Smart-industrial был самым сложным IoT-моделированием, созданным для курса IoT. Сложность этого случая была в основном из-за расположения сети, а также из-за логических связей между устройствами IoT.

Упражнения имитировали промышленное применение, когда электричество вырабатывалось с помощью солнечной панели и ветряных турбин, временно хранилось в батареях, а затем использовалось на промышленной производственной линии, состоящей из приводов и компонентов. Такое же электричество использовалось и для таких вспомогательных устройств, как охлаждающие устройства и фонари.

 

 Рисунок 51 - Схема Cisco Packet Tracer для интеллектуального промышленного моделирования

Расположение сети

Компоновка сети была более сложной по сравнению с ранее проанализированными примерами, физическое разделение сетей, достигнутое путем создания отдельных физических контейнеров, требовалось из-за логики упражнения.

Топология сети была разделена на пять основных подсетей: две, где были подключены устройства IoT, производящие и накапливающие электроэнергию, одна для корпоративного офисного здания, одна, где были расположены устройства IoT, использующие электроэнергию, и последняя для общего контроля IoT. Все эти сети были связаны между собой центральным маршрутизатором, расположенным в сети управления IoT. Эта не избыточная компоновка может не подходить для реальных промышленных приложений, однако она помогла упростить работу Cisco Packet Tracer.



Рисунок 52 - Топология Smart-Industrial Network

Самой простой сетью было корпоративное офисное здание ЛВС. Сеть состояла в основном

маршрутизатор подключен к центральному маршрутизатору и локальному офисному коммутатору. ПК и офисный DHCP-сервер также были подключены к локальному коммутатору.

В силу конструкции сети ни один из офисных компьютеров не смог получить доступ к домашней странице IoT или любому другому устройств IoT. Фактически целью было изолировать и ограничить доступ к управляющему устройству IoT только для авторизованного пользователя, физически подключенного к сети управления IoT.

Море и Земля были двумя сетями, в которых были подключены устройства IoT, производящие электричество, обе эти ЛВС были подключены к центральному центральному маршрутизатору.

Земля была сетью на основе коммутатора, используемой для моделирования функционирования фермы солнечных батарей, где электричество производилось и хранилось в интеллектуальных батареях IoT.

Чтобы упростить конструкцию, для подключения устройств IoT к коммутатору использовались только прямые медные кабели. В реальных условиях предпочтительнее использовать оптическую или беспроводную технологию для преодоления предела расстояния связи, обусловленного медными кабелями. В той же сети был установлен DHCP-сервер для распределения локальных IP-адресов по устройству, подключенному к наземной сети.

Сеть моря была концептуально похожа на сухопутную сеть, на самом деле, также в этом случае,

Ветровые турбины IoT производили электричество, а затем хранили их в батареях. Как и в предыдущей сети, также использовался традиционный коммутатор, подключенный к главному базовому маршрутизатору, однако основное подключение к ветровым турбинам IoT обеспечивалось 3G.

Сотовая сеть 3G использовалась для дифференциации настройки, давая возможность студентам ознакомиться с различными типами сетей, но также для того, чтобы придать более реалистичный вид сети над морем.

Как объяснялось в предыдущем примере SaaS Smart-Home 2, из-за сети 3G необходимо установить дополнительное оборудование. Антенна была необходима, чтобы обеспечить через предопределенную APN возможность подключения к турбинам. Серверный компонент центрального офиса также был необходим для консолидации сигнала от вышек сотовой связи, поступающих через коаксиальный кабель, в Ethernet. Сервер центрального офиса был затем подключен к коммутатору наземной сети. Как и в предыдущей настройке, также в морской сети был установлен DHCP-сервер для распространения IP-адресов на устройства IoT.

Четвертой и менее сложной сетью была IoT industrialWLAN. Это простая сеть

обеспечивает беспроводное подключение к устройствам IoT, которые потребляют энергию от батарей IoT, расположенных в морской и наземной сети. Беспроводной сигнал был создан локальным маршрутизатором WLAN, подключенным к центральному центральному маршрутизатору.

Последней, но самой важной сетью была сеть управления IoT.

Цель сетей состояла в том, чтобы быть главной точкой соединения между другими WLAN и

LAN, но также концептуально работать в качестве основного пункта управления для устройств IoT.

Все устройства IoT фактически были подключены к серверу IoT, расположенному в локальной сети управления IoT. Сердцем этой сетки было ядро ​​роутеров. Поскольку устройство являлось центральной точкой подключения, для подключения всех других подсетей требовались дополнительные карты NIC.

Протокол маршрутизации RIP также сыграл ключевую роль в симуляции, позволив удаленным устройствам IoT подключиться к серверу IoT. Как было объяснено ранее, RIP является очень старым, но простым протоколом маршрутизации, который из-за своей простоты настройки был выбран для использования в автоматизации IoT.

Кроме того, IoTserver также подключался к маршрутизатору WLAN, обеспечивая подключение WLAN к ПК диспетчерской и двум интеллектуальным устройствам, которые имитировали систему обнаружения вторжений.

План IoT

Настройка IoT была аналогична всем остальным трем случаям, даже если устройства фактически были подключены к разным локальным сетям, все они были логически связаны с сервером IoT, размещенным в локальной сети комнаты управления.

Как и прежде, все устройства IoT имели одни и те же имя пользователя и пароль. Из-за структуры сети в этом упражнении Cisco Packet Tracer только компьютеры, подключенные к локальной сети комнаты управления, могли получить доступ к домашней странице IoT.



 Рисунок 53. Домашняя страница подключенного устройства IoT

Как показано на рисунке 53, в «умных» промышленных учениях уже было настроено несколько устройств IoT, таких как: солнечная панель, ветряные турбины, батареи, детектор движения, веб-камера, блок переменного тока, датчик температуры и интеллектуальный источник света IoT.

Для солнечных панелей, ветряных турбин и аккумуляторов, расположенных в наземной и морской сети, не требуется никакой внутренней информации, так как для подключения генераторов энергии к аккумуляторам требуется только кабель IoT.

Четкие инструкции по подключению слотов ввода и вывода устройства IoT были перечислены в вкладка спецификации устройства. Как видно на рисунке 54, выходной порт солнечной панели - D0, а вход батареи - D0, кабель был подключен соответствующим образом.



Как показано на рисунке 56 ниже, при наблюдении за часами окружающей среды было очень очевидно увидеть пиковое время производства солнечной электроэнергии.

 

 Рисунок 56 - Пик производства электроэнергии в дневное время

Было также отмечено, что даже при отсутствии какого-либо устройства, подключенного к батарее, потребляющей заряд, по умолчанию происходит постоянный разряд батареи.

Как упоминалось ранее, сервер IoT размещался в сети управления IoT.

Сервер, как и в других моделях IoT, использованные статические IP-адреса также выполнял роль DNS-сервера, переводя адрес iotcontrolpage.com в свой собственный IP-адрес.

Наряду с сервером к контрольной сети IoT был также подключен пример решения для наблюдения за IoT. В этом случае имитировалась система безопасности, работающая в диспетчерской электростанции, которая при обнаружении движения автоматически запускала трансляцию с веб-камеры на несколько секунд.

Эта автоматизация IoT может быть вызвана нажатием ALT на клавиатуре и наведением курсора мыши на детектор движения. При подключении к iotcontrolpage.com через браузер также можно было увидеть изменение значка веб-камеры, отображающего рамку некоторых изображений. Как только никакие движения не были обнаружены, веб-камера автоматически остановилась.



 Рисунок 57 - Пример трансляции с веб-камеры при срабатывании детектора движения

Другие образцы моделирования IoT были для устройств, подключенных к промышленной сети IoT, таких как: интеллектуальная лампа и автоматический блок переменного тока с термометром, двигателем и потенциометром.

Как было объяснено ранее, интеллектуальная лампа не требовала никакого интеллектуального бэкэнда, поскольку сама по себе являлась очень интеллектуальным устройством, фактически в устройство были встроены датчик движения и света, что позволяло самой лампе принимать решение о закрытии крышки в случае обнаружения объекта или, если уже поздно, и солнечного света не видно. Лампа была включена в пример Cisco Packet Tracer для того, чтобы показать также возможность подключения устройств к батарее IoT, чтобы потреблять энергию. Как показано на рисунке 58 ниже, специальный кабель IoT использовался для соединения двух устройств, спецификации порта были доступны на вкладке спецификации устройства.

 Пример IoT микроконтроллера

Как и во всех трех других упражнениях Cisco Packet Tracer, также в случае Smart-industrial был приведен пример устройств, не подключенных к IoT, с использованием микроконтроллера.

Как показано на рисунке 61, случай воспроизвел аналогичный сценарий IoT, размещенный в наземная сеть, где солнечная панель вырабатывает электричество, а батарея хранит энергию. Разница была в том, что устройства были напрямую подключены к блоку SBC, который передавал данные на плату.

 Рисунок 61 - Пример настройки микроконтроллера

С помощью пользовательской программы Blockly SBC постоянно считывает данные, поступающие с панели и от батареи, на двух отдельных ЖК-экранах выдает небольшой текст о состоянии произведенной и сохраненной энергии. В случае, если оба значения были низкими, светодиод аварийной сигнализации был закрыт, наряду с выводом на ЖК-дисплей сообщения о низком заряде батареи и низком уровне заряда панели, как показано на выше рисунок 61.

Полную логику программы Blockly можно найти в Приложении 1.

 