ПОИСК НЕИСПРАВНОСТЕЙ в сетях Wi-Fi

И.Ильина-Сидорова, инженер центра технической поддержки Cisco / iilyinas@cisco.com

DOI: 10.22184/2070-8963.2018.75.6.40.51

Поиск неисправностей в беспроводных сетях – задача, достаточно сильно отличающаяся от аналогичной в традиционных проводных сетях.

Классификация проблем

В сравнении с проводными сетями беспроводные характеризуются другим способом доступа к среде и физически иной передачей сигнала, что накладывает свой отпечаток на процесс поиска неисправностей. Помимо этого, беспроводная природа подключения привносит неопределенность в положение клиента в пространстве.

Достаточно удобно проводить процесс поиска неисправностей, относя возникшую проблему к одному из заранее определенных классов, со своими шагами проверок, которые позволят ее сузить и понять. Для сетей WLAN (Wi-Fi) целесообразно выделить следующие классы проблем:

- физическая (аппаратная) неисправность;
- дефект прошивки или устранимый производственный дефект (брак);
- проблемы настройки;
- программный дефект;
- неверно выбранный дизайн решения.

Следует отметить, что в процессе решения может выясниться, что класс проблемы был изначально определен неверно. В идеальной ситуации это не должно приводить к большим задержкам при поиске решения, однако в реальной ситуации, конечно, может замедлить восстановление нормальной работы сети.

Для выбора класса проблемы можно воспользоваться следующей схемой последовательности вопросов:

- **Что?** (Какое именно устройство; одно, несколько или все имеющиеся);
- **Где?** (В какой части офиса/здания/производственной зоны проблема наблюдается, а в какой части – нет);
- **Когда?** (Когда проблема начала проявляться; предшествовала ли ей нормальная работа сети; когда проблема точно не проявлялась);
- **Что еще?** (Вносились ли какие-либо изменения в сеть, расположение точек доступа; проводились ли в здании ремонтные работы или инсталляции чего-либо; переезжали ли отделы; появлялись ли в близлежащих помещениях новые арендаторы и т.д).

Для более полной информации о схемах начальных опросов следует обратиться к специальной литературе (см., например, методы Кепнера-Трего и "Пяти почему" (5Why)). Если проблема проявляется лишь на одном устройстве при наличии нескольких подобных, имеет смысл предполагать **физическую неисправность** устройства. В случае если подобие неполно, допустим, при существенном различии в инсталляции (например, одна из точек доступа висит на стене напротив лифтов, а другая – в фальш-потолке офисной зоны), предпочтительно поменять местами заведомо рабочее и потенциально сбойное устройства для проверки: не связана ли неисправность с физическим положением устройства. Понятно, что при этом необходимо по той же схеме провести замену всех соединительных кабелей.

Если проблема проявляется только на определенном типе оборудования (на всех устройствах определенного типа), то физическая неисправность

конкретного устройства маловероятна. Однако в случае неверной инсталляции это возможно, например, при нарушении герметичности корпуса у точек доступа, предназначенных для инсталляции вне помещений. В этом случае необходимо проверить, существуют ли отличия в применении потенциально сбойной модели для проверки гипотезы о **неверно выбранном дизайне** решения. Если таких отличий нет, или если дизайн проверен и соответствует возможностям оборудования (согласно документации производителя, возможности оборудования позволяют использовать его в данной схеме и настройка оборудования также выполнена согласно документации), можно предполагать **программный дефект** или **дефект прошивки**. Очевидно, что в процессе проверки дизайна возможно обнаружение **ошибок конфигурации** и их исправление. При новой инсталляции для конечного пользователя, как правило, достаточно трудно провести грань между программным дефектом и сбоем прошивки/производственным браком. Однако это не критично. В таком случае необходимо работать с поставщиком оборудования для решения проблемы. При новых инсталляциях определенную проблему представляет отсутствие данных о заведомо рабочем режиме сети. Это неудобство можно нивелировать, используя пилотные сети, а также с помощью поставщика решений, который может предоставить дополнительную информацию о тестовых инсталляциях. В случае если сеть в прошлом работала успешно, мы можем исключить вероятность производственных дефектов полностью (при условии, что задействованный функционал не менялся) и полностью сосредоточиться на локализации **программного дефекта**. При этом следует отметить, что проблемы при производстве встречаются настолько реже проблем с программным обеспечением, что их вероятностью можно в целом пренебречь. В случае проблем со всеми устройствами имеет смысл предположить, что в описании проблемы упущена какая-либо важная деталь, позволяющая сузить описание, либо что проблема **не лежит в области беспроводных сетей** (например, сбой в проводной сети может привести к потере соединения между контроллером и всеми точками доступа, при этом и контроллер, и точки доступа будут функционировать). Очевидно, что не во всех сетях возможно провести такой анализ, однако чем полнее он будет проведен, тем более будет упрощен процесс устранения неисправности.

Можно резюмировать, что в общем случае, когда рассматривается несколько устройств с достаточно схожими характеристиками, алгоритм проверки идет от физической неисправности к проверке настроек и дизайна в целом, и далее к программной неисправности (и возможному производственному браку).

Алгоритм проверки

Физическая неисправность – это далеко не всегда заметный глазу дефект. Помимо очевидных случаев (допустим, точку доступа уронили при монтаже и ее корпус разбит), возможен выход из строя электронных компонентов. Иногда такое устройство продолжает частично функционировать, что еще больше затрудняет анализ.

Если устройство выглядит совершенно вышедшим из строя и не включается, имеет смысл заменить источник питания (кабель, порт на коммутаторе, розетку) на гарантированно рабочую (не на свободную/резервную). Возможно переключить устройство, которое работало на этом источнике на потенциально сбойный источник, однако это следует делать с осторожностью, так как неисправность может привноситься источником питания (поэтому имеет смысл делать так только в случае, когда потенциально сбойное устройство нормально включается с проверенным рабочим источником питания). Это позволит локализовать проблему – и, возможно, избежать дорогостоящей замены.

Следует отметить, что иногда физическую замену устройства выполняют до прохода всех стадий поиска неисправности – как один из этапов исследования проблемы. Этот подход обоснован в случае критичного простоя, поскольку в идеальном случае приводит к наиболее быстрому восстановлению работоспособности системы. К сожалению, такой вариант решения существенно снижает возможность понять, что вызвало проблему и предотвратить появление аналогичных проблем в будущем.

К возможным осложнениям при замене необходимо отнести отсутствие устройства (особенно дорогостоящего) в ЗИПе, срыв сроков замены и отсутствие рабочей конфигурации устройства. Все эти осложнения устраняются лишь превентивно, соблюдением политик по сохранению конфигураций устройств, а также использованием в сети оборудования сетевого управления (с возможностью хранения конфигураций различных версий и т.д.).

Дефект прошивки (или производственный брак, который возможно исправить перепрошивкой устройства) можно выделить в отдельный класс проблем именно потому, что, будучи близким по характеристикам к физической неисправности, такой дефект все же зачастую исправим. То есть если дефект уже известен, возможно его превентивное исправление, и замена оборудования не требуется. Это позволяет сэкономить ресурсы на замене. В случае если дефект

трудноустраним (например, необходим консольный доступ в течение достаточно длительного времени, а устройство смонтировано на мачте), возможна аппаратная замена на другое устройство с исправленной прошивкой и проведение работ по устранению неисправности отдельно. Для минимизации проявления таких дефектов необходимо периодически проверять веб-сайт производителей оборудования на наличие новостей о таких производственных дефектах и поддерживать связь с поставщиками оборудования.

Проблемы настройки оборудования – наиболее частая причина сбоев. Здесь основной тактикой должен являться анализ внесенных изменений. К сожалению, зачастую технический персонал не придает должного значения документированию всех проводимых действий или даже пытается скрыть действия, которые могли повлечь за собой возникновение неисправности. Политика хранения версий конфигураций и учет внесения изменений помогут получить исчерпывающую информацию в случае необходимости. Большую услугу здесь может оказать тестовая сеть, где различные варианты конфигурации можно промоделировать – и, таким образом, локализовать проблемный сценарий. Далее можно обратиться к документации на оборудование (или к представителю производителя или к поставщику, если документация отсутствует или неполна), чтобы выяснить, какие изменения нужно внести для исправления проблемы. Это необходимо также для более точного описания проблемы производителю оборудования в случае, если проблема окажется связана с программной ошибкой, и для поиска временного решения. Если моделирование проблемы в тестовой сети невозможно, следует максимально упростить сценарий с целью сделать его рабочим, а далее усложнять его, постепенно доводя до того, который используется в реальной сети, отслеживая, в какой именно момент проблема возникнет снова. Например, в случае проблем с доступом пользователей к беспроводной сети при наличии портала с авторизацией по open id можно предложить:

- сначала создать еще одну, открытую сеть, используя ту же точку доступа;
- если подключение клиента, у которого отмечались проблемы, проходит нормально – настроить аутентификацию с порталом, но используя статические credentials;
- если подключение проходит теперь нормально, настроить аутентификацию по open id;
- если по достижении идентичной конфигурации проблема не воспроизводится (а старое решение по-прежнему не работает), можно использовать новую сеть для временного доступа (workaround) и одновременно продолжать анализ старой конфигурации для поиска ошибок.

Интересным вопросом для проблем, связанных с настройкой оборудования, являются новые сети. В них невозможно провести сравнение с заведомо хорошей конфигурацией. В этом случае нам для сравнения необходима пилотная сеть или хотя бы подробная документация на оборудование (configuration guides, blueprints). В новых сетях мы совершенно не можем исключить вероятность неверного дизайна, и всегда есть вероятность того, что оборудование не сможет работать желательным образом (хотя она, безусловно, невелика в случае построения сети грамотными специалистами). При подозрении проблемы с конфигурацией устройства мы, по сути, вновь проходим тот же цикл вопросов, что и при определении типа проблемы, однако на другом уровне. Мы стараемся локализовать место возникновения проблемы (устройство), а затем собрать диагностическую информацию, которая подтвердит/опровергнет наши выводы.

В случае подозреваемых проблем:

- на стороне клиента – собираем логи клиента и трафик беспроводного соединения, а также в случае наличия контроллера – дебаг-выводы, отражающие состояния клиента (например, для оборудования компании Cisco, debug client <mac-address>), собираем информацию о месте подключения (документацию по обследованию сети, wireless survey);
- на стороне точки доступа – собираем логи точки доступа (если есть) и контроллера (если он присутствует в сети), трафик беспроводного соединения, трафик между точкой доступа и контроллером (если мы используем схему lightweight APs);
- на стороне контроллера – собираем логи контроллера (для контроллеров Cisco начинаем с show msglog, show traplog и show run-config);
- на стороне оборудования мониторинга – собираем логи мониторинговой системы, контроллера, трафик между контроллером и системой мониторинга;
- на стороне аутентифицирующего сервера – собираем логи на сервере аутентификации, на контроллере и, возможно, трафик между ними;
- на стороне сети – собираем сетевой трафик между "нашими" устройствами и анализируем его на предмет возможных сбросов.

Как видно, набор данных, на основании которых мы делаем анализ, частично перекрывается. Это позволяет не тратить лишние ресурсы на разбор заведомо невероятных гипотез и быстрее получать необходимый набор данных для анализа. **Проблемы, связанные с программным дефектом** – наиболее часто рапортуются в службы технической поддержки,

однако зачастую оказываются проблемами другого рода. В случае обнаружения в логах exceptions, kernel panics и прочих подобных сообщений с высоким уровнем важности (severity), мы можем с высокой вероятностью предполагать наличие программного дефекта. В таком случае необходимо проверить, присутствует ли этот дефект в числе известных производителю (в случае Cisco – используя bug toolkit на сайте) и в какой версии программного обеспечения этот дефект исправлен. В случае же неожиданных результатов работы программного обеспечения или зависания устройств рекомендуется вначале проверить другие возможные причины возникновения проблемы. Для сетевого инженера невозможно полностью исправить данную проблему самостоятельно, однако зачастую возможно найти обходной путь, который существенно снизит влияние проблемы на сеть (workaround). Для этого при обнаружении программного дефекта необходимо попытаться понять, какая подсистема оборудования подвержена дефекту, а затем попробовать задействовать аналогичный функционал, не используя ее. Например, при обнаружении бага в режиме FlexConnect можно попробовать перевести точку доступа в режим Local. Этот режим, конечно, создаст дополнительную нагрузку на канал связи между точкой доступа и контроллером, а также на контроллер, однако эта дополнительная нагрузка может оказаться допустимой на время, необходимое производителю для исправления дефекта и предоставления нового ПО. Именно поэтому в случае если проблема неизвестна производителю, имеет смысл смоделировать проблему у себя и стараться максимально участвовать в процессе ее решения. Безусловно, это может оказаться невозможным в случае ограниченных ресурсов или повышенной критичности рабочей сети.

Неверный дизайн – это самая болезненная ошибка, которую допускают инженеры при построении сетей. В случае беспроводных сетей к вопросам capacity (емкость), bandwidth (ширина канала), необходимого функционала добавляются ограничения, накладываемые "материальным" миром (размещение точек доступа и их питание, требования по качеству покрытия), которые меняются в зависимости от желаемого функционала сети, возможной интерференции с другими устройствами заказчика... К счастью, эти проблемы зачастую выявляются и устраняются при пилотных запусках. Для предотвращения проникновения ошибок такого рода в production необходимо тщательное проведение нагрузочных испытаний. Тестированию должен подлежать не только сам факт подключения или использования желаемого функционала, но и качество предоставляемого сервиса, а также возможность работы в случае полной нагрузки некоторого участка сети и поведение сети в случае перегрузки. В общем случае можно предполагать наличие неверного дизайна, если описание проблемы включает в себя упоминание о неработающем изначально функционале или существенном ухудшении сервиса при введении сети в эксплуатацию. В такой ситуации в качестве решения может выступать как полное, так и частичное изменение сети, что зачастую невозможно осуществить в короткие сроки. Поэтому, как это ни грустно, иногда в качестве временного решения приходится ограничивать функционал сети (например, вместо использования всеми сотрудниками только беспроводного подключения переводить стационарные станции на "обычное" проводное подключение).

Тестовый сценарий

Предположим, что некая компания имеет развернутую в своем офисе беспроводную сеть. Офис расположен в отдельно стоящем малоэтажном здании, на территории бизнес-парка, в окружении подобных построек. На первом этаже здания находится зона приема посетителей, санузлы, хозяйственные помещения, а также небольшое кафе и зона отдыха. Также имеются рабочие помещения и комнаты для переговоров. На более высоких этажах располагаются исключительно рабочие места и санузлы. В здании имеется лифт. Перед вводом в эксплуатацию (до ввоза мебели) было проведено радиообследование, его результаты доступны для анализа. К сожалению, представлены только суммарные результаты по общему покрытию (одновременно и для 5 ГГц, и для 2,4 ГГц). Согласно данным радиообследования, сила сигнала (RSSI) колеблется между –60 и –40, а уровень шума (noise floor) не поднимается выше –75 (в основном колеблется около –90).

Для целей обеспечения беспроводного доступа были сконфигурированы две беспроводные сети – корпоративного пользования и гостевая. Для гостевой сети функционирует портал, данные для подключения к которому гостевые пользователи получают у секретаря (для каждого пользователя генерируется уникальная учетная запись). В корпоративной сети подключение происходит с проверкой машинного сертификата, а также учетной записи пользователя.

Наблюдаются следующие проблемы:

- иногда (с момента запуска сети в эксплуатацию) гостевые пользователи не могут подключиться к сети (чаще всего это происходит во второй половине дня и в пятницу);

Рис.1. Скриншот с подробной информацией о клиенте, испытывающем проблемы с подключением

- некоторые гостевые пользователи не могут подключиться, так как портал неактивен;
- больше всего нареканий на работу сети поступает в середине дня в зоне кафе (при этом есть пользователи, использующие доступ к сети из зоны кафе без каких-либо проблем в любое время).

Имеет смысл начать решение с более точного определения проблемы и разбиения ее на подзадачи.

В случае проблем с порталом необходимо как можно более точно удостовериться, что имеют в виду пользователи, описывая неработающий портал. Отсутствие IP-адреса, постоянная перезагрузка страницы портала, отсутствующая страница портала, сообщение об ошибке сертификата на портале, повторный вывод формы аутентификации, долгая загрузка формы аутентификации, отсутствие перенаправления после аутентификации – все это может быть смешано пользователями в одном описании: "портал не активен". При получении описания такого вида проблем крайне желательно получать логи и скриншоты наблюдаемой ошибки, а также описание ожидаемого поведения системы.

Очевидно, что две различные беспроводные сети могут иметь как общие, так и различающиеся проблемы. То есть в процессе поиска неисправностей необходимо учитывать, что выдвигаемые гипотезы для одной сети должны удовлетворять симптомам, наблюдаемым в другой сети.

Можно также отметить, что первый пункт описания затрагивает потенциально все устройства, в то время как второй и третий пункты проявляются только на определенных клиентских устройствах.

```
ip dhcp pool GuestClients
   network 192.168.65.0 255.255.255.192
   default-router 192.168.65.1
   dns-server 192.168.10.27
   lease 7
!
```

Рис.2. Проверка DHCP-сервера: есть ошибки

В качестве временного решения, найденного инженерами компании, используется перезагрузка коммутатора, в который подключены точки доступа первого этажа (используемые гостевыми пользователями). Однако известны случаи, когда и после такой перезагрузки часть гостевых пользователей не могла подключиться к сети.

Удобнее всего, безусловно, исследовать проблему в момент ее проявления в сети. В нашем случае проблема возникает достаточно часто, чтобы "поймать" ее вживую.

Подробную информацию о клиенте, испытывающем проблемы с подключением, можно видеть на скриншоте (рис.1).

Как видно на иллюстрации, клиент пытается получить IP-адрес. В нормальных условиях этот процесс проходит достаточно быстро, и клиент переходит в состояние ожидания веб-аутентификации. Здесь мы можем выдвинуть следующие гипотезы: проблема на стороне клиента, проблема на стороне беспроводного решения, проблема на стороне проводной сети или DHCP-сервера. Поскольку аналогичный сценарий не фиксируется для корпоративной сети, проблема на стороне беспроводной сети маловероятна; проблема на стороне проводной сети также маловероятна до тех пор, пока путь трафика к DHCP-серверам совпадает. Проведя тестовое подключение одного и того же клиента к корпоративной и гостевой сетям, мы можем убедиться в том, что клиент работает нормально (в корпоративной сети, но не в гостевой). Таким образом, основным "подозреваемым" становится DHCP-сервер и его настройки для гостевой сети.

Предположив это, мы проверяем DHCP-сервер (рис.2): налицо сразу несколько ошибок!

В результате быстрого временного и незадокументированного решения в качестве DHCP-сервера для гостевой сети использовался коммутатор первого этажа. Размер пула адресов также не выдерживает критики – он слишком мал для данной компании и одновременно срок выдачи адреса установлен в семь дней (не часов), что приводит к исчерпанию пула. Очевидно, что перезагрузка этого коммутатора приводила к очистке таблицы выданных адресов и некоторому высвобождению адресов. Однако в случае большого количества посетителей адресный пул все равно исчерпывался. Так неверно выбранный дизайн вкупе с ошибкой конфигурации привел к проблеме, негативно влияющей на имидж компании. Эта ошибка хорошо объясняет первую часть тестового сценария. Однако локализация проблемы приема в зоне кафе и "неактивность" портала (при этом устройство получает IP-адрес) требуют отдельного разбирательства.

При уточнении проблемы "неактивности" пришлось использовать метод воспроизведения проблемы, поскольку получить непосредственно устройство, на котором проблема возникала, оказалось невозможно. Такой метод несет в себе некоторую неопределенность – даже если проблема возникает при воспроизведении, мы не можем быть стопроцентно уверены, что это именно та проблема, которая возникла на исходном устройстве и, следовательно, не можем быть уверены в том, что решение воспроизведенной проблемы подойдет для решения проблемы исходной.

В процессе воспроизведения проблемы был получен скриншот (рис.3): HTTPS-reidirect – функциональность, хотя и востребованная рядом заказчиков, но требующая определенных знаний от конечного пользователя, так как всегда вызывает появление предупреждения в окне браузера. В данном тестовом сценарии администратор сети не планировал ее использовать, однако она осталась включенной по ошибке. Поскольку ее наличие не предполагалось, сертификат не обновлялся, а также не использовался корпоративный CA. В результате часть браузеров полностью блокировала возможность перехода на страницу портала (без специальных настроек), а часть – генерировало окно с предупреждением, если при подключении осуществлялся HTTPS, а не HTTP-redirect.

В данном тестовом сценарии предполагается, что заказчик принял решение изменить конфигурацию контроллера, полностью отключив HTTPS-redirect. Безусловно, это может приводить к отсутствию портала в случае, если браузер коммуницирует с использованием HTTPS (такой запрос не будет перенаправлен на портал, а просто будет сброшен контроллером, как и любой другой трафик до аутентификации).

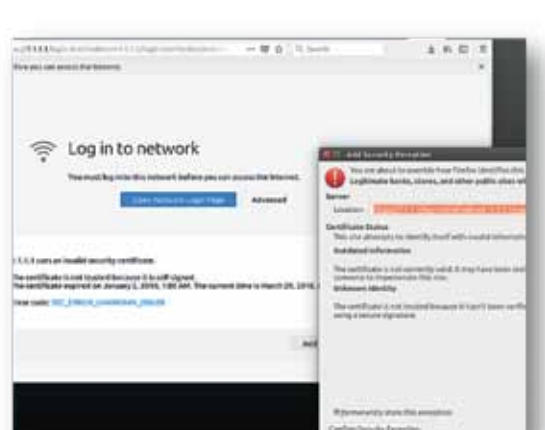

Рис.3. Скриншот, полученный в процессе воспроизведения проблемы

Наконец, пришло время анализа третьей составляющей проблемы – ухудшения приема в зоне кафе. Чем характеризуется зона кафе в данном офисе? Согласно тестовому сценарию, в кафе наличествует открытая терраса. Также мы можем предположить наличие источника помех в диапазоне 2,4 ГГц – микроволновой печи, которая может использоваться для разогрева блюд. Для участков открытой территории с Wi-Fi-покрытием достаточно логично предположить использование диапазона 2,4 ГГц. Безусловно, в случае небольшой террасы покрытие (хотя бы частично) может обеспечиваться за счет точек доступа, установленных внутри помещения и использующих диапазон 5 ГГц. Это может объяснять тот факт, что часть клиентов не испытывает проблем при работе в кафе – они используют 5 ГГц, который не подвержен влиянию работы микроволновой печи.

Для подтверждения этой гипотезы необходимо провести радиообследование во время возникновения проблемы. Важно отметить, что результаты в разных диапазонах должны быть представлены раздельно.

Подводя итоги, отметим, что процесс поиска неисправностей в беспроводных сетях – это не обязательно рутинное занятие, однако он проходит гораздо эффективнее, если проводить его, придерживаясь определенного алгоритма. Использование разделения проблемы на подгруппы и дальнейшее уточнение приводит к достаточно быстрому пониманию проблемы, что, в свою очередь, помогает получить ее быстрое решение. А ведь именно это – правильно работающая сеть – и является конечной целью поиска неисправностей. ■

TROUBLESHOOTING in Wi-Fi networks

I.Ilyina-Sidorova, engineer of the technical support center
Cisco / iilyinas@cisco.com

Troubleshooting wireless networks is a task quite different from that in traditional wired networks.

Classification of problems

In comparison with wired networks, wireless ones are characterized by a different way of accessing the environment and physically transmitting the signal, which leaves its imprint on the troubleshooting process. Moreover, the wireless nature of the connection brings uncertainty to the client's location in space.

It is convenient enough to conduct a troubleshooting process by relating a problem to one of the predefined classes, with its own check steps that will allow it to be narrowed and understood. In terms of WLAN (Wi-Fi) networks, it is useful to distinguish the following classes of problems:

- physical (hardware) failure;
- defect of the firmware or disposable manufacturing defect (fault);
- configuration problems;
- software defect;
- wrong design of the solution.

It should be noted that in the solution process it may become clear that the problem class was initially identified incorrectly. Ideally, this should not lead to large delays in finding a solution, but in a real situation, of course, it can slow down the restoration of normal network operation.

To select a problem class, you can use the following sequence of questions:

- **What?** (Which device, one, several or all available);
- **Where?** (In which part of the office / building / production area the problem is observed, and in which part it is not);
- **When?** (When the problem began to manifest itself, whether the normal operation of the network preceded it, when the problem did not manifest itself exactly);
- **What else?** (Have any changes been made to the network, location of the access points, were there any repairs or installations in the building, did the departments move, did new tenants appear in the nearby premises, etc.).

For more complete information on the initial survey schemes, reference should be made to the special literature (see, e.g., Kepner-Trego and "Five Why" (5Why) methods). If the problem occurs only on one device in the presence of several similar ones, it makes sense to assume a physical failure of the device. If the similarity is incomplete, e.g., if there is a significant difference in the installation (e.g., one of the access points is mounted on the wall opposite the elevators and the other is installed in the false ceiling of the office area), it is preferable to swap a deliberately working and potentially faulty device for checking: whether the malfunction is related to the physical position of the device. It is clear that in this case, it is necessary to replace all connecting cables by the same scheme.

If the problem occurs only on a certain type of equipment (on all devices of a certain type), then a **physical failure** of a particular device is unlikely. However, in the case of incorrect installation it is possible, e.g., if the caseof the access points intended for installation outdoorsis not sealed. In this case, it is necessary to check whether there are differences in the application of the potentially faulty model to test the hypothesis of the **wrong design** of the solution. If there are no such differences, or if the design is checked and corresponds to the capabilities of the equipment (according to the manufacturer's documentation, the capabilities of the equipment allow it to be used in this scheme and the equipment is also configured according to the

documentation), you can assume a **software defect** or a **firmware defect**. Obviously, in the design verification process, it is possible to detect **configuration errors** and correct them. With a new installation, as a rule,it is quite difficult for the end user to draw a line between a **software defect** and a firmware failure / production fault. However, this is not critical. In this case it is necessary to work with the equipment supplier to solve the problem. With new installations, a certain problem is the lack of data on the known operational mode of the network. This inconvenience can be leveled using pilot networks, and also with the help of a solution provider, which can provide additional information about test installations. In the event that the network has worked successfully in the past, we can exclude the possibility of manufacturing defects completely (provided that the functionality involved has not changed) and completely concentrate on localizing the software defect. At the same time, it should be noted that problems in production are encountered so less often with problems with software that their probability can generally be neglected. In case of problems with all devices, it makes sense to assume that the description of the problem misses an important detail that allows us to narrow the description, or that the problem **does not lie in the field of wireless networks** (e.g., a failure in a wired network can lead to loss of connection between the controller and all access points, while the controller and access points will function). Obviously, such an analysisis possible not for all networks, however, the more complete it will be, the more easily the process of troubleshooting will be simplified.

It can be summarized that in general, when several devices with sufficiently similar characteristics are considered, the verification algorithm goes from physical failure to verification of settings and design in general, and further to a software malfunction (and possible production fault).

Testing algorithm

A **physical fault** is not always a noticeable defect. In addition to the obvious cases (e.g., the access point was dropped during installation and its case is broken), electronic components may be damaged. Sometimes this device continues to partially function, which makes analysis even more difficult.

If the device looks completely out of order and does not turn on, it makes sense to replace the power source (cable, port on the switch, socket) with a guaranteed good one (not the free / standby one). It is possible to switch the device that operated on this source to a potentially faulty source, but this should be done with caution, since a malfunction may be introduced by the power supply (therefore it makes sense to do so only in the event that a potentially faulty device normally turns on with a verified working power source). This will allow to localize the problem and, possibly, avoid an expensive replacement.

It should be noted that sometimes physical replacement of the device is performed before the passage of all stages of troubleshootingas one of the stages of the problem investigation. This approach is justified in case of critical downtime, since in the ideal case it leads to the most rapid recovery of the system's efficiency. Unfortunately, this solution significantly reduces the ability to understand what caused the problem and prevent the appearance of similar problems in the future.

Possible failures during the replacement include the absence of a device (especially expensive) in the spare parts stock, the failure to replace in time and the lack of a working configuration of the device. All these complications are eliminated only

preventively, by observing the policy of saving device configurations, and using network management equipment (with the possibility of storing configurations of different versions, etc.) in the network.

The firmware defect (or the production fault, which can be corrected by re-flashing the device) can be identified in a separate class of problems only because this defect is often capable of being correcteddue to it being close to the characteristics of a physical fault. That is, if the defect is already known, its preventive correction is possible, and replacement of the equipment is not required. This saves resources for replacement. If the defect is difficult to remove (e.g., console access is required for a sufficiently long time and the device is mounted on a mast), a hardware replacement can be made to another device with the correct firmware and work on troubleshooting separately. To minimize the occurrence of such defects, it is necessary to periodically check the equipment manufacturers website for news about such manufacturing defects and keep in touch with the equipment suppliers.

Equipment configuration problems are the most frequent cause of failure. Here the main tactic is to analyze the changes made. Unfortunately, often the technical staff does not give due importance to documenting all the actions carried out or even trying to hide the actions that could lead to the malfunction. The policy of storing configuration versions and accounting for changes will help to get comprehensive information if necessary. A test network can do a great service here, where different configuration options can be simulated and, thus, a problem scenariocan be localized. Next, you can refer to the hardware documentation (or to the manufacturer's representative or to the supplier if the documentation is missing or incomplete) to find out what changes need to be made to correct the problem. This is also necessary to more accurately describe the problem to the equipment manufacturer in the event that the problem is caused by a software error and to find a workaround. If modeling a problem in a test network is impossible, you should simplify the script as much as possible in order to make it work, and then complicate it, gradually bringing it up to the one used in the real network, keeping in mind at which point the problem will arise again. For example, if there are problems with users'accessing to the wireless network, if there is a portal with the open idauthorization, you can offer:

- first create another open network using the same access point;
- if the connection of the client that has problems is carried out normally, configure the authentication with the portal, but using static credentials;
- if the connection is now normal, configure the open id authentication;
- if the problem is not reproduced when the identical configuration is reached (and the old solution is still does not work), you can use a new network for temporary access (workaround) and at the same time continue analyzing the old configuration to search for errors.

New networks are an interesting issue for the problems associated with setting up the equipment. They cannot be compared with a known good configuration. In this case, for comparison, we need a pilot network or at least detailed documentation for the equipment (configuration guides, blueprints). In new networks, we absolutely cannot rule out the possibility of incorrect design, and there is always a possibility that the equipment will not be able to work in the desired way (although it is certainly small in case of building a network by competent specialists). If you suspect a problem with the configuration of the device, in fact, we again go through the same cycle of questions as when determining the type of problem, but at a different level. We try to locate the problem location (device) and then collect diagnostic information that will confirm / disprove our conclusions.

In case of suspect problems:

- on the client side – we collect client logs and wireless traffic, and debug findings, if there is a controller, reflecting client states (e.g., for Cisco equipment, debug client <mac-address>), collect information about the connection point (the documentation for the network survey, wireless survey);
- on the access point side – we collect point logs (if any) and the controller (if anyin the network), traffic to the wireless connection, traffic between the access point and the controller (if we use the lightweight APs scheme);
- on the controller side – we collect the controller logs (for Cisco controllers, start with the show msglog, show traplog and show run-config);
- on the monitoring equipment side – we collect logs of the monitoring system, controller, traffic between the controller and the monitoring system;
- on the side of the authenticating server – we collect logs on the authentication server, on the controller and, possibly, traffic between them;

- on the network side – we collect network traffic between "our" devices and analyze it for possible resets.

As it is shown, a set of data, based on which we make analysis, partially overlaps. This allows you not to spend extra resources on analyzing obviously improbable hypotheses and to get the necessary data set for analysis faster. The **problems associated with a software defect** are most often reported to technical support services, but are often problems of a different kind. If we detect exceptions, kernel panics, and other similar messages with a high severity level in the logs, we can very likely assume a software defect. In this case, it is necessary to check whether this defect is present in the number known to the manufacturer (in the case of Cisco, using bug toolkit on the website), and in which version of the software this defect is fixed. In the case of unexpected results of software operation or device lockup, it is recommended to first check other possible causes of the problem. For a network engineer, it is impossible to completely correct this problem independently, but it is often possible to find a workaround that significantly reduces the impact of the problem on the network. To do this, if a software defect is detected, you must try to understand which hardware subsystem is affected by the defect, and then try to involve the same functionality without using such subsystem. For example, if you detect a bug in FlexConnect mode, you can try to switch the access point to Local mode. This mode, of course, will create additional load on the communication channel between the access point and the controller, and also on the controller, however this additional load can be acceptable for the time necessary for the manufacturer to correct the defect and provide new software. That's why if the problem is unknown to the manufacturer, it makes sense to simulate the problem at home and try to participate as much as possible in the process of solving it. Of course, this can be impossible in case of limited resources or increased criticality of the network.

A **wrong design** is the most painful mistake that engineers make when building networks. In the case of wireless networks, the limitations imposed by the "material" world (placement of access points and their power, coverage quality requirements) that vary depending on the desired network functionality,possible interference with other customer devicesare added to the issues of capacity, bandwidth, required functionality... Fortunately, these problems are often identified and eliminated during pilot launches. To prevent the intrusion of errors of this kind in production, thorough stress testing is necessary. Testing should be subject not only to the fact of connecting or using the desired functionality, but also the quality of the service provided, as well as the possibility of working in the case of full load of some part of the network and the behavior of the network in case of overload. In general, it is possible to assume the wrong design, if the problem description includes a mention of initially non-operating functionality or a significant deterioration of the service when the network is put into operation. In this situation, both a complete and a partial change in the network can be a solution, which is often impossible to implement in a short time. Therefore, sad as it may be, sometimes it is necessary to limit the functionality of the network as a temporary solution (e.g., instead of using only a wireless connection by all employees, you should transfer stationary workplaces to "normal" wired connection).

Testing scenario

Let's suppose that a certain company has a wireless network deployed in its office. The office is located in a separate low-rise building, on the territory of a business park, surrounded by similar buildings. On the first floor of the building there is a reception area for visitors, toilets, utility rooms, as well as a small cafe and recreation area. There are also working rooms and meeting rooms. On higher floors, only workplaces and bathrooms are located. There is an elevator in the building. Before the commissioning (before the moving-in of furniture), a radio survey was conducted, its results are available for analysis. Unfortunately, only the total results for the total coverage are submitted (simultaneously for both 5 GHz and 2.4 GHz). According to the radio survey, the signal strength (RSSI) ranges between -60 and -40, and the noise floor does not rise above -75 (mostly around -90).

For wireless access purposes, two wireless networks were configured, corporate and guest. For the guest network, there is a portal, data for connection to which the guest users receive from the secretary (for each user a unique account is generated). In the corporate network, the connection occurs with the verification of the machine certificate as well as the user account.

The following problems are observed:

- sometimes (from the moment the network is put into operation), guest users cannot connect

Fig.1. Screenshot with detailed information about the client experiencing connection problems

```
ip dhcp pool GuestClients
   network 192.168.65.0 255.255.255.192
   default-router 192.168.65.1
   dns-server 192.168.10.27
   lease 7
!
```

Fig.2. Checking the DHCP server: there are errors.

to the network (most often in the afternoon and on Friday);

- some guest users cannot connect because the portal is inactive;
- most complaints about the network are received in the middle of the day in the cafe area (there are users using access to the network from the cafe area without any problems at any time).

It makes sense to start a solution with more precise definition of the problem and its decomposition into subtasks.

In case of problems with the portal, you need to make sure as accurately as possible what users mean by describing a non-working portal. The absence of an IP address, the constant reloading of the portal page, the missing portal page, the message from the certificate error on the portal, the repeated output of the authentication form, the long loading of the authentication form, the absence of redirection after authentication – allthis can be confused by the users describing: "portal is not active". When obtaining a description of this type of problem, it is highly desirable to obtain logs and screenshots of the observed error, as well as a description of the expected behavior of the system.

Obviously, two different wireless networks can have both common and different problems. That is, in the process of troubleshooting, it should be borne in mind that the proposed hypotheses for one network should satisfy the symptoms observed in another network.

It can also be noted that the first item of the description affects potentially all devices, while the second and third items only appear on certain client devices.

As a temporary solution found by the company's engineers, the switch is rebooted, to which the first-floor access points (used by guest users) are connected. However, there are cases when even after such a reboot a part of guest users could not connect to the network.

It is most convenient, of course, to investigate the problem at the moment of its manifestation on the network. In our case, the problem arises often enough to "catch" it live. For detailed information about the client experiencing connectivity problems, you can see in the screenshot (Fig.1).

As you can see in the picture, the client tries to get an IP address. Under normal circumstances, this process passes quickly enough, and the client goes into a state of waiting for web authentication. Here we can put forward the following hypotheses: a client-side problem, a problem on the wireless side, a problem on the side of a wired network or a DHCP server. Since a similar scenario is not fixed for the corporate network, the problem on the wireless network side is unlikely; the problem on the wired network side is also unlikely until the traffic path to the DHCP servers is the same. Having performed testing connection of the same client to the corporate and guest networks, we can make sure that the client is working fine (in the corporate network but not in the guest one). Thus, the main "suspect" is the DHCP server and its settings for the guest network.

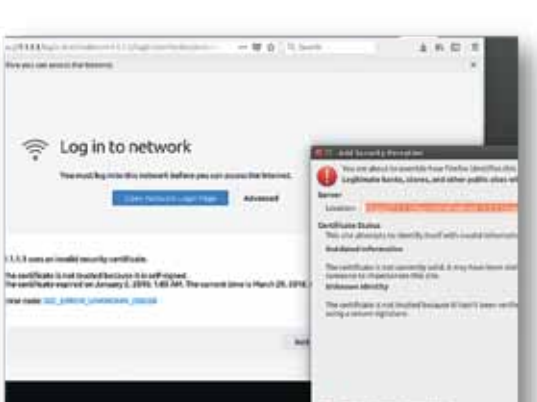

Fig.3. Screenshot obtained during simulation of the problem

Assuming this, we check the DHCP server (Fig.2): several errors are immediately apparent!

As a result of a fast temporary and undocumented solution, the first-floor switch was used as the DHCP server for the guest network. The size of the address pool also does not stand up to criticism – itis too small for this company and at the same time, the date for issuing the address is set at seven days (not hours), which leads to the depletion of the pool. Obviously, restarting this switch resulted in clearing the table of issued addresses and some freeing addresses. However, in the case of a large number of visitors, the address pool was still exhausted. Thus, incorrectly selected design, coupled with a configuration error led to a problem that adversely affects the image of the company. This error explains the first part of the test scenario well. However, the localization of the reception problem in the cafe area and the "inactivity" of the portal (with the device receiving an IP address) require a separate investigation.

When clarifying the problem of "inactivity" we had to use the method of reproducing the problem, because it was impossible to get directly the device on which the problem arose. This method carries some uncertainty, even if the problem occurs during simulation, we cannot be absolutely sure that this is exactly the problem that has arisen on the source device and, therefore, we cannot be sure that the solution of the simulated problem is suitable for solving the originalproblem.

During the simulation of the problem, a screenshot was obtained (Fig.3): HTTPS-redirect is a functionality, although demanded by a number of customers, but requiring certain knowledge from the end user, since it always causes an alert in the browser window. In this test scenario, the network administrator did not plan to use it, but it remained turned on by mistake. Since its availability was not intended, the certificate was not updated, nor was the corporate CA used. As a result, some browsers completely blocked the ability to go to the portal page (without special settings), and another part generated a warning window if HTTPS was being used when connecting instead of HTTP-redirect.

In this test scenario, it is assumed that the customer has decided to change the controller configuration by completely disabling HTTPS-redirect. Of course, this can lead to a lack of a portal in case the browser communicates using HTTPS (such a request will not be redirected to the portal, but will simply be reset by the controller, like any other traffic prior to authentication).

Finally, the time has come for analyzing the third component of the problem – deterioration of reception in the cafe area. What are the characteristics of the area of the cafe in this office? According to the test scenario, there is an open terrace in the cafe. Also, we can assume the presence of a source of interference in the 2.4 GHz band – amicrowave oven, which can be used to warm up dishes. For areas of open territory with Wi-Fi-coverage, it is logical to assume the use of the 2.4 GHz band. Of course, in the case of a small terrace, a cover (at least partially) can be provided by access points installed inside the room and using a 5 GHz band. This may explain the fact that some customers do not experience problems when working in a cafe – they use 5 GHz, which is not affected by the operation of the microwave oven.

To confirm this hypothesis, it is necessary to conduct a radio survey during the occurrence of the problem. It is important to note that the results in different ranges should be submitted separately.

Summarizing, we note that the process of troubleshooting wireless networks is not necessarily a routine activity, but it goes much more efficiently if you follow it, adhering to a certain algorithm. Using the division of the problem into subgroups and further refinement leads to a fairly rapid understanding of the problem, which in turn helps to get its quick solution. And after all it is a correctly working network which is the ultimate goal of troubleshooting. ■