# Catalyst 3750系列交換器上的ISE流量重新導向

## 目錄



## 簡介

本文介紹使用者流量重新導向如何運作，以及交換器重新導向封包所需的條件。

## 必要條件

### 需求

思科建議您具有思科身份服務引擎(ISE)配置經驗，並瞭解以下主題的基本知識：

- ISE部署和中央Web驗證(CWA)流程
- Cisco Catalyst交換機的CLI配置

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7
- Cisco Catalyst 3750X系列交換器軟體版本15.0及更新版本
- ISE軟體1.1.4及更新版本

# 背景資訊

對於大多數使用ISE的部署，交換機上的使用者流量重定向是一個關鍵元件。所有這些流量都涉及交換機使用流量重定向：

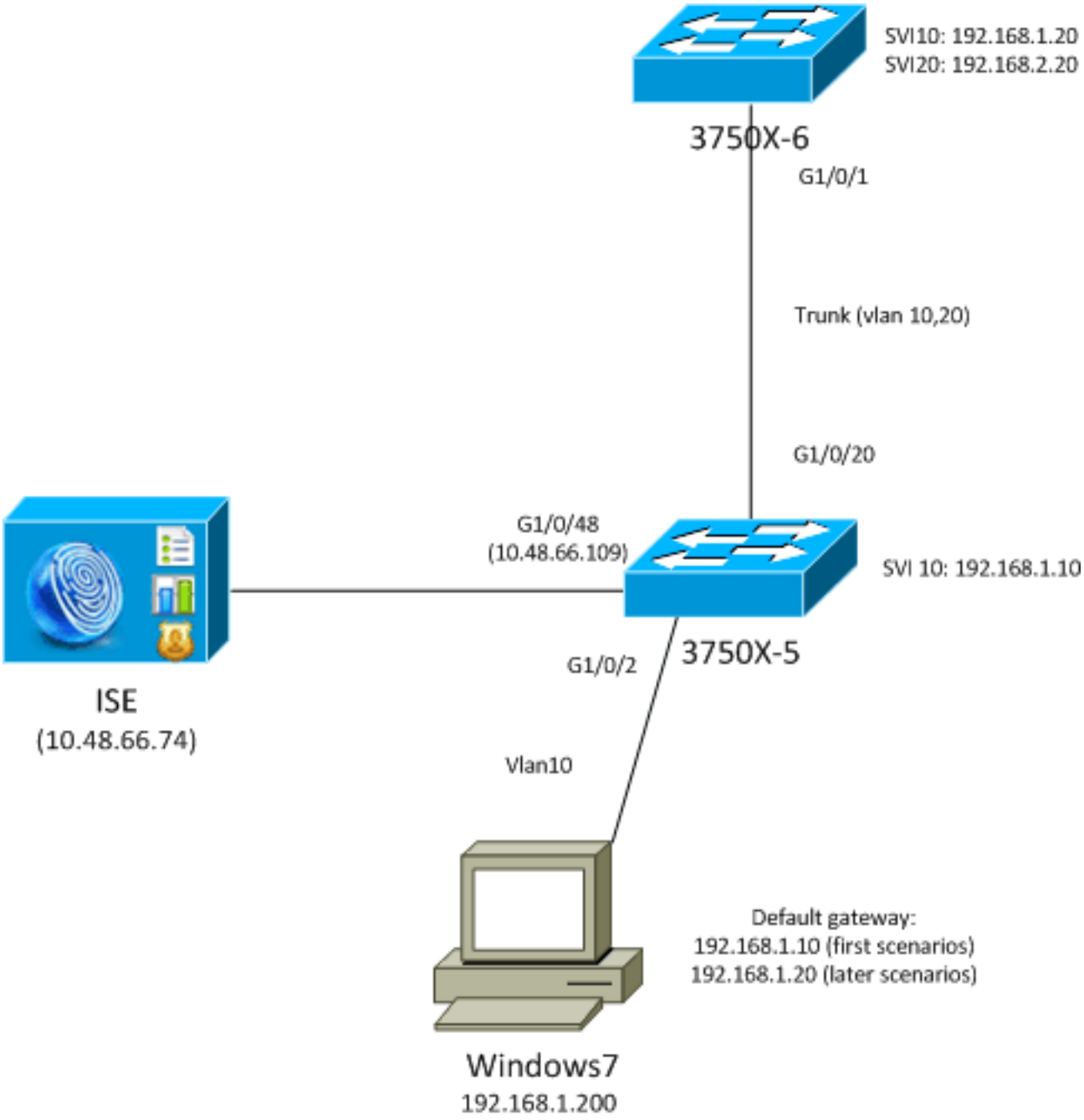
- CWA
- 使用者端布建(CPP)
- 裝置註冊(DRW)
- 本機請求方調配(NSP)
- 流動裝置管理(MDM)

錯誤配置的重定向是部署存在多個問題的原因。典型的結果是網路准入控制(NAC)代理無法正確彈出或無法顯示訪客門戶。

如果交換器沒有與使用者端VLAN相同的交換器虛擬介面(SVI)，請參閱前三個範例。

# 疑難排解

## 測試方案




在客戶端上執行測試，應將客戶端重定向到ISE進行調配(CPP)。 使用者是透過MAC驗證略過(MAB)或802.1x進行驗證。ISE使用重定向訪問控制清單(ACL)名稱(REDIRECT_POSTURE)和重定向URL（重定向到ISE）返回授權配置檔案：

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
    URL Redirect ACL:  REDIRECT_POSTURE
```

```
        URL Redirect:  https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D5D015F1B47
     Acct Session ID:  0x00011D90
              Handle:  0xBB000D5E

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

可下載ACL(DACL)會允許此階段的所有流量：

```
bsns-3750-5#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1 (per-user)
   10 permit ip any any
```

重新導向ACL允許此流量而不進行重新導向：

- 到ISE的所有流量(10.48.66.74)
- 網域名稱系統(DNS)和網際網路控制訊息通訊協定(ICMP)流量

所有其他流量都應重新導向：

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
   30 deny icmp any any (10 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

交換器與使用者位於同一VLAN中的SVI:

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
```

在接下來的部分中，將對此進行修改以顯示潛在的影響。

## 流量無法到達重新導向ACL

當您嘗試ping任何主機時，應該會收到回應，因為該流量沒有重新導向。若要確認，請運行此調試：

```
debug epm redirect
```

對於客戶端傳送的每個ICMP資料包，調試應顯示：

```
Jan 9 09:13:07.861: epm-redirect:IDB=GigabitEthernet1/0/2: In
epm_host_ingress_traffic_qualify ...
Jan 9 09:13:07.861: epm-redirect:epm_redirect_cache_gen_hash:
IP=192.168.1.201 Hash=562
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: CacheEntryGet Success
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: Ingress packet on
[idb= GigabitEthernet1/0/2] didn't match with [acl=REDIRECT_POSTURE]
```

若要確認，請檢查ACL:

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
    30 deny icmp any any (4 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

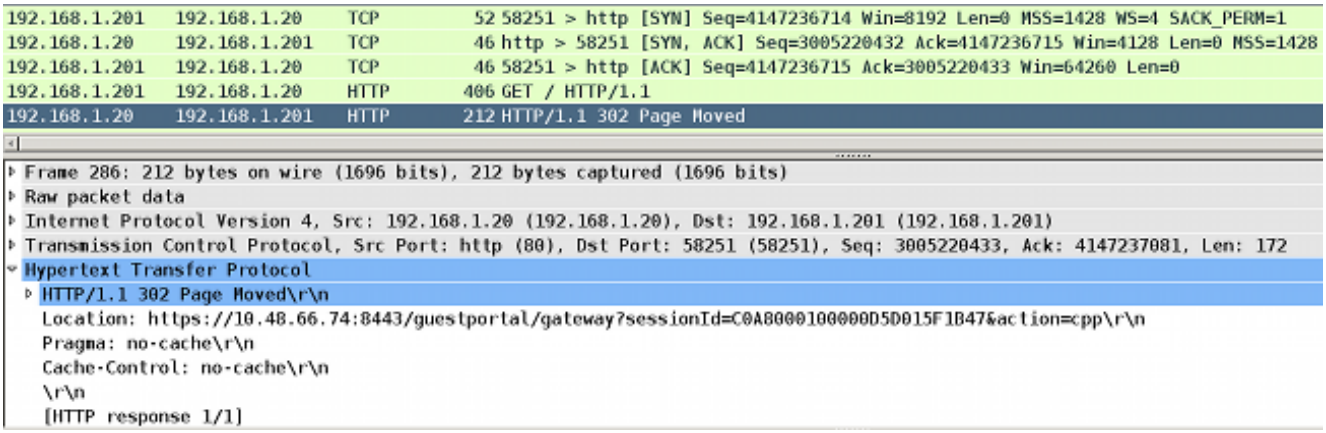
## 流量達到重新導向ACL

### 案例1 — 目的地主機位於同一個VLAN中，且存在，且為SVI 10 UP

當您向交換機直接到達第3層(L3)的IP地址（交換機的網路具有SVI介面）發起流量時，會發生以下情況：

1. 使用者端對同一VLAN中的目的地主機(192.168.1.20)發起位址解析通訊協定(ARP)解析要求，並接收回應（ARP流量永遠不會重新導向）。

2. 交換器會攔截該作業階段，即使交換器上未設定目的地IP位址也是如此。客戶端與交換機之間的TCP握手已完成。在這個階段，沒有其它資料包在交換機外部傳送。在此案例中，使用者端(192.168.1.201)已啟動與位於該VLAN(192.168.1.20)中的另一台主機的TCP作業階段，交換器的SVI介面為UP（IP位址為192.168.1.10）：




3. 建立TCP作業階段並傳送HTTP要求後，交換器會傳回具有重新導向至ISE（位置標頭）的HTTP回應。

   這些步驟由debug確認。有幾個ACL命中：

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2]
matched with [acl=REDIRECT_POSTURE]
epm-redirect:Fill in URL=https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp for redirection
epm-redirect:IP=192.168.1.201: Redirect http request to https:
//10.48.66.74:8443/guestportal/gateway?sessionId=C0A8000100000D5D015F1B47&action=cpp
epm-redirect:EPM HTTP Redirect Daemon successfully created
```

這也可以通過更詳細的調試得到證實：

```
debug ip http all

http_epm_http_redirect_daemon: got redirect request
HTTP: token len 3: 'GET'
http_proxy_send_page: Sending http proxy page
http_epm_send_redirect_page: Sending the Redirect page to ...
```

4. 客戶端直接連線到ISE(安全套接字層(SSL)會話到10.48.66.74:8443)。 此封包不會觸發重新導向：

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] didn't
match with [acl=REDIRECT_POSTURE]
```

**附註**：交換器會攔截作業階段，因此可以使用嵌入式封包擷取(EPC)在交換器上擷取流量。 上次捕獲是在交換機上使用EPC進行的。

### 案例2 — 目的地主機位於同一個VLAN中，不存在，且為SVI 10 UP

如果目的主機192.168.1.20關閉（沒有響應），客戶端不會收到ARP應答（交換機不會攔截ARP），客戶端也不會傳送TCP SYN。永遠不會發生重新導向。

這就是為什麼NAC代理使用預設網關進行發現。預設網關應始終響應並觸發重定向。

### 案例3 — 目的地主機位於不同的VLAN中，且存在，且為SVI 10 UP

以下是在這種情況下會發生的情況：

1. 客戶端嘗試訪問HTTP://8.8.8.8。
2. 該網路不在交換機的任何SVI上。
3. 客戶端向預設網關192.168.1.10（已知目標MAC地址）傳送該會話的TCP SYN。
4. 重新導向的觸發方法與第一個範例完全相同。
5. 交換機會攔截該會話並返回重定向到ISE伺服器的HTTP響應。
6. 客戶端訪問ISE伺服器時不會出現問題（流量沒有重定向）。

**附註**：預設網關是位於同一台交換機上還是位於上游裝置上，都無所謂。僅需要從該網關接收ARP響應才能觸發重定向過程。此外，有必要允許通過預設網關的ISE可訪問性。如果防火牆位於補丁上，請特別注意，尤其是如果防火牆是第2層(L2)防火牆，並且L2資料包經過不同的鏈路（則可能需要在防火牆上繞過TCP狀態）。

### 案例4 — 目的地主機位於不同的VLAN中，不存在，且為SVI 10 UP

此案例與案例3完全相同。無論遠端VLAN中的目的地主機是否存在，此案例均無關。

### 案例5 — 目的地主機位於不同的VLAN中，且存在，且SVI 10已關閉

如果交換器與使用者端不在同一VLAN中設有SVI UP，則它仍可執行重新導向，但只有在符合特定條件時才能執行。

交換機的問題是如何從不同的SVI將響應返回給客戶端。很難確定應使用哪個源MAC地址。

此流程與SVI為UP時不同：

1. 使用者端將TCP SYN傳送到不同VLAN(192.168.2.20)中的主機，其中目的地MAC位址設定為在上游交換器上定義的預設閘道。此封包抵達重新導向ACL，如偵錯所示。
2. 交換器會驗證是否有傳回使用者端的路由。請記住，SVI 10已關閉。
3. 如果交換器沒有另一個具有傳回使用者端的路由的SVI，即使企業策略管理器(EPM)日誌指示已到達ACL，該資料包也不會被攔截或重定向。遠端主機可能傳回SYN ACK，但交換器沒有傳回使用者端(VLAN10)的路由且捨棄封包。封包無法僅交換回(L2)，因為它已到達重新導向ACL。
4. 如果交換器確實具有透過不同SVI到達使用者端VLAN的路由，便會攔截該封包並照常執行重新導向。使用URL-redirect的回應不會直接傳送到使用者端，而是會根據路由決定透過不同的交換器/路由器。

注意這裡的不對稱性：

- 從客戶端接收的流量被交換機本地攔截。
- 基於該路由，通過上游交換機傳送包括該HTTP重定向的響應。
- 這時，防火牆可能會發生典型問題，且需要TCP略過。
- 到ISE的流量（未被重定向）是對稱的。只有重定向本身是非對稱的。

### 案例6 — 目的地主機位於不同的VLAN中，不存在，且SVI 10已關閉

此案例與案例5完全相同。無論遠端主機是否存在。正確的路由非常重要。

### 案例7 - HTTP服務已關閉

如案例6所示，交換器上的HTTP程式非常重要。如果已停用HTTP服務，EPM會顯示封包到達重新導向ACL:

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] matched
with [acl=REDIRECT_POSTURE]
```

但是重新導向永遠不會發生。

HTTP重定向不要求交換機上的HTTPS服務，但HTTPS重定向需要該服務。NAC代理可以將兩者用於ISE發現。因此，建議同時啟用兩者。

### 重定向ACL — 協定和埠不正確，無重定向

請注意，交換器只能攔截在標準連線埠上運作的HTTP或HTTPS流量（TCP/80和TCP/443）。 如果HTTP/HTTPS在非標準埠上運行，則可以使用**ip port-map http**命令進行配置。此外，交換機的HTTP伺服器必須偵聽該埠(**ip http埠**)。

## 相關資訊

- 使用交換機和身份服務引擎進行中央Web身份驗證的配置示例
- 思科身份服務引擎使用手冊，版本1.2
- 技術支援與文件 - Cisco Systems