통합

다음 섹션에서는 Cisco ISE의 기능을 지원하기 위해 스위치 및 무선 컨트롤러에 필요한 컨피그레이션에 대해 설명합니다.

표준 웹 인증을 지원하도록 스위치 활성화

인증 시의 URL 리디렉션을 위한 프로비저닝을 포함하여 Cisco ISE에 대해 표준 웹 인증 기능을 활성화하려면 스위치 구성에 다음 명령을 포함해 주십시오.

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

가상 RADIUS 트랜잭션을 위한 로컬 사용자 이름 및 비밀번호 정의

스위치가 이 네트워크 세그먼트에 대한 RADIUS 서버인 경우에도 Cisco ISE 노드와 통신할 수 있게 하려면 다음 명령을 입력합니다.

```
username test-radius password 0 abcde123
```

로그 및 계정 타임스탬프 정확도 유지를 위한 NTP 서버 컨피그레이션

다음 명령을 입력하여 Cisco ISE에 설정한 것처럼 스위치에 NTP 서버를 지정합니다.

```
ntp server <IP_address>|<domain_name>
```

AAA 기능을 활성화하는 명령

802.1X 및 MAB 인증 기능을 포함하여 Cisco ISE와 스위치 간에 다양한 AAA 기능을 활성화하려면 스위치에서 다음 명령을 입력합니다.

```
aaa new-model
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius
! Required for VLAN/ACL assignment
aaa authorization network default group radius
! Authentication & authorization for webauth transactions
aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
```

```
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
aaa accounting update periodic 5

! Update AAA accounting information periodically every 5 minutes

aaa accounting system default start-stop group radius
!
```

스위치에서의 **RADIUS** 서버 컨피그레이션

다음 명령을 입력하여 RADIUS 소스 서버 역할을 하는 Cisco ISE와 상호 작용하도록 스위치를 구성합니다.

```
!
radius-server <ISE Name>

! ISE Name is the name of the ISE PSN

address ipv4 <ip address> auth-port 1812 acct-port 1813

! IP address is the address of the PSN. This example uses the standard RADIUS ports.

key <passwd>

! passwd is the secret password confiugured in Cisco ISE

exit
```

참고 인증에 Active Directory를 사용하는 RADIUS 요청에 더 긴 응답 시간을 제공하도록 3회 재시도와 함께 데드 기준 시간으로 30초를 구성하는 것이 좋습니다.

RADIUS CoA(Change of Authorization)를 활성화하는 명령

다음 명령을 입력하여 Cisco ISE에서 포스처 기능을 지원하는 RADIUS CoA 동작을 스위치가 적절하게 처리할 수 있도록 하는 설정을 지정합니다.

```
aaa server radius dynamic-author

client <ISE-IP> server-key 0 abcde123
```

참고

- Cisco ISE는 Cisco IOS 소프트웨어 기본값인 포트 1700을 사용하지만 CoA에 대해서는 RFC 기본 포트 3799를 사용합니다. 기존의 Cisco Secure ACS 5.x 고객은 기존 ACS 구현의 일부분으로 CoA를 사용 중인 경우 이 포트가 포트 3799로 이미 설정되어 있을 수 있습니다.
- 공유 암호 키는 네트워크 디바이스를 추가하는 동안 Cisco ISE에 구성한 키와 동일해야 하며 IP 주소는 PSN IP 주소여야 합니다.

디바이스 추적 및 **DHCP** 스누핑을 활성화하는 명령

Cisco ISE에서 선택적인 보안 기반 기능을 제공하려는 경우 다음 명령을 입력하여 스위치 포트에서 동적 ACL의 IP 교체를 위해 디바이스 추적 및 DHCP 스누핑을 활성화할 수 있습니다.

```
! Optional

ip dhcp snooping

! Required!

! Configure Device Tracking Policy!
device-tracking policy <DT_POLICY_NAME>
no protocol ndp
tracking enable

! Bind it to interface!
interface <interface_id>
device-tracking attach-policy<DT_POLICY_NAME>
```

RADIUS 계정 관리에서는 DHCP 스누핑을 활성화해도 IOS 센서에서 DHCP 속성을 Cisco ISE로 전송하지 않습니다. 이러한 경우에는 VLAN에서 DHCP 스누핑을 활성화하여 DHCP를 활성 상태로 설정해야 합니다.

VLAN에서 DHCP 스누핑을 활성화하려면 다음 명령을 사용합니다.

```
ip dhcp snooping
ip dhcp snooping vlan 1-100
```

802.1X 포트 기반 인증을 활성화하는 명령

스위치 포트에 대해 802.1X 인증을 전역적으로 설정하려면 다음 명령을 입력합니다.

```
dot1x system-auth-control
```

중요 인증에 대해 **EAP**를 활성화하는 명령

LAN을 통한 신청자 인증 요청을 지원하려면 다음 명령을 입력하여 중요 인증에 대한 EAP(액세스할 수 없는 인증 바이패스)를 활성화합니다.

```
dot1x critical eapol
```

복구 지연을 사용하여 **AAA** 요청을 제한하는 명령

중요 인증 복구 이벤트가 발생하면 다음 명령을 입력하여 Cisco ISE가 복구 후 서비스를 다시 시작할 수 있도록 밀리초 단위의 지연을 자동으로 적용하도록 스위치를 구성할 수 있습니다.

```
authentication critical recovery delay 1000
```

시행 상태에 따른 **VLAN** 정의

네트워크의 알려진 시행 상태에 따라 VLAN 이름, 번호 및 SVI(Switch Virtual Interface)를 정의하려면 다음 명령을 입력합니다. 해당 VLAN 인터페이스를 생성하여 네트워크 간에 라우팅을 활성화할 수 있습니다. 이는 엔드포인트(PC, 노트북 등)와 엔드포인트를 네트워크에 연결하는 데 사용되는 IP 폰 모두에서 동일한 네트워크 세그먼트를 통해 전달되는 여러 소스의 트래픽을 처리할 때 특히 유용할 수 있습니다.

```
vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>

name VOICE

!

interface <VLAN_number>

description ACCESS

ip address 10.1.2.3 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

ip helper-address <Cisco_ISE_IP_address>

!
```

```
interface <VLAN_number>

description VOICE

ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>
```

스위치에서의 로컬(기본) ACL(Access List) 정의

다음 명령을 입력하여 Cisco ISE가 인증 및 권한 부여를 위해 필요한 동적 ACL 업데이트를 수행할 수 있도록 이전 스위치(12.2(55)SE 이전 버전의 Cisco IOS 소프트웨어 릴리스)에서 다음 기능을 활성화합니다.

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal


permit tcp any host <Cisco_ISE_IP_address> eq www
```

```
permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest
  deny ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
```

참고 무선 컨트롤러의 컨피그레이션은 CPU 사용률을 높이고 시스템이 불안정해질 수 있는 위험을 높일 수 있습니다. 이는 IOS 문제로, Cisco ISE에 부정적인 영향을 미치지 않습니다.

802.1X 및 MAB에 대한 스위치 포트 활성화

802.1X 및 MAB에 대해 스위치 포트를 활성화하려면 다음 단계를 수행합니다.

단계 **1** 모든 액세스 스위치 포트의 인터페이스 구성 모드로 진입합니다.

interface range FastEthernet0/1-8

단계 **2** 트렁크 모드가 아닌 액세스 모드용으로 스위치 포트를 활성화합니다.

switchport mode access

단계 **3** 액세스 VLAN을 정적으로 구성합니다. 이렇게 하면 액세스 VLAN에 대한 로컬 프로비저닝을 제공하며, 개방형 모드 인증을 사용하려면 다음과 같이 구성해야 합니다.

switchport access vlan <*VLAN_number*>

단계 **4** 음성 VLAN을 정적으로 구성합니다.

switchport voice vlan <*VLAN_number*>

단계 **5** 개방형 모드 인증을 활성화합니다. 개방형 모드를 사용하면 인증이 완료되기 전에 트래픽을 데이터 및 음성 VLAN에 브리지할 수 있습니다. 프로덕션 환경에서는 무단 액세스를 방지하기 위해 포트 기반 ACL을 사용하는 것이 좋습니다.

개방형 모드 인증을 활성화하면 포트 ACL에 따라 AAA 서버 응답 전에 사전 인증 액세스도 활성화됩니다.

authentication open

단계 **6** 포트 기반 ACL을 적용하여 인증되지 않은 엔드포인트에서 액세스 VLAN에 기본적으로 브리지해야 하는 트래픽을 확인합니다. 먼저 모든 액세스를 허용하고 정책을 나중에 시행해야 하므로, 스위치 포트를 통한 모든 트래픽을 허용하기 위해 ACL-ALLOW를 적용해야 합니다. 네트워크를 완전하게 파악하고 기존의 최종 사용자 경험에는 아직 영향을 주지 않아야 하므로, 현재 모든 트래픽을 허용하는 기본 Cisco ISE 권한 부여는 이미 생성한 상태여야 합니다.

AAA 서버에서 동적 ACL을 앞에 추가하도록 ACL을 구성해야 합니다.

ip access-group ACL-ALLOW in

참고 DSBU 스위치의 Cisco IOS 소프트웨어 릴리스 12.2(55)SE 이전 버전에서는 RADIUS AAA 서버의 동적 ACL을 적용하려면 포트 ACL이 필요합니다. 기본 ACL을 포함하지 않으면 스위치가 할당된 동적 ACL을 무시합니다. Cisco IOS 소프트웨어 릴리스 12.2(55)SE에서는 기본 ACL이 자동으로 생성되어 적용됩니다.

참고 여기서는 기존 네트워크에 영향을 주지 않고 802.1X 포트 기반 인증을 활성화할 것이므로 실험의 이 부분에서는 ACL-ALLOW를 사용합니다. 이후 연습에서는 프로덕션 환경에 대해 원치 않는 트래픽을 차단하는 다른 ACL-DEFAULT를 적용할 것입니다.

단계 **7** 다중 인증 호스트 모드를 활성화합니다. 다중 인증은 기본적으로 MDA(Multi-Domain Authentication)의 상위 집합입니다. MDA에서는 데이터 도메인에 엔드포인트를 하나만 허용합니다. 다중 인증을 구성할 때는 MDA에서와 마찬가지로 음성 도메인에는 인증된 전화 하나를 포함할 수 있지만 데이터 도메인에서는 데이터 디바이스를 수에 제한 없이 인증할 수 있습니다.

같은 물리적 액세스 포트에서 음성 및 여러 엔드포인트를 허용합니다.

authentication host-mode multi-auth

참고 여러 데이터 디바이스(가상화된 디바이스 또는 허브에 연결된 물리적 디바이스)가 IP 전화기에 연결되는 경우 액세스 포트의 물리적 링크 상태 인식 성능이 저하될 수 있습니다.

단계 **8** 다음과 같은 명령으로 다양한 인증 방법 옵션을 활성화합니다.
다음과 같이 재인증을 활성화합니다.
authentication periodic
다음과 같이 RADIUS 세션 시간 초과를 통한 재인증을 활성화합니다.
authentication timer reauthenticate server
authentication event fail action next-method
데드 서버의 경우 다음과 같이 중요 인증 VLAN 방법을 구성합니다.
authentication event server dead action reinitialize vlan *<VLAN_number>*
authentication event server alive action reinitialize
다음과 같이 802.1X 및 MAB에 대한 IOS Flex-Auth 인증을 구성합니다.
authentication order dot1x mab
authentication priority dot1x mab

단계 **9** 다음과 같이 스위치 포트에서 802.1X 포트 제어를 활성화합니다.
authentication port-control auto
authentication violation restrict

단계 **10** 다음과 같이 MAB(MAC Authentication Bypass)를 활성화합니다.
mab

단계 **11** 다음과 같이 스위치 포트에서 802.1X를 활성화합니다.
dot1x pae authenticator

단계 **12** 다음과 같이 재전송 기간을 10초로 설정합니다.
dot1x timeout tx-period *10*

참고 802.1X tx-period 시간 초과는 10초로 설정해야 합니다. 결과에 대해 잘 알고 있는 경우가 아니면 이 값을 변경하지 마십시오.

단계 **13** portfast 기능을 활성화합니다.
spanning-tree portfast

ID 기반 네트워킹 서비스를 기반으로 802.1X를 활성화하는 명령

다음 예에서는 802.1X, MAB 및 웹 인증을 사용하는 순차적 인증 방법을 허용하도록 구성된 제어 정책을 보여줍니다.

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

```
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
!


policy-map type control subscriber DOT1XMAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
   30 authorize
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
!
```

다음 예에서는 MAB, 802.1X 및 웹 인증을 사용하는 순차적 인증 방법을 허용하도록 구성된 제어 정책을 보여줍니다.

```
policy-map type control subscriber MABDOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
   20 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class ALL_FAILED do-until-failure
   10 authentication-restart 60
 event authentication-success match-all
  10 class DOT1X do-until-failure
   10 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

인터페이스에서 서비스 정책 적용:

```
interface GigabitEthernet1/0/4
 switchport mode access
 device-tracking attach-policy pol1
 ip access-group sample in
 authentication timer reauthenticate server
 access-session port-control auto
 mab
```

```
dot1x pae authenticator
dot1x timeout tx-period 10
dot1x timeout auth-period 10
spanning-tree portfast
service-policy type control subscriber DOT1XMAB
```

EPM 로깅을 활성화하는 명령

Cisco ISE 기능에 대해 사용 가능한 문제 해결 및 기록을 지원하려면 스위치에서 표준 로깅 기능을 설정합니다.

epm logging

SNMP 트랩을 활성화하는 명령

스위치가 이 네트워크 세그먼트에서 적절한 VLAN을 통해 Cisco ISE로부터 전송되는 SNMP 트랩을 수신할 수 있는지 확인합니다.

snmp-server community public RO

snmp-server trap-source *<VLAN_number>*

프로파일링을 위해 SNMP v3 쿼리를 활성화하는 명령

다음 명령을 사용하여 Cisco ISE 프로파일링 서비스를 지원하기 위해 SNMP v3 폴링이 올바르게 수행되도록 하려면 스위치를 구성합니다. 그 전에는 **SNMP Settings(SNMP** 설정**)** 창의 Cisco ISE GUI에서 SNMP 설정을 구성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add | Edit(**추가 | 편집**)** > **SNMP Settings(SNMP** 설정**)**입니다.

Snmp-server user *<name> <group>* **v3 auth md5** *<string>* **priv des** *<string>*

snmp-server group *<group>* **v3 priv**

snmp-server group *<group>* **v3 priv context***vlan-1*

참고 각 상황 정보에 대해 **snmp-server group** *<group>* **v3 priv context** *vlan-1* 명령을 구성해야 합니다. **snmp show context** 명령은 모든 상황 정보를 나열합니다.

연결 문제가 없는데 SNMP 요청 시간이 초과되는 경우에는 시간 초과 값을 늘릴 수 있습니다.

프로파일러가 수집하도록 할 **MAC** 알림 트랩을 활성화하는 명령

Cisco ISE 프로파일러 기능이 네트워크 엔드포인트에서 정보를 수집할 수 있도록 적절한 MAC 알림 트랩을 전송하려면 스위치를 구성합니다.

```
mac address-table notification change

mac address-table notification mac-move

snmp trap mac-notification change added

snmp trap mac-notification change removed
```

스위치에서의 **RADIUS** 유휴 시간 초과 컨피그레이션

스위치에서 RADIUS 유휴 시간 초과를 구성하려면 다음 명령을 사용합니다.

```
Switch(config-if)# authentication timer inactivity
```

여기서 *inactivity*는 클라이언트 활동이 권한이 부여되지 않은 활동으로 간주될 때까지의 비활성 간격(초)입니다.

Cisco ISE에서는 세션 비활성 타이머가 적용되어야 하는 모든 권한 부여 정책에 대해 이 옵션을 활성화할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

iOS 신청자 프로비저닝을 위한 무선 **LAN** 컨트롤러 컨피그레이션

단일 **SSID**용

Apple iOS 기반 디바이스(iPhone 또는 iPad)가 동일한 무선 액세스 포인트에서 SSID 간을 전환할 수 있도록 지원하려면 **FAST SSID change** 기능을 활성화하도록 무선 컨트롤러를 구성해야 합니다. 이 기능을 사용하면 iOS 기반 디바이스가 SSID 간을 보다 빠르게 전환할 수 있습니다.

듀얼 **SSID BYOD**용

이중 SSID BYOD를 지원하려면 고속 SSID를 활성화해야 합니다. 고속 SSID 변환이 활성화되면 무선 컨트롤러를 통해 클라이언트가 SSID 사이를 빠르게 이동할 수 있습니다. 고속 SSID가 활성화되면 클

라이언트 항목이 지워지지 않고 지연이 적용되지 않습니다. Cisco Wireless Controller에서 고속 SSID를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless Controller 컨피그레이션 가이드를 참조하십시오.

무선 컨트롤러 구성 예

```
WLC (config)# FAST SSID change
```

일부 Apple iOS 기반 디바이스에서는 무선 네트워크에 연결을 시도하는 동안 다음 오류 메시지가 표시될 수 있습니다.

```
Could not scan for Wireless Networks.(무선 네트워크를 스캔할 수 없습니다.)
```

이 오류 메시지는 디바이스 인증에 영향을 주지 않으므로 무시해도 됩니다.

모바일 디바이스 관리 상호운용성을 위해 무선 LAN 컨트롤러에서 ACL 구성

미등록 디바이스 및 인증서 프로비저닝을 리디렉션하려면 권한 부여 정책에 사용할 ACL을 무선 컨트롤러에서 구성해야 합니다. ACL의 순서는 다음과 같이 지정해야 합니다.

단계 **1** 서버에서 클라이언트로의 모든 아웃바운드 트래픽을 허용합니다.

단계 **2** (선택 사항) 문제 해결용으로 클라이언트에서 서버로의 ICMP 클라이언트 인바운드 트래픽을 허용합니다.

단계 **3** 미등록/규정 미준수 디바이스에 대해 MDM 에이전트를 다운로드하고 규정 준수 확인을 진행할 수 있도록 MDM 서버 액세스를 허용합니다.

단계 **4** 웹 포털과 supplicant 및 인증서 프로비저닝 플로우에 대해 클라이언트->서버->Cisco ISE로의 모든 인바운드 트래픽을 허용합니다.

단계 **5** 이름 확인용으로 클라이언트에서 서버로의 인바운드 DNS 트래픽을 허용합니다.

단계 **6** IP 주소용으로 클라이언트에서 서버로의 인바운드 DHCP 트래픽을 허용합니다.

단계 **7** 회사 정책에 따른 Cisco ISE로의 리디렉션용으로 클라이언트->서버->회사 리소스로의 모든 인바운드 트래픽을 거부합니다.

단계 **8** (선택 사항) 나머지 트래픽을 허용합니다.

예

다음 예제에서는 미등록 디바이스를 BYOD 흐름으로 리디렉션하기 위한 ACL을 보여 줍니다. 이 예제에서 Cisco ISE IP 주소는 10.35.50.165, 내부 회사 네트워크 IP 주소는 192.168.0.0 및 172.16.0.0(리디렉션용), MDM 서버 서브넷은 204.8.168.0입니다.

그림 ***1:*** 미등록 디바이스 리디렉션용 ***ACL***

General

Access List Name: NSP-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819