Рекомендации по настройке контроллера беспроводной ЛВС

Содержание

Введение

В этом документе приводятся краткие советы по решению некоторых, связанных с беспроводной унифицированной инфраструктурой, проблем, запросы о которых часто направлялись в Центр технической поддержки (TAC).

Задача заключается в предоставлении важных замечаний, которые можно использовать в большинстве случаев реализации сети для минимизации возможных проблем.

Примечание: Не все сети обладают одинаковыми параметрами, поэтому некоторые советы могут быть неприменимы для данной конкретной установки. Перед внесением изменений в действующую сеть всегда необходимо выполнять проверку.

Предварительные условия

Требования

Cisco рекомендует ознакомится со следующими темами:

- Сведения о настройке контроллера беспроводной ЛВС и облегченной точки доступа (LAP) для базовых операций
- Базовые сведения о протоколе облегченных точек доступа (LWAPP) и методы обеспечения беспроводной безопасности

Используемые компоненты

Сведения, содержащиеся в данных документах, касаются следующих версий программного и аппаратного обеспечения:

- WLC Cisco серий 2000 / 2100 / 4400, на которых используется микропрограмма 3.2 или 4.0
- Точки доступа на основе LWAPP серии 1230, 1240, 1130, 10x0 и 1500

Сведения в этом документе были получены от приборов в специфической лабораторной среде. Все устройства, используемые в этом документе, были запущены с чистой (заданной по умолчанию) конфигурацией. Если сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в документе Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Лучшие решения

Wireless/RF

При работе с беспроводными (радиочастотными) сетями рекомендуется использовать следующие проверенные приемы.

- При развертывании беспроводных сетей необходимо всегда выполнять соответствующий анализ узлов, чтобы гарантировать необходимое качество обслуживания для беспроводных клиентов. Требования к развертыванию служб голоса или местоположения более жесткие, чем для служб данных. Автоматический RF можно использовать для управления настройками каналов и питания, но с его помощью нельзя исправить неправильную структуру RF.
- Анализ узлов должен быть выполнен с использованием устройств, режим работы которых соответствует режимам обеспечения питания и радиовещания устройств, которые будут использоваться в действующей сети. Например, не используйте радио 350 802.11B с всенаправленной антенной для изучения области покрытия, если в окончательной сети используется двойное радио 1240 для 802.11A и G.
- Используя эту же идею, ограничьте количество идентификаторов наборов служб (SSID), настроенных на контроллере. С помощью модели точки доступа можно настроить 8 или 16 одновременных SSID, но поскольку для каждой WLAN/SSID необходимы отдельные тестовые ответы и аварийная сигнализация, количество помех RF увеличивается по мере добавления SSID. В результате определенные небольшие беспроводные станции, такие как PDA, WiFi-телефоны и устройства для считывания штрих-кода, не могут обработать большой объем базовых данных SSID (BSSID). Это в свою очередь приводит к возникновению блокировок, перезагрузок или сбоев при соединении. Чем больше количество SSID, тем больше потребность в аварийной сигнализации, тем меньшее пространство RF остается доступным для передачи действительных данных.
- В средах RF с обширными свободными пространствами, таких как заводы, где точки доступа разнесены и не экранированы стенами, возможно, потребуется изменить пороговое значение мощности излучения, заданное по умолчанию и равное -65 дБм, на более низкое значение, например -76 дБм. Это позволяет уменьшить помехи при передаче данных между каналами (количество BSSID, "услышанных" от беспроводных клиентов в определенный момент времени). Оптимальное значение зависит от характеристик среды каждого узла, поэтому значение необходимо оценить после анализа узлов.

  Пороговое значение мощности излучения — это выраженное в дБм предельное значение уровня сигнала, относительно которого алгоритм контроля выходной мощности (TPC) настраивает уровни мощности в нисходящем порядке так, чтобы это было значение мощности, при котором "слышен" третий по мощности модуль, расположенный рядом с AP.
- В работе определенного клиентского ПО 802.11 могут возникнуть проблемы, если им будет "услышано" более определенного фиксированного количества BSSID (например, 24 или 32 BSSID). После уменьшения порогового значения выходной мощности и, следовательно, среднего уровня передачи AP, можно уменьшить количество BSSID, доступных для этого клиента.
- Не следует включать активную балансировку нагрузки, если в своей области сеть не располагает большим числом плотно расположенных точек доступа, тем более при передаче по беспроводной сети голосовых данных. Если эта функция включается для определенных точек доступа, расположенных на большом расстоянии друг от друга, может возникнуть путаница с алгоритмом роуминга определенных клиентов, а также могут возникнуть проблемы с обеспечением области покрытия для определенных областей. В последних версиях программного обеспечения эта функция по умолчанию отключена.

Сетевые подключения

Рекомендации для сетевых подключений.

- Не использовать протокол STP на контроллерах.

Для большинства топологий не требуется использование протокола STP, запущенного на контроллере. По умолчанию поддержка STP отключена.

Для коммутаторов сторонних производителей рекомендуется отключение STP для каждого порта.

Используйте команду для проверки:

```
Cisco Controller) >show spanningtree switch

STP Specification..................... IEEE 802.1D
STP Base MAC Address.................. 00:18:B9:EA:5E:60
Spanning Tree Algorithm.............. Disable
STP Bridge Priority................... 32768
STP Bridge Max. Age (seconds)......... 20
STP Bridge Hello Time (seconds)....... 2
STP Bridge Forward Delay (seconds)..... 15

(Cisco Controller) >
```

- Хотя большинство конфигураций настраиваются без прерывания рабочего процесса, рекомендуется перезагрузить контроллеры после изменения следующих настроек конфигурации.
    - Управление адресом
    - Настройка SNMP имеет первостепенное значение, если используется более раннее ПО.
- Для всех магистральных портов, подключенных к контроллерам, определите неиспользуемые сети VLAN.

  Например, для коммутаторов Cisco IOS®, если включен интерфейс управления сети VLAN 20 и для двух различных WLAN применяются сети VLAN 40 и 50, на стороне коммутатора используйте следующую команду конфигурации:

```
switchport trunk allowed vlans 20,40,50
```

- Не настраивайте служебный порт с наложением подсети для интерфейса управления.
- Не оставляйте без изменений для интерфейса адрес 0.0.0.0, например, ненастроенный служебный порт. Это может повлиять на обработку DHCP в контроллере.

  Проверка выполняется следующим образом:

```
(Cisco Controller) >show interface summary
Interface Name        Port  Vlan Id   IP Address       Type     Ap Mgr
--------------------  ----  --------  ---------------  -------  ------
ap-manager            LAG   15        192.168.15.66    Static   Yes
example               LAG   30        0.0.0.0          Dynamic  No
management            LAG   15        192.168.15.65    Static   No
service-port          N/A   N/A       10.48.76.65      Static   No
test                  LAG   50        192.168.50.65    Dynamic  No
virtual               N/A   N/A       1.1.1.1          Static   No
```

- Не следует использовать LAG, если только все порты контроллера не имеют одну и ту же конфигурацию Уровня 2 на стороне коммутатора. Например, следует избегать фильтрации определенных сетей VLAN для одного порта, но не для других.
- Если используется LAG, при балансировке трафика, исходящего из сети, контроллер полагается на коммутатор. Предполагается, что трафик, принадлежащий AP (LWAPP или сети для беспроводного пользователя) всегда поступает на один и тот же порт. Используйте только параметры балансирования нагрузки ip-src или ip-src ip-dst в конфигурации коммутатора EtherChannel. Некоторые модели коммутатора по умолчанию используют неподдерживаемые механизмы балансирования нагрузки и именно поэтому проверка имеет первостепенное значение.

  Проверка механизма балансирования нагрузки EtherChannel выполняется следующим образом:

```
switch#show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip
```

```
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
```

Изменение конфигурации коммутатора (IOS) выполняется следующим образом:

```
switch(config)#port-channel load-balance src-dst-ip
```

- Не следует настраивать LAG-соединение, использующееся для нескольких подключений. LAG необходимо использовать для всех портов, принадлежащих одному EtherChannel, подключенному к одному и тому же физическому коммутатору. Это ограничение можно обойти за счет использования определенных режимов работы только с функциональностью межстекового EtherChannel 3750.
- Если топология LAG *не* используется, всегда следует создавать AP-диспетчер для каждого физического порта для обеспечения резервируемости и масштабируемости.
- Не следует настраивать резервный порт для интерфейса AP-диспетчера, даже если эта возможность поддерживалась в более ранних версиях. Резервируемость обеспечивается за счет нескольких интерфейсов AP-диспетчера, как уже упоминалось ранее в этом документе.

Структура сети

Для структуры сети рекомендуется использовать следующие проверенные приемы.

- Необходимо ограничить количество точек доступа для каждой сети VLAN. Рекомендуемое количество: от 30 до 60 (зависит от характеристик сети). Это ограничение используется для минимизации проблем с повторным соединением при сбое в работе сети.
- Что касается первого совета, то не рекомендуется задавать более 20 точек доступа в одной сети VLAN с использованием интерфейса управления контроллера. Возможно, что из-за большого количества транслируемых сообщений, создаваемых точками доступа, некоторые сообщения об обнаружении отбрасываются. Это приводит к более медленному объединению точек доступа.
- Что касается структуры, то трафик, инициируемый ЦП, отправляется с управляемого адреса контроллера. Например, ловушки SNMP, запросы проверки подлинности RADIUS и т.д.

  Исключением из этого правила является трафик, зависящий от DHCP и отправляемый с интерфейса, связанного с настройками WLAN, для ПО контроллера версии 4.0 и более поздних версий. Например, если WLAN использует динамический интерфейс, DHCP-запрос направляется с использованием этого адреса Уровня 3.

  Это необходимо помнить при настройке политик брандмауэра или планировании топологии сети. Важно избегать настройки динамического интерфейса в той же подсети, что и сервер, который должен быть доступен для ЦП контроллера, например, RADIUS-сервер, поскольку при этом могут возникнуть проблемы с асимметричной маршрутизацией.

Мобильность

Советы по обеспечению мобильности.

- Все контроллеры, входящие в группу мобильности, должны иметь один и тот же IP-адрес для виртуального интерфейса, например, 1.1.1.1. Это важно для обеспечения поддержки роуминга. Если не все контроллеры в группе мобильности используют один виртуальный интерфейс, может сложиться впечатление, что роуминг между контроллерами функционирует стабильно, но передача управления не завершается и клиент на некоторое время теряет соединение.

  Проверка выполняется следующим образом:

```
(Cisco Controller) >show interface summary

Interface Name      Port   Vlan Id   IP Address       Type     Ap Mgr
-----------------   -----  --------  ---------------  -------  ------
ap-manager           LAG   15        192.168.15.66    Static   Yes
```

```
management          LAG   15        192.168.15.65    Static   No
service-port        N/A   N/A       10.48.76.65      Static   No
test                LAG   50        192.168.50.65    Dynamic  No
virtual             N/A   N/A       1.1.1.1          Static   No
```

- Адрес виртуального шлюза должен быть **немаршрутизируемым** в инфраструктуре сети. Он должен быть доступен только для беспроводного клиента во время подключения к контроллеру и всегда недоступен для проводного соединения.
- Все контроллеры должны быть настроены для одного и того же режима транспорта LWAPP (уровень 2 или уровень 3).
- Между интерфейсами управления всех контроллеров должна существовать возможность подключения по IP-протоколу.
- Все контроллеры должны быть настроены с использованием одного и того же имени группы мобильности. Для Cisco WiSM оба контроллера должны быть настроены с использованием одного и того же имени группы мобильности для прозрачной маршрутизации к 300 точкам доступа.
- На всех контроллерах должна быть запущена одна версия ПО для контроллеров.
- Необходимо включить MAC-адрес и IP-адрес каждого контроллера в группу мобильности. Эти данные необходимы, поскольку все контроллеры настраиваются с использованием MAC-адреса и IP- адреса всех остальных членов группы мобильности. MAC- и IP- адреса других контроллеров должны быть включены в группу мобильности на странице Controller > Mobility Groups GUI каждого контроллера.
- Не следует создавать излишне большие группы мобильности. В группу мобильности должны быть включены только те контроллеры, имеющие точки доступа в области, в которой для клиента доступно физическое перемещение, например, все контроллеры с точками доступа в здании. Если необходимо обеспечить группу мобильности для нескольких отдельно стоящих зданий, необходимо ее разбить на несколько групп мобильности. Благодаря этому экономятся ресурсы памяти и ЦП, поскольку для контроллеров нет необходимости в поддержании больших списков действительных клиентов, мошенников и точек доступа в группе, с которой не планируется взаимодействие.

  Необходимо помнить, что резервируемость WLC достигается за счет групп мобильности. Поэтому в определенных ситуациях может возникнуть необходимость в увеличении размера группы мобильности, включая добавление дополнительных контроллеров для обеспечение резервируемости (например, топология N+1).
- Если в группе мобильности существует более одного контроллера, то после перезагрузки контроллера нормальным явлением будет выдача предупреждений о неавторизованном использовании точки доступа в сети. Это происходит из-за времени, которое затрачивается на обновление списков точек доступа, клиентов и мошенников между членами группы мобильности.
- Параметр обязательности DHCP в настройках WLAN позволяет заставить клиентов отправлять/обновлять адрес DHCP при каждом соединении с WLAN до того, как они смогут отправить или получить другой трафик в сети. С точки зрения безопасности благодаря этому обеспечивается возможность более жесткого контроля используемых IP-адресов, но при этом также может быть затронуто общее время роуминга до того, как трафик снова сможет быть передан.

  Также это может повлиять на реализацию клиентов, которые не обновляют DHCP до истечения срока аренды. Например, могут возникнуть проблемы с передачей голосовых данных в телефонах Cisco 7920 или 7921 при роуминге, если этот параметр включен, поскольку контроллер не поддерживает передачу трафика голосовых данных или сигнализации до завершения фазы DHCP. Это может повлиять на работу серверов печати сторонних поставщиков. Не рекомендуется пользоваться этой функцией, если в беспроводной сети имеются клиенты, работающие под управлением не Windows, а других ОС. Причина заключается в том, что использование строгого контроля может привести к возникновению проблем с возможностью подключения в зависимости от метода реализации DHCP-клиента. Проверка выполняется следующим образом:

```
(Cisco Controller) >show wlan 1

WLAN Identifier.................................. 1
Profile Name..................................... 4400
Network Name (SSID).............................. 4400
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
```

```
Wired Protocol................................. None
```

Безопасность

Советы по обеспечению безопасности.

- Рекомендуется задать для тайм-аута по протоколу RADIUS значение, равное 5 секундам. Значение по умолчание, равное 2 секундам, является приемлемым для быстрого переключение при сбое RADIUS, но может быть недостаточным для расширенной проверки подлинности на транспортном уровне сети (EAP-TLS) или если сервер RADIUS должен подключаться к внешним базам данных (Active Directory, NAC, SQL и т.д.).

  Проверка выполняется следующим образом:

```
(Cisco Controller) >show radius summary
Vendor Id Backward Compatibility..... Disabled
Credentials Caching.................... Disabled
Call Station Id Type................... IP Address
Administrative Authentication via RADIUS.... Enabled
Aggressive Failover.................... Disabled
Keywrap................................ DisabledAuthentication Servers

!--- This portion of code has been wrapped to several lines due to spatial
!--- concerns.

Idx  Type  Server Address    Port    State    Tout RFC3576
---  ----  ---------------  ------  --------  ----  -------
1    N     10.48.76.50      1812    Enabled   2    Enabled

IPSec -AuthMode/Phase1/Group/Lifetime/Auth/Encr
-----------------------------------------------
Disabled - none/unknown/group-0/0 none/none
```

  Настройка выполняется следующим образом:

```
config radius auth retransmit-timeout 1 5
```

- Проверьте пользователя SNMPv3, настроенного по умолчанию. По умолчанию для контроллера задается имя пользователя, которое следует изменить или отключить.

  Проверка выполняется следующим образом:

```
(Cisco Controller) >show snmpv3user

SNMP v3 User SNMP v3 User Name AccessMode Authentication Encryption
-------------------- ----------- -------------- ----------
default Read/Write HMAC-MD5 CBC-DES
```

  Настройка выполняется следующим образом:

```
config snmp v3user delete default
config snmp v3user create nondefault rw hmacsha des authkey encrkey
```

  Необходимо помнить, что настройки SNMP должны быть идентичными для контроллера и Wireless Control System (WCS). Также необходимо использовать ключи шифрования и хеширования, соответствующие используемым политикам безопасности.

- При выполнении веб-проверки подлинности с использованием страницы внешней проверки подлинности, не следует использовать сервер, который одновременно используется как веб-сервер и прокси-сервер для размещения страницы подключения. Контроллер обеспечивает возможность прохождения HTTP-трафика от беспроводных клиентов к серверу для завершения проверки подлинности. Благодаря этому обеспечивается возможность перехода клиента к различным ресурсам с помощью прокси-службы, существующей на сервере.

- Для контроллеров значение тайм-аута по умолчанию для запроса удостоверения EAP составляет 1 секунду, что неприемлемо для таких случаев, как реализация одноразовых паролей или Smart Card, где пользователь должен ввести PIN-код или пароль до того, как беспроводной клиент сможет ответить на запрос об удостоверении. Для автономных точек доступа по умолчанию задается значение, равное 30 секундам, поэтому это необходимо учитывать при автономной миграции к беспроводным сетям инфраструктуры.

  Изменение выполняется следующим образом:

  ```
  config advanced eap identity-request-timeout 30
  ```

- В агрессивных средах рекомендуется включить проверку подлинности точки доступа с пороговым значением равным 2. При этом будет обеспечена возможность обнаружения возможных заимствований прав и минимизации вторжений с использованием ложных данных.

  Настройка выполняется следующим образом:

  ```
  config wps ap-authentication enable
  config wps ap-authentication threshold 2
  ```

- Касательно предыдущего совета, защиту фреймов управления (MFP) можно также использовать для проверки подлинности всего трафика управления на 802.11, обнаруженного между ближайшими точками доступа в беспроводной инфраструктуре. Необходимо помнить, что при реализации драйверов определенных часто используемых беспроводных карт сторонних поставщиков возникают проблемы с обработкой дополнительных элементов сведений, добавленных MFP. До тестирования и начала использования MFP, убедитесь, что используются новейшие драйверы от производителя карты.

- NTP имеет первостепенное значение для нескольких функций. Обязательно использование синхронизации NTP для контроллеров, если используются какие-либо из следующих функций: Location, SNMPv3, проверка подлинности точки доступа или MFP.

  Настройка выполняется следующим образом:

  ```
  config time ntp server 1 10.1.1.1
  ```

  При выполнении проверки проконтролируйте наличие в журнале прерываний записей, похожих на следующую:

  ```
  30 Tue Feb 6 08:12:03 2007 Controller time base status -
  Controller is in sync with the central timebase.
  ```

- При использовании протокола проверки подлинности с предварительным согласованием вызова EAP-Microsoft версии 2 (PEAP-MSCHAPv2), с Microsoft XP SP2 и управлении беспроводной карты с помощью службы Wireless Zero Configuration (WZC) Microsoft необходимо применить исправление Microsoft KB885453 . Это предотвращает возникновение нескольких проблем проверки подлинности, связанных с PEAP Fast Resume.

- Если по причинам безопасности беспроводных клиентов необходимо разделить на несколько подсетей, каждая из которых будет обладать различными политиками безопасности, рекомендуется использовать одну или несколько беспроводных локальных сетей (например, каждая из которых имеет отличный от других Уровень 2 политики шифрования) с функцией переопределения AAA. Эта функция позволяет задавать настройки для каждого пользователя. Например, при этом можно переместить пользователя в специальный динамический интерфейс в отдельной виртуальной локальной сети или применить для каждого пользователя список Управления доступом.

- Хотя контроллеры и точки доступа поддерживают WLAN с SSID с одновременным использованием защищенного доступа Wi-Fi (WPA) и WPA2, часто возникает проблема, при которой некоторые драйверы беспроводных клиентов не могут обработать комплексные настройки SSID. Как правило, рекомендуется использовать простые политики безопасности для любого SSID, например, использовать одну WLAN/SSID с WPA и протоколом целостности временных ключей (TKIP), а также отдельную с WPA2 и улучшенным стандартом шифрования (AES).

Общее администрирование

При общем администрировании рекомендуется использовать следующие проверенные приемы.

- До обновления рекомендуется выполнить двоичное резервное копирование конфигурации. WLC поддерживают преобразование данных более ранних конфигураций до новых версий, однако обратный процесс не поддерживается. Это касается как значительных, так и незначительных изменений версий.
- Использование более новой конфигурации в более раннем выпуске может привести к отсутствию настроек (списков доступа, интерфейсов и т.д.) или к неправильной работе функций. Если необходимо уменьшить функциональность контроллера, рекомендуется после этого очистить конфигурацию, восстановить адрес интерфейса управления и загрузить файл двоичной резервной копии с помощью TFTP.

Как переместить файл сбоя WLC с WLC CLI на TFTP-сервер

Для передачи файла сбоя WLC от WLC CLI на TFTP-сервер используйте следующие команды:

```
transfer upload datatype crashfile
transfer upload serverip <IP-адрес TFTP-сервера>

transfer upload path <введите путь к каталогу>

transfer upload filename <имя файла сбоя>

transfer upload start<да>
```

Примечание: При вводе пути к каталогу **"/"** обычно означает корневой каталог, заданный по умолчанию на TFTP-сервере.

Ниже представлен пример:

```
(Cisco Controller) >debug transfer tftp enable

(Cisco Controller) >debug transfer trace enable

(Cisco Controller) >transfer upload datatype crashfile

(Cisco Controller) >transfer upload filename aire2cra.txt

(Cisco Controller) >transfer upload path /

(Cisco Controller) >transfer upload serverip X.Y.Z.A

(Cisco Controller) >transfer upload start

Mode..................................... TFTP TFTP Server
IP.................................. X.Y.Z.A TFTP
Path..................................... / TFTP
Filename................................. aire2cra.txt Data
Type..................................... Crash File

Are you sure you want to start? (y/N) yes
Thu Dec 29 10:13:17 2005: RESULT_STRING: TFTP Crash File transfer starting.
Thu Dec 29 10:13:17 2005: RESULT_CODE:1

TFTP Crash File transfer starting.
Thu Dec 29 10:13:21 2005: Locking tftp semaphore, pHost=X.Y.Z.A
pFilename=/aire2cra.txt Thu Dec 29 10:13:22 2005:
Semaphore locked, now unlocking,
pHost=X.Y.Z.A pFilename=/aire2cra.txt Thu Dec 29 10:13:22 2005:
Semaphore successfully unlocked,
pHost=X.Y.Z.A pFilename=/aire2cra.txt Thu Dec 29 10:13:22 2005:
tftp rc=0, pHost=X.Y.Z.A pFilename=/aire2cra.txt


pLocalFilename=/mnt/application/bigcrash
Thu Dec 29 10:13:22 2005: RESULT_STRING: File transfer operation
completed successfully.
Thu Dec 29 10:13:22 2005: RESULT_CODE:11 File transfer operation
completed successfully.
```

Дополнительные сведения

- **Вопросы и ответы по облегченным точкам доступа**
- **Вопросы и ответы по устранению неполадок в работе контроллера беспроводной ЛВС**
- **Вопросы и ответы по модулю контроллера Cisco для беспроводной ЛВС**
- **Вопросы и ответы по контроллерам беспроводной ЛВС**
- **Управление радиоресурсами в унифицированных беспроводных сетях**
- **Поддержка беспроводных сетей**
- **Поддержка технологии беспроводных сетей (WLAN)**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/105395/wlc-config-best-practice.shtml

---