CHAPTER 16

Blocking Unknown Unicast Flooding

This chapter describes how to block unknown unicast packet flooding (UUFB) in the forwarding path and includes the following sections:

Information About UUFB

UUFB limits unknown unicast flooding in the forwarding path to prevent the security risk of unwanted traffic reaching the VMs. UUFB prevents packets received on both vEthernet and Ethernet interfaces destined to unknown unicast addresses from flooding the VLAN. When UUFB is applied, VEMs drop unknown unicast packets coming in on the uplink ports.

After you disable unknown unicast packets globally, you can then allow unicast flooding on either a single interface or all interfaces in a port profile.

You can also configure an interface or a port profile to never allow unknown unicasts to be blocked.

Guidelines and Limitations

UUFB configuration has the following guideline.

- Before configuring UUFB, make sure the VSM HA pair and all VEMs have been upgraded to Release 4.2(1)SV1(4a) by entering the **show module** command.
- You must explicitly disable UUFB on virtual service domain (VSD) ports. This can be done in the VSD port profiles. For more information, see the Chapter 16, “Configuring a Port Profile to Allow Unknown Unicast Flooding”.

- You must explicitly disable UUFB on the ports of an application or VM using MAC addresses other than the one given by VMware.
- You can configure an interface to make sure that an unknown unicast is never blocked using the "Configuring an Interface to Allow Unknown Unicast Flooding" procedure on page 16-3.

Default Settings

The following table lists the UUFB default settings.

Parameters	Default
uufb enable	disabled
switchport uufb disable	disabled

Configuring UUFB

This section includes the following procedures:

Blocking Unknown Unicast Flooding Globally on the Switch

Use this procedure to globally block unknown unicast packets from flooding the forwarding path for the switch.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **[no] uufb enable**
3. **show uufb status**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters CLI global configuration mode.
Step 2	**[no] uufb enable** **Example:** n1000v(config)# uufb enable n1000v(config)#	Configures UUFB globally for the VSM.
Step 3	**show uufb status** **Example:** n1000v(config)# show uufb status UUFB Status: Enabled n1000v(config)#	(Optional) Displays the UUFB global setting for the VSM.
Step 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config [##] 100% n1000v(config)#	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring an Interface to Allow Unknown Unicast Flooding

Use this procedure to allow unknown unicast packets to flood a vEthernet interface if you have blocked flooding globally for the VSM.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can use this procedure to make sure unknown unicasts are never blocked on a specific interface, regardless of the global setting.
- If you have previously blocked unknown unicast packets globally, you can then allow unicast flooding on either a single interface or all interfaces in a port profile.

  To allow unicast flooding on all interfaces in a port profile, see the "Configuring a Port Profile to Allow Unknown Unicast Flooding" procedure on page 16-5.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*
3. **[no] switchport uufb disable**
4. **show** **running-config vethernet** *interface-number*

5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters CLI global configuration mode.
Step 2	**interface vethernet** *interface-number* **Example:** n1000v(config)# interface vethernet 100 n1000v(config-if)#	Enters CLI interface configuration mode for the specified interface.
Step 3	**[no] switchport uufb disable** **Example:** n1000v(config-if)# switchport uufb disable n1000v(config-if)#	Disables blocking of unicast packet flooding for the named interface.

Step 4	**show running-config vethernet** *interface-number*
	
	Example:
	n1000v(config-if)# show running-config interface veth100
	
	!Command: show running-config interface Vethernet100
	!Time: Fri Jun 10 12:43:53 2011
	
	version 4.2(1)SV1(4a)
	
	interface Vethernet100
	  description accessvlan
	  switchport access vlan 30
	  switchport uufb disable
	
	n1000v(config-if)#
		(Optional) Displays the running configuration for the interface for verification.

Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config [##] 100% n1000v(config-if)#	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring a Port Profile to Allow Unknown Unicast Flooding

Use this procedure to allow unknown unicast packets to flood the interfaces in an existing vEthernet port profile if you have disabled unicast flooding globally for the VSM.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can use this procedure to make sure unknown unicasts are never blocked on a specific port profile, regardless of the global setting.
- If you have previously blocked unknown unicast packets globally, you can then allow unicast flooding on either a single interface or all interfaces in a port profile.

  To allow unicast flooding on a single interface, see the "Configuring an Interface to Allow Unknown Unicast Flooding" procedure on page 16-3.
- You have previously configured the vEthernet port profile that you want to allow flooding for.

SUMMARY STEPS

1. **config t**
2. **port-profile** *profile-name*
3. **[no] switchport uufb disable**
4. **show running-config port-profile** *profile-name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters CLI global configuration mode.

Step 1	**port-profile** *profile-name*
	
	Example:
	`n1000v(config)# port-profile accessprof`
	`n1000v(config-port-prof)#`
		Enters configuration mode for the named port profile.

Step 2	**[no] switchport uufb disable**
	
	Example:
	`n1000v(config-port-prof)# switchport uufb disable`
	`n1000v(config-port-prof)#`
		Disables blocking of unicast packet flooding for all interfaces in the named port profile.

	Command	Purpose

Step 3	**show running-config port-profile** *profile-name*
	
	Example:
	n1000v(config-port-prof)# show running-config port-profile accessprof
	
	!Command: show running-config port-profile accessprof
	!Time: Fri Jun 10 12:06:38 2011
	
	version 4.2(1)SV1(4a)
	port-profile type vethernet accessprof
	  vmware port-group
	  switchport mode access
	  switchport access vlan 300
	  switchport uufb disable
	  no shutdown
	  description all_access
	
	n1000v(config-port-prof)#
		(Optional) Displays the configuration for the named port profile for verification.

Step 4	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config [##] 100% n1000v(config-port-prof)#	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the UUFB Configuration

You can use the following commands to verify the UUFB configuration:

Command	Purpose
show uufb status	Displays the UUFB global setting for the VSM.
show running-config port-profile *profile-name*	Displays the running configuration for a specific port profile.
show running-config interface vethernet *interface-number*	Displays the running configuration for a specific interface.
vemcmd show port uufb-override	Displays UUFB disable state for each port.

UUFB Example Configurations

The following example shows how to block unknown unicast packets from flooding the forwarding path globally for the VSM.

Example:

```
n1000v# config t
n1000v(config)# uufb enable
n1000v(config)# show uufb status
UUFB Status: Enabled
n1000v(config)# copy running-config startup-config
[########################################] 100%
n1000v(config)#
```

The following example shows how to allow unknown unicast packets to flood vEthernet interface 100 if you have disabled UUFB globally for the VSM.

Example:

```
n1000v# config t
n1000v(config)# interface vethernet 100
n1000v(config-if)# switchport uufb disable
n1000v(config-if)# show running-config interface veth100

!Command: show running-config interface Vethernet100
!Time: Fri Jun 10 12:43:53 2011

version 4.2(1)SV1(4a)

interface Vethernet100
  description accessvlan
  switchport access vlan 30
  switchport uufb disable

n1000v(config-if)#
```

The following example shows how to allow unknown unicast packets to flood the interfaces in an existing port profile if you have disabled UUFB globally for the VSM.

Example:

```
n1000v# config t
n1000v(config)# port-profile accessprof
n1000v(config-port-prof)# switchport uufb disable
n1000v(config-port-prof)# show running-config port-profile accessprof

!Command: show running-config port-profile accessprof
!Time: Fri Jun 10 12:06:38 2011

version 4.2(1)SV1(4a)
port-profile type vethernet accessprof
  vmware port-group
  switchport mode access
  switchport access vlan 300
  switchport uufb disable
  no shutdown
  description all_access

n1000v(config-port-prof)#
```

Additional References

For additional information related to UUFB, see the following sections:

- Related Documents, page 16-8
- Standards, page 16-8

Related Documents

Related Topic	Document Title
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*
Interface configuration	*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)*
Port Profile configuration	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*
Layer 2 switching configuration	*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for UUFB

This section provides the UUFB release history.

Feature Name	Releases	Feature Information
UUFB	4.2(1)SV1(4a)	This feature was introduced.