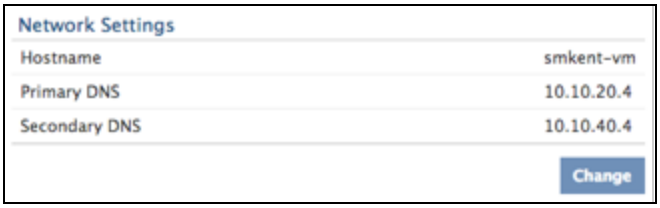
Configure ERSPAN with the Nexus 1000V

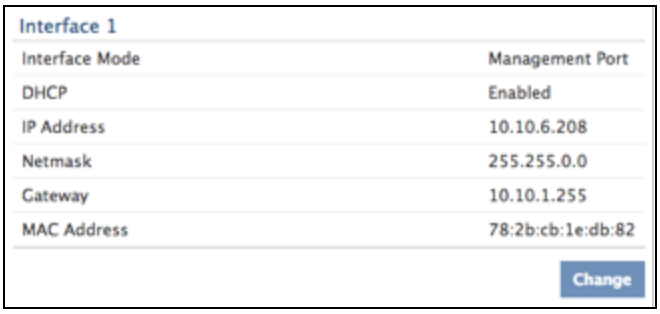
The Encapsulated Remote Switched Port Analyzer (ERSPAN) allows you to monitor traffic on multiple network interfaces or VLANs and then send the monitored traffic to one or more destinations. This guide explains how to configure ERSPAN on an installed ExtraHop appliance using the Nexus 1000V running on a Windows machine. The guide assumes experience using Cisco products.

To configure ERSPAN on an ExtraHop appliance, complete the following steps.

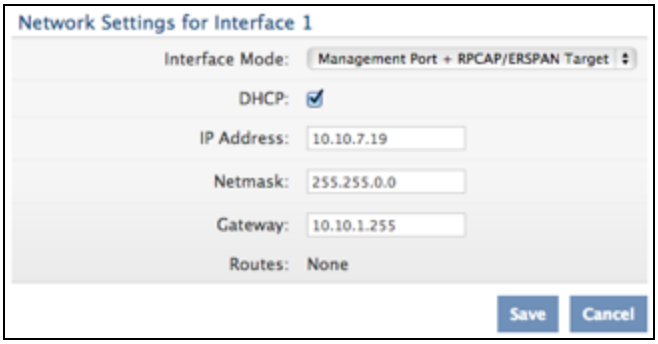
1. Log in to the Admin UI (`https://<extrahop_ip>/admin`).
2. Go to the **Network Settings** section and click **Connectivity**.



3. Go to the **Interface 1** section and click **Change**.



4. On the Network Settings for Interface 1 page, click the **Interface Mode** drop-down list and select **Management Port + RPCAP/ERSPAN Target**.



5. Complete the remaining fields and click **Save**.
6. Depending on your configuration set or disable the remaining interfaces.

For more information about setting up the network interfaces, refer to the *Connectivity*section of the *Admin UI Help.*

7. Log into your virtual supervisor module (VSM).
8. Determine virtual Ethernet hosts that you want to monitor.

```
Switch# Show int virt
```

9. Enter config mode.

```
Switch# config terminal
```

10. Create new monitor session aka, a port mirroring session

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

11. Enter the ExtraHop ERSPAN target IP.

```
switch(config-erspan-src)# destination ip 10.10.247.93
```

12. Set an ERSPAN ID.

```
switch(config-erspan-src)# erspan-id 1
```

13. Set the MTU to 9000.

```
switch(config-erspan-src)# mtu 9000
```

To minimize the chance of drops, set the ERSPAN MTU as high as possible. On the Cisco Nexus 1000V, change the default MTU of 1500 to the current max of 9000. In addition, consider turning off TCP segmentation offloading on the operating systems involved in forwarded communication.

14. Add data sources.
    a. The following example shows data being taken from a guest.

```
switch(config-erspan-src)# source interface vethernet 3-5
both
```

    In this example, `both` means the VM is both sending and receiving data.

    b. The following example shows data being taken from all traffic received by the VLAN.

```
switch(config-erspan-src)# source vlan 1010 rx
```

15. Enable the monitoring session.

```
switch(config-erspan-src)# no shut
```

16. Exit from ERSPAN source to config mode.

```
switch(config-erspan-src)# exit
```

17. Exit config mode to the enable prompt

```
switch(config)# exit
```

18. Save your changes.

```
switch# copy running-config startup-config
```

19. Check the settings.

```
switch# show monitor session 1
```

A functioning monitoring session will look similar to this example.

```
   session 1
---------------
type               : erspan-source
state              : up
source intf        :
    rx             : Veth3          Veth4          Veth5
    tx             : Veth3          Veth4          Veth5
    both           : Veth3          Veth4          Veth5
source VLANs       :
    rx             : 1010
    tx             :
    both           :
source port-profile :
    rx             :
    tx             :
    both           :
filter VLANs       : filter not specified
destination IP     : 10.10.247.93
ERSPAN ID          : 1
ERSPAN TTL         : 64
ERSPAN IP Prec.    : 0
ERSPAN DSCP        : 0
ERSPAN MTU         : 9000
ERSPAN Header Type: 2
```

20. Log in to the ExtraHop Web UI (`https://<extrahop_ip>/extrahop`) to view monitored traffic.

Related Documentation

- Cisco: *Configuring an ERSPAN Port Profile*
- ExtraHop: *ExtraHop Admin UI Help*