АККУРАТНЫЙ пример конфигурации с платформой Cisco Identity Services Engine

Содержание

Введение

Этот документ описывает конфигурацию и поведение Топологии аутентификации границы сети (NEAT) в простом сценарии. АККУРАТНЫЙ использует Протокол сигнализации сведений о клиенте (CISP) для распространения MAC - адресов клиента и сведений о виртуальной локальной сети (VLAN) между коммутаторами средства проверки подлинности и соискателем.

В этом примере конфигурации оба коммутатор средства проверки подлинности (также названный средством проверки подлинности) и коммутатор соискателя (также названный соискателем) выполняют аутентификацию 802.1x; средство проверки подлинности аутентифицирует соискателя, который, в свою очередь, аутентифицирует ПК тестирования.

Предварительные условия

Требования

Cisco рекомендует ознакомиться со стандартом аутентификации IEEE 802.1x.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Два коммутатора Cisco Catalyst серии 3560 с программным обеспечением Cisco IOS, релиз 12.2 (55) SE8; один коммутатор действует как средство проверки подлинности и другие действия как соискатель.
- Платформа Cisco Identity Services Engine (ISE), выпуск 1.2.
- ПК с Microsoft Windows XP, пакет обновления 3.

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.

Настройка

Данный пример покрывает примеры конфигурации для:

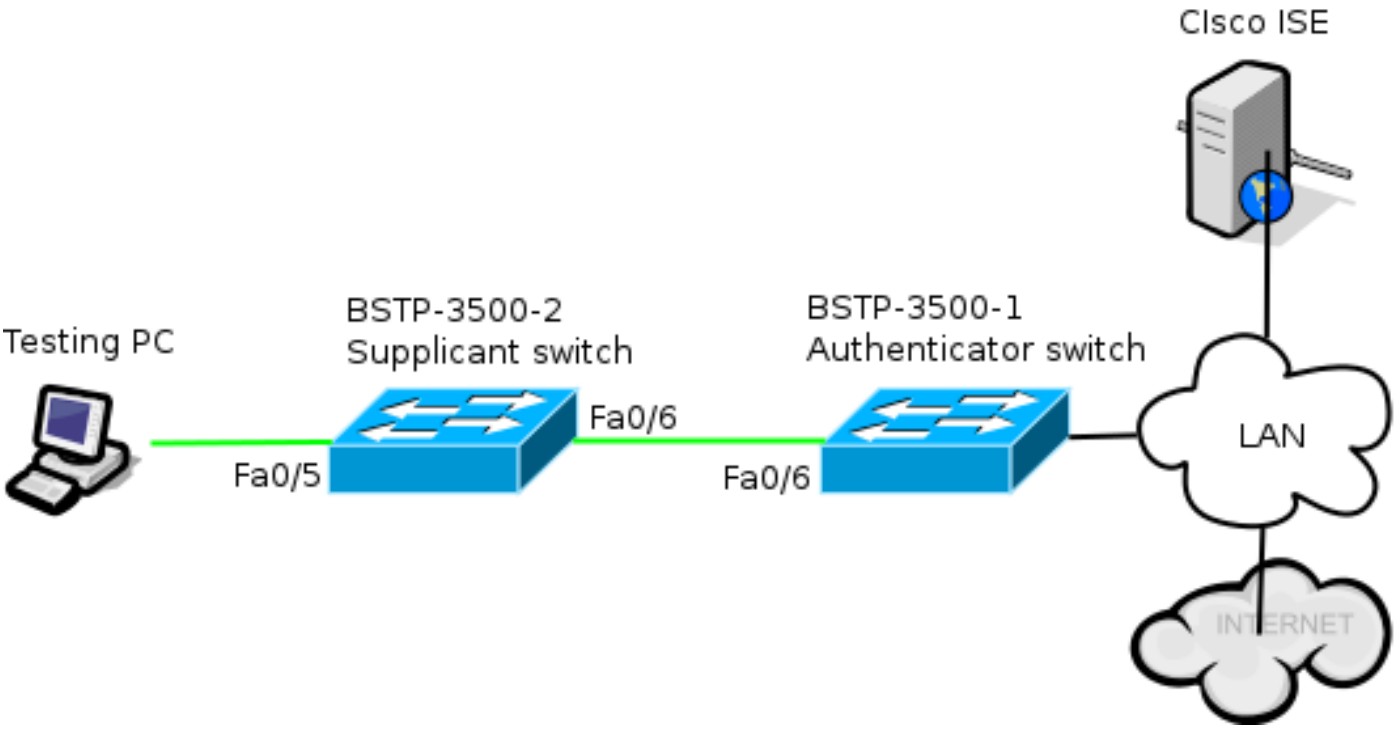
- Коммутатор средства проверки подлинности
- Коммутатор соискателя
- Cisco ISE

Конфигурации являются минимумом, необходимым для выполнения этого осуществления лабораторной работы; они не могли бы быть оптимальными для или выполнить другие потребности.

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

Эта схема сети иллюстрирует подключение, используемое в данном примере. Черное пятно указывает логический или физическое подключение, и зеленые линии указывают на ссылки, аутентифицируемые с помощью 802.1x.



Конфигурация коммутатора средства проверки подлинности

Средство проверки подлинности содержит основные элементы, необходимые для dot1x. В данном примере команды, которые являются определенными для АККУРАТНОГО или CISP, являются полужирными.

Это - базовая проверка подлинности, авторизация, и бухгалтерский (AAA) конфигурация:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

radius-server host 10.48.66.107 auth-port 1812 acct-port 1813 key cisco

! Enable authenticator switch to authenticate the supplicant switch.
dot1x system-auth-control
! Enable CISP framework.
cisp enable

! configure uplink port as access and dot1x authentication.
interface FastEthernet0/6
switchport mode access
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
```

CISP включен глобально, и взаимосвязанный порт настроен в средстве проверки подлинности и режиме доступа.

Конфигурация коммутатора соискателя

Точная конфигурация соискателя крайне важна для всей настройки для работы как ожидалось. Конфигурация данного примера содержит типичный AAA и конфигурацию dot1x.

Это - основная конфигурация AAA:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

radius-server host 10.48.66.107 auth-port 1812 acct-port 1813 key cisco

! Enable supplicant switch to authenticate devices connected
dot1x system-auth-control

! Forces the switch to send only multicast EAPOL packets when it receives either
unicast or multicast packets, which allows NEAT to work on the supplicant
switch in all host modes.
dot1x supplicant force-multicast

! Enable CISP framework operation.
cisp enable
```

Соискатель должен был настроить учетные данные и должен предоставить метод Протокола EAP, который будет использоваться.

Соискатель может использовать Алгоритм представления сообщения в краткой форме 5 (MD5) EAP и Гибкую аутентификацию EAP с помощью Защищенного протокола (FAST) (среди других типов EAP) для аутентификации в случае CISP. Для хранения конфигурации ISE к минимуму данный пример использует EAP-MD5 для аутентификации соискателя к средству проверки подлинности. (По умолчанию вызвал бы использование EAP-FAST, который требует инициализации Учетных данных защищенного доступа [PAC]; этот документ не покрывает тот сценарий.)

```
! configure EAP mode used by supplicant switch to authenticate itself to
authenticator switch eap profile EAP_PRO
method md5

! Configure credentials use by supplicant switch during that authentication.
dot1x credentials CRED_PRO
 username bsnsswitch
password 0 C1sco123
```

Соединение соискателя к средству проверки подлинности уже настроено, чтобы быть магистральным портом (в отличие от конфигурации порта доступа на средстве проверки подлинности). На данном этапе это ожидается; когда ISE возвратит корректный атрибут, конфигурация динамично изменится.

```
interface FastEthernet0/6
switchport trunk encapsulation dot1q
 switchport mode trunk
dot1x pae supplicant
 dot1x credentials CRED_PRO
 dot1x supplicant eap profile EAP_PRO
```

Порт, который соединяется с Компьютером с операционной системой Windows, имеет минимальную настройку и показан здесь для ссылки только.

```
interface FastEthernet0/5
switchport access vlan 200
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

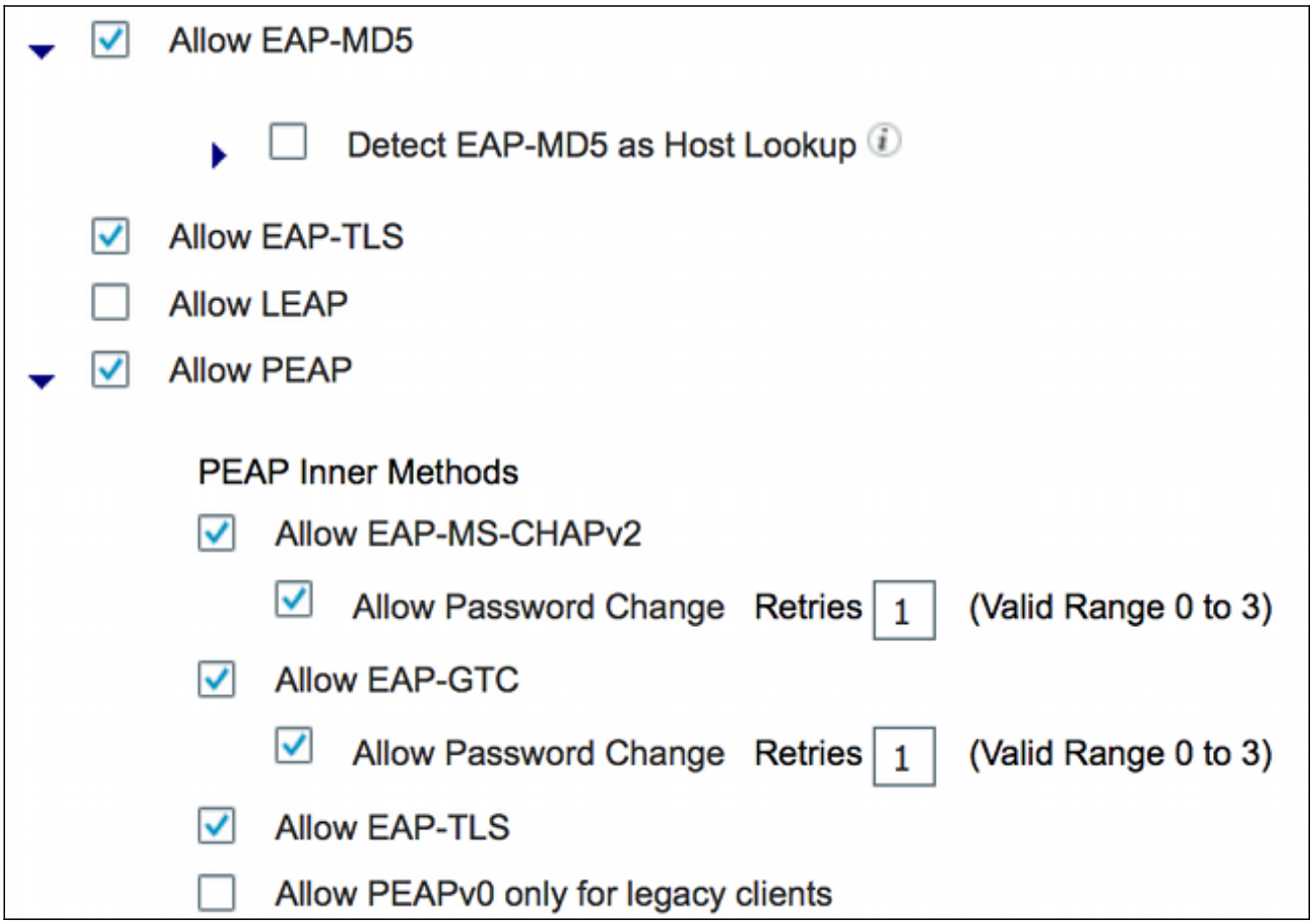
Конфигурация ISE

Эта процедура описывает, как установить основную конфигурацию ISE.

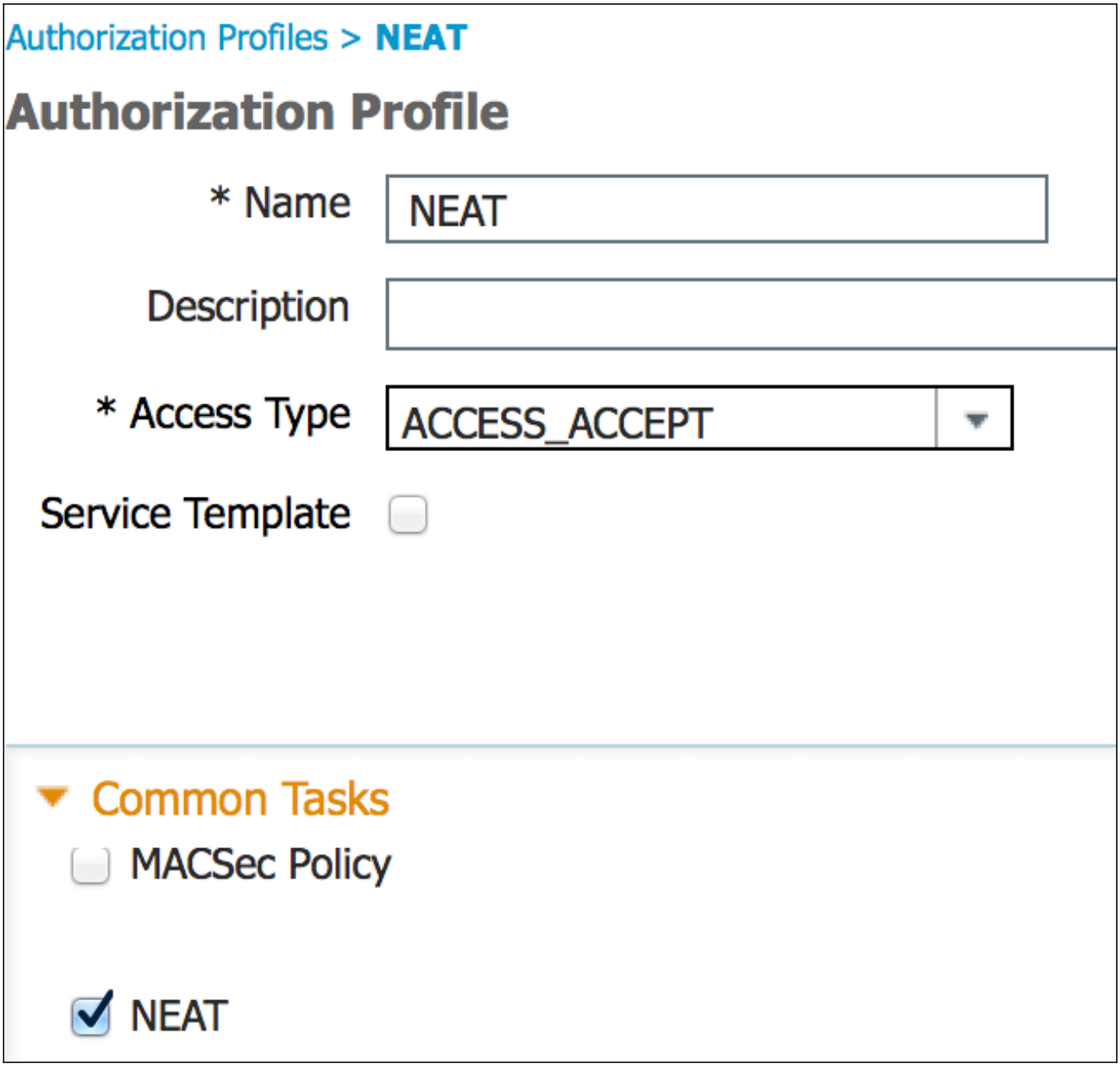
1. Включите протоколы обязательной аутентификации.

   В данном примере соединенный проводом dot1x позволяет EAP-MD5 аутентифицировать соискателя на средстве проверки подлинности и позволяет Защищенному расширяемому протоколу аутентификации (PEAP) - Версия протокола 2 (MSCHAPv2) Квитирования с аутентификацией Microsoft аутентифицировать Компьютер с операционной системой Windows на соискателе.

   Перейдите к **Политике> Результаты> Аутентификация> Разрешенные протоколы**, выберите **список сервиса протокола**, используемый проводным dot1x, и гарантируйте, что включены протоколы в этом шаге.



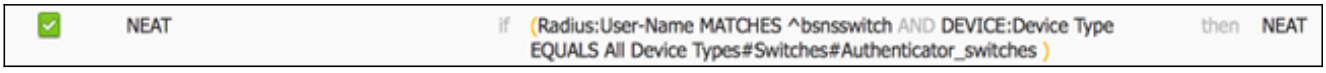
2. Создайте политику авторизации. Перейдите к **Политике> Результаты> Авторизация> Политика авторизации**, и создайте или обновите политику, таким образом, это содержит АККУРАТНЫЙ как возвращенный атрибут. Это - пример такой политики:



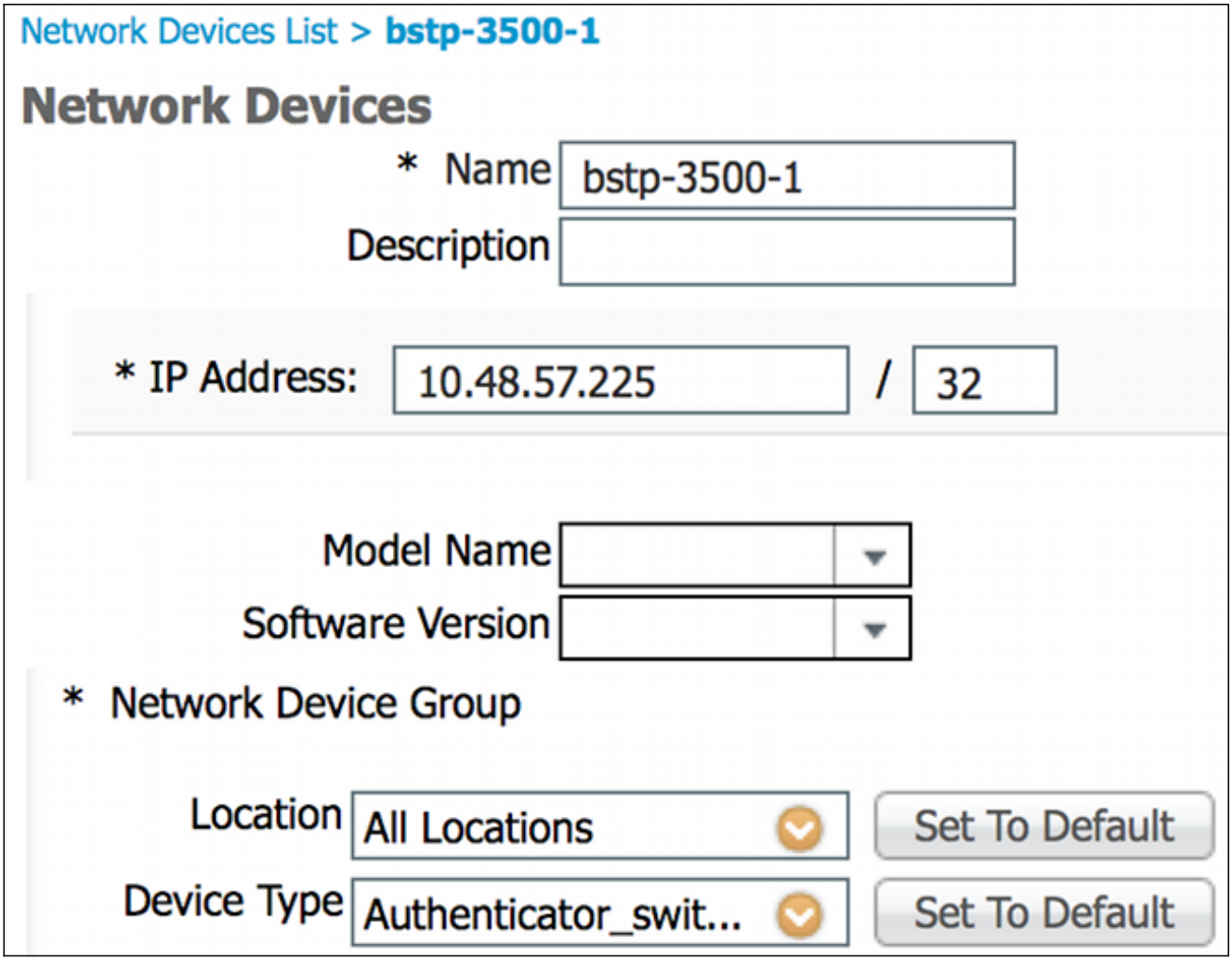
Когда опция NEAT включена, ISE возвращается device-traffic-class=switch как часть авторизации. Эта опция необходима для изменения режима порта средства проверки подлинности с доступа на транк.

3. Создайте правило авторизации для использования этого профиля. Перейдите к **Политике> Авторизация**, и создайте или обновите правило.

   В данном примере создана группа специального устройства по имени Authenticator_switches, и все соискатели передают имя пользователя, которое начинается с bsnsswitch.



4. Добавьте коммутаторы к соответствующей группе. Перейдите к **администрированию> Сетевые ресурсы> Сетевые устройства** и **нажмите Add**.



В данном примере, BSTP-3500-1 (средство проверки подлинности) часть группы Authenticator_switches; BSTP-3500-2 (соискатель) не должен быть частью этой группы.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно. В этом разделе описываются два способов поведения:

- Аутентификация между коммутаторами
- Аутентификация между Компьютером с операционной системой Windows и соискателем

Это также объясняет три дополнительных ситуации:

- Удаление аутентифицированного клиента от сети
- Удаление соискателя
- Порты без dot1x на соискателе

Примечания:

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом

"Важные сведения о командах отладки".

Аутентификация коммутатора соискателя к коммутатору средства проверки подлинности

В данном примере соискатель аутентифицируется на средстве проверки подлинности. Шаги в процесс:

1. Соискатель настроен и включен порт fastethernet0/6. Обмен dot1x заставляет соискателя использовать EAP для передачи предварительно сконфигурированного имени пользователя и пароля к средству проверки подлинности.
2. Средство проверки подлинности выполняет обмен RADIUS и предоставляет учетные данные для проверки ISE.
3. Если учетные данные корректны, ISE возвращает атрибуты, требуемые АККУРАТНЫМ (device-traffic-class=switch), и средство проверки подлинности изменяет своего switchport mode с доступа на транк.

Данный пример показывает обмен информацией CISP между коммутаторами:

```
bstp-3500-1#debug cisp all
Oct 15 13:51:03.672: %AUTHMGR-5-START: Starting 'dot1x' for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB
Oct 15 13:51:03.723: %DOT1X-5-SUCCESS: Authentication successful for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID
Oct 15 13:51:03.723: %AUTHMGR-7-RESULT: Authentication result 'success' from
'dot1x' for client (001b.0d55.2187) on Interface Fa0/6 AuditSessionID
0A3039E10000000600757ABB
Oct 15 13:51:03.723: Applying command... 'no switchport access vlan 1' at Fa0/6
Oct 15 13:51:03.739: Applying command... 'no switchport nonegotiate' at Fa0/6
Oct 15 13:51:03.748: Applying command... 'switchport trunk encapsulation dot1q'
at Fa0/6
Oct 15 13:51:03.756: Applying command... 'switchport mode trunk' at Fa0/6
Oct 15 13:51:03.756: Applying command... 'switchport trunk native vlan 1' at
Fa0/6
Oct 15 13:51:03.764: Applying command... 'spanning-tree portfast trunk' at Fa0/6
Oct 15 13:51:04.805: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB

Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Received action Run Authenticator
Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Authenticator received event Start in
state Not Running
Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Authenticator state changed to Waiting
link UP
Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 13:51:05.669: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to
up
Oct 15 13:51:06.793: CISP-EVENT (Fa0/6): Received action Run Authenticator
Oct 15 13:51:06.793: CISP-EVENT (Fa0/6): Authenticator received event Start in
state Waiting link UP (no-op)
Oct 15 13:51:07.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/6, changed state to up
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Authenticator received event Link UP in
state Waiting link UP
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:07.799: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Proposing CISP version: 1
```

```
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Authenticator state changed to Idle
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 13:51:07.799: CISP-EVENT: Received action Start Tick Timer
Oct 15 13:51:07.799: CISP-EVENT: Started CISP tick timer
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:12.942: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:18.084: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:23.226: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:28.377: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:28.377: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:29.400: CISP-EVENT: Stopped CISP tick timer
Oct 15 13:51:36.707: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x22 Length:0x001C
Type:REGISTRATION
Oct 15 13:51:36.707: Payload: 0200E84B
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Proposed CISP version: 1
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Negotiated CISP version: 1
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Sync supp_id: 59467
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:36.707: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x22 Length:0x001C
Type:REGISTRATION
Oct 15 13:51:36.707: Payload: 01000000
Oct 15 13:51:36.724: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x23 Length:0x003A
Type:ADD_CLIENT
Oct 15 13:51:36.724: Payload: 010011020009001B0D5521C10300050 ...
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c1 (vlan: 200)
to authenticator list
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Notifying interest parties about new
downstream client 001b.0d55.21c1 (vlan: 200)
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client info at Authenticator
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c0 (vlan: 1)
to authenticator list
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Notifying interest parties about new
downstream client 001b.0d55.21c0 (vlan: 1)
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client info at Authenticator
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:36.724: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x23 Length:0x0018
Type:ADD_CLIENT
```

Однажды проверка подлинности и авторизация успешно выполняются, обмен CISP происходит. Каждый обмен имеет ЗАПРОС, который отправлен соискателем и ОТВЕТОМ, который служит ответом и подтверждением от средства проверки подлинности.

Выполнены два отдельных обмена: REGISTRATION и ADD_CLIENT. Во время обмена REGISTRATION соискатель сообщает средству проверки подлинности, что это CISP-способно, и средство проверки подлинности тогда подтверждает это сообщение. Обмен ADD_CLIENT используется для информирования средства проверки подлинности об устройствах, связанных с локальным портом соискателя. Как с REGISTRATION, КЛИЕНТ ADD инициируется на соискателе и подтверждается средством проверки подлинности.

Введите эти команды показа для проверки связи, ролей и адресов:

```
bstp-3500-1#show cisp clients

Authenticator Client Table:
---------------------------
MAC Address VLAN Interface
--------------------------------
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6

bstp-3500-1#show cisp registrations

Interface(s) with CISP registered user(s):
----------------------------------------
Fa0/6
Auth Mgr (Authenticator)
```

В данном примере роль Средства проверки подлинности правильно назначена на корректный интерфейс (fa0/6), и зарегистрированы два MAC-адреса. MAC-адреса являются соискателем на порту fa0/6 на VLAN1 и на VLAN200.

Проверка сеансов аутентификации dot1x может теперь быть выполнена. fa0/6 порт на восходящем коммутаторе уже аутентифицируется. Это - обмен dot1x, который инициирован, когда включен BSTP-3500-2 (соискатель):

```
bstp-3500-1#show authentication sessions

Interface MAC Address Method Domain Status Session ID
Fa0/6 001b.0d55.2187 dot1x DATA Authz Success 0A3039E10000000700FB3259
```

Как ожидалось на данном этапе на соискателе нет никаких сеансов:

```
bstp-3500-2#show authentication sessions
No Auth Manager contexts currently exist
```

Аутентификация компьютера с операционной системой Windows к коммутатору соискателя

В данном примере Компьютер с операционной системой Windows аутентифицируется на соискателе. Шаги в процесс:

1. Компьютер с операционной системой Windows включен в порт FastEthernet 0/5 на BSTP-3500-2 (соискатель).
2. Соискатель выполняет проверку подлинности и авторизация с ISE.
3. Соискатель сообщает средству проверки подлинности, что новый клиент связан на

порту.

Это - связь от соискателя:

```
Oct 15 14:19:37.207: %AUTHMGR-5-START: Starting 'dot1x' for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID 0A3039E200000013008F77FA
Oct 15 14:19:37.325: %DOT1X-5-SUCCESS: Authentication successful for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID
Oct 15 14:19:37.325: %AUTHMGR-7-RESULT: Authentication result 'success' from
'dot1x' for client (c464.13b4.29c3) on Interface Fa0/5 AuditSessionID
0A3039E200000013008F77FA
Oct 15 14:19:37.341: CISP-EVENT (Fa0/5): Received action Add Client
Oct 15 14:19:37.341: CISP-EVENT (Fa0/5): Adding client c464.13b4.29c3 (vlan: 200)
to supplicant list
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Supplicant received event Add Client in
state Idle
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Adding client c464.13b4.29c3 (vlan: 200)
to the ADD list
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Adding client c464.13b4.29c3 (vlan: 200)
to ADD CLIENT req
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 14:19:37.341: CISP-TXPAK (Fa0/6): Code:REQUEST ID:0x24 Length:0x0029
Type:ADD_CLIENT
Oct 15 14:19:37.341: Payload: 010011020009C46413B429C30300050 ...
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Started 'retransmit' timer (30s)
Oct 15 14:19:37.341: CISP-EVENT: Started CISP tick timer
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Supplicant state changed to Request
Oct 15 14:19:37.341: CISP-RXPAK (Fa0/6): Code:RESPONSE ID:0x24 Length:0x0018
Type:ADD_CLIENT
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Supplicant received event Receive Packet
in state Request
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Stopped 'retransmit' timer
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): All Clients implicitly ACKed
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Supplicant state changed to Idle
Oct 15 14:19:38.356: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID 0A3039E200000013008F77FA
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Received action Run Authenticator
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Authenticator received event Start in
state Not Running
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Authenticator state changed to Waiting
link UP
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Sync supp_id: 0
Oct 15 14:19:38.373: CISP-EVENT: Stopped CISP tick timer
Oct 15 14:19:39.162: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to
up
```

Обмен ADD_CLIENT происходит, но не необходим никакой обмен REGISTRATION.

Для проверки поведения на соискателе введите **показ cisp регистрационная** команда:

```
bstp-3500-2#show cisp registrations

Interface(s) with CISP registered user(s):
-----------------------------------------
Fa0/5
Auth Mgr (Authenticator)
Fa0/6
802.1x Sup (Supplicant)
```

У соискателя есть роль соискателя к средству проверки подлинности (fa0/6 интерфейс) и роль средства проверки подлинности к Компьютеру с операционной системой Windows (fa0/5 интерфейс).

Для проверки поведения на средстве проверки подлинности введите **показ cisp** команда

клиентов:

```
bstp-3500-1#show cisp clients

Authenticator Client Table:
-------------------------
MAC Address VLAN Interface
--------------------------------
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6
c464.13b4.29c3 200 Fa0/6
```

Новый MAC-адрес появляется на средстве проверки подлинности под VLAN 200. Это - MAC-адрес, который наблюдался в запросах AAA на соискателе.

Сеансы аутентификации должны указать, что то же устройство связано на fa0/5 порту соискателя:

```
bstp-3500-2#show authentication sessions

Interface MAC Address Method Domain Status Session ID
Fa0/5 c464.13b4.29c3 dot1x DATA Authz Success 0A3039E20000001501018B58
```

Удаление аутентифицированного клиента от сети

Когда клиент удален (например, если порт закрыт), средство проверки подлинности уведомлено посредством обмена DELETE_CLIENT.

```
Oct 15 15:54:05.415: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x25 Length:0x0029
Type:DELETE_CLIENT
Oct 15 15:54:05.415: Payload: 010011020009C46413B429C30300050 ...
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Removing client c464.13b4.29c3
(vlan: 200) from authenticator list
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client c464.13b4.29c3 (vlan: 200)
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 15:54:05.415: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x25 Length:0x0018
Type:DELETE_CLIENT
```

Удаление коммутатора соискателя

Когда соискатель отключен или удален, средство проверки подлинности представляет оригинальную конфигурацию назад порту во избежание проблем безопасности.

```
Oct 15 15:57:31.257: Applying command... 'no switchport nonegotiate' at Fa0/6
Oct 15 15:57:31.273: Applying command... 'switchport mode access' at Fa0/6
Oct 15 15:57:31.273: Applying command... 'no switchport trunk encapsulation
dot1q' at Fa0/6
Oct 15 15:57:31.290: Applying command... 'no switchport trunk native vlan 1' at
Fa0/6
Oct 15 15:57:31.299: Applying command... 'no spanning-tree portfast trunk' at
Fa0/6
Oct 15 15:57:31.307: Applying command... 'switchport access vlan 1' at Fa0/6
Oct 15 15:57:31.315: Applying command... 'spanning-tree portfast' at Fa0/6
Oct 15 15:57:32.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/6, changed state to down
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Authenticator received event Link DOWN
```

```
in state Idle
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Removing client 001b.0d55.21c1
(vlan: 200) from authenticator list
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client 001b.0d55.21c1 (vlan: 200)
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Removing client 001b.0d55.21c0 (vlan: 1)
from authenticator list
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client 001b.0d55.21c0 (vlan: 1)
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Authenticator state changed to Not
Running
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 15:57:33.262: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state
to down
```

В то же время соискатель удаляет клиентов, которые представляют соискателя от таблицы CISP, и деактивировал CISP на том интерфейсе.

Порты Без dot1x на Коммутаторе Соискателя

Информация о CISP, которая распространяется от соискателя к средству проверки подлинности, служит только в качестве другого уровня осуществления. Соискатель сообщает средству проверки подлинности обо всех разрешенных адресах MAC, которые связаны с ним.

Сценарий, который, как правило, неправильно понимается, является этим: если устройство включено на порту, которому не включили dot1x, MAC-адрес изучен и распространяется к восходящему коммутатору через CISP.

Средство проверки подлинности позволяет связь, которая прибывает от всех клиентов, изученных через CISP.

В сущности это - роль соискателя, чтобы ограничить доступ устройств через dot1x или другие методы, и распространиться MAC-адрес и сведения о виртуальной локальной сети (VLAN) к средству проверки подлинности. Средство проверки подлинности действует как средство обеспечения выполнения информации, предоставленной в тех обновлениях.

Как пример, новая VLAN (VLAN300) была создана на обоих коммутаторах, и устройство было включено в порт fa0/4 на соискателе. Порт fa0/4 является простым портом доступа, который не настроен для dot1x.

Эти выходные данные от соискателя показывают новый зарегистрированный порт:

```
bstp-3500-2#show cisp registrations

Interface(s) with CISP registered user(s):
----------------------------------------
Fa0/4
Fa0/5
Auth Mgr (Authenticator)
Fa0/6
802.1x Sup (Supplicant)
```

На средстве проверки подлинности новый MAC-адрес видим на VLAN 300.

```
bstp-3500-1#show cisp clients

Authenticator Client Table:
```

```
--------------------------
MAC Address VLAN Interface
--------------------------------
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6
001b.0d55.21c2 300 Fa0/6
c464.13b4.29c3 200 Fa0/6
 68ef.bdc7.13ff 300 Fa0/6
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

> **Примечание:**
>
> Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**
>
> Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Эти команды помогают вам устранять неполадки АККУРАТНЫЙ и CISP; этот документ включает примеры для большинства из них:

- **отладьте cisp, который все** - показывают обмену информацией CISP между коммутаторами.
- **покажите, что cisp сводка** - отображает сводку статуса интерфейса CISP на коммутаторе.
- **покажите, что cisp регистрация** - указывает на интерфейсы, которые участвуют в обменах CISP, ролях тех интерфейсов, и являются ли интерфейсы частью АККУРАТНЫХ.
- **покажите, что cisp клиенты** - отображают таблицу MAC-адресов известного клиента и их местоположения (VLAN и интерфейс). Это полезно в основном от средства проверки подлинности.