27429 VIEWS 175 HELPFUL 12 REPLIES

Nathan Spitzer Beginner 01-05-2011 09:40 AM

DHCP Snooping

Scenerio:

As part of a tech refresh project at a large campus and due to several issues caused by (I)users plugging in home routers to the network and causing DHCP issues I am looking to enable DHCP snooping. During the tech refresh the access switches will be upgraded first then the core. The new access switches are 4510R+E/Sup7 running latest IOS XE base license and only doing switching . The new cores are 6509 Sup 720's configured as a VSS cluster, handle all the routing for VLANS and have the IP helper statements. The DHCP server that supports all the VLANS is a Windows 2008 server directly connected to the core.

I have also read all the info I could find on DHCP snooping but am still a little fuzzy about if it changes how the DHCP server handles requests.

Questions:

- Given that the access switches are only switching, they only need DHCP snooping turned on (both globally and on the VLANS) and their uplinks to the core set as trusted, right? In particular they dont need IP helper statements or layer-3 interfaces for all of their VLANS, right?
- While I understand that DHCP snooping will only be marginally effective if it is not turned on on the core, there is no reason I cannot deploy it first at the access layer without touching the core configurations to avoid large amounts of change-control paperwork, right? Then when the core is upgraded and DHCP snooping properly enabled it will work.
- I got that on the access layer switches the uplinks to the core are trusted, but I am not 100% on whether the same interfaces are trusted on the cores. I dont think so but want to be sure. Of cource the cores do trust the actual interface the DHCP server is plugged in on
- The most confusing part is all the Option-82 stuff. As near as I can tell its optional for the server to

use the Option-82 information. I believe that if all I do is turn DHCP snooping on globally and on the right VLANS the DHCP relaying between the core and the DHCP server will continue working just like it is today, is that correct?

Are there really any gotchas to this or in my case do I really just need to turn it on globally and per vlan, trust the uplinks on the acccess switches and the DHCP server interface on the core and call it a day?

Thanks

Nathan Spitzer

Sr. Network Communications Analyst

Lockheed Martin

Solved! Go to Solution.

Other Switching

Everyone's tags (2)

dhcp snooping

I have this problem too

5 Helpful

Reply

1 ACCEPTED SOLUTION

Peter Paluch Hall of Fame Cisco Employee

01-06-2011 01:54 AM

✔ Re: DHCP Snooping

Hello Nathan,

> Given that the access switches are only switching, they only need DHCP snooping turned on (both globally and on the VLANS) and their uplinks to the core set as trusted, right?

Correct.

```
In particular they dont need IP helper statements or layer-3 interfaces for all of their
VLANS, right?
```

Correct. The **ip helper-address** statement would be necessary only if the switches were performing inter-VLAN routing and the DHCP server was located in a different VLAN.

```
While I understand that DHCP snooping will only be marginally effective
if it is not turned on on the core, there is no reason I cannot deploy
it first at the access layer without touching the core configurations to
 avoid large amounts of change-control paperwork, right? Then when the
core is upgraded and DHCP snooping properly enabled it will work.
```

To my best knowledge, the contrary is true. The DHCP Snooping is **an access layer protection service** - it does not belong into the core of the network. There is nothing to protect in the core once the DHCP messages have beein properly sanitized at the network boundary. For some inexplicable reason, many people think that the DHCP Snooping must be activated throughout the network. The fact is that the DHCP Snooping protects from

- DHCP messages being sent to ineligible devices
- Ineligible devices posing as DHCP servers

From this it naturally follows that it is the network boundary, or the access layer, where this protection is most effective. So in your case, I believe that activating the DHCP Snooping **only** on the access layer is actually what you want to do.

```
I got that on the access layer switches the uplinks to the core are
trusted, but I am not 100% on whether the same interfaces are trusted on
 the cores. I dont think so but want to be sure. Of cource the cores do
trust the actual interface the DHCP server is plugged in on
```

If you planned to activate the DHCP Snooping on the core devices then the uplinks between the access and core switches would need to be configured as trusted both on the core and access switches. Otherwise, the core ports would drop DHCP messages received from clients because the access layer switches running DHCP Snooping insert the DHCP Option 82 into the sanitized DHCP messages, and untrustred ports drop all DHCP messages that have Option 82 present.

From the 2960 Configuration Guide at

http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swdhcp82.html#wp1078853

The switch drops a DHCP packet when one of these situations occurs:

- *A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or*

DHCPLEASEQUERY packet, is received from outside the network or firewall.

- *A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.*
- *The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.*
- *A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.*

As I indicated, however, I personally discourage running the DHCP Snooping on core devices - I see no reason for that. Please correct if I am wrong here!

```
The most confusing part is all the Option-82 stuff. As near as I can
tell its optional for the server to use the Option-82 information. I
believe that if all I do is turn DHCP snooping on globally and on the
right VLANS the DHCP relaying between the core and the DHCP server will
continue working just like it is today, is that correct?
```

LOL, my favourite stuff about the DHCP Snooping is the Option 82 Interesting how much confusion this topic brings...

The Option 82 was originally created in order to provide the DHCP relay agent the ability to identify itself and the client that sent the original unmodified DHCP message. The DHCP server then may use this information to perform some special assignment policies to the client. The format of the Option 82 is not strictly specified, only its basic structure is fixed. You can read more about it and all the rationale in the RFC 3046. One of the key points to remember here, however, is that the DHCP server may or may not recognize the Option 82, but regardless of that, it has to copy the value of the Option 82 received in a client's DHCP message to all its replies sent to that client.

The DHCP Snooping uses the Option 82 differently. It **does not expect nor require** that the DHCP server understands the Option 82 or handles it in the special way. The Option 82 is inserted by the access switches performing the DHCP Snooping and it contains two important parts:

- The Circuit ID that identifies the **port** to which the client is connected (the VLAN and the physical port location in a switch)
- The Remote ID that identifies **the access switch** to which the client is connected (by the MAC address of the switch)

See http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swdhcp82.html#wp1105589

Now, when an access switch performing the DHCP Snooping receives a DHCP client message on an untrusted port, this will happen:

- The switch will insert the Option 82 into the client's DHCP message. The Option 82 will identify the particular switch and the port where the client is attached
- The switch will forward the DHCP message according to its destination MAC address (i.e. in a completely normal way)
- The server will receive the DHCP message containing the Option 82. It is irrelevant to DHCP Snooping whether the server takes the value of the Option 82 into consideration. However, when the server replies, it will insert the original value of the Option 82 to the response.
- The access switch will eventually receive the DHCP response. By looking at the Option 82, it knows exactly through which port shall the message be forwarded back to the client – and only to the client – even if the response was broadcasted!

Note that the Option 82 helps tremendously to exactly identify the access switch and its port where the client is attached. If other switches with DHCP Snooping received this DHCP message (because of flooding or because of broadcast addressing requested by the client), they would drop this message because they would understand after looking at the Option 82 that the client is attached elsewhere. The Option 82 thereby helps to assure that the DHCP communication between a particular client and DHCP server will not leak to other clients.

There is one gotcha related to the Option 82. A switch performing DHCP Snooping inserts the Option 82 into the DHCP messages from clients. However, each DHCP message contains a field called GIADDR where the IP address of the relay agent is recorded if the DHCP message was relayed. Clearly, when a DHCP message passes through a DHCP Snooping switch, it is not relayed (i.e. taken from one VLAN and rerouted into another), so an access switch does not modify the GIADDR field which remains set to 0.0.0.0. However, at least the Cisco DHCP Server implementation in IOS performs a sanity check on received DHCP messages and it **drops DHCP messages that contain the Option 82 but whose GIADDR field is set to 0.0.0.0 (i.e. unitialized)**. This can be seen the **debug ip dhcp server packet** output:

```
Router# debug ip dhcp server packet
*Sep 9 01:59:40: DHCPD: inconsistent relay information.
*Sep 9 01:59:40: DHCPD: relay information option exists, but giaddr is zero
```

Under normal circumstances, such a sanity check is logical – how come that a DHCP message contains the Option 82 (i.e. the DHCP Relay Agent Information Option) when there is no DHCP Relay identified in the GIADDR field? However, with the DHCP Snooping on access layer switches, such DHCP messages are normal and expected. Therefore, it is necessary to deactivate this sanity check on the Cisco box that is running the DHCP server using either the global configuration command **ip dhcp relay information trust-all** or only on selected routed (i.e. L3) interfaces using the interface level command **ip dhcp relay information trusted**.

To sum it up:

- The Option 82 is A Good Thing (TM) because it helps to deliver the DHCP messages only to the client for which they are intended. All suggestions to deactivate the insertion of the Option 82 on

access switches running DHCP Snooping are junk The Option 82 is inserted by DHCP Snooping switches into DHCP messages by default - no extra configuration is needed.

- Go through the most straightforward way - when deploying the DHCP Snooping, do not initially modify anything regarding the Option 82. Verify whether your clients can receive their IP config via DHCP. If yes then there is nothing more to tweak. Otherwise, proceed further.
- If you are running a DHCP server on an IOS-based device (router, switch), you may need to use the command **ip dhcp relay information trust-all** (global config) or **ip dhcp relay information trusted** (interface level) to allow the DHCP messages with the added Option 82 and unitialized GIADDR field to be accepted. These commands are necessary **only** on the device where the DHCP server is running, not on the access layer switches. You may want first to perform the debug as I suggested earlier, and only if you see that the packets are being dropped, add these commands to the configuration.
- I am not sure if these commands have to be added also to a switch performing DHCP Relay function - I may verify that tomorrow in a lab.
- If you are using a different DHCP server you have to try it experimentally whether it is happy with DHCP messages having Option 82 present and GIADDR field unitialized

Sorry for the lengthy answer... I hope I did not bore you to death. You are welcome to ask further! I'll try to be more concise the next time

Best regards,

Peter

View solution in original post

Everyone's tags (2)

dhcp snooping

165 Helpful

Reply

12 REPLIES

Peter Paluch Hall of Fame Cisco Employee 01-06-2011 01:54 AM

✔ Re: DHCP Snooping

Hello Nathan,

> Given that the access switches are only switching, they only need DHCP snooping turned on (both globally and on the VLANS) and their uplinks to the core set as trusted, right?

Correct.

```
In particular they dont need IP helper statements or layer-3 interfaces for all of their
VLANS, right?
```

Correct. The **ip helper-address** statement would be necessary only if the switches were performing inter-VLAN routing and the DHCP server was located in a different VLAN.

```
While I understand that DHCP snooping will only be marginally effective
if it is not turned on on the core, there is no reason I cannot deploy
it first at the access layer without touching the core configurations to
 avoid large amounts of change-control paperwork, right? Then when the
core is upgraded and DHCP snooping properly enabled it will work.
```

To my best knowledge, the contrary is true. The DHCP Snooping is **an access layer protection service** - it does not belong into the core of the network. There is nothing to protect in the core once the DHCP messages have beein properly sanitized at the network boundary. For some inexplicable reason, many people think that the DHCP Snooping must be activated throughout the network. The fact is that the DHCP Snooping protects from

- DHCP messages being sent to ineligible devices
- Ineligible devices posing as DHCP servers

From this it naturally follows that it is the network boundary, or the access layer, where this protection is most effective. So in your case, I believe that activating the DHCP Snooping **only** on the access layer is actually what you want to do.

```
I got that on the access layer switches the uplinks to the core are
trusted, but I am not 100% on whether the same interfaces are trusted on
 the cores. I dont think so but want to be sure. Of cource the cores do
trust the actual interface the DHCP server is plugged in on
```

If you planned to activate the DHCP Snooping on the core devices then the uplinks between the access and core switches would need to be configured as trusted both on the core and access switches. Otherwise, the core ports would drop DHCP messages received from clients because the access layer switches running DHCP Snooping insert the DHCP Option 82 into the sanitized DHCP messages, and untrustred ports drop all DHCP messages that have Option 82 present.

From the 2960 Configuration Guide at

http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swdhcp82.html#wp1078853

The switch drops a DHCP packet when one of these situations occurs:

- *A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.*

- *A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.*

- *The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.*

- *A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.*

As I indicated, however, I personally discourage running the DHCP Snooping on core devices - I see no reason for that. Please correct if I am wrong here!

```
The most confusing part is all the Option-82 stuff. As near as I can
tell its optional for the server to use the Option-82 information. I
believe that if all I do is turn DHCP snooping on globally and on the
right VLANS the DHCP relaying between the core and the DHCP server will
continue working just like it is today, is that correct?
```

LOL, my favourite stuff about the DHCP Snooping is the Option 82 Interesting how much confusion this topic brings...

The Option 82 was originally created in order to provide the DHCP relay agent the ability to identify itself and the client that sent the original unmodified DHCP message. The DHCP server then may use this information to perform some special assignment policies to the client. The format of the Option 82 is not strictly specified, only its basic structure is fixed. You can read more about it and all the rationale in the RFC 3046. One of the key points to remember here, however, is that the DHCP server may or may not recognize the Option 82, but regardless of that, it has to copy the value of the Option 82 received in a client's DHCP message to all its replies sent to that client.

The DHCP Snooping uses the Option 82 differently. It **does not expect nor require** that the DHCP server understands the Option 82 or handles it in the special way. The Option 82 is inserted by the access switches performing the DHCP Snooping and it contains two important parts:

- The Circuit ID that identifies the **port** to which the client is connected (the VLAN and the physical port location in a switch)
- The Remote ID that identifies **the access switch** to which the client is connected (by the MAC address of the switch)

See http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swdhcp82.html#wp1105589

Now, when an access switch performing the DHCP Snooping receives a DHCP client message on an untrusted port, this will happen:

- The switch will insert the Option 82 into the client's DHCP message. The Option 82 will identify the particular switch and the port where the client is attached
- The switch will forward the DHCP message according to its destination MAC address (i.e. in a completely normal way)
- The server will receive the DHCP message containing the Option 82. It is irrelevant to DHCP Snooping whether the server takes the value of the Option 82 into consideration. However, when the server replies, it will insert the original value of the Option 82 to the response.
- The access switch will eventually receive the DHCP response. By looking at the Option 82, it knows exactly through which port shall the message be forwarded back to the client - and only to the client - even if the response was broadcasted!

Note that the Option 82 helps tremendously to exactly identify the access switch and its port where the client is attached. If other switches with DHCP Snooping received this DHCP message (because of flooding or because of broadcast addressing requested by the client), they would drop this message because they would understand after looking at the Option 82 that the client is attached elsewhere. The Option 82 thereby helps to assure that the DHCP communication between a particular client and DHCP server will not leak to other clients.

There is one gotcha related to the Option 82. A switch performing DHCP Snooping inserts the Option 82 into the DHCP messages from clients. However, each DHCP message contains a field called GIADDR where the IP address of the relay agent is recorded if the DHCP message was relayed. Clearly, when a DHCP message passes through a DHCP Snooping switch, it is not relayed (i.e. taken from one VLAN and rerouted into another), so an access switch does not modify the GIADDR field which remains set to 0.0.0.0. However, at least the Cisco DHCP Server implementation in IOS performs a sanity check on received DHCP messages and it **drops DHCP messages that contain the Option 82 but whose GIADDR field is set to 0.0.0.0 (i.e. unitialized)**. This can be seen the **debug ip dhcp server packet** output:

```
Router# debug ip dhcp server packet
*Sep 9 01:59:40: DHCPD: inconsistent relay information.
*Sep 9 01:59:40: DHCPD: relay information option exists, but giaddr is zero
```

Under normal circumstances, such a sanity check is logical - how come that a DHCP message contains the Option 82 (i.e. the DHCP Relay Agent Information Option) when there is no DHCP Relay identified in the GIADDR field? However, with the DHCP Snooping on access layer switches, such DHCP messages are normal and expected. Therefore, it is necessary to deactivate this sanity check on the Cisco box that is running the DHCP server using either the global configuration command **ip dhcp relay information trust-all** or only on selected routed (i.e. L3) interfaces using the interface level command **ip dhcp relay information trusted**.

To sum it up:

- The Option 82 is A Good Thing (TM) because it helps to deliver the DHCP messages only to the client for which they are intended. All suggestions to deactivate the insertion of the Option 82 on access switches running DHCP Snooping are junk The Option 82 is inserted by DHCP Snooping switches into DHCP messages by default - no extra configuration is needed.
- Go through the most straightforward way - when deploying the DHCP Snooping, do not initially modify anything regarding the Option 82. Verify whether your clients can receive their IP config via DHCP. If yes then there is nothing more to tweak. Otherwise, proceed further.
- If you are running a DHCP server on an IOS-based device (router, switch), you may need to use the command **ip dhcp relay information trust-all** (global config) or **ip dhcp relay information trusted** (interface level) to allow the DHCP messages with the added Option 82 and unitialized GIADDR field to be accepted. These commands are necessary **only** on the device where the DHCP server is running, not on the access layer switches. You may want first to perform the debug as I suggested earlier, and only if you see that the packets are being dropped, add these commands to the configuration.
- I am not sure if these commands have to be added also to a switch performing DHCP Relay function - I may verify that tomorrow in a lab.
- If you are using a different DHCP server you have to try it experimentally whether it is happy with DHCP messages having Option 82 present and GIADDR field unitialized

Sorry for the lengthy answer... I hope I did not bore you to death. You are welcome to ask further! I'll try to be more concise the next time

Best regards,

Peter

View solution in original post

Everyone's tags (2)

dhcp snooping

165 Helpful Reply

Nathan Spitzer Beginner 01-06-2011 05:46 AM

Re: DHCP Snooping

First, thanks a lot for the long answers. It looks like I mostly got it but as I suspected there were a few subtleties I missed. Like you suspected, the main things I'm trying to protect against are stupid (I)users creating unauthorized DHCP servers. I have some labs that sometimes go "off the reservation" and play around or people think how smart they are and bring in a linksys router from home for more ethernet ports. I've chased several of these over the years.

The two main things I didnt put together were:

- The (access) switch will insert the Option 82 into the client's DHCP message. The Option 82 will identify the particular switch and the port where the client is attached

and

- *The switch drops a DHCP packet when...A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port*.

I didnt realise the access switches payed any attention to the option-82 information. Since they do, that is what prevents DHCP broadcasts from hopping from access-switch to access-switch, NOT the core filtering it (like I thought).Since my DHCP servers are not running on IOS I should not have any problems. I do have my test 3560 that I'm going to run some tests but thanks again for taking the time for a good complete answer.

Actually pretty slick!

0 Helpful Reply

mbazelenik Beginner 06-10-2016 03:35 AM

Hello, again everyone,

Hello, again everyone,

In my case I have two switches in the row and on both are AP's connected. The problem is that on the second one I can't get an IP if snooping is activated, the AP' on first are OK. SWITCHES ARE CONECTED WITH ETHER CHANNEL! This is very important!

Debug gives me this output and I just can't find any info what the heck is telling me exactly (these msg yust to be clear "if_input to Fa0/1") see below:

006082: Jun 10 12:08:52.720: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
006083: Jun 10 12:08:52.720: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Fa0/1, MAC da: ffff.ffff.ffff, MAC sa: d022.bec4.6809, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: d022.bec4.6809
006084: Jun 10 12:08:52.720: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
006085: Jun 10 12:08:56.167: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak. Was not set
006086: Jun 10 12:08:56.167: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak. Was Fa0/1

006087: Jun 10 12:08:56.167: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak. Was not set
006088: Jun 10 12:08:56.167: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
006089: Jun 10 12:08:56.167: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Fa0/1, MAC da: ffff.ffff.ffff, MAC sa: d022.bec4.6809, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: d022.bec4.6809
006090: Jun 10 12:08:56.167: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (10)
006091: Jun 10 12:09:04.548: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak. Was not set
006092: Jun 10 12:09:04.548: DHCPSNOOP(hlfm_set_if_input): Clearing if_input for pak. Was Fa0/1
006093: Jun 10 12:09:04.548: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak. Was not set
006094: Jun 10 12:09:04.548: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)

I also tried with these option-82 scenarios no succes obviouslly. Switches are conected over trunk ports, secured ports are also "uplinks" to DHCP (cisco router).

Anyway when I disable the snooping scenario on second swith the wifi client gets an IP. So I must be doing something wrong on current switch!

Some config info:

Uplink ports to other switch:

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode auto
 ip dhcp snooping trust
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode auto
 ip dhcp snooping trust

!

!

interface FastEthernet0/1
 description **** AP port *****
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

!

Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
  circuit-id default format: vlan-mod-port
  remote-id: 0022.0d61.8180 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface	Trusted	Allow option	Rate limit (pps)
GigabitEthernet0/1	yes	yes	unlimited
Custom circuit-ids:			
GigabitEthernet0/2	yes	yes	unlimited
Custom circuit-ids:			

How the client connection looks with the enabled snooping.

SSID [Public] :

MAC Address	IP address	IPV6 address	Device	Name	Parent	State
d022.bec4.6809	0.0.0.0	::	ccx-client	-	self	Assoc

Finally I found these info, which looks exactly like my problem!

http://jacob-network.com/3289/dhcp-dicover-failure-in-a-port-channel

Andrej

0 Helpful

Reply

blue phoenix Beginner

10-03-2016 07:16 AM

Hi Nathan,

Hi Nathan,

I don't know if this helps...

Just did a lab where I have a use vlan 30 on another switch block and a dhcp server in vlan 10(a router) on another switch block. The switch blocks communicate via the 2 core routers.

I have also the trouble of finding out where to enable the dhcp snooping feature. With hit and miss configs, what I did was enable this 3 global commands on the access switch on the user side or vlan 30 (it's an L3 switch because I need to enable the L0 interface for management).

ip dhcp snooping vlan 30
no ip dhcp snooping information option
ip dhcp snooping

and then enable ip dhcp snooping trust on the uplink port to the distribution switch.

interface Ethernet2/1
switchport trunk encapsulation dot1q
switchport mode trunk
ip dhcp snooping trust

From there, I would just remove ip add dhcp and again add ip add dhcp on the interface of my router that emulates as the pc of the user in vlan 30.

The router successfully acquire the IP address.

Is this the proper steps to implement this? No need to put ip dhcp snooping or ip dhcp snooping trust on the ports that connect to the DHCP server?.

Cheers,

0 Helpful

Reply

Julio Carvajal Advisor

12-17-2012 11:34 AM

DHCP Snooping

Hello Peter,

What a great answer. Man you rock....

Julio

Julio Carvajal
Senior Network Security and Core Specialist

0 Helpful Reply

Peter Paluch Hall of Fame Cisco Employee 12-17-2012 03:12 PM

Re: DHCP Snooping

Hello Julio,

Thank you very much - I am honored!

Best regards,

Peter

0 Helpful Reply

nir.fisher Beginner 06-12-2013 11:52 AM

DHCP Snooping

Hello peter ,

I have been looking at you answer because I am having some issues with my implementation of

Dhcp snooping at my netwrok.

First of all I must join everybody else and tell you that its wonderful to see how much you care and give such

greate answers and explanations .

I have a few questions myself

1. I understand that dhcp snooping is not needed in the core and best implemented at the access layer.

what about the aggregation layer ?.

2. I have 2960 at the access and nexus 5k at the aggregate and 7k at the core.

most user vlans are terminated at the nexus 5k switch but some vlans are terminated at a FW so its L2 from the access to the core which is connected to the FW. if I get you right you would recommend to implement dhcp snooping on the access vlans which are terminated at the aggregate ONLY on the access switches + add option 82 ?

3.about the other vlans which are terminated at the FW you would recommend to implement snooping on all switches at all 3 layers ?

4. If I add option 82 at the access layer I MUST configure the Downlinks from the aggregate to the access as Trusted ?

even though they are not ports leading to the DHCP server or the packet would be dropped.

5.I also have vlans at a VRF at the Nexus 5K , do you think there is any difference or things to pay attention ?

6. what debug commands could show me a packets has been dropped ? is there a way to generate syslog on dropped packets ?

thank you very much

0 Helpful Reply

markpawson Beginner 12-25-2012 11:55 AM

DHCP Snooping

Peter,

Thank you very much for this wonderful answer, that is very generous and kind of you.

Mark.

0 Helpful Reply

lisacoody Beginner

05-22-2013 09:02 AM

Re: DHCP Snooping

Thank you! Thank you! Thank you!

0 Helpful

Reply

Ketan Bheda Beginner

10-17-2017 03:12 AM

Re: DHCP Snooping

Hi Peter,

What are the chances of getting DHCP Snooped, if I have two core switches doing only switching and both are connected via etherchannel with the group of 5 trunk ports.

Here I apply trust command on those ports of Core on which my access switches are connected and then my users with that same switch.

Will I be getting snooped if I dint apply on those group of trunk ports which are used as etherchannel?

0 Helpful

Reply

thebradnet Beginner

01-31-2019 06:10 PM

Re: DHCP Snooping

That...was...awesome! I have I couldn't make sense of the Option 82 and this made total sense. I've watched two tutorials and read Cisco documentation. Nice job

0 Helpful

Reply

johann.aicher Beginner

04-18-2019 07:55 AM

Re: DHCP Snooping

Hi Peter,

great article. Thank you!

But with CAT 3650/3850 you get in troubles if you do not find out that it behaves like a Cisco router and not as an old stile

Catalyst Switch...

show ip dhcp relay information trusted-source

List of trusted sources of relay agent information option:

- NONE! Blank!

On all other CAT systems like 6500 / 6800 / 4500 / 3560... By default

show ip dhcp relay information trusted-source
All interfaces are trusted source of relay agent information option

If you use a CAT3650/3850 as a routing device for small offices with or without a local DHCP Server connected with IP-helper address on Vlans and you use a CAT 2960(S)/(X) as an access switih with DHCP snooping enabled - have fun and search for a solution!

On CAT3650/3850 you have to use the command: **ip dhcp relay information trust-all** to get it up and running.

Best regards

Johann

5 Helpful

Reply

Latest Contents

CCNA Command Summary

0 10

Created by JasperJamal42835 on 03-06-2020 07:24 AM

Taken fully from http://nusdsmhs.ss4.sharpschool.com/UserFiles/Servers/Server_41705/Image/CCNA%20IOS%20Commands%20Summary%2010-1-14.pdf Troubleshooting, Editing, Port #'s show ip interface brief (display interface designations, IP address a... view more

Cisco SDWAN Viptela - Everything about Certificates Deployme...

1 15

Created by Rajiv Yadav on 03-06-2020 01:34 AM

Hi All, After completing POCs and providing support to customers for Viptela, I got to know there are many Engineers who are confused about the certificates which need to be signed by the Root CA and also are not sure about the how to get the whitel... view more

Inline FW configuration help needed!

0 0

Created by Smorgan on 03-05-2020 12:38 PM

Hello! I am trying to put a FW 5506 inline (Routed Mode) between our corporate network and an ICS network controlled by a PLC. If I directly connect devices to the FW and assign their corresponding FW interface as the Default Gate Way traffic has no issue... view more

Cisco DNA Software Demo Series: Wireless Assurance

0 0

Created by gajewell on 03-05-2020 11:27 AM

https://engage2demand.cisco.com/LP=19215 Learn how Cisco wireless assurance provides real-time and historical analytics for deep network visibility and simplified troubleshooting. Learn how you can easily manage all of your connected devices and se... view more

Cisco DNA Software Demo Series: Cisco DNA Center Overview

0 0

Created by gajewell on 03-05-2020 11:22 AM

https://engage2demand.cisco.com/LP=19138 Thursday, March 19, 2020 10:00AM Pacific Daylight Time (San Francisco, GMT-07:00) Cisco DNA Center offers customers a low-risk, lower-cost, incremental approach to adopting network technologies in their branch, cam... view more

Create

Please login to create content

+ Discussion
+ Video
+ Blog
+ Document

Related Content

Discussions
Blogs
Documents
Events
Videos

Recommended

Subject	Author	Posted
✔ DHCP snooping with port-security	glogloglik	08-07-2019 01:48 AM
✔ Cisco 892 DHCP snooping not blocking DH...	Sam Brynes	12-10-2019 11:06 PM
✔ IP DHCP snooping question	Siemens_SWP	11-30-2009 11:11 PM
✔ DHCP snooping isn't snooping!	mrjdh	06-02-2019 01:54 PM
✔ DHCP Snooping & Option 82	david.mitchell	04-04-2013 01:56 AM

Top