PfR Bandwidth Visibility Distribution for xDSL Access

In a network where the hub and spoke devices are connected via a multipoint tunnel, the hub site does not know about bandwidth limitations at the spoke devices. Without the updated information about bandwidth limitations, Performance Routing (PfR) cannot optimize the application traffic. Usually the spoke device connection to the Internet service provider (ISP) is a DSL connection, which can experience periodic bandwidth changes. PfR bandwidth visibility is a PfR enhancement that provides accurate maximum bandwidth information to peering PfR elements so that accurate policies can be applied automatically.

Restrictions for PfR Bandwidth Visibility

- PfR bandwidth resolution is not supported with PfR active mode because there is no throughput data for traffic-classes.
- PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

Information About PfR Bandwidth Visibility

ADSL Definition

Digital Subscriber Line (DSL) technology is a modem technology that uses existing twisted pair telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. The term xDSL covers a number of similar yet competing forms of DSL, including Asymmetric DSL (ADSL/ADSL2), Symmetric DSL (SDSL), High Speed DSL (HDSL), Rate Adaptive (RADSL), and Very High Bit Data Rate DSL (VDSL) for delivering up to 52 Mbps downstream.

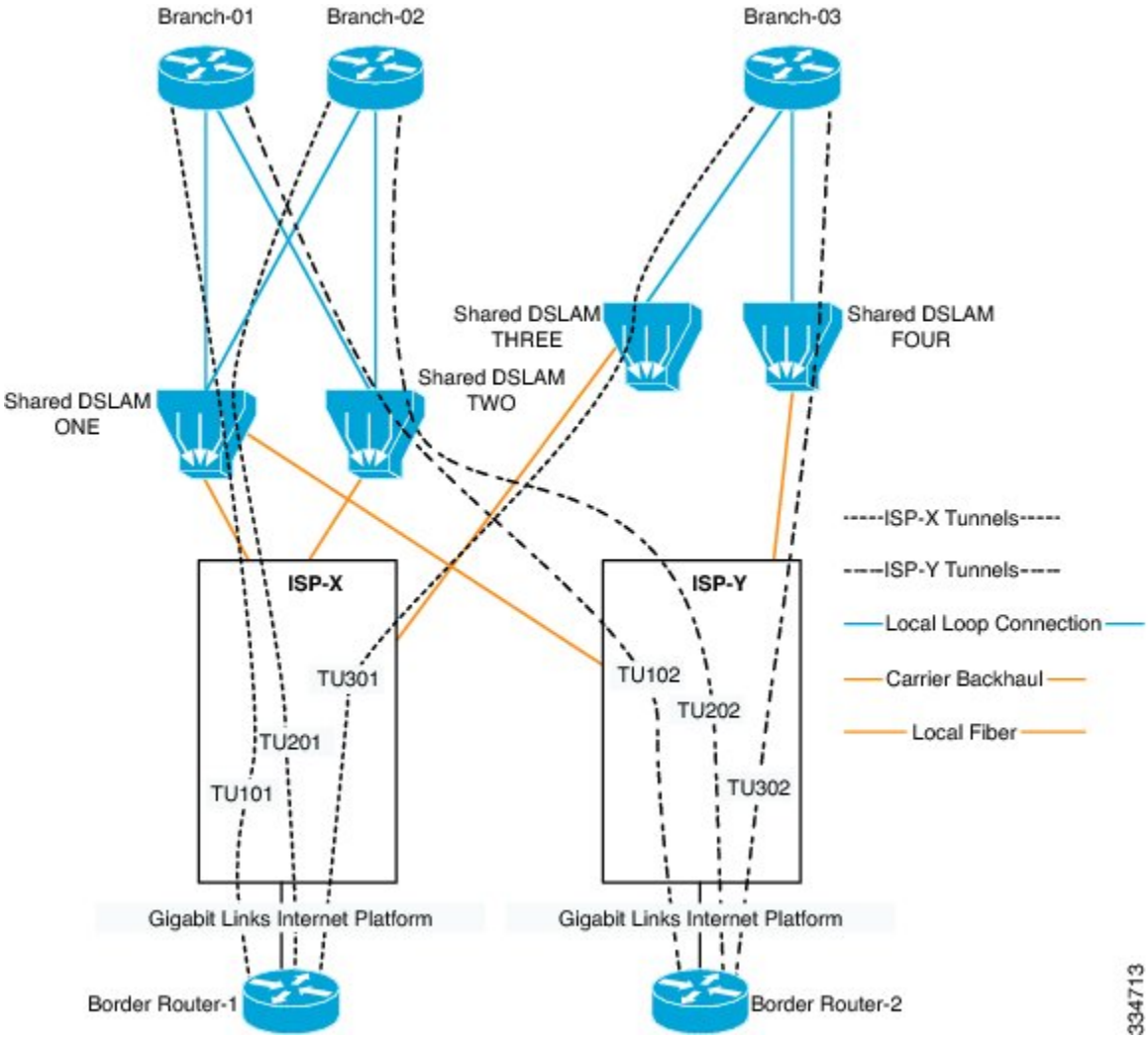
With Asymmetric DSL, unlike the less common Symmetric DSL, the bandwidth is greater for downloading data than for uploading data.

At the customer end of the connection, a DSL modem converts data from the digital signals used by computers into a voltage signal of a suitable frequency range, which is then applied to the phone line. At the exchange end, a Digital Subscriber Line Access Multiplexer (DSLAM) terminates the DSL circuits and aggregates them, where they are handed off to other networking transports. In the case of ADSL, the voice component is also separated at this step, either by a filter integrated in the DSLAM or by specialized filtering equipment installed before it.

PfR Bandwidth Visibility Challenges

In a network where the hub and spoke devices are connected via a multi-point tunnel, the hub site does not know about bandwidth limitations at the spoke devices. Without the updated information about bandwidth limitations, Performance Routing (PfR) cannot optimize the application traffic. Usually the spoke device connection to the Internet Service Provider (ISP) is a DSL connection, which can experience periodic bandwidth changes. For an example of such a network, see the network diagram below.

Figure 1: Hub and Spoke Devices with ADSL Connnections



PfR can redirect application traffic from one DMVPN/MGRE tunnel to another if the hub-spoke link utilization crosses a configured threshold, but PfR has no visibility into how congested a particular spoke is. There is a need for a mechanism that can discover updated receive (Rx) and transmit (Tx) limits at the spoke side and propagate the limit information to the hub, where the limit information can be used by PfR to effectively manage the application traffic.

Scenarios Creating ADSL Bandwidth Visibility Challenges

There are three main ADSL scenarios which can cause PfR bandwidth visibility challenges:

- ADSL retrain—Automatic or manual intervention can force the DSLAM into line reconditioning and retraining in which the bandwidth allocation for the line changes. The interventions can occur without notice. For an upwards retrain, the impact on the branch is minimal. For a downwards retrain, the branch can lose bandwidth, a common issue in congested exchanges. The ability to monitor and assess when to move the traffic through another tunnel is key to maintaining a smooth retraining.

- ADSL congestion—During congested periods, traffic can be held up. Under these circumstances it is imperative that the branch traffic be allowed to take the best possible path—and be distributed as well as possible over all links.
- ADSL intermittent faults—There are occasions (sometimes quite frequent) when there are intermittent faults that cause minor outages. The investigation of these issues normally takes several working days (no SLA). Significant numbers of these intermittent faults manifest themselves as drops at the higher usage of the "allocated" bandwidth. The ability must exist to effectively change the usage profile of any single tunnel to rebalance the traffic loadings until the ISP has repaired the issue.

PfR Bandwidth Visibility Resolution

Bandwidth visibility is a Performance Routing (PfR) enhancement that provides accurate maximum bandwidth information to peering PfR elements so that accurate policies can be applied automatically. In a network where bandwidth visibility is an issue, there are typically hub and spoke devices connected via a multi-point tunnel, and the hub site does not know about bandwidth limitations at the spoke devices. Without the updated information about bandwidth limitations, PfR cannot optimize the application traffic. Currently the bandwidth limitations are updated manually, but this is not a scalable solution.

PfR bandwidth visibility leverages the existing PfR target discovery feature. The existing SAF-based peering infrastructure can be used to propagate the bandwidth information, as well as target information, from a spoke device to the hub device. On the hub, the PfR master controller builds a database of peers and tracks their maximum receive and transmit bandwidth information. The border routers track the total amount of bandwidth transmitted to a given peer network and report it back to the master controller. If the total amount of bandwidth transmitted to a given peer at any time exceeds certain percentage of the receiving capacity of that peer, PfR can reroute that application traffic to an alternate link, avoiding congestion at the spoke device.

Note PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

To enable PfR bandwidth resolution, PfR target discovery must be configured on all devices on which PfR bandwidth-resolution is to be enabled. PfR bandwidth resolution is then enabled on all master controller devices. Both dynamic and static target discovery is supported by PfR bandwidth resolution. After bandwidth resolution is enabled, receive and transmit bandwidth limits are dynamically discovered and propagated using PfR target discovery. A mechanism is available to allow an overwrite of the dynamically discovered limits.

Note PfR bandwidth resolution is not supported with PfR active mode because there is no throughput data for traffic-classes.

How to Configure PfR Bandwidth Visibility

Configuring PfR Target Discovery and MC Peering for a Hub Site in Multihop Networks

Perform this task to configure PfR master controller (MC) peering at the master controller at the headend of the network, usually a hub site master controller. The master controller must be a device with routing capability. This task assumes a multihop type of network where the network cloud between the hub site and the branch sites is not under the control of the customer or is not SAF-enabled. In this design, the hub site MC will be a Service Advertisement Facility (SAF) forwarder hub with which the branch MC SAF forwarders peer to exchange advertisements. The hub site MC will accept peering requests from branch MCs with the same SAF domain ID and MD5 authentication.

Note In this task, dynamic PfR target discovery is enabled. This method is desirable when SAF is already enabled in the network for other applications or there is existing neighbor adjacency between MCs and SAF. For example, in a DMVPN WAN, if the PfR MCs coexist on the DMVPN tunnel devices, they also have SAF adjacency and do not require static peering.

Note PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **target-discovery**
5. **mc-peer** [**head-end** | *peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco device as a master controller.
Step 4	**target-discovery** **Example:** `Device(config-pfr-mc)# target-discovery`	Configures PfR target discovery. • In this example, dynamic PfR target discovery is configured.
Step 5	**mc-peer** [**head-end** | *peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] **Example:** `Device(config-pfr-mc)# mc-peer head-end loopback1 description SJ-hub`	In this example, the PfR master controller peering is configured to show that this device is the hub (headend) device. • Use the **domain** keyword to specify a SAF domain ID to be used for MC peering. The *domain-id* argument is in the range of 1 to 65535. If the SAF domain ID is not specified, the default value of 59501 is used.
Step 6	**end** **Example:** `Device(config-pfr-mc)# end`	(Optional) Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Configuring PfR Target Discovery and MC Peering for a Branch Office in Multihop Networks

Perform this task to configure PfR MC peering using static mode for PfR target discovery at a branch office that is acting as a spoke router. In this example, the IP address of the PfR master controller hub device at a head office (headend) of the network is configured as a loopback interface to allow MC peering. This task assumes a multihop type of network where the network cloud between the hub site and the branch offices is not under the control of the customer.

Note PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

Before you begin

PfR master controller (MC) peering must be configured on a device with routing capability located at the hub site (headend) of the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
5. **target-discovery**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco device as a master controller.
Step 4	**mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] **Example:** `Device(config-pfr-mc)# mc-peer 10.11.11.1 loopback1`	In this example, the IP address of the PfR master controller hub device at a head office (headend) of the network is configured as the peer address.
Step 5	**target-discovery** **Example:** `Device(config-pfr-mc)# target-discovery`	Configures dynamic PfR target discovery.
Step 6	**end** **Example:** `Device(config-pfr-mc)# end`	(Optional) Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Enabling Bandwidth Resolution

This task is performed on all PfR master controllers in every hub and spoke in the participating site.

Before you begin

Note PfR target discovery must be configured before enabling bandwidth resolution. Both dynamic and static target discovery is supported by PfR bandwidth resolution. PfR bandwidth resolution is not supported with PfR active mode because there is no throughput data for traffic-classes.

Note PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **bandwidth-resolution**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**bandwidth-resolution** **Example:** `Device(config-pfr-mc)# bandwidth-resolution`	Enables bandwidth resolution.

Overwriting Dynamically Discovered Receive and Transmit Bandwidth Limits

Perform this task at a PfR master controller to manually specify the maximum receive (Rx) and transmit (Tx) limits for a PfR external interface. When bandwidth-resolution is enabled, receive and transmit bandwidth limits are dynamically discovered and propagated using PfR target discovery. Use this task to overwrite the dynamically discovered limits using PfR bandwidth resolution.

After an external interface has been configured for a border router, PfR automatically monitors the utilization of external links on a border router every 20 seconds. The utilization is reported back to the master controller and, if the utilization exceeds the specified limit, PfR selects another exit link for traffic classes on that link. Only absolute values, in kilobits per second (kbps), can be specified to overwrite the dynamically discovered bandwidth limits.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **maximum utilization receive absolute** *kbps*
7. **max-xmit-utilization absolute** *kbps*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Device(config-pfr-mc)# border 10.1.1.2`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router.

	Command or Action	Purpose
		• At least one border router must be specified to create a PfR-managed network. A maximum of ten border routers can be controlled by a single master controller. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.
Step 5	**interface** *type number* **external** **Example:** `Device(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	Configures a border router interface as a PfR-managed external interface and enters PfR border exit interface configuration mode. • External interfaces are used to forward traffic and for active monitoring. • A minimum of two external border router interfaces are required in a PfR-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller. **Note** Entering the **interface** (PfR) command without the **external** or **internal** keyword places the router in global configuration mode and not PfR border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.
Step 6	**maximum utilization receive absolute** *kbps* **Example:** `Device(config-pfr-mc-br-if)# maximum utilization receive absolute 500000`	Sets the maximum utilization threshold of incoming traffic that can be transmitted over a PfR-managed entrance link interface. • Use the **absolute** keyword and *kbps* argument to specify the absolute maximum utilization on a PfR managed entrance link in kbps.
Step 7	**max-xmit-utilization absolute** *kbps* **Example:** `Device(config-pfr-mc-br-if)# max-xmit-utilization absolute 500000`	Configures the maximum utilization on a single PfR managed exit link. • Use the **absolute** keyword and *kbps* argument to specify the absolute maximum utilization on a PfR managed exit link in kbps.
Step 8	**end** **Example:** `Device(config-pfr-mc-br-if)# end`	Exits PfR border exit interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for PfR Bandwidth Visibility

Example: Configuring PfR Bandwidth Resolution

Note PfR target discovery must be configured before bandwidth resolution is enabled. Both dynamic and static target discovery is supported by PfR bandwidth resolution.

The following configuration can be used in multihop networks where the network cloud between the head office and branch offices or remote sites is not controlled by the customer or is not SAF-enabled. Configuration examples are shown for three master controllers, one at the head office and two at branch offices. PfR bandwidth resolution is enabled on all PfR master controller (MC) devices. Output for the **show pfr master bandwidth-resolution** command is shown for all three sites.

Note In the following examples, the hub and spoke device hostnames were configured as "Router-hub," "Router-spoke1," or "Router-spoke2," but the device can be any device with routing capability that supports PfR.

Hub MC Bandwidth Resolution Configuration

The hub device has routing capability and is in the head office. In this example, PfR bandwidth resolution is enabled on the master controller.

```
Router-hub> enable
Router-hub# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# bandwidth-resolution
Router-hub(config-pfr-mc)# end
```

Spoke1 MC Bandwidth Resolution Configuration

The spoke1 device has routing capability and is in a branch (spoke) office. In this example, PfR bandwidth resolution is enabled on the master controller at the branch office.

```
Router-spoke1> enable
Router-spoke1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# bandwidth-resolution
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC Bandwidth Resolution Configuration

The spoke2 device has routing capability and is in a second branch (spoke) office. In this example, PfR bandwidth resolution is enabled on the master controller at the second branch office.

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# bandwidth-resolution
Router-spoke2(config-pfr-mc)# end
```

Example Output for PfR Bandwidth Resolution

The following output is from the master controller for the hub device after PfR bandwidth resolution is enabled:

```
Router-hub# show pfr master bandwidth-resolution all

Border Router: 10.20.20.2           External Interface: Tu10
MC-peer address  Overlay address   Rx BW [kbps]   Tx BW [kbps]  Tx Load [kbps]
172.17.51.1      10.110.110.2      1000           900           0
172.20.61.1      10.110.110.3      1000           900           35

Border Router: 10.20.20.3           External Interface: Tu20
MC-peer address  Overlay address   Rx BW [kbps]   Tx BW [kbps]  Tx Load [kbps]
172.17.51.1      10.90.90.2        1000           900           18
172.20.61.1      10.90.90.3        803            903
```

The following output is from the master controller for the hub device after PfR bandwidth resolution is enabled and displays the output for the master controller peer at IP address 172.20.61.1:

```
Router-hub# show pfr master bandwidth-resolution 172.20.61.1

PfR Bandwidth Resolution Database
MC-peer: 172.20.61.1
Border Router  External Interface  Overlay Address  Rx BW [kbps] Tx BW [kbps] Tx Load [kbps]

10.20.20.2     Tu10                10.110.110.3     1000         900          35

10.20.20.3     Tu20                10.90.90.3       803          903          0
```

Feature Information for PfR Bandwidth Visibility

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for PfR Bandwidth Visibility

Feature Name	Releases	Feature Information
PfR Bandwidth Visibility Distribution for xDSL Access	15.3(1)T Cisco IOS XE Release 3.8S	PfR bandwidth visibility is a PfR enhancement that provides accurate maximum bandwidth information to peering PfR elements so that policies can be applied automatically. The following commands were introduced or modified: **bandwidth-resolution**, **debug pfr border bandwidth-resolution**, **debug pfr master bandwidth-resolution**, **show pfr master bandwidth-resolution**.