

# Administration of Symantec PacketShaper 11.9.1

Symantec 250-440

Version Demo

Total Demo Questions: 9

Total Premium Questions: 90

Buy Premium PDF

<https://passqueen.com>

[support@passqueen.com](mailto:support@passqueen.com)

## Topic Break Down

| Topic                                                        | No. of Questions |
|--------------------------------------------------------------|------------------|
| Topic 1, PacketShaper Overview                               | 4                |
| Topic 2, PacketShaper Installation and Initial Configuration | 3                |
| Topic 3, Monitoring Network Traffic                          | 21               |
| Topic 4, Traffic Management                                  | 48               |
| Topic 5, Managing PacketShaper                               | 12               |
| Topic 6, Troubleshooting PacketShaper                        | 1                |
| Topic 7, Mix Questions                                       | 1                |
| Total                                                        | 90               |

#### QUESTION NO: 1

A backup process must be visible in total link-utilization reporting, but it must not be subject to normal PacketShaper bandwidth-control enforcement.

Which two (2) statements describe the result of applying an ignore policy to the backup traffic class? (Select two)

- A. The traffic remains included in total link-traffic accounting.
- B. The traffic is excluded from normal bandwidth-control enforcement.
- C. The traffic is discarded when the link becomes congested.
- D. The traffic receives a guaranteed minimum bandwidth allocation.
- E. The traffic is removed from all PacketShaper reporting.

**ANSWER: A B**

#### Explanation:

An ignore policy causes matching traffic to be ignored for normal PacketShaper policy enforcement while it remains counted as part of link traffic under management. This satisfies the requirement to retain accurate overall utilization visibility without shaping the selected backup flow.

An ignore policy does not block traffic and does not make it disappear from link accounting. It also does not establish a guaranteed minimum bandwidth allocation.

#### QUESTION NO: 2

Which two (2) tasks does response time measurement (RTM) allow an administrator to perform? (Select two)

- A. Measure the quality of users' network experience
- B. Examine host, performance and CPU statistics
- C. Measure the quality of packet exchange times
- D. Measure the number of times traffic flows match a class
- E. Examine performance statistics and performance graphs

**ANSWER: A C**

#### Explanation:

Response Time Measurement (RTM) on PacketShaper is intended to characterize application responsiveness from the network traffic observed by the appliance. It correlates request-and-response packet exchanges and calculates the elapsed time associated with those exchanges. Consequently, *Measure the quality of users' network experience* is correct: response time is a practical indicator of the responsiveness users perceive while interacting with a network application. RTM results let an administrator identify whether users are experiencing slow application transactions and use that information when investigating network or application delivery conditions.

*Measure the quality of packet exchange times* is also correct because packet exchange timing is the direct measurement RTM performs. By observing the timing between relevant request and response traffic, PacketShaper produces response-time information rather than merely reporting traffic volume. These measurements are useful for monitoring interactive application behavior and recognizing changes in service responsiveness over time. PacketShaper's traffic-visibility and performance-management purpose is described by Broadcom at [PacketShaper](#). For general background on interpreting network performance measurements and delay, see [RFC 3393: IP Packet Delay Variation Metric](#).

#### QUESTION NO: 3

Which module allows an administrator to set bandwidth minimums and maximums, control bandwidth allocation, and ensure clear streams for voice and video?

- A. Acceleration
- B. Shaping
- C. Monitoring
- D. Measurement engine

**ANSWER: B**

**Explanation:**

**Shaping** is the PacketShaper module used to enforce bandwidth-control policies for traffic classes. It lets an administrator define a minimum bandwidth allocation so an important application or traffic flow receives a reserved share when the link is busy, and a maximum allocation to prevent a flow from consuming more than its intended limit. Shaping policies also determine how available bandwidth is distributed among classes, enabling administrators to prioritize latency-sensitive voice and video traffic over less time-critical traffic.

This capability is particularly important during congestion, when unmanaged traffic competition can introduce delay, jitter, and packet loss that impair real-time communications. By classifying voice and video streams and assigning appropriate bandwidth guarantees, limits, and priority treatment, the Shaping module helps maintain predictable service for those streams while still allowing other applications to use remaining capacity. PacketShaper combines application-aware traffic visibility with policy-based bandwidth management so that these controls can be applied to meaningful traffic categories rather than only to ports or addresses. Broadcom identifies PacketShaper as a network performance and traffic-management solution; product information is available at [Broadcom PacketShaper](#). Additional product documentation and support resources are available through the [Broadcom Support Portal](#).

**QUESTION NO: 4**

A single web server hosts two SSL-enabled business applications. The applications use different certificate common names, but they use the same PacketShaper device definition. An administrator has already created a class for the first application using Secure Service Intelligence (SSI).

Which two (2) actions allow the administrator to create a separate class for the second application? (Select two)

- A. Retain the existing device definition for the web server.
- B. Specify the second application's certificate Common Name.
- C. Replace the SSL service group with an HTTP service group.
- D. Use the clear-text HTTP URL as the distinguishing criterion.
- E. Create a different class only by assigning a new priority policy.

**ANSWER: A B**

**Explanation:**

SSI can use SSL certificate information to classify encrypted application traffic. To identify the second application, the administrator must use the second application certificate's Common Name as the matching criterion.

Because both applications are hosted on the same web server, the device definition can remain the same. Changing the device would not distinguish applications that share the same server. URL matching is not the appropriate differentiator for the encrypted SSL application in this scenario.

**QUESTION NO: 5**

An administrator is investigating complaints that an interactive TCP application is slow. In the Monitor Response Time window, the administrator needs the value that represents TCP connection-establishment latency rather than application transaction time.

Which value should the administrator examine?

- A. Network delay
- B. Round Trip
- C. Server delay
- D. Total delay

**ANSWER: B**

**Explanation:**

**Round Trip** is the connection-establishment measurement. It represents the average time from transmission of the client SYN packet until return of the server ACK packet. This helps distinguish network and handshake latency from the subsequent time used for an application transaction.

Total delay includes the overall transaction experience, while network delay concerns transit time for packets required by the transaction. Server delay is associated with application or server processing rather than TCP session establishment.

#### QUESTION NO: 6

Which option allows an administrator to differentiate Citrix-based applications and protect their performance?

- A. Choose Priority 7 from the matching rule's Citrix-specific classification criteria to identify print traffic.
- B. Assign the default partition and policy to all parts of the Citrix traffic tree, regardless of application urgency.
- C. Enable discovery and let PacketShaper discover the Citrix-based applications, then create a traffic class for each one.
- D. When Citrix applications generate a large amount of print traffic, merge multiple Citrix-based applications into one traffic class

**ANSWER: A**

**Explanation:**

Choosing Priority 7 from the matching rule's Citrix-specific classification criteria to identify print traffic allows PacketShaper to distinguish Citrix printing from more interactive Citrix application activity. Citrix ICA traffic can carry different virtual channels and workloads within what would otherwise appear to be a single Citrix session. PacketShaper's Citrix-aware classification can use the Citrix priority information exposed in that traffic to place printing into a dedicated traffic class. The administrator can then apply an appropriate policy to that class, such as assigning it a lower priority or controlling its bandwidth, so print jobs do not contend unnecessarily with latency-sensitive user interaction.

This is valuable because Citrix print operations may involve substantial data transfer, particularly with complex documents or graphics. Identifying the Priority 7 print workload gives the administrator a precise classification point for policy enforcement while preserving responsiveness for the Citrix applications users actively operate. This approach is consistent with PacketShaper's role of recognizing application-specific traffic attributes and applying class-based QoS controls. Broadcom describes PacketShaper as a solution for application visibility and traffic control at [Broadcom PacketShaper](#). Citrix also documents printing as a distinct HDX workload in its [Citrix printing documentation](#).

#### QUESTION NO: 7

What are the two (2) main functions of the Symantec PacketShaper? (Select two)

- A. Control of network traffic

- B. Next generation firewall
- C. Network traffic visibility
- D. Increased bandwidth
- E. Secure transparent proxy

**ANSWER: A C**

**Explanation:**

Symantec PacketShaper's core value is understanding how a network is being used and then applying policy to manage that use. **Network traffic visibility** is a principal function because PacketShaper identifies, classifies, and reports on applications, protocols, hosts, and traffic flows. This application-aware visibility gives administrators the information needed to recognize bandwidth consumption, prioritize business-relevant activity, and investigate changing traffic patterns. **Control of network traffic** is the complementary principal function: PacketShaper applies traffic-management policies, including prioritization, rate control, and bandwidth allocation, to shape how identified traffic uses available WAN capacity. Together, visibility and control form the product's operational workflow: classify traffic accurately, observe its effect on network resources, and enforce policies that protect important applications and user experience. Broadcom describes PacketShaper as a solution for application visibility and control, including intelligent traffic classification and policy-based management. These capabilities are also consistent with the PacketShaper product family's focus on WAN optimization and application performance management rather than simply adding physical bandwidth. See Broadcom's [PacketShaper product overview](#) and its [technical knowledge base](#) for product documentation and configuration guidance.

**QUESTION NO: 8**

A parent traffic class has a rate policy applied. A child class beneath it has no policy configured locally. Traffic is classified into the child class during a period of link congestion.

Which policy applies to the child-class traffic?

- A. The parent class rate policy
- B. A Default policy with no bandwidth control
- C. An automatically created priority policy
- D. No policy until one is configured on the child class

**ANSWER: A**

**Explanation:**

The child class inherits the effective policy from its parent when no policy is applied directly to the child. In this case, the parent rate policy governs traffic that is classified into the child class.

A locally configured priority, discard, ignore, or other policy on the child would replace inherited treatment for that child. However, merely creating a child class does not remove the policy inheritance relationship.

**QUESTION NO: 9**

What statement accurately describes Folder classes and Default classes?

- A. Folder classes are used for exceptions, and Default classes are used to define how matches for traffic flows are found
- B. Folder classes are used for organization, and Default classes are used to catch unclassified traffic
- C. Folder classes and Default classes always share the same parent classes
- D. Folder classes are used to catch unclassified traffic, and Default classes are used for organization

**ANSWER: B**

**Explanation:**

Folder classes are used for organization, and Default classes are used to catch unclassified traffic. In PacketShaper's traffic-class hierarchy, a folder class is a structural container: it helps an administrator arrange related traffic classes into meaningful groups and build a manageable classification tree. It is not intended to represent a particular application, protocol, host group, or matching rule. This organizational role is particularly useful in large policies, where classes may be grouped by business unit, application family, service type, or policy purpose.

A Default class has a different operational role. It provides the fallback classification for traffic that reaches a parent class but does not match one of that parent's more specific child classes. Consequently, it ensures that otherwise unclassified traffic is still placed into a defined branch of the hierarchy, where PacketShaper can account for it and apply the relevant policy behavior. This fallback behavior makes Default classes important for maintaining complete traffic coverage while allowing specific child classes to take precedence when their matching criteria are met. Broadcom's PacketShaper product information is available at [Broadcom PacketShaper](#), and product documentation and support resources are available through the [Broadcom Support Portal](#).