Configurazione della macchina virtuale sul server blade UCS come destinazione SPAN

Sommario

Introduzione

In questo documento viene descritto come acquisire un flusso di traffico che è completamente esterno al Cisco Unified Computing System (UCS) e indirizzarlo a una macchina virtuale (VM) che esegue uno strumento di analisi all'interno del Cisco Unified Computing System. L'origine e la destinazione del traffico da acquisire si trovano all'esterno dell'UCS. L'acquisizione può essere iniziata su uno switch fisico collegato direttamente all'UCS o su pochi hop di distanza.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCS
- VMware ESX versione 4.1 o successiva
- ERSPAN (Encapsulated Remote Switch Port Analyzer)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 6503 con 12.2(18)ZYA3c
- Cisco UCS serie B con versione 2.2(3e)

- VMWare ESXi 5.5 build 1331820

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

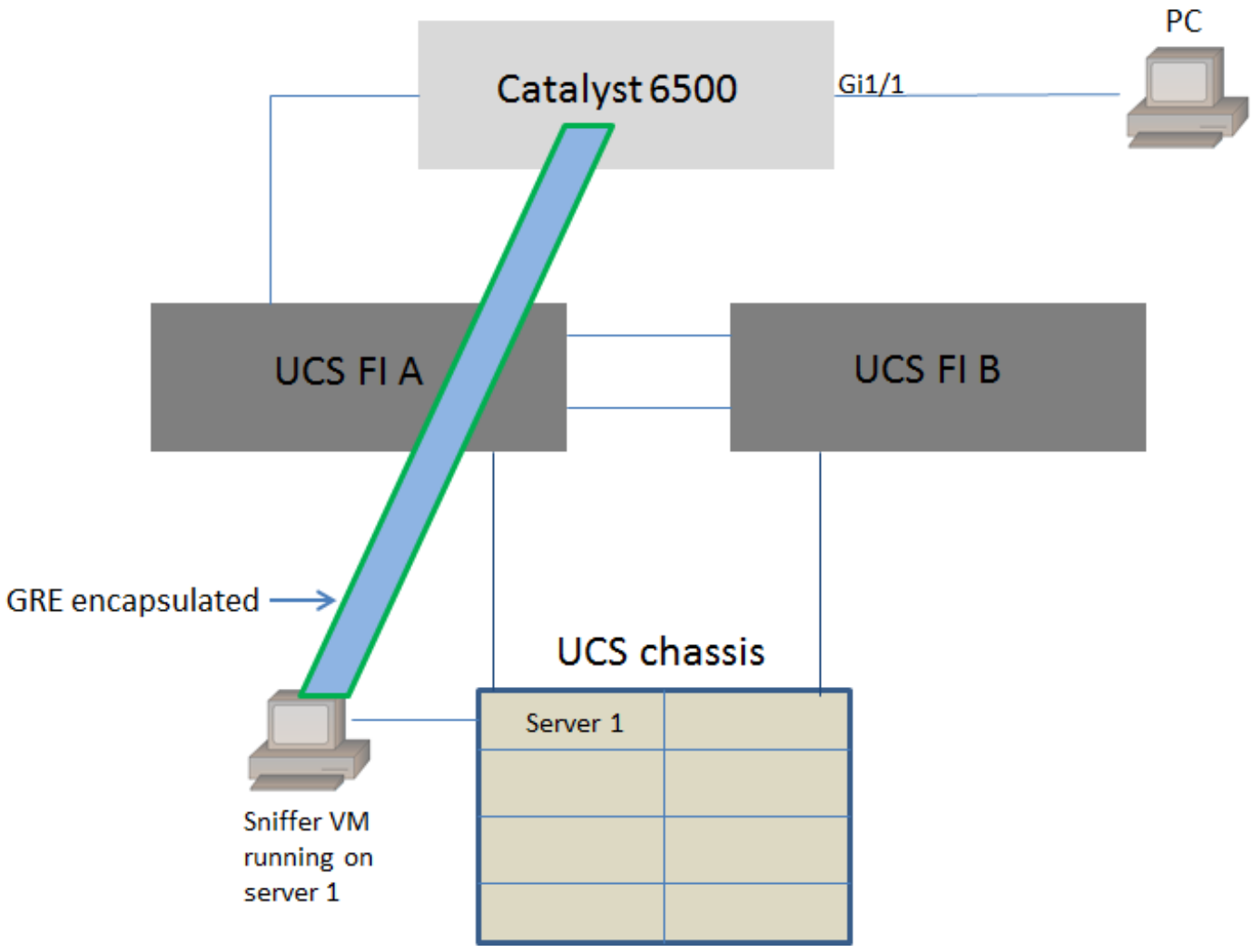
Premesse

UCS non dispone della funzionalità RSPAN (Remote SPAN) per ricevere il traffico SPAN da uno switch connesso e indirizzarlo a una porta locale. Pertanto, l'unico modo per ottenere questo risultato in un ambiente UCS è tramite la funzionalità ERSPAN (Encapsulated RSPAN) su uno switch fisico e l'invio del traffico acquisito alla VM tramite IP. In alcune implementazioni, la VM che esegue lo strumento di sniffer non può avere un indirizzo IP. Questo documento spiega la configurazione richiesta quando la VM sniffer ha un indirizzo IP e lo scenario senza un indirizzo IP. L'unico limite qui è che la VM sniffer deve essere in grado di leggere l'incapsulamento GRE/ERSPAN dal traffico che le viene inviato.

Configurazione

Esempio di rete

Nel presente documento si è tenuto conto di questa topologia:



Èin corso il monitoraggio del PC collegato a Gigabit Ethernet 1/1 di Catalyst 6500. Il traffico su Gigabit Ethernet 1/1 viene acquisito e inviato alla VM sniffer in esecuzione all'interno di Cisco UCS sul server 1. La funzione ERSPAN sullo switch 6500 acquisisce il traffico, lo incapsula tramite GRE e lo invia all'indirizzo IP della VM sniffer.

Sniffer VM con indirizzo IP

> **Nota:** I passaggi descritti in questa sezione possono essere utilizzati anche nello scenario in cui lo sniffer viene eseguito in un server bare-metal su un blade UCS anziché su una VM.

Questi passaggi sono necessari quando la VM sniffer può avere un indirizzo IP:

- Configurare la VM sniffer all'interno dell'ambiente UCS con un indirizzo IP raggiungibile dallo switch 6500
- Eseguire lo strumento sniffer nella VM
- Configurare una sessione di origine ERSPAN sullo switch 6500 e inviare il traffico acquisito direttamente all'indirizzo IP della VM

La configurazione dello switch 6500 prevede quanto segue:

```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.2
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit
CAT6K-01(config-mon-erspan-src)#no shut
CAT6K-01(config-mon-erspan-src)#end
```

Nell'esempio, l'indirizzo IP della VM sniffer è 192.0.2.2

Sniffer VM senza indirizzo IP

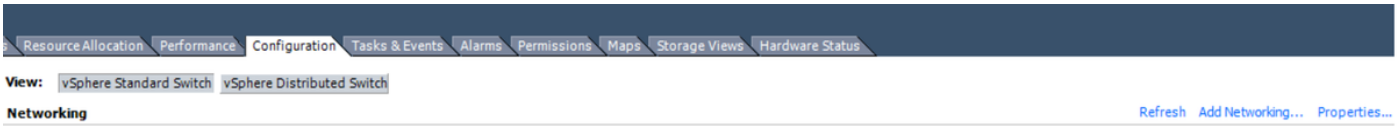
Questi passaggi sono necessari quando la VM sniffer non può avere un indirizzo IP:

- Configurare la macchina virtuale sniffer all'interno dell'ambiente UCS
- Eseguire lo strumento sniffer nella VM
- Creare una seconda VM che possa avere un indirizzo IP nello stesso host e configurarla con un indirizzo IP raggiungibile dallo switch 6500
- Configurare il gruppo di porte sullo switch VMWare vSwitch in modo che sia in modalità promiscua
- Configurare una sessione di origine ERSPAN sullo switch 6500 e inviare il traffico acquisito all'indirizzo IP della seconda VM

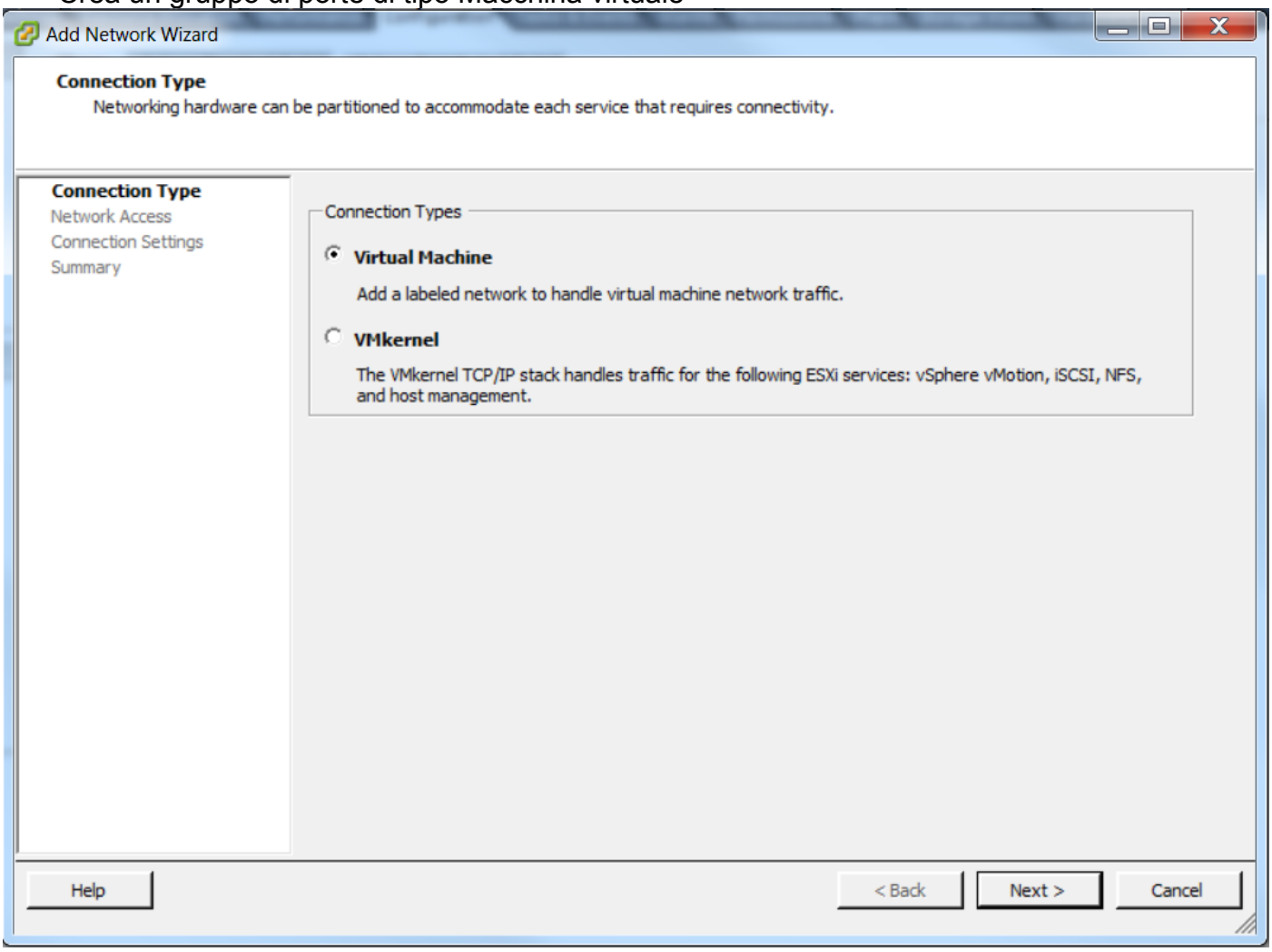
La procedura seguente mostra la configurazione richiesta per VMWare ESX: Andare direttamente al passaggio 2 se è già stato configurato un gruppo di porte.

1. Creare un gruppo di porte delle macchine virtuali e assegnarvi le due macchine virtuali

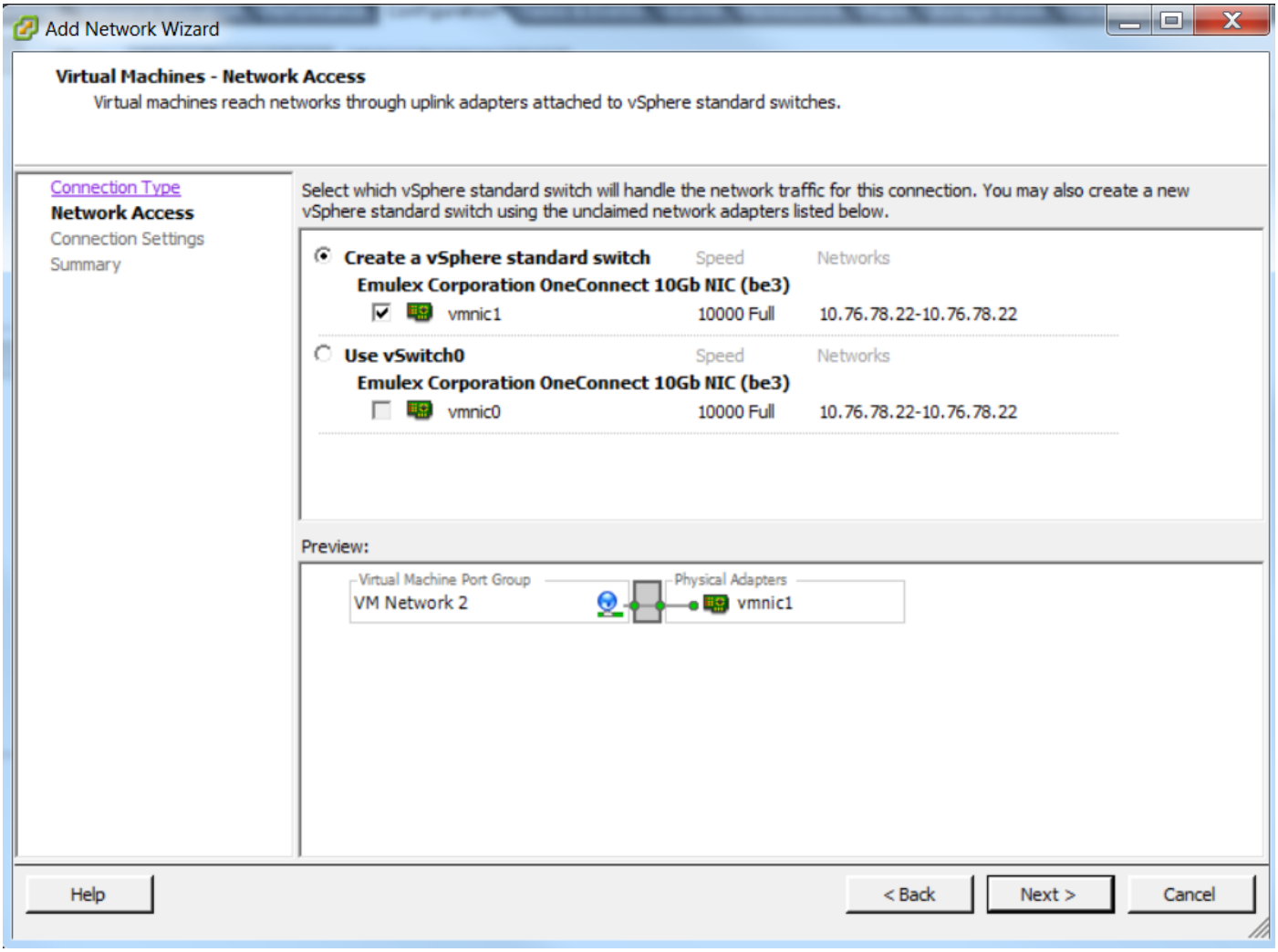
- Passare alla scheda **Rete** e fare clic su **Aggiungi rete in vSphere Standard Switch**



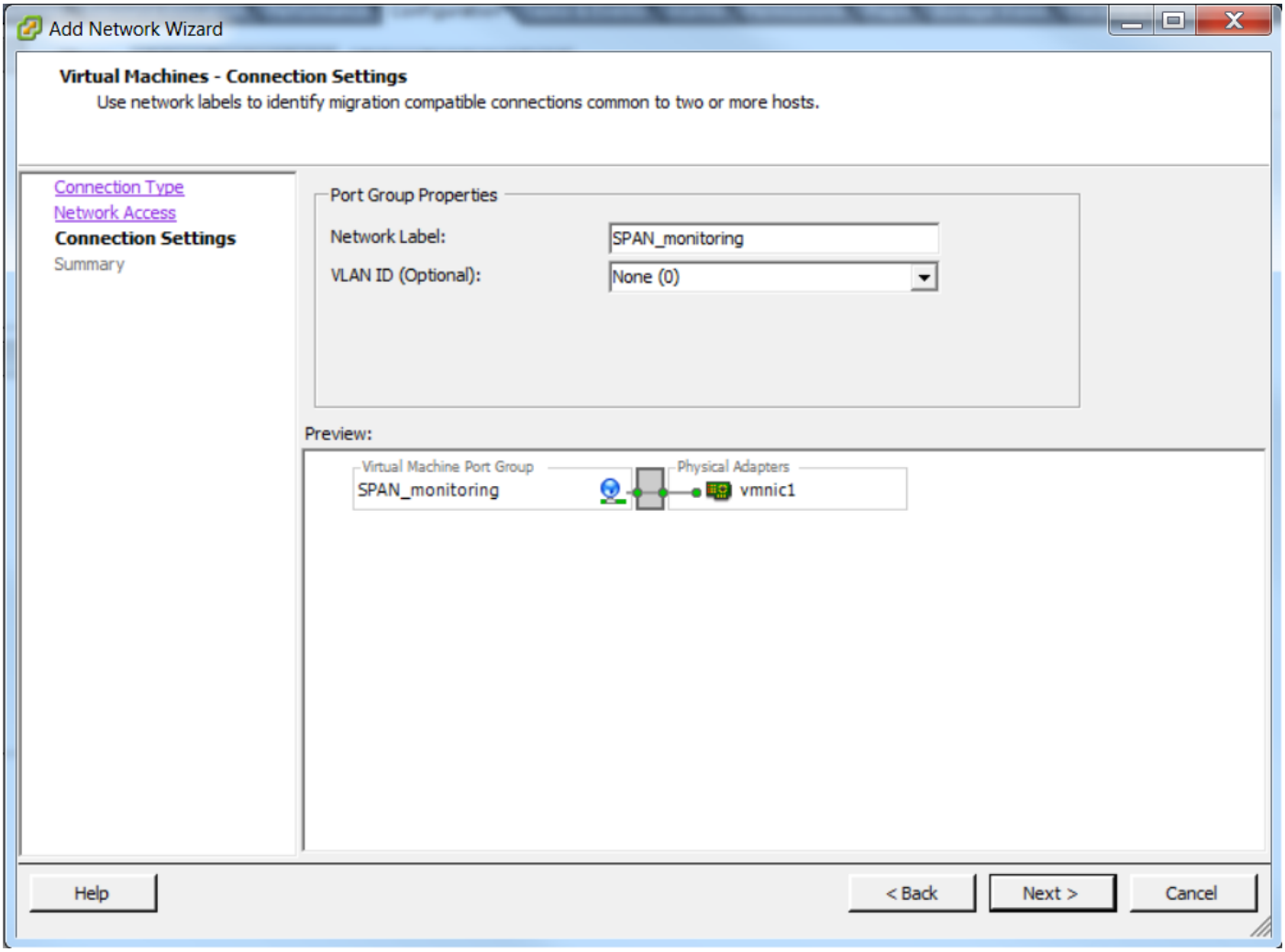
- Crea un gruppo di porte di tipo Macchina virtuale



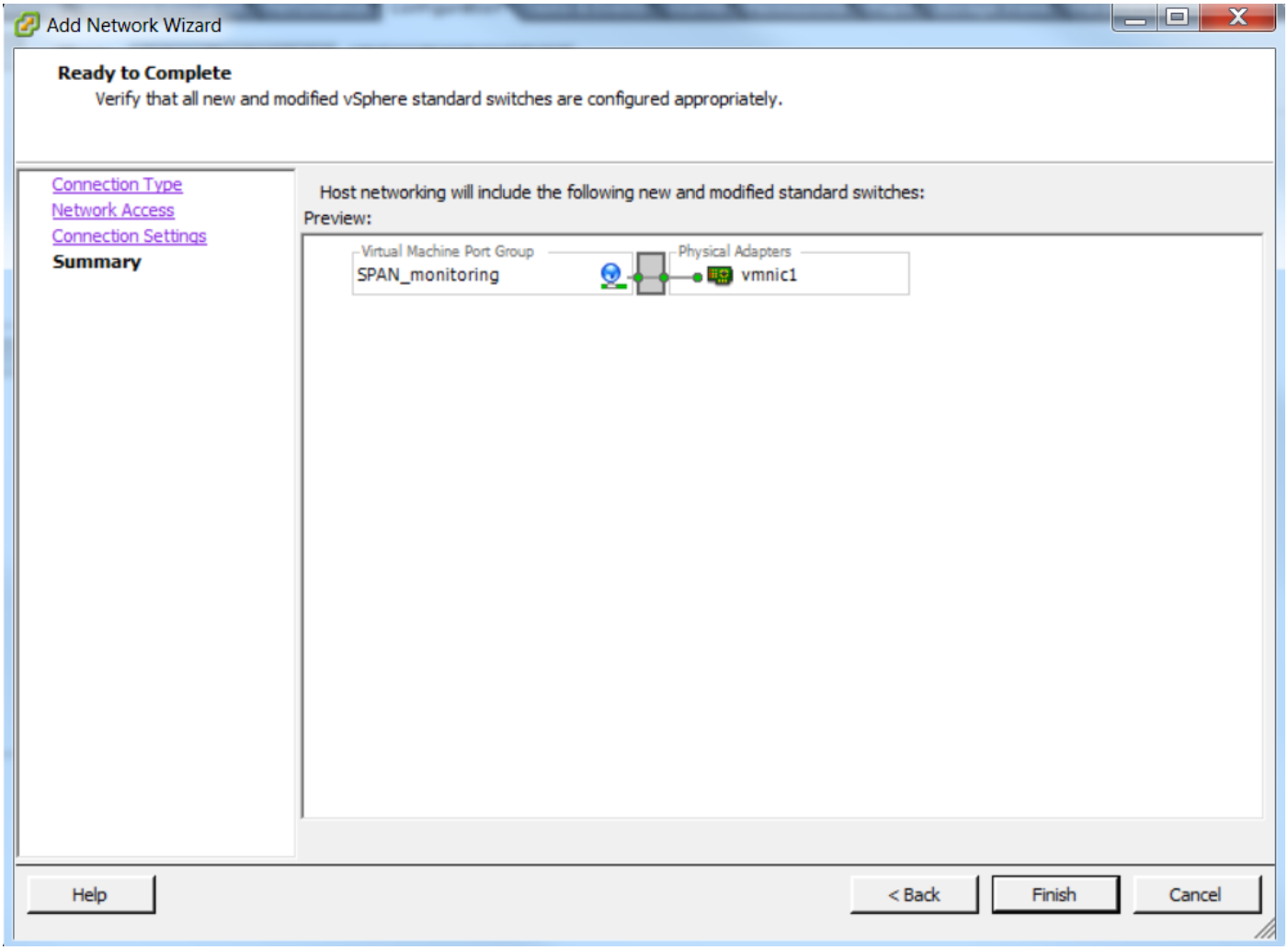
- Assegnare un'interfaccia fisica (vmnic) al gruppo di porte come mostrato in questa immagine.



- Configurare un nome per il gruppo di porte e aggiungere la VLAN desiderata, come mostrato nell'immagine.



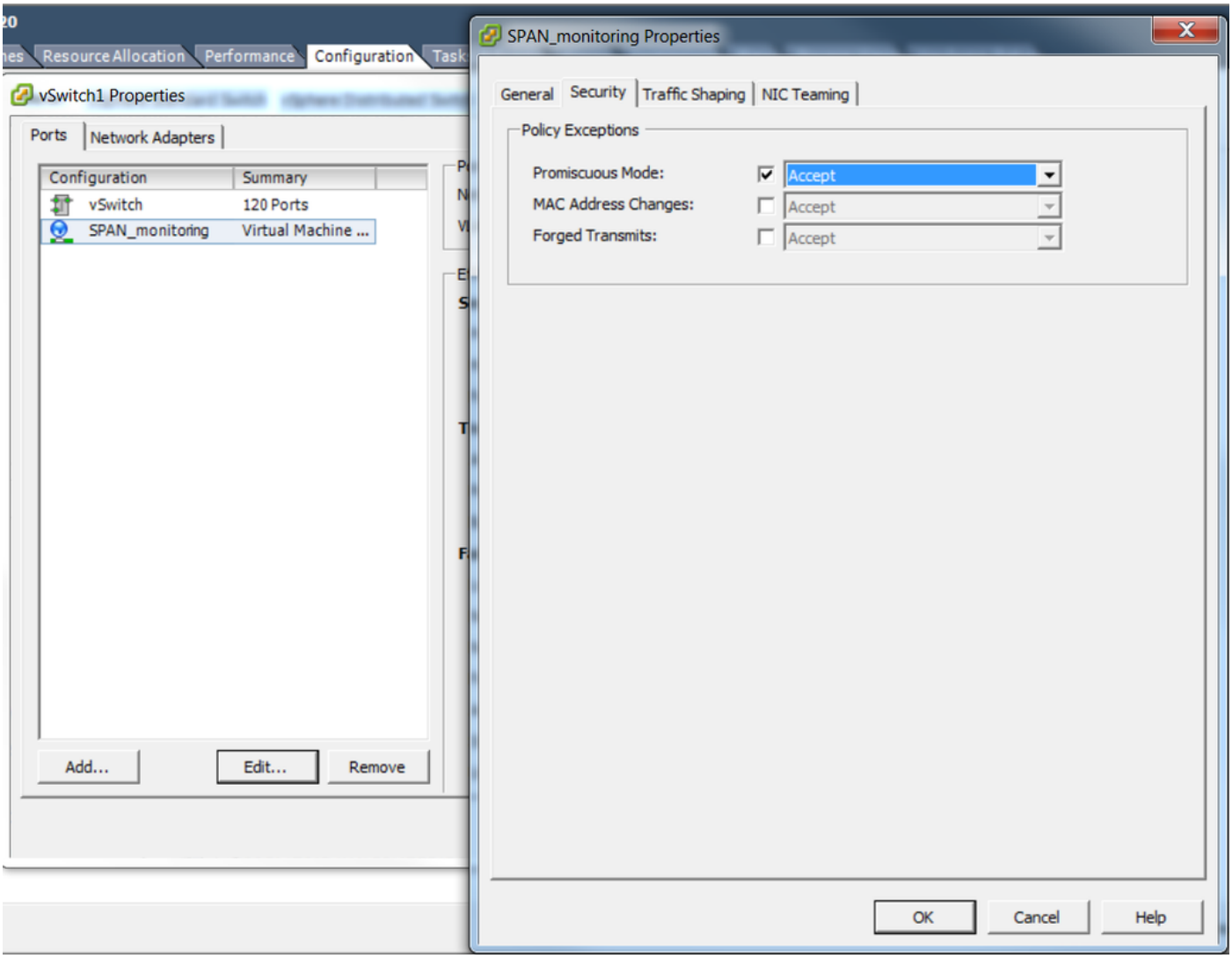
- Verificare la configurazione e fare clic su **Finish** (Fine), come mostrato nell'immagine.



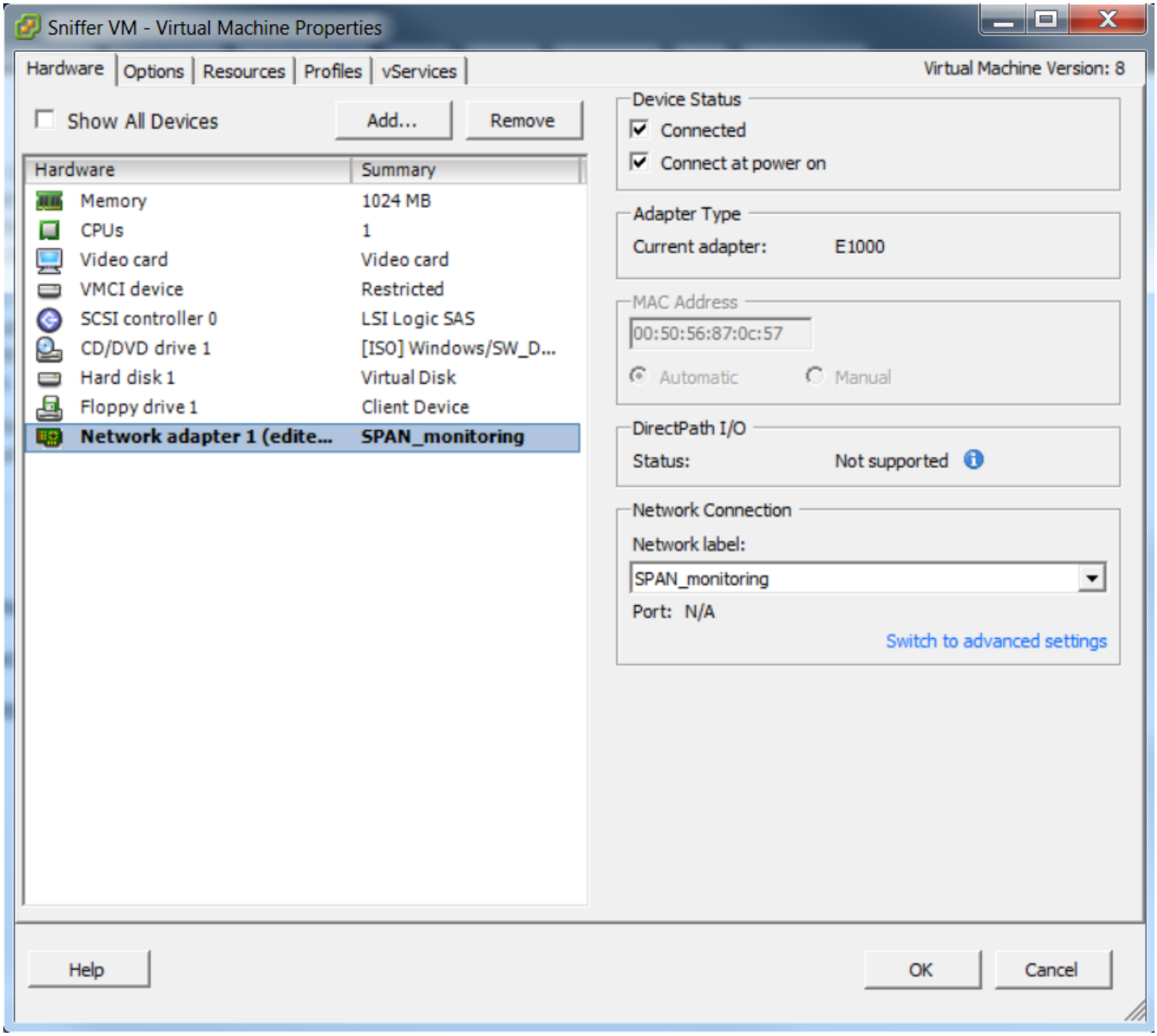
2. Configurare il gruppo di porte in modo promiscuo come mostrato nell'immagine.

- Il gruppo di porte deve essere visualizzato nella scheda **Rete**
- Fare clic su **Proprietà**

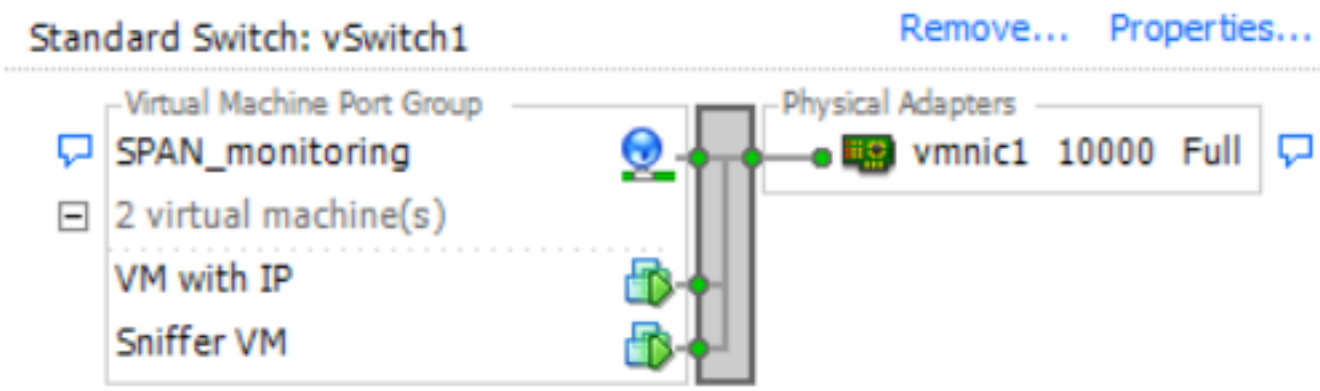
- Selezionare il gruppo di porte e fare clic su **Modifica**
- Andare alla scheda **Sicurezza** e modificare l'impostazione della modalità promiscua su Accetta, come mostrato nell'immagine



3. Assegnare le due macchine virtuali al gruppo di porte dalla sezione Impostazioni macchina virtuale.



4. Le due macchine virtuali devono essere ora visualizzate nel gruppo porte nella scheda **Rete**.



In questo esempio, la VM con IP è la seconda VM con un indirizzo IP e la VM Sniffer è la VM con lo strumento Sniffer senza un indirizzo IP.

5. Questa procedura mostra la configurazione dello switch 6500:

```
CAT6K-01(config)#monitor session 1 type erspan-source
```

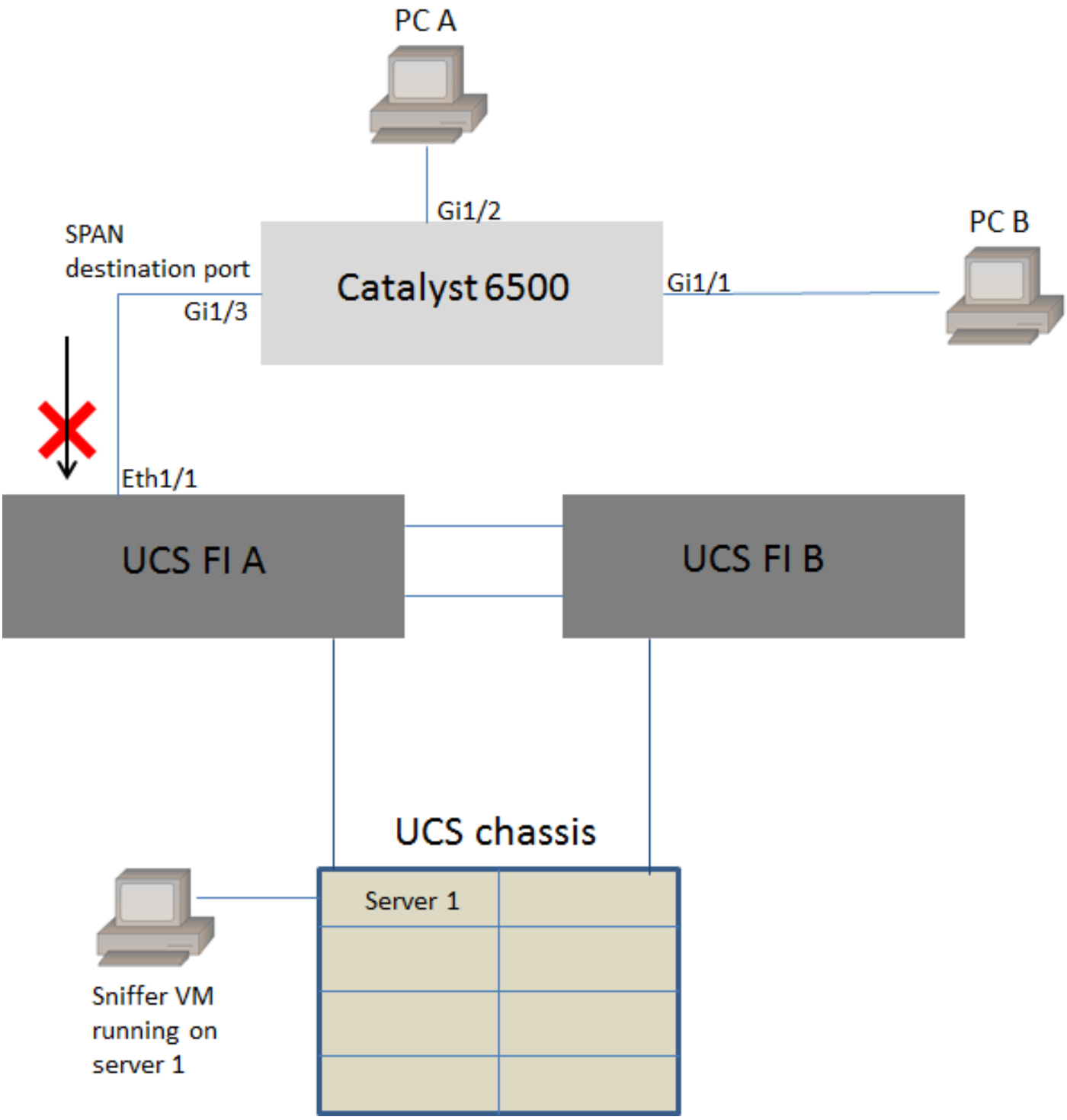
```
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit
CAT6K-01(config-mon-erspan-src)#no shut
CAT6K-01(config-mon-erspan-src)#end
```

Nell'esempio, l'indirizzo IP della seconda VM (VM con IP) è 192.0.2.3.

Con questa configurazione, lo switch 6500 incapsula i pacchetti acquisiti e li invia alla VM con l'indirizzo IP. La modalità promiscua di VMWare vSwitch consente alla VM sniffer di vedere anche questi pacchetti.

Scenario di errore

In questa sezione viene descritto uno scenario di errore comune quando si utilizza la funzione SPAN locale su uno switch fisico anziché la funzione ERSPAN. La topologia è la seguente:



Il traffico tra il PC A e il PC B viene monitorato utilizzando la funzione SPAN locale. La destinazione del traffico SPAN è diretta alla porta collegata all'interconnessione del fabric UCS (FI).

La macchina virtuale con lo strumento di rilevamento viene eseguita all'interno dell'UCS sul server 1.

Questa è la configurazione dello switch 6500:

```
CAT6K-01(config)#monitor session 1 source interface gigabitEthernet 1/1, gigabitEthernet 1/2
CAT6K-01(config)#monitor session 1 destination interface gigabitEthernet 1/3
```

Tutto il traffico che scorre sulle porte Gig1/1 e Gig1/2 verrà replicato sulla porta Gig1/3. Gli indirizzi MAC di origine e destinazione di questi pacchetti saranno sconosciuti a UCS FI.

Nella modalità host finale Ethernet UCS, l'URI scarta questi pacchetti unicast sconosciuti.

Nella modalità di commutazione Ethernet UCS, l'FMI apprende l'indirizzo MAC di origine sulla porta collegata allo switch 6500 (Eth1/1) e quindi invia i pacchetti a valle ai server. La sequenza di eventi si verifica:

1. Per una maggiore facilità di comprensione, si consideri il traffico diretto solo tra il PC A (con indirizzo mac aaaa.aaaa.aaa) e il PC B (con indirizzo mac bbbb.bbbb.bbb) sulle interfacce Gig1/1 e Gig1/2
2. Il primo pacchetto viene inviato dal PC A al PC B e viene visualizzato su UCS FI Eth1/1
3. Il FI apprende l'indirizzo mac aaaa.aaaa.aaaa su Eth1/1
4. Il FI non conosce l'indirizzo mac di destinazione bbbb.bbbb.bbbb e invia il pacchetto a tutte le porte della stessa VLAN
5. Anche la VM sniffer, nella stessa VLAN, visualizza questo pacchetto
6. Il pacchetto successivo va dal PC B al PC A
7. Quando si raggiunge Eth1/1, l'indirizzo mac bbbb.bbbb.bbbb viene appreso su Eth1/1
8. La destinazione del pacchetto è per mac-address aaaaa.aaaa.aaaa
9. Il FI scarta questo pacchetto come indirizzo mac aaaa.aaaa.aaaa viene appreso su Eth1/1 e il pacchetto è stato ricevuto su Eth1/1 stesso
10. I pacchetti successivi, destinati all'indirizzo mac aaaa.aaaa.aaaa o all'indirizzo mac bbbb.bbb.bbb, vengono scartati per lo stesso motivo

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Configurazione della modalità promiscua su uno switch virtuale o un gruppo di porte
- SPAN, RSPAN ed ERSPAN su Catalyst 6500
- Decapsulamento del traffico ERSPAN con strumenti open source
- Documentazione e supporto tecnico – Cisco Systems