1. x. x.

На эти элементы нужно обратить внимание до процесса обновления:

- Гарантируйте выполнение резервной копии, прежде чем вы попытаетесь обновить.
- Отключите Высокую доступность перед выполнением обновления.
- NCS завершения работы перед выполнением обновления. Выполните **команду ncs stop** для остановки NCS.

Используйте эту команду для обновления от NCS 1.0 до NCS 1.1. x. x:

```
# application upgrade NCS-upgrade-bundle-1.0.2.x.tar.gz wcs-ftp-repo
```

В предыдущей команде, **NCS-upgrade-bundle-1.1. x. x. tar.gz** является файлом связки (bundle) обновления, который доступен на программном обеспечении Загрузки (только зарегистрированные клиенты). Репозиторий, используемый в примере, **wcs-ftp-repo**, может быть любым допустимым репозиторием. Это примеры конфигураций репозитория:

Репозиторий FTP:

```
#
configure (config)#
repository wcs-ftp-repo (config-Repository)#
url ftp://ip-address (config-Repository)#
user ftp-user password plain ftp-user (config-Repository)#
exit (config)#
exit #
```

Репозиторий SFTP:

```
# configure
(config)# repository wcs-sftp-repo
(config-Repository)# url sftp://ip-address
(config-Repository)# user ftp-user password plain ftp-user
(config-Repository)# exit (config)# exit #
```

Репозиторий TFTP:

```
# configure
(config)# repository wcs-tftp-repo
(config-Repository)# url tftp://ip-address
(config-Repository)# exit (config)# exit #
```

Import map от WCS

Экспорт/характеристика импорта карты доступен в WCS 7.0. Эта функция описана подробно в руководстве по конфигурации WCS 7.0.

После вас export map от вашего сервера WCS можно импортировать этот набор карт в сервере NCS. Шаги для импорта карт покрыты руководством по конфигурации WCS 7.0.

Примечание: Важно, чтобы AP в вашем сервере WCS были сначала добавлены к вашему серверу NCS до импорта карт, так как AP на ваших картах WCS также включены во время процесса экспорта. AP, которые не были добавлены к вашему NCS, но присутствуют на экспортируемом результате карт этажа по ошибкам, которые отображены, когда вы импортируете те карты в NCS.

Высокая доступность - фундаментальная теория операции

NCS HA реализация в NCS обеспечивает до двух основных систем NCS для переключений при отказе к одному вторичному (резервному) NCS. Второй сервер требуется, который имеет достаточные ресурсы (ЦП, жесткий диск, сетевое подключение) для принятия операции NCS, если отказывает основной NCS. Каждый экземпляр базы данных на вторичном NCS является горячим резервированием для соответствующего основного NCS.

Нотацией, которая используется для описания основной и резервные системы, является `N:M`, где N = количество основных систем в операции и M = количество резервных систем, которые выполняют резервное копирование основная система (системы).

В NCS поддерживаются эти конфигурации HA:

`1:1 – 1 Primary, 1 Secondary`
Размер дополнительного сервера должен быть больше, чем или равным основному серверу, например если основным сервером NCS является средний OVA, то вторичным сервером NCS должен быть средний или большой OVA.

Основной и дополнительный сервер могут быть соединением медосмотра и виртуального устройства. Например, если основной сервер NCS является физическим устройством, дополнительный сервер может быть или физическим устройством или большим виртуальным устройством OVA, например, конфигурация сервера и калибровка большого OVA совпадают с физическим устройством.

Контроль исправности (HM) является новым процессом, внедренным в NCS, который является основным компонентом, который управляет использованием HA системы. HM разделен на эти множественные подмодули, каждый из которых обрабатывают определенный набор функций:

- Базовый HM — ответственный за эти задачи:конфигурация полной системы HAподдерживает механизм состояний для системы HAзапустите/остановите HM и JVM NCSзапустите/остановите и монитор других подмодулей в HMрегистрация маркеров основной/вторичной парыаутентифицирует HM определенный сеанспринимает все решения относительно аварийного переключения и восстановление после отказа
- Сердцебиение — подмодуль Сердцебиения ответственен за поддержание связи между

основным и вторичным HMs. Связь происходит по HTTPS (порт по умолчанию 8082). Значение таймаута составляет 2 секунды. Механизм повторения был внедрен для повторения подключения установления между P-HM и SHM. Если HM не получает ответ после отправления запроса биения в периоде ожидания, это повторяет связь установления путем отправления другого запроса биения. Общее число повторных попыток равняется 3. После того, как связь не имеет быть установленной после того, как 3 повторных попытки, HMs примет соответствующие меры согласно определенным сценариям:основной сервер выключается: это - классический случай аварийного переключения. В этом сценарии, когда SHM не получает запросы HeartBeat в течение 6 секунд (3 повторных попытки x 2 секунды), это инициирует механизм аварийного переключения на вторичном NCS.дополнительный сервер выключается: в этом сценарии P-HM не получает ответ HeartBeat от SHM в течение 6 секунд (3 повторных попытки x 2 секунды). Когда это происходит, P-HM изменяет свое состояние на PRIMARY_ALONE, выдает аварийные сигналы и изменения в режим прослушивания – ждущий для получения любых сообщений от вторичного устройства для восстановления ссылки между P-HM и S-HM.

- Монитор приложения — подмодуль Монитора Приложения ответственен за связь с платформой NCS (JVM NCS) на локальном сервере для получения сведений о статусе. Связь через SOAP по HTTPS.
- Монитор DB — подмодуль Монитора DB настраивает DB для репликации. Это не ответственно за саму репликацию DB, поскольку это выполнено через базу данных составляющий собственность протокол репликации.
- Синхронизация файлов — подмодуль Синхронизации файлов имеет 4 субкомпонента:Файл Archiver: периодически просматривает каталоги, ища файлы, которые модифицировались. Это собирает любые такие файлы и добавляет их к Архиву на магнитных лентахАгент передачи файла (FTA): ответственный за передачу Архива на магнитных лентах сжатия назначению (другой сервер, т.е. основной к вторичному или вторичному к основному).Servlet выгрузки файла (FUS): работает на дополнительном сервере и дубликат к FTA. То, когда это получает файл, FU передает его потоком непосредственно к экстрактору TAR, а не создайте файл на локальном диске (избегает ненужных дисковых операций). FTA и FU связываются по HTTPS.Центр сбора статистических данных: поддерживает статистику операций передачи файла со времени, когда запускается сервер.

База данных NCS является базовым элементом хранилища данных системы и должна быть реплицирована между основным и резервными системами в real-time без потери данных. Это - основной принцип использования NCS HA. Данные хранятся 1 из 2 способов:

1. База данных NCS
2. Данные прикладной программы

Данные прикладной программы являются рядом однородных файлов, который содержит эти данные:

- файл пароля базы данных: реплицированный в режиме реального времени (11 секунд)
- Файлы лицензии NCS: реплицированный через пакетную обработку (каждые 500 секунд)
- все файлы в соответствии с корневым каталогом tftp: реплицированный через пакетную обработку (каждые 500 секунд)
- запланированные Сгенерированные отчеты: реплицированный в режиме реального времени (11 секунд)

Контроль исправности: контроль исправности (HM) является основным компонентом, который управляет/контролирует доступностью HA системы. Существуют множественные подмодули, которые обрабатывают различные функции через HM.

Базовый HM: ответственный за эти переговоры:

- Настраивает систему HA
- Поддерживает механизм состояний для системы HW
- Запустите/остановите HM
- Запустите/остановите и контролируйте другие подмодули в HM
- Регистрация маркеров основной вторичной пары
- Принимает все решения относительно аварийного переключения и восстановление после отказа

Операция аварийного переключения

После первоначального развертывания NCS полная конфигурация основного NCS реплицирована в хост вторичного NCS. Во время нормальной работы (т.е. основной NCS в рабочем состоянии), база данных от основного реплицирована во вторичный NCS.

В дополнение к репликации базы данных файлы данных прикладной программы также реплицированы во вторичный NCS. Частота репликации составляет 11 секунд (real-time файлы) и 500 секунд (пакетные файлы).

Требования NCS для использования NCS HA Функция

Клиент должен выполнять ту же версию NCS и на основных и на вторичных серверах NCS. NCS HA обладают, очевидно для контроллера беспроводной локальной сети, т.е. нет никакого требования к версии программного обеспечения для WLC, AP и MSE.

Конфигурация функции HA

Эти параметры должны быть настроены на основном NCS:

- НАЗВАНИЕ/IP-АДРЕС вторичного NCS
- адрес электронной почты администратора сети для системного уведомления
- руководство или опция автоматического аварийного переключения

Вторичный NCS должен всегда быть новой установкой, и эта опция должна быть выбрана во время процесса установки NCS. Например, автономный или основной NCS не может быть преобразован во вторичный NCS. Автономный NCS может быть преобразован в Основной HA.

Примечание: Репликация базы данных между P-NCS и S-NCS использует порт 1522, поэтому гарантируйте, что этот порт открыт на всех сетевых устройствах, таков как межсетевые экраны, коммутаторы, маршрутизаторы и т.д, вдоль сетевого пути между основными и вторичными серверами NCS.

Пример – установка и процесс конфигурирования

В данном примере это 1:1 NCS HA система

```
Primary NCS: 172.19.27.84

Secondary NCS: 172.19.27.159
```

Первый шаг должен установить и настроить Вторичный NCS. При настройке Основного NCS для HA Вторичный NCS должен быть установлен и достижимый Основным NCS.

Примечание: Ключевая точка для запоминания - то, что, когда P-NCS является рабочим/в рабочем состоянии, не работает S-NCS. Когда Дополнительный сервер находится в режиме ожидания, эти сервисы работают на дополнительном сервере: HM, Apache и база данных. Когда P-NCS переходит к нерабочему состоянию, HM на Дополнительном сервере запускает процесс JVM NCS. Только тогда делает S-NCS, становятся доступными.

Порт Контроля исправности должен установить на целевой машине установки NCS. Значение порта по умолчанию является портом 8082. Этот номер порта только имеет значение локального компьютера (порт локального компьютера).

```
Check Health Monitor Port...
Please change the Health Monitor web port if needed. Health Monitor (DEFAULT: 8082):
[root@NCSlinux1NCS]#
```

Ключ проверки подлинности для Контроля исправности должен также быть создан во время процесса установки. Этот ключ только используется внутренне P-HM и S-HM для аутентификации. Это должно быть то же включают и основного и дополнительные серверы.

Как сообщили ранее, только одна серверная лицензия NCS должна быть куплена. Например, отдельная лицензия NCS не должна быть куплена для вторичного NCS. Тот же файл лицензии NCS находится и на основном и на вторичном NCS. Так как JVM NCS только работает или на основном или на вторичном устройстве (не оба), файл лицензии только активен в одной системе в данный момент времени.

Администратор сети также должен предоставить параметры настройки почтового сервера для почтового уведомления для процесса HA. Это требуется для руководства HA операция (вмешательство System Manager). Перейдите к этой странице следующим образом: **Администрирование> Параметры настройки> Почтовый сервер**

Конфигурация на основном вторичном устройстве NCS

Параметры настройки NCS

Выберите **Administration> High Availability**. Как выделено, HA в настоящее время не настраивается в этой системе.

Из меню на левой стороне экрана, выберите **HA Configuration**. Это берет вас к этому окну. При вводе запрошенную информацию в Общий раздел заголовка и нажимаете **Save и кнопку Enable**, конфигурация сохранена и HA включена.

Необходимо ввести эту информацию: IP-адрес S-NCS, ключа проверки подлинности, адреса электронной почты для уведомлений, которые будут передаваться, тип аварийного переключения. Можно принять решение сохранить эту информацию, не включая HA, или сохранить и включить HA.

Мониторинг NCS HA операция

После того, как вы выполняете предыдущий шаг, информация о статусе сообщения в NCS предоставляет сведения о конфигурации HA и включено ли это.

Контроль исправности – вторичный NCS

На экране Health Monitor на вторичном NCS вы видите информацию о состоянии вторичного NCS и типа аварийного переключения, который был настроен. Также это позволяет администратору сети устанавливать тип уровня сообщения регистрации и способность перехватить/загрузить файлы журнала. Вы можете также события view, замеченные SHM с связанными штампами времени.

Пример Первичного сбоя – Аварийное переключение в ручном режиме

В данном примере вторичный NCS был настроен с аварийным переключением в ручном режиме. Например, администратор сети уведомлен через электронную почту, что основной NCS испытал условие `down`. Контроль исправности на Вторичном NCS обнаруживает неисправное состояние Основного NCS. Так как аварийное переключение в ручном режиме было настроено, администратор сети должен вручную инициировать S-NCS для принятия функциональности NCS от Основного NCS. Если вы входите в SHM, это сделано. Даже при том, что S-NCS не работает, SHM может быть связан с через этот синтаксис:

```
https://<SNCS_ip_address>:HM_port/
```

SHM отображает сообщения в отношении событий, которые замечены. Так как Аварийное переключение в ручном режиме было настроено, SHM ждет системного администратора для призыва процесса аварийного переключения. Как только Аварийное переключение в ручном режиме было выбрано, это сообщение отображено как S-ncs-запускаются. Как только процесс аварийного переключения был завершен, что означает, что процесс репликации базы данных NCS завершен, и процесс JVM S-NCS запустился, тогда S-NCS является активным NCS.

Контроль исправности на Вторичном устройстве NCS предоставляет сведения о статусе и Основного NCS и Дополнительных серверов. Отказовозвращение может инициироваться через SHM, как только P-NCS восстановился с неисправного состояния. *Процесс отказовозвращения всегда инициируется вручную* для предотвращения колеблющегося условия, которое может иногда происходить, когда существует сбой сетевого подключения.

Восстановление после отказа

Когда вопросы на сервере, которые размещают P-NCS, были решены, отказовозвращение может вручную инициироваться. Как только это сделано, экран отображен на S-NCS. Когда вы инициируете отказовозвращение, базу данных NCS по S-NCS и любым другим файлам, которые изменились, так как S-NCS принял операцию NCS, синхронизируются между S-NCS и P-NCS. Как только синхронизация базы данных была завершена, JVM P-NCS запущен P-HM. Когда JVM P-NCS работает, этот экран отображен на SHM.

Автоматическое аварийное переключение

Автоматическое аварийное переключение является намного более простым процессом. Все действия настройки являются тем же кроме *Автоматического аварийного переключения*, выбран. После того, как настроенный, администратор сети не должен взаимодействовать с S-HM для операции аварийного переключения для имения место. Только во время

отказовозвращения требуемое ручное вмешательство.

Добавьте контроллер к NCS

- Выберите **Configure> Controllers> Add Controller** для добавления коммутатора. Контроллеры беспроводной связи Cisco (WLC) могут быть включены вручную или через Файл csv.
- После добавления контроллеров они размещены временно на странице Monitor> Unknown Devices, в то время как NCS пытается связаться с контроллерами, которые вы добавили. Как только связь с контроллером была успешна, шаги контроллера от страницы Monitor> Unknown Devices до страницы Monitor> Controllers. Если NCS не в состоянии успешно связаться с контроллером, это остается в Мониторе>, Неизвестные устройства и состояние ошибки отображены.

Добавьте коммутатор к NCS

Выберите **Configure> Switches> Add Switches** для добавления коммутатора. Коммутаторы могут быть добавлены индивидуально, или несколько блоков коммутаторов могут быть импортированы через Файл csv.

После того, как коммутатор добавлен, он размещен временно на странице Monitor> Switches, в то время как NCS пытается связаться с этим коммутатором. Как только связь с коммутатором была успешна, NCS перемещает коммутатор от страницы Monitor> Unknown Devices до страницы Monitor> Switches. Если NCS не в состоянии успешно связаться с коммутатором, это остается в Мониторе>, Неизвестные устройства и состояние ошибки отображены.

Настройка коммутатора Catalyst

Существует три шага для клиентской конфигурации безопасности на коммутаторах Cisco Catalyst: AAA, RADIUS и 802.1X/прорерк¦ ПОЕЛИННОСТИ MAC.

Конфигурация AAA

```
aaa new-model
!
aaa authentication login login-none none
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting update periodic 2
aaa accounting dot1x default start-stop group radius
!
ip device tracking
```

См. Обзор AAA для получения дополнительной информации.

Эта конфигурация является конфигурацией коммутатора Cisco для Проверки подлинности RADIUS и для Cisco ISE / ACS и для серверов RADIUS не-Cisco.

Конфигурация IOS

```
radius-server attribute 6 on-for-login-auth
```

```
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 10 tries 3
radius-server host 40.40.1.10 auth-port 1812 acct-port
1813 key secret
radius-server timeout 10
radius-server key secret
radius-server vsa send cisco-nas-port
radius-server vsa send accounting
radius-server vsa send authentication
```

Дополнительные сведения см. в следующих документах:

- Переупорядочивание сервера RADIUS на сбое
- Атрибут RADIUS 8 (Обрамленный IP-адрес) в запросах доступа
- Справочник по командам системы безопасности Cisco IOS

Конфигурация Аутентификации 802.1X и MAC — Эта конфигурация коммутатора предоставляет три функции: аутентификация для клиентов 802.1x, позвольте клиентам продвигаться сеть, которые отказывают аутентификацию 802.1x (событие генерируется/передается к NCS для отказавшей аутентификации 802.1x), Обход проверки подлинности MAC (MAB) для IP - устройств, которые не имеют соискателя 802.1x.

Настройка Cisco IOS

```
dot1x system-auth-control
interface <interface>
 description *** Dot1x Client ***
 switchport mode access
 authentication port-control auto
 authentication open
 < - monitor mode: allows client on the network if it
fails 802.1x auth dot1x pae authenticator mab
authentication order mab dot1x <- for devices without
802.1x capability or credentials !
```

См. IEEE 802.1X Настройки Аутентификация На основе порта для получения дополнительной информации.

MAC-уведомление для Trap-сообщений (неидентификационные клиенты) — Эта характеристика коммутатора Cisco IOS вперед trap-сообщения SNMP от коммутатора до NMS, например, сервера NCS, для уведомлений MAC, клиентов не802.1x.

Настройка Cisco IOS

```
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change

interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface
level config for MAC Notification
  snmp trap mac-notification change removed <- interface
level config for MAC Notification
```

Debug snmp packet Команд отладки

Изменение show mac address-table notification Команд показа

См. Trap-сообщения Уведомления об изменении MAC Настройки для получения дополнительной информации.

Конфигурация системного журнала (только идентификационные клиенты) — Эта конфигурация вперед сообщения системного журнала с Коммутатора Catalyst на сервер NCS.

Конфигурация IOS
archive log config   notify syslog contenttype plaintext logging facility auth logging <IP address of NCS server>

Планирование беспроводной сети

Планирование программного средства

Встроенное программное средство планирования предоставляет путь к администраторам сети в определении, что требуется в развертываниях беспроводной сети. Как часть процесса планирования, различные критерии введены в программное средство планирования. Выполните следующие действия:

1. Задайте префикс AP и метод размещения точек доступа (автоматический по сравнению с руководством).
2. Выберите тип AP и задайте антенну и для полосы на 5 ГГц и для на 2.4 ГГц.
3. Выберите протокол (полоса) и минимальная желаемая пропускная способность на полосу, которая требуется для этого плана
4. Позвольте планировать режим опции усовершенствования для данных, голоса, местоположения. Данные и Голос предоставляют запасы прочности для справки дизайна. Запасы прочности помогают дизайну для определенных порогов RSSI, который подробно изложен в онлайновой справке. Местоположение с режимом отслеживания разлагает на множители в AP, который мог быть развернут для увеличения точности размещения. Местоположение, как правило, требует более плотных развертываний, чем данные и флажок location помогают плану относительно объявленной точности размещения.
5. Оба опции *Demand и Override* обеспечивают планирование любых особых случаев, где существует высокоплотное из клиентского присутствия такие конференц-залы или лекционные залы.Генерируемое предложение содержит их:Подробные данные плана этажаПравовая оговорка/Область/ПредположенияПредложенное размещение точек доступаПокрытие и скорость передачи данных HeatmapАнализ покрытия

Редактор карт

Интегрированный редактор карт в NCS составляет объекты и препятствия на полу. Модификация характеристик карты этажа приводит к более точной модели распространения RF, которая отображена в прогнозирующих картах тепла. Характеристики затухания для объектов и препятствий помогают прогнозирующему механизму отображать

более реалистическую прогнозирующую карту тепла. редактирует сделанный к карте этажа, помогает задавать области и области, такие как:

- Зона уверенного приема и Маркеры — используемый для уведомлений местоположения
- Периметр — определяет внешнюю границу
- Включение местоположения и Области Исключения — используемый для событий location и уведомлений

Объекты и препятствия, которые могут быть заданы:

- Стены (Свет и тяжелый) — 2dB и 13 дБ
- Кабина (Стены) — 1 дБ
- Двери (Свет и тяжелый) — 4 дБ и 15 дБ
- Стекло (двери, окна, стены) — 1.5 дБ

Import map от WCS до NCS

Экспорт/характеристика импорта карты доступен в WCS 7.0. Эта функция описана подробно в руководстве по конфигурации WCS 7.0.

После экспортирования карт от исходного сервера WCS этот набор карт может быть импортирован в целевой сервер NCS. Шаги для импорта карт покрыты Руководством по конфигурации NCS.

Примечание: Важно, чтобы AP в сервере WCS были сначала добавлены к серверу NCS до импорта карт, так как AP на картах WCS также включены во время процесса экспорта. AP, которые не были добавлены к вашему NCS, но присутствуют на экспортируемом результате карт этажа по ошибкам, отображаемым, когда вы импортируете те карты в NCS.

Используйте NCS для развертывания беспроводной локальной сети

Шаблоны конфигурации

Шаблоны конфигурации являются наборами конфигураций, которые могут быть применены к устройствам в уровне системы или глобальном уровне. Они могут быть снова использованы для изменения существующих конфигураций. Шаблоны могут также использоваться для репликации конфигурации в другие устройства, добавленные впоследствии. Шаблоны конфигурации могут использоваться для планирования изменений конфигурации в предопределенную дату и время. Возможности аудита в NCS могут также усилить шаблоны config для определения различий в config между NCS и существующей конфигурацией контроллера.

Группы конфигурации (группы config)

Группы config являются простым способом для группировки контроллеров логически. Эта функция предоставляет способ управлять контроллерами с подобными конфигурациями. Шаблоны могут быть извлечены от существующего контроллера до условия новые контроллеры или существующие контроллеры с параметрами дополнительной настройки.

Группы config могут также использоваться для планирования наборов конфигурации от того, чтобы быть настроенным. Перезагрузки контроллера могут также планироваться/располагаться каскадом в зависимости от эксплуатационных требований. Группами мобильности, DCA и контролем конфигурации контроллера можно также управлять с помощью групп config.

Группы config используются при собирании в группу узлов для более легкого управления (группы мобильности, DCA и параметры настройки управляющего домен) и для планирования удаленных изменений конфигурации. Узлы групп для обеспечения соответствия политикой конфигурации.

- При добавлении Контроллеров — Контроллеры в WCS представлены и могут быть отодвинуты к недавно группа config
- При применении Шаблонов — Обнаруженный или уже существующий шаблон (шаблоны) может тогда быть применен к контроллеру
- Контроль — Гарантирует, что основанный на шаблоне аудит выбран в контрольных параметрах настройки и затем контроллерах аудитов в группе, чтобы гарантировать, что они соответствуют политике

Используйте NCS для Мониторинга Беспроводной сети

RRM/CleanAir

Профили RF и Группы поддерживаются в версии 1.1 NCS и для шаблонов создания Профиля RF и для шаблонов группы точек доступа. При использовании NCS 1.1 для создания Профилей RF посредством создания шаблонов, это дает администратору простой путь, чтобы создать и последовательно применять шаблоны к группам контроллеров. Потоки процессов то же, как был ранее обсужден в наборе функций Контроллера с некоторыми незначительными, но важными различиями.

Процесс совпадает с ранее обсужденный в этом, вы сначала создаете Профили RF, затем применяете профили через группы точек доступа. Различия находятся в том, как это сделано от NCS и в использовании Шаблонов для развертывания по сети.

Создайте профиль RF с Cisco главный NCS 1.1

На Cisco Главные NCS там являются двумя способами, которыми можно приблизиться к построению или управлению Профилем RF. Выберите **Configure> Controllers> (IP-адрес контроллера)> 802.11> Профили RF** для доступа к профилям для отдельного контроллера.

Это отображается, все Профили RF в настоящее время представляют на выбранном контроллере и позволяют вам вносить изменения в присвоения группы точек доступа или Профили. Те же ограничения в отношении профиля, который в настоящее время применяется к группе точек доступа, в действительности как с Графическим интерфейсом контроллера. Необходимо отключить сеть или отменить присвоение профиля RF от группы точек доступа.

При создании нового профиля NCS побуждает вас выбирать существующий шаблон. Если это первоначально, к этому обращаются, вы направлены к диалогу Создания Шаблона для шаблона Контроллера 802.11.

Выберите **Configure> Controller Template Launch Pad> 802.11> Профили RF**, чтобы перейти к Панели запуска Шаблона Контроллера непосредственно.

В обоих случаях новый профиль RF создан на NCS с помощью шаблона. Это - предпочтительный способ, так как он позволяет администратору усиливать поток операций NCS и применять шаблоны и конфигурации ко всем или выбирать группы контроллеров и уменьшать ошибки конфигурации и несоответствия.

Выполните следующие действия:

1. Для создания Шаблона профиля RF выберите **новый**:
2. Конфигурация шаблона/параметров настройки почти идентична с добавлением имени шаблона. Сделайте это описательным для легкого распознавания в будущем. Измените настройки по мере необходимости или требуемый и выберите **Save**.**Примечание:** Если вы выбираете пороговое значение для TPCv2, и это не выбранный алгоритм TPC для группы RF, то это значение проигнорировано.**Примечание:** Простая установка для изменения для проверки является минимальным питанием TPC. Минимальное питание может быть повышено при выборе значения дБм, которое является больше, чем текущий уровень мощности, назначенный RRM. Это помогает проверять операцию Профилей RF.
3. Как только вы снижаете, Сохраняют опции, внизу экрана изменяютсяВыберите **Apply to Controllers**, и диалоговое окно controller, кажется, отображает список контроллеров, которыми управляет этот сервер NCS.
4. Выберите save config, чтобы высветить, выбрать контроллер, что вы хотите иметь профиль в наличии на и выбрать **Save.**
5. Теперь при просмотре экрана RF Profiles вы видите новый созданный шаблон.Предыдущие шаги могут быть повторены, чтобы создать и применить дополнительные шаблоны как требуется, например, для 802.11b.

Примените профили RF к группам точек доступа с NCS

Как с конфигурацией WLC для Профилей RF, недавно созданные профили могут быть применены к контроллеру с помощью групп точек доступа, на которые они назначены. Чтобы сделать это, или ранее сохраненный шаблон VLAN группы точек доступа или недавно созданный шаблон могут использоваться.

Выберите **Configure> Controller Template Launch Pad** и выберите **AP Group VLANs**.

Для создания нового шаблона выберите **New** и заполните необходимую информацию.

Выберите вкладку **RF Profiles** для добавления Профилей RF.

Если вы сохраняете шаблон, предупреждающее сообщение появляется.

Как сообщили в предыдущем сообщении, изменении интерфейса, что назначенное использование WLAN разрушает сопоставления VLAN для AP FlexConnect, примененных в этой группе. Гарантируйте, что интерфейс является тем же перед переходом.

Как только вы выбираете **OK**, диалог заменен опцией для **Применения к Контроллерам**. Выберите эту опцию.

Выберите контроллер (контроллеры), к которому должен быть применен шаблон.

NCS отвечает рабочим состоянием на том, был ли шаблон успешно применен к выбранному контроллеру (контроллерам).

Если шаблон не был выдвинут успешно, NCS предоставляет сообщение, которое сообщает причину для сбоя. В данном примере профиль RF, который применен к группе, не присутствует на одном из контроллеров, к которым был применен шаблон.

Примените Профиль RF снова, в частности к тому контроллеру и затем повторно примените группу точек доступа для генерации успешного сообщения.

Как только группа точек доступа была развернута с примененными Профилями RF (выберите кнопку **Apply to Access Points**), только точки доступа, подключенные к контроллерам, где группа точек доступа была развернута успешно, доступны для выбора от.

Примечание: До этой точки никакие реальные изменения не были внесены в Инфраструктуру RF, но это изменяется, когда AP перемещены в группу, которые содержат новые Профили RF. Когда AP перемещен в или из группы точек доступа, перезагрузки точки доступа для приведения в рабочее состояние новой конфигурации.

Выберите AP, чтобы добавить к группе точек доступа и выбрать **OK**. Предупреждающее сообщение появляется.

NCS отображает статус изменения.

Используйте NCS, чтобы повторно добиться проблем

- CleanAir
- клиентское устранение проблем
- инструмент аудита
- информационная панель безопасности
- SPT

Используйте NCS для оптимизации использования беспроводной сети

- отчёты
- производительность беспроводной сети (RRM)
- производительность (полоса пропускания глобальной сети (WAN))

Информационная панель

Компоненты информационной панели были улучшены в NCS 1.0. существует много усовершенствований к компонентам домашней страницы:

- проводная/беспроводная интеграция: компоненты теперь также отображают

соединенные проводом сведения о клиенте и данные коммутатора
- поток операций кастомизации компонента: что может быть настроено, как настроить
- отдельные компоненты могут быть обновлены. Скорость обновления может быть настроена индивидуально также.
- простота кастомизации и домашней страницы компонента: все редактирование завершено непосредственно на домашней странице (никакая потребность перейти к странице edit). Перетаскивание для добавления/перемещения компонентов
- интуитивный поток операций: гиперссылки компонента предоставляют простоту навигации, например, клиентского подлинного распределения к фильтруемой клиентской странице списка

Это кастомизации основного пользователя для Информационной панели:

- перетаскивание dashlet: компоненты могут быть перестроены на странице
- добавьте/удалите информационные панели: добавьте/удалите новые вкладки
- переупорядочение информационной панели
- переименование информационной панели
- редактирование плана: может задать количество столбцов для dashlets, добавив/удалив dashlets
- переименование dashlets
- множественные случаи dashlet: пользователь может добавить тот же dashlet и настроить содержание в каждом
- настраиваемый план информационной панели: количество столбцов на странице для компонентов

Кастомизация Dashlet:

- ручное обновление: позволяет пользователям обновлять отдельное dashlet содержание
- отредактируйте название dashlet
- измените размеры: минимизируйте (уменьшите до названия и строки состояния), восстановление (восстанавливает к исходному размеру), увеличьте (активный dashlet занимает область информационной панели),
- отсоединение: отсоедините/восстановите изображение dashlet содержание в новом окне
- близко: удаляет dashlet из Информационной панели. Может быть добавлен снова через экран “Add Dashlet”
- множественные параметры экрана: график или таблица
- визуальный индикатор, чтобы отобразиться, был ли настроен dashlet.

Одиночное представление проводных / беспроводных клиентов в dashlet

Существует одиннадцать dashlet компонентов, которые предоставляют сведения о проводном / беспроводных клиентах:

- Клиентское количество Ассоциацией/Аутентификацией
- Клиентское количество беспроводным/проводным
- Трафик клиента
- Клиентский сигнал тревоги и сводка событий
- Трафик клиента
- Клиентское устранение проблем
- Клиентский статус положения

- Подробный статус материально-технических ресурсов
- Время работы без сбоев устройства
- Лучшие 5 устройств загрузкой ЦПУ
- Лучшие 5 устройств загруженностью памяти

Соединенный проводом только dashlets

- Проводное клиентское распределение скорости
- Лучшие 5 коммутаторов клиентским количеством

Кастомизация диаграмм областей

Диаграммы в dashlets как Клиентское количество Беспроводным/Проводным и Клиентским количеством Ассоциацией / Аутентификация имеют диаграммы множественной области, которые зависят от выбора оперативной панели фильтра диаграмм, которая имеет All/Wireless/Wire" и Связывалась/Аутентифицировала соответственно как опции в панели фильтра. Замеченные диаграммы областей могут быть наложены (множественные области пересекают друг друга), или сложенный (множественные области вертикально сложены – один по другому). Индикацию относительно того, сложено ли это или наложено, показывают вместе с названием оси у. Причина для различных типов представлений (сложенный или наложенный) состоит в том, чтобы дать пользователю лучшую индикацию относительно показываемого набора данных.

Мониторинг клиентов и пользователей

NCS предоставляет способность контролировать и соединенный проводом и беспроводные клиенты (**Монитор> Клиенты и Пользователи**). Это предоставляет унифицированное представление всех клиентов в сети. Эти фильтры доступны.

Во время навигации к странице списка Клиентов и Пользователей Все Связанные Клиенты отображены по умолчанию. Существует 14 существующих фильтров, которые позволяют пользователю просматривать подмножество клиентов. Подробная информация предоставлена в таблице. Кроме того, существует опция для создания пользовательских фильтров:

- Быстрый фильтр
- Усовершенствованный фильтр

Клиентские фильтры списка	
Фильтр	**Результаты**
Все	Все клиенты включая неактивный
Клиенты на 2.4 ГГц	Все активные беспроводные клиенты, использующие радиодиапазон на 2.4 ГГц
Клиенты на 5 ГГц	Все активные беспроводные клиенты, использующие радиодиапазон на 5.0 ГГц
Все легковесные клиенты	Все клиенты соединились с легковесным AP
Все автономные клиенты	Все клиенты соединились с автономным AP

Все проводные клиенты	Все клиенты непосредственно соединились с коммутатором, которым управляет NCS
Связанные клиенты	Все клиенты соединились независимо от того, аутентифицируется ли это или нет
Клиенты обнаружены MSE	Все клиенты, обнаруженные MSE включая проводной и беспроводное
Клиенты обнаружены за прошлые 24 часа	Все клиенты обнаружены за прошлые 24 часа
Клиенты с проблемами	Клиенты, которые привязаны, но не завершили политику.
Исключенные клиенты	Все легковесные беспроводные клиенты, исключаемые контроллером
H-REAP, локально аутентифицируемый	Клиенты соединились с AP H-REAP и аутентифицировались локально
Новые Клиенты обнаружены за прошлые 24 часа	Все новые клиенты обнаружены за прошлые 24 часа
Выполнение клиентов	Клиенты, которые завершили всю политику набора и находятся в активном состоянии.
Клиенты WGB	Все клиенты WGB

Столбцы в Клиентской Таблице Списка могут быть настроены непосредственно на этой странице.

Столбцы в Клиентской Таблице Списка могут быть настроены непосредственно на странице списка **Клиентов и Пользователей**. Выберите или отменяйте столбцы, чтобы отобразить или сразу скрыть столбец.

Набор по умолчанию отображаемых столбцов и их заказа может быть перезагружен к значению по умолчанию через **Кнопку сброса**.

В столбцах переупорядочивания заказа о перетащите столбец непосредственно на странице и переместите его в желаемый заказ/местоположение.

Клиент и страница пользователя: подробные данные столбца	
Атрибут	**Комментарии**
IP-адрес	IP-адрес клиента
MAC-адрес	MAC-адрес клиента
Username	Имя пользователя на основе аутентификации 802.1x. Неизвестный

	отображен для клиента, связанного без имени пользователя
Введите	Значок представляет легкий вес, автономное или проводного клиента.
Поставщик	Поставщик устройства произошел из OUI
Название AP	Беспроводные сети только
Device Name	Имя устройства сетевой проверки подлинности, например, WLC, коммутатор.
Местоположение карты	Местоположение карты присоединенного устройства.
Положение	Последний клиентский статус положения
SSID	Беспроводные сети только
Имя профиля	Беспроводные сети только
Сети VLAN	Устройство VLAN работает
Статус	Статус текущего клиента
Interface	Интерфейс контроллера (радио) или интерфейс коммутатора (соединил того клиента проводом), подключение к.
Протокол	802.11 - радио 802.3 - соединенный проводом.
Скорость	Скорость порта Ethernet - соединенный проводом только. Показ, “Н/Д” для радио
Время ассоциации	Прошлое время начала ассоциации AP, радио только
Длина сеанса	Длина сеанса
Тип проверки подлинности	WPA, WPA2, 802.1x, и т.д.
Тип авторизации	Проводной тип авторизации от ISE
Трафик (МБ)	Трафик (передал/получил) на этом сеансе в МБ
Средняя пропускная способность сеанса (кбит/с)	Средняя пропускная способность сеанса в кбит/с
Автоматизированный тестовый прогон	Указывает, является ли клиент в автоматическом тестовом режиме
MAC-адрес AP	Беспроводные сети только

IP-адрес AP	Беспроводные сети только
Якорный контроллер	Легковесное радио только
РАБОТАЕТ	Клиент завершил всю политику набора.
CCX	Легковесное радио только
Название хоста клиента	Соединенный проводом и радио. Результат обратного просмотра DNS.
IP-адрес устройства	IP-адрес присоединенного устройства (WLC, коммутатор или AP AIO).
Порт	Порт коммутатора на WLC
E2E	Легковесное радио только.
Шифр шифрования	Беспроводные сети только
MSE	Сервер MSE, управляющий этим клиентом
RSSI	Беспроводные сети только
SNR	Беспроводные сети только
Идентификатор сеанса	Контрольный идентификатор сеанса, используемый в ISE и коммутаторе
Время сеанса	Время session start в течение времени Session start активного сеанса – открывает сеанс время окончания для неактивного сеанса
Название уличного торговца	Название уличного торговца произошло из OUI

Панель инструментов клиент/список пользователей предоставляет ряд программных средств, которые могут быть вызваны на выбранном (один или больше) клиенты.

Монитор> Клиенты и Пользователи: Поддерживаемые команды	
Команда	**Тип клиента**
Устранение неисправностей	Все
Тестовое меню	
Тестирование канала	Легковесное радио только
Радио-измерения	Легковесное радио только
Статистика V5	Легковесное радио CCX v5 только
Рабочие параметры	Легковесное радио CCX v5 только
Отключить	Легковесное радио только

Удалить	Легковесное радио только
Меню More	
Профили	Легкий вес (CCXv5)
Переместитесь причина	Легковесное радио только
Недавняя карта	Легковесное радио только
Существующая карта	Легковесное радио только
Сеансы	Все
Обнаружение AP	Легковесное радио только
История местоположения	Легковесное радио только
Включите зеркальный режим	Легковесное радио только
Речевые метрики	Легковесное радио только
Клиенты дорожки	Легковесное радио только
Определите неизвестных клиентов	Все

Пример действия: рабочие параметры

Кнопка с зависимой фиксацией к на левой стороне выбирает конкретного клиента для отображения клиентских подробных данных в этом клиентском списке.

легковесный беспроводной клиент

проводной клиент

В этом снимке экрана клиент в нижней части списка является легковесным беспроводным клиентом (Тип: Легковесное радио).

Пример для проводного клиента.

Проводное Устранение проблем / Устранение проблем Беспроводного клиента

В NCS 1.0, обоих соединенных проводом и беспроводных мониторингах и устранении проблем был интегрирован с идентификационными сервисами. Интеграция между проводным управлением / управлением беспроводной сети была достигнута через три сетевых элемента:

- Контроллеры WLAN Cisco (WLC)
- Характеристики безопасности коммутатора Cisco Catalyst: AAA, RADIUS, 802.1x и проверка подлинности MAC, trap-сообщения уведомления MAC (неидентификационные

клиенты), системный журнал (только идентификационные клиенты)
- Платформа Cisco Identity Services Engine (ISE)

Все клиенты – соединенный проводом и радио – отображены на странице Clients и Users (**Монитор> Клиенты и Пользователи**).

Проводные клиенты отображают **Название AP** как *Н/Д*. Информация о порте коммутатора предоставлена в **Интерфейсах**.

Беспроводной клиент, устраняющий неполадки

Для запуска Инструмента диагностики клиентов щелкните по кнопке с зависимой фиксацией налево от клиентского элемента списка. Как только клиент выбран, щелкните по значку **Устранения проблем** на панели инструментов.

Окно отображено для клиента.

Сообщения журнала могут быть получены из контроллера с использованием Регистрационного Инструмента анализа.

См. модуль контроля за соблюдением политик (PEM) для получения дополнительной информации о состоянии PEM.

Программное средство Истории события предоставляет пользователю сообщения о событии от клиента и AP.

Тестовый Инструмент анализа (клиенты CCXv5)

Проводное клиентское устранение проблем

NCS 1.0 предоставляет встроенное управление проводных и беспроводных устройств/клиентов. Одна из основных характеристик в NCS 1.0 контролирует и устраняет неполадки для проводного и беспроводных клиентов. SNMP используется, чтобы обнаружить клиентов и собрать данные клиента. ISE опрошен периодически для собирания клиентских статистических данных и других атрибутов для начальной загрузки отнесенных компонентов информационной панели и отчётов.

Если ISE добавлен к системам, и устройства аутентифицируются на нем, Клиентские Подробные отображения страницы дополнительные сведения, маркированные как Безопасность.

Для навигации к Клиентской Странице устранения проблем щелкните по значку **Устранения проблем** в меню программных средств в верхней части страницы.

Это берет пользователя к странице, показанной в снимке экрана. В данном примере устройство клиента имеет подключение ссылки, но подведенную проверку подлинности MAC.

На правой стороне экрана строка инструментов с этими элементами все отнесенные к устранению проблем:

- Инструмент диагностики клиентов
- Анализ журнала

- История события
- История с учетом контекста

История события предоставляет сообщения, отнесенные событиям подключения для этого клиента. В данном примере клиент был не в состоянии успешно аутентифицироваться. Дата/время предоставлена для помощи администратору сети в устранении проблем этого клиента.

ISE предоставляет опознавательные записи на NCS через API REST. Администратор сети может выбрать период времени для получения опознавательных записей от ISE. В данном примере опознавательная запись указывает, что пользователь не был найден в базе данных ISE.

Функции RF/Беспроводных сетей

Клиенты дорожки

Когда эти клиенты соединяются с сетью, эта функция позволяет администратору сети отслеживать определенных клиентов и уведомляться. Эта опция активирована от> Users Монитора и страницы Clients.

Для отслеживания одиночного клиента нажмите **кнопку Add**, и подокно появляется, где пользователь может ввести MAC-адрес клиента наряду с отслеживанием истечения (Никогда или заданная дата завершения).

Если пользователь хочет отследить несколька клиентов, клиентский список может быть импортирован. Получающееся окно позволяет пользователю списку импорта MAC - адресов клиента через файл csv.

Типовой файл csv может быть загружен, который предоставляет формат данных.

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

Настройки уведомлений

Существует три опции для уведомлений:

1. Очищенные Истекшие Записи — пользователь может заставить продолжительность поддерживать отслеженных клиентов в базе данных NCS. Клиенты могут быть очищены:после 1 неделипосле 2 недельпосле 1 месяцапосле 2 месяцевпосле 6 месяцевсохраненный неопределенно
2. Когда NCS передает уведомление о выслеженном клиенте, частота уведомления — пользователь может задать:на первом обнаруженииина каждом обнаружении
3. Метод уведомления — пользователь может задать для отслеженного события клиента, чтобы генерировать сигнал тревоги или послать электронное письмо.

Отображение выслеженных клиентов

После того, как отслеженные сведения о пользователе были введены, окно Tracked Clients позволяет пользователю просматривать статус существующих выслеженных клиентов.

ID неизвестного пользователя

Не все пользователи/устройства аутентифицируются через 802.1x (например, принтеры). В этом случае сеть администрирует, имеют опцию для присвоения названия к устройству.

Если устройство клиента аутентифицируется на сети через веб-аутентификацию, WCS может не иметь информации имени пользователя для того клиента. В этом сценарии клиенты могут хотеть сопоставить имена пользователей с клиентами, даже если они используют веб-аутентификацию.

1. Выберите **Monitor> Clients**.И радио и соединенные проводом клиенты отображены. Как ранее описано, панель инструментов расположена в предыдущем списке клиентов, который позволяет пользователю вызывать много действий:устранение неполадоктест (тестирование канала, радио-измерение, статистика CCXv5, параметры операции)отключитьудалите (разъедините беспроводного клиента),
2. Нажмите **Определить** значок **Неизвестных пользователей** на панели инструментов.Это заканчивается со всплывающим окном.
3. **Нажмите Add** для ввода клиентских подробных данных.Отдельный MAC-адрес и соответствующее имя пользователя могут быть добавлены.Однажды клиент и MAC-адрес был добавлен, WCS использует эту таблицу для клиентского поиска на основе соответствующего MAC-адреса.

Карты тепла в реальном времени

Одна из новых характеристик в NCS 1.0, опция для отображения карт тепла в реальном времени. Это значение используется по умолчанию. Выберите **Monitor> Maps> Properties** для навигации к параметрам настройки.

Мониторинг коммутаторов Cisco Catalyst Использование NCS

Проводная информация о материально-технических ресурсах определена этими методами:

- Проводное клиентское обнаружение через trap-сообщения SNMP, Последовательный опрос SNMP и сообщения системного журнала от коммутаторов
- ISE движущийся на север API для дополнительных сведений, таких как положение, профилировщик, учет, и т.д

NCS предоставляет характеристике проверки четности WCS 7.x для клиента, отслеживающего и сообщающего на всех клиентах (соединенный проводом и радио). Кроме того, NCS перекрестный запускает устранение проблем ISE для проводных клиентов. Дальнейший уровень интеграции ISE через перекрестный запуск отчётов о ISE с данными, не содержавшимися в WCS.

Эти данные коммутатора предоставлены в NCS:

- Физические Активы, например, шасси, модули, порт и источник питания от MIB Объекта
- Флэш - устройство/Partition/Files
- Установленный образ программного обеспечения
- Интерфейс Ethernet

- IP - интерфейс
- Интерфейс виртуальной локальной сети (VLAN)
- VLAN и VTP
- EtherChannel
- STP
- StackWise (поддерживаемый только на коммутаторах Cisco Catalyst 3750)

Монитор> Коммутатор отображает эти данные коммутатора:

- IP-адрес
- Device Name: имя хоста, как дали в конфигурации IOS коммутатора
- Тип устройства: модель коммутатора
- Достижимость: Подключение SNMP
- Клиентское количество: количество клиентов непосредственно соединилось с коммутатором

Отображенный IP-адрес является гиперссылкой, и щелчок по нему берет пользователя для **Настройки> Коммутатор Ethernet> (IP-адрес)>** экран **Summary**.

Проводные клиенты обнаружены через trap-сообщения SNMP, Последовательный опрос SNMP и сообщения системного журнала от коммутаторов.

С NCS коммутаторы Cisco Catalyst могут быть проверены для этой информации:

- Шасси: UDI, имя модели, время работы без сбоев
- MEMORY/CPU UTILIZATION
- Статус портов/интерфейсов
- Уровень 2 (VLAN, VTP, связующее дерево)
- Среда: статус источников питания и вентиляторов
- Память и файлы в системе
- Клиенты (соединены проводом)

Связующее дерево

Подробная информация связующего дерева для каждого экземпляра связующего дерева предоставлена:

- Порт STP
- Роль порта
- Приоритет порта
- Стоимость пути
- Состояние порта
- Тип порта

StackWise Cisco

Для коммутаторов Cisco Catalyst, которые поддерживают технологию StackWise, каждая роль коммутаторов в стеке предоставлена включая его роль в стеке, приоритете коммутатора, состоянии и версии программного обеспечения.

Интерфейсные подробные данные

Сведения о статусе на всех Интерфейсах Ethernet отображены.

Информация сетевого уровня 3 также предоставлена (VLAN сопоставлению IP-подсети).

ИНФОРМАЦИЯ VLAN

Подробные данные VLAN также доступны от NCS. И системный параметр по умолчанию и настраиваемые VLAN отображены. ИДЕНТИФИКАТОР VLAN, название и тип отображены на одиночном экране.

Клиентские страницы списка

Отчёты (Перекрестный запуск и масштаб)

NCS 1.0 предоставляет встроенное управление проводных и беспроводных устройств/клиентов. SNMP используется для сбора данных клиента. ISE опрошен периодически для собирания клиентских статистических данных и других атрибутов для начальной загрузки отнесенных отчётов.

Выберите **Reports> Reports Launch Pad**. Выберите отчёт для создания/кастомизации.

Новые отчёты

Возглавьте соединения N

Это сообщает, показывает вершину N пользователи в установленный срок времени на основе этих метрик:

- Попытки подключения
- Переданные попытки
- Неудачные попытки

Этот отчет содержит эти столбцы:

- Username
- Количество общих попыток подключения
- Количество переданных попыток подключения
- Количество попыток сбоя подключения

Ассоциация AP

Это списки отчета вся ассоциация AP детализирует для беспроводных клиентов и подобна отчётам о Сеансе клиента.

Количество статуса положения

Этот отчёт предоставляет диаграмму тенденции для показа клиентского статуса положения в течение долгого времени. Диаграмма является диаграммой областей; нижней областью является количество клиентов, передал проверку положения, и верхняя область является

количеством клиентов, которые отказали проверку положения.

Сигналы тревоги/События

Сигналы тревоги и события предоставляют одиночный просмотр сигналов тревоги и событий для проводного и беспроводного. Сводка постоянного аварийного сигнала и браузер отображены в нижнем правом угле экрана независимо от того, какой экран пользователь идет. NCS 1.0 предоставляет сигнальные представления общего назначения включая эти страницы:

- Страницы списка аварийных сигналов
- Сигнальные подробные страницы
- Страницы Списка событий
- Подробные страницы события
- Сигнальный поиск по категориям и sub категория
- Окно сводки аварийных сигналов
- Сигнальная информационная панель
- Аварийные действия (подтверждают, очищают, назначают, отменяют присвоение, удаляют, и т.д.),
- Аварийное оповещение (Электронная почта, trap-сообщение)
- Навигация страницы аварийных сигналов (от и до различных взглядов)
- Панель краткого обзора аварийных сигналов - развертка к фильтруемому списку
- Запустите существующую страницу устранения проблем WCS из страницы аварийных сигналов

Столбцы могут быть настроены такой, как отображено, скрыты и переупорядочены. Меры могут быть приняты на одном или более сигналах тревоги одновременно.

Быстрый фильтр

Эта функция позволяет пользователю фильтровать на одном или более столбцах на основе текстовой строки, введенной в фильтр, поданный наверху каждого столбца. Это предоставляет дополнительное фильтруемое представление сигналов тревоги для проводных и беспроводных сигналов тревоги.

Страница аварийных сигналов – быстрый фильтр

Усовершенствованный фильтр

Усовершенствованный фильтр предоставляет еще большую возможность поиска. Это предоставляет способность искать на определенных полях с различными условиями, теми, которые содержат, не содержат, запускаются с и заканчиваются. Эта схема показывает различные параметры фильтрации. Кроме того, Усовершенствованный Фильтр позволяет вложению условия и булевской переменной (AND/OR) условия быть заданным.

Страница аварийных сигналов – усовершенствованный фильтр

Точно так же События могут быть отображены и фильтр на легко. Это также задало, быстрые и усовершенствованные фильтры. Эти фильтры работают почти таким же способом как они, то же просачивается Сигналы тревоги.

Страница событий Страница события - быстрый фильтр Страница события -

усовершенствованный фильтр

Проверка подлинности пользователя AAA через TACACS +/RADIUS использование ACS 4.2

Для TACACS + пользователи для аутентификации успешно в NCS несколько изменений требуются в ACS 4.2. Новый Сервисный HTTP NCS должен быть добавлен на странице Interface Configuration для TACACS + (Cisco IOS).

Весь набор TACACS Листа задач Группы пользователей NCS + Настраиваемые атрибуты должен быть скопирован в области для текста Настраиваемых атрибутов HTTP NCS как показано в снимке экрана для пользователя AAA. То же в силе для Группы пользователей.

Для Аутентификации Пользователя RADIUS необходимо скопировать новый лист задач Группы пользователей NCS настраиваемые атрибуты Радиуса в Cisco IOS / PIX 6.x раздел атрибутов RADIUS для Пользователя/Группы пользователей.

От NCS добавьте новый TACACS +/Radius серверная запись в **администрировании> AAA> TACACS + Серверы / Радиус**. Установите режим AAA в **администрировании> AAA> Параметры настройки режима AAA** к **TACACS + / Радиус** соответственно. Перевход в систему как пользователь AAA.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация