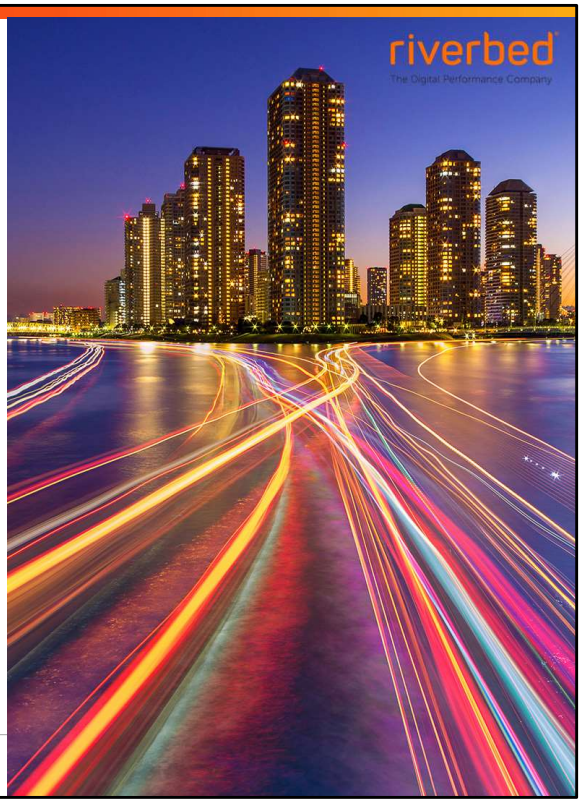
Learning Objectives

After completing this module, you will be able to:

- Describe the Virtual Desktop Infrastructure.
- Optimize Citrix ICA.
- Verify optimization of Citrix traffic.
- Describe the requirements of backup and replication traffic.
- Tune SteelHeads for throughput.
- Optimize array-based replication.
- Optimize Lotus Notes.
- Optimize NFS.
- Optimize Oracle Forms.



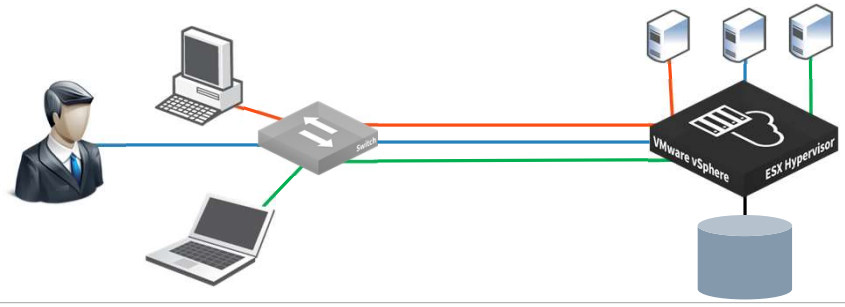
Key Points

- Not all applications are born the same, many have specific requirements.
- The SteelHead recognizes many of the most commonly used applications.
- SteelHeads can be adjusted to suit many applications in many environments.

Describe Virtual Desktop Infrastructure

An Introduction to VDI – *Virtual Desktop Infrastructure*

- Form of virtualization
  - Desktops rather than servers
- Users connect to a virtual desktop on a server in the datacenter
- Enables a fully personalized experience
- Each user has their own, dedicated virtual machine



riverbed 5

Virtual Desktop Infrastructure (VDI) is a form of virtualization that virtualizes desktops rather than servers.

It allows the running of a user desktop inside a virtual machine that lives on a server in the datacenter and enables fully personalized desktops for each user with all the security and simplicity of centralized management.

This key difference between VDI and a standard remote desktop deployment is that the latter will typically utilize shared desktops whereas with VDI, each user has their own, dedicated virtual machine.

This does require greater resources but also gives a much more stable and customizable experience.

Benefits of VDI

- VDI offers a number of key benefits:
  - Use of the same image
  - Platform independence
  - OS migration
  - No expensive desktop hardware upgrades
  - Agile working
  - Snapshot technology
  - Support for legacy applications
  - Easier troubleshooting
  - Security

riverbed 6

The adoption of VDI has seen huge growth in recent in years with no sign of slowing down. This is because VDI offers some key benefits:

Use of the same image: One of the key benefits of VDI is that multiple desktops can be created using the same operating system and applications, including settings. This enables rapid deployment and greatly simplifies management.

Platform independence: Within a VDI environment, the virtual desktop can be accessed from any platform: PC, Mac, Linux and even mobile devices. Outside of a VDI infrastructure, hardware dependent images need to be maintained with the correct drivers installed for each. This also has implications for platform purchase, ensuring sufficient CPU, memory and disk and also correct hardware components. In addition, there will have to be completely different images for MAC and PC.

OS migration: Imagine the roll out of a Windows 10 deployment to a large organization, which is currently at, say, Windows 7. Prior to VDI, you would have to look at the existing equipment and most likely upgrade hardware, memory, disks, etc. VDI makes this far easier by pushing out the Windows 10 image from a central location.

No expensive desktop hardware upgrades: Tied to the above point, upgrading the OS and/or applications often goes hand-in-glove with hardware upgrades. Again, this is avoided with VDI as the hardware is both centralized and virtualized.

Agile working: Another key benefit of VDI is that it allows users to work from any location at any time, using any device, providing they have internet access. From a business perspective this increases productivity and job satisfaction for employees, who benefit from the flexibility and freedom to work from wherever they choose.

Snapshot technology: A key benefit of virtualization is the ability to roll back to an earlier point in time using snapshotting technologies. Not only does this give great flexibility, but also provides resilience against data loss, corruption and malware.

Support for legacy applications: For some businesses, certain key applications are not supported by modern operating systems. Virtual desktops can be maintained on these legacy systems, which can be locked down using security policies.

Easier troubleshooting: It is far easier troubleshooting a central, common desktop, rather than a remote desktop, where the problem might even be in hardware. Also, the ability to simply roll back to an earlier, working snapshot provides a very quick resolution to many problems.

Security: With VDI, the data is not stored on the device, so if the client device (e.g., laptop, tablet or phone) is ever stolen, the corporate data is still secure in the datacenter. You can also secure an image from external devices to prevent data from being copied from the virtual desktop to the local machine. It is also far easier to ensure that the latest virus and security updates are always applied to the central image.

Key VDI Vendors

- Microsoft
  - Microsoft *Remote Desktop Services*, sitting on top of Hyper-V, allows users to access virtual desktops using the RDP protocol.
- VMware
  - Horizon View - VMware vSphere virtual desktops accessed by either View clients using the PCoIP protocol, or browser-based clients using the Blast protocol and HTML5.
- Citrix
  - XenApp - Application Virtualization
  - XenDesktop – Desktop Virtualization
  - Uses ICA on ports 1494 and 2598

Microsoft: In Windows 2008R2 and later, Microsoft *Remote Desktop Services*, sitting on top of Hyper-V, allows users to access virtual desktops using the RDP protocol. See the following page for more information: https://blogs.technet.microsoft.com/enterprisemobility/2009/08/19/microsoft-vdi-overview/

VMware: VMware Horizon View has VMware vSphere virtual desktops accessed by either View clients using the PCoIP protocol, or browser-based clients using the Blast protocol and HTML5.

Citrix: Citrix has two key VDI solutions: *XenApp,* which provides both application and desktop virtualization, and *XenDesktop*, which provides desktop virtualization. The key difference between the two is that *XenDesktop* provides a desktop operating system so when you connect to the desktop you are the only person using it. This compares to *XenApp* where you are sharing it with other people who could affect performance. Communication between the Citrix client (*Receiver*) and server is transported using the ICA protocol. Citrix ICA traffic is usually transported on TCP port 1494. Citrix ICA traffic is transported on TCP port 2598 if Citrix session reliability is enabled. When you enable Citrix session reliability, the client tunnels its ICA traffic inside the Common Gateway Protocol (CGP) port 2598.

How Can Riverbed Help?

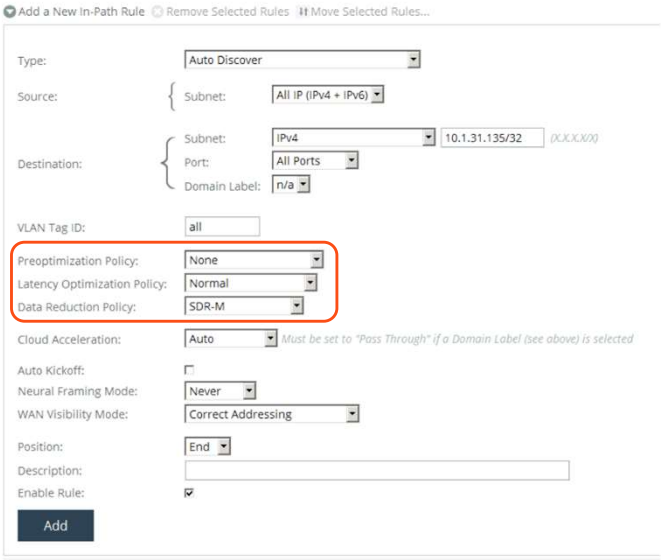
- Like other applications, VDI is sensitive to both bandwidth and latency.
- Riverbed can help in two main ways:
  - Moving the delivery of the VDI sessions to the branch using SteelFusion
  - Directly optimizing and applying QoS to the traffic
- Be aware that VDI traffic is dependent on user interaction and so not as predictable as standard transactional traffic such as SMB.
  - From the user perspective, the benefits will not be so obvious
- Key benefits are:
  - Reduced bandwidth utilization
  - A more stable and consistent user experience
  - Fewer dropped sessions when, say, a print job is run

riverbed 8

As with many types of applications, the performance of VDI is dependent on both bandwidth and latency. For restricted WAN bandwidths, sessions can drop when a large print job is run because the print server (and data) is usually at the DC while the client printer is normally at the branch. Furthermore, VDI traffic is quite sensitive to latency. Mouse and keyboard performance can become so slow that applications running over the virtual desktop can be unusable.

Optimize General VDI Traffic

- General configuration steps:
  1. Disable native compression.
  2. Minimize SH induced latency.
     - Disable neural framing.
     - Create an in-path rule for SDR-M.
     - Create an MX-TCP QoS class/rule.



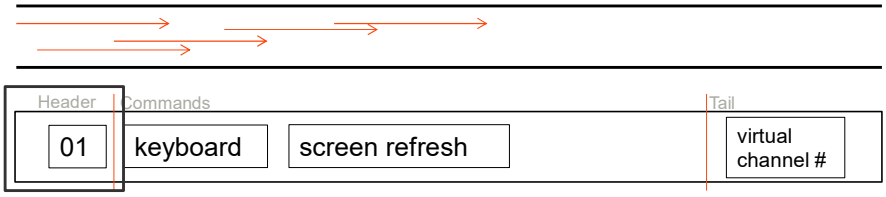
riverbed 9

Riverbed SteelHeads can optimize both RDP and Citrix traffic. In addition, the Application Flow Engine recognizes PCoIP, RDP and Citrix traffic, enabling QoS to be configured. It is by this combination of optimization and QoS that we can significantly improve the user VDI experience. This will ensure that users obtain a much more consistent experience, with fewer connections dropping during, say, a print job while at the same time allowing more VDI connections for the same bandwidth.

Optimize Citrix ICA

Citrix-Specific Optimizations

- Citrix uses ICA: Proprietary protocol developed by Citrix
- Sends mouse clicks, print, file transfer, audio/video, and so on
  - All traffic encrypted and compressed
- Single TCP connection between client/server
  - Each type of traffic has a virtual channel – 15 or 16 defined
  - Each like a mini-protocol within the ICA protocol



- QoS devices are left to do something with the priority bits

Citrix uses the proprietary ICA protocol, which is used to send mouse click, print, file transfer data, and audio/video in a compressed and encrypted format. The ICA traffic within a Citrix session is comprised of many categories of traffic called virtual channels.

Virtual Channels and ICA Priority Groups

- A virtual channel provides a specific function of Citrix ICA remote computing architecture, such as print, client drive mapping (CDM), audio and video.
- Categorized by priority
  - Virtual channels carrying real-time traffic, such as audio and video, are tagged with higher priority than channels carrying bulky, transactional traffic such as print and CDM.
- The ICA priority groups are as follows:
  - Very High (priority 0)
  - High (priority 1)
  - Medium (priority 2)
  - Low (priority 3)

Multi-Stream ICA

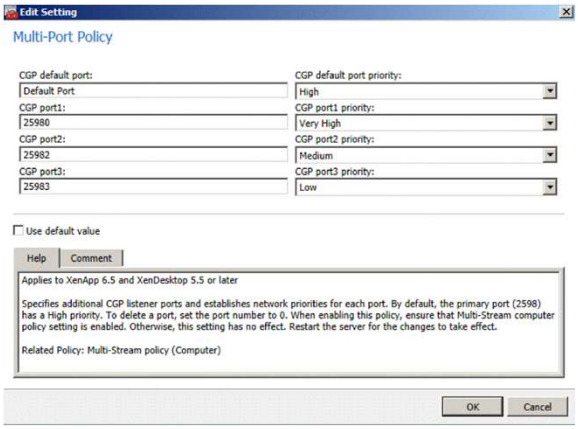
- By default, Citrix uses a single TCP connection between client and server.
  - Each type of traffic has its own virtual channel within the connection.
  - This is known as *Single-Stream ICA.*
- XenApp 6.5 and XenDesktop 5.5 introduced a new feature, called *multi-stream ICA* (only when you enable Citrix session reliability).
  - Enables use of multiple TCP connections within a single Citrix session.
  - Carries traffic on port 2598 and three other user-configurable ports as defined in the multi-port Citrix Computer Policy.
  - Each individual port corresponds to an ICA priority group.
  - Enables network-based QoS policies to be applied directly to the individual priority groups.

By default, Citrix uses a single TCP connection between client and server with each type of traffic having its own virtual channel within that. This is known as *single-stream ICA.*

In XenApp 6.5 and XenDesktop 5.5, Citrix introduced a new feature called *multi-stream ICA*. This enables the use of multiple TCP connections within a single Citrix session. Multi-stream ICA carries traffic on port 2598 and three other user-configurable ports as defined in the multi-port Citrix computer policy. Each individual port corresponds to an ICA priority group and enables you to apply true network-based QoS policies to the priority groups for the virtual channel traffic that they carry. Multi-stream ICA is available only when you enable Citrix session reliability.

Multi-Stream ICA – Multi-Port Policy

- An example of a Citrix Multi-Port Policy is shown below. Note the default port that corresponds to 2598 and an ICA priority of *High.*



Multi-Stream ICA – SteelHead Auto-Negotiation

- The client-side SteelHead can be configured to automatically negotiate multi-stream ICA for the client-side outer connection.
- This creates four TCP connections, each with a different priority group.
- These map to a pre-defined Citrix application on the SteelHead as shown below.
- A QoS Profile can then be created that maps each ICA priority to a class.

Citrix-Multi-Stream-ICA-Priority-0	Citrix very high priority - for real-time traffic like audio
Citrix-Multi-Stream-ICA-Priority-1	Citrix high priority - for interactive traffic like graphics, keyboard and mouse
Citrix-Multi-Stream-ICA-Priority-2	Citrix medium priority - for bulk traffic like drive mapping
Citrix-Multi-Stream-ICA-Priority-3	Citrix low priority - for background traffic like printing

In RiOS 9.1 and later, the client-side SteelHead can be configured, via a single checkbox in the Citrix settings, to automatically negotiate multi-stream ICA for the outer connection between the client and client-side SteelHead.

This then creates four TCP connections, each with a different priority group, which directly map to a pre-defined Citrix application on the SteelHead as shown.

This is useful, as you can then create a QoS profile on the SteelHead for Citrix ICA traffic, ensuring that each ICA priority is mapped to an appropriate class.

Citrix Client Drive Mapping (CDM)

- Client Drive Mapping lets client C:\ drive inside remote desktop
  - Usually mapped as V:\ drive
  - Client D:\ drive mapped as W:\ etc.
- "Local" drag and drop results in WAN traffic
  - Server → client protocol different to server → client
  - The SteelHead understands and optimizes both
- Customers have seen a 10min transfer reduced to 10s

Client Drive Mapping (CDM) is a feature that enables users to access their local drives (such as network drives, USB drives, CD-ROM drives, and hard disk drives) from within an ICA session.

When you use CDM to access a mapped drive the end-user desktop experience can be negatively affected by the underlying network performance.

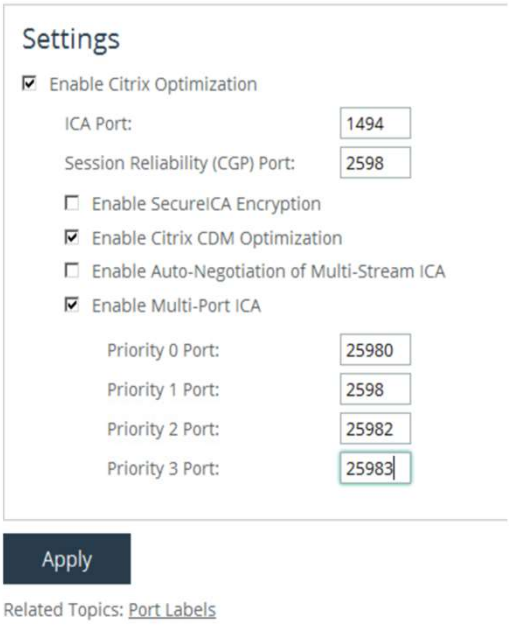
The SteelHeads can be configured to optimize this and thus improve the end-user experience when reading and writing to files on a mapped drive.

In addition to SDR this also has latency optimization, so the improvement in end-user experience is significant.

Configure Citrix Optimization

For each SteelHead seeing Citrix traffic:

1. Remove ports 1494 and 2598 from the *Interactive* port label.
2. Select **Enable Citrix Optimization** and specify the ports if necessary.
3. Optionally, enable client drive mapping (CDM).
4. If multi-stream ICA is being used, click **Enable Multi-Port ICA** and specify the ports.
5. If the ICA session is using high encryption, check **Enable SecureICA Encryption**.
6. Click **Apply** and restart the optimization service.



riverbed 17

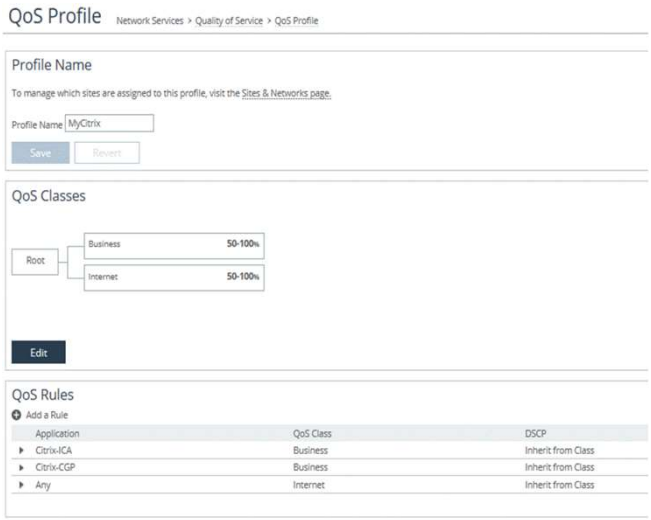
The overall steps required in order to optimize Citrix are as follows:

1. Remove ports 1494 and 2598 from the *Interactive* port label.
2. Click *Enable Citrix Optimization* and specify the ports if they are different.
3. Optionally, enable client drive mapping (CDM).
4. If multi-port ICA is being used, click *Enable Multi-Port ICA* and specify the ports according to what is configured in the multi-port policy.
5. If the ICA session is using high encryption then also check *Enable SecureICA Encryption.*
6. Click *Apply* and restart the optimization service.

These steps must be performed on both the client- and server-side SteelHeads.

QoS Classification for Citrix Traffic

- Recommended in mixed-use environments where Citrix users perform printing and use CDM
- Ensures consistent desktop experience by prioritizing according to latency (priority) and bandwidth
- The Application Flow Engine recognizes Citrix traffic and can be used to assign ICA traffic into an appropriate class



riverbed 18

Use QoS to classify Citrix traffic in a mixed-use environment, where Citrix users perform printing and use client drive-mapping features, as this improves the desktop computing experience for end-users.

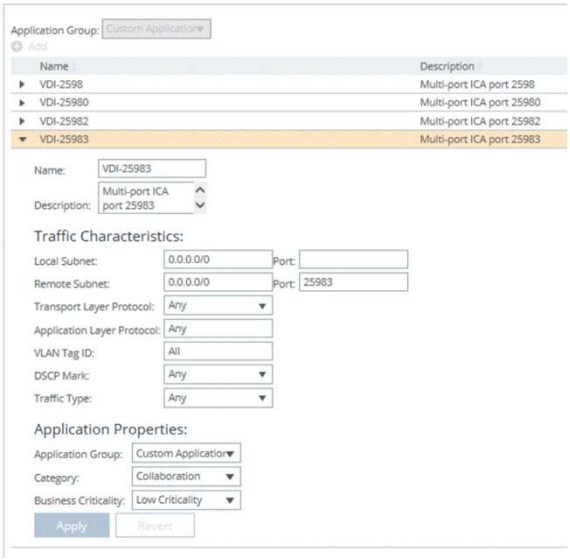
By applying QoS, citrix traffic can be prioritized according to:

- **Latency** - where interactive traffic has a higher priority than, say, printing or CDM traffic.
- **Bandwidth** - ensuring that a particular traffic class has a minimum amount of guaranteed bandwidth on the network, while at the same time ensuring the amount of bandwidth assigned to that traffic does not overrun the network and starve out other applications.

The *Application flow Engine (AFE)* can be used to classify the Citrix ICA traffic and recognizes Citrix traffic on TCP ports 1494 and 2598. You can then use AFE to classify Citrix ICA traffic into a QoS class that is assigned with a higher priority than the QoS classes for other network traffic.

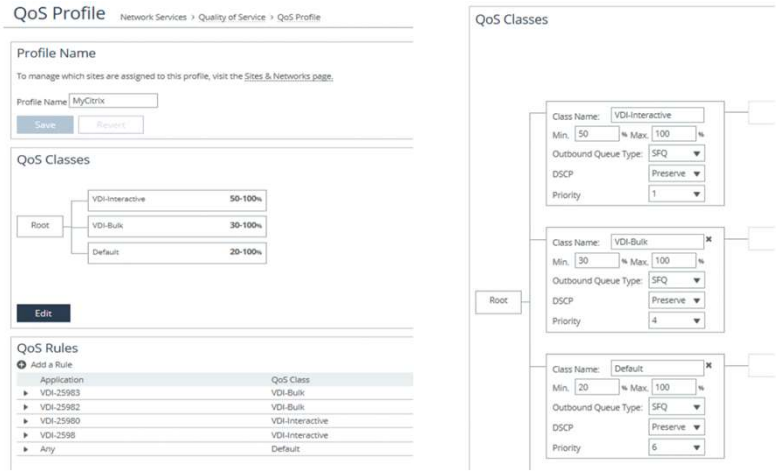
QoS with Multi-Port ICA Traffic – Custom Application

1. If you are not using auto-negotiation of MultiStream ICA, create a custom application for each port, for example (see screenshot):



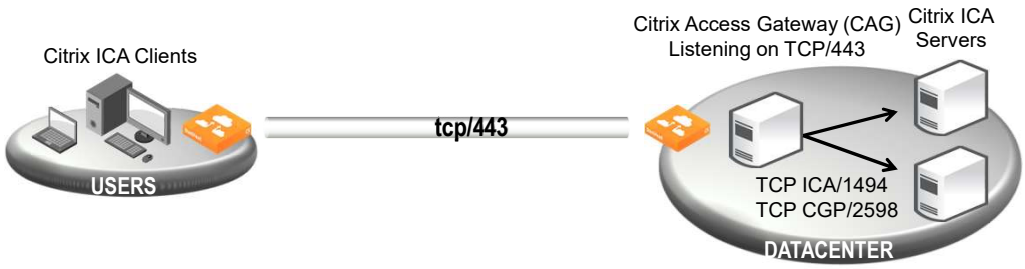
QoS with Multi-Port ICA Traffic – QoS Profile

2. Create a QoS Profile for multi-port ICA traffic using QoS rules that map the Citrix application into an appropriate QoS Class for each of the Citrix classes:



Common Gateway Protocol over SSL – Overview

- Uses Citrix Access Gateway (CAG) to provide secure remote users of XenApp and XenDesktop access over SSL VPN
- Proxies the Citrix ICA traffic over HTTPS or SSL to the end-user
- The overall setup looks like the following:



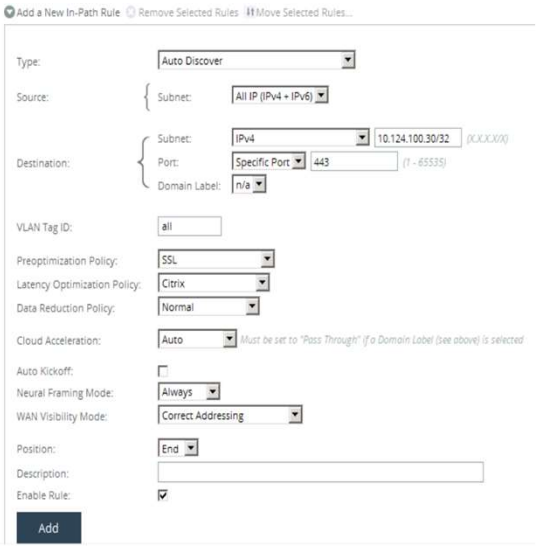
Citrix Access Gateway (CAG) is an appliance that provides secure remote access to users of XenApp and XenDesktop over SSL VPN.

CAG is also known as Access Gateway Enterprise Edition (AGEE) and NetScaler Gateway.

CAG proxies the Citrix ICA traffic delivered from these applications and passes the traffic securely over HTTPS or SSL to the end-user.

Common Gateway Protocol over SSL – Configuration

1. Configure SSL optimization.
2. Install CAG certificate.
3. Create an in-path rule for Citrix traffic.
   - Specify a pre-optimization policy of *SSL* and a latency optimization of *Citrix*.



This is relatively easy to optimize once you realize that it is simply ICA wrapped in SSL. The key method is to configure SSL optimization, just as you would for any other HTTPS site, so you will need an appropriate certificate for the server, but then you will need to create an in-path rule that specifies that this is Citrix traffic. The key is to specify a pre-optimization policy of *SSL* and a latency optimization of *Citrix*.

Note that SDR-M bandwidth optimization is performed automatically with Citrix latency optimization.

Reduction for Citrix Small Packet Real-Time Traffic

- It is recommended to enable enhanced data reduction for real-time Citrix traffic that is sent in small packets, such as keystrokes, mouse clicks, and other Citrix packets that are less than 64 bytes.
- To enable or disable Citrix optimization for small packets, use the following command:
  - **`[no] protocol citrix smallpkts enable`**
- To check whether or not optimization for small Citrix packets is enabled, use the following command:
  - **`show protocol citrix smallpkts`**
- Configure on both the client-side and server-side SteelHeads.

riverbed 23

Riverbed recommends that you enable enhanced data reduction for real-time Citrix traffic that is sent in small packets, such as keystrokes, mouse clicks, and other Citrix packets that are less than 64 bytes.

Optimization for small, low-overhead Citrix packets is disabled by default.

To enable or disable Citrix optimization for small packets, use the following command:
`[no] protocol citrix smallpkts enable`

To check whether or not optimization for small Citrix packets is enabled, use the following command:
`show protocol citrix smallpkts`

You must perform this configuration on both the client-side and server-side SteelHeads.

Verify Optimization of Citrix Traffic

Verify Citrix Optimization – Current Connections Report

- You should see **CITRIX** in the Application column:

CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time	Application
		192.168.122.202:49182	192.168.121.198:2598	59	32	46%	2014/10/28 10:53:57	CITRIX
		192.168.122.202:49183	192.168.121.198:25980	4	2	54%	2014/10/28 10:54:17	CITRIX
		192.168.122.202:49185	192.168.121.198:25982	5	2	58%	2014/10/28 10:54:17	CITRIX
		192.168.122.202:49186	192.168.121.198:25983	5	2	62%	2014/10/28 10:54:17	CITRIX

- In the above example, the four unique TCP connections show that multi-port ICA is being used, showing the four TCP ports configured in the multi-port policy.

Verify Citrix Optimization – Using the CLI

- **`show protocol citrix [cdm | smallpkts | auto-msi]`**
  - Displays Citrix status
- Options:
  - **`cdm`**
    - Displays whether Citrix client device mapping (CDM) is enabled or disabled and other CDM information
  - **`smallpkts`**
    - Displays whether Citrix small packets optimization is enabled or not
  - **`auto-msi`**
    - Displays whether Citrix auto-negotiate multi-stream ICA is enabled or not

Verify Citrix Optimization – CLI Example

```
branchsh > show protocol citrix
Citrix optimization enabled: yes
Citrix SecureICA enabled: yes
Citrix ICA port: 1494
Citrix Session Reliability (CGP) port: 2598
Citrix Multi-Port ICA enabled: no
Citrix Multi-Stream ICA auto-negotiation enabled: yes
Citrix small packets optimization: no
branchsh > show protocol citrix auto-msi
Citrix Multi-Stream ICA auto-negotiation enabled: yes
```

Putting it all Together – Real World Use Case

Scenario	A global publisher used Citrix so that offices worldwide could connect to their DC in New York where their application was hosted. They had recently opened up offices in South Africa and Malaysia and had users in those locations connecting back to the US using Citrix clients.
Issue	Although sites within the US experienced good performance, users outside of the US were struggling with connections being dropped when print jobs ran, and client-drive mapping was not working correctly. This was a particular problem for their new offices in South Africa and Malaysia, which had limited WAN links and where performance was bringing productivity almost to a standstill.
Solution	The customer contacted one of Riverbed's partners who sold them a SteelHead solution, complete with Professional Services to configure the optimization of their Citrix traffic. The result was that the user experience in South Africa and Malaysia was greatly improved with far fewer connections being dropped. In particular, CDM and printing was now fast.

Describe the Requirements of Backup and Replication Traffic

Overview of Backup & Replication

- In the modern enterprise, application availability is key.
- In the age of the digital transformation, downtimes of even a few hours can lead to significant loss of productivity and revenue.
- Modern backup & replication software needs to:
  a) Backup large amounts of data quickly, protecting against data loss.
  b) Recover the data quickly to protect against service outage.

In the modern enterprise, application availability is key. Back in the 90s, and even well into the mid 2000s, the majority of businesses could survive substantial IT system downtimes of several days.

It was back to pen and paper for a while as tapes were recovered from off-site, servers were rebuilt, operating systems and applications reinstalled and the data finally recovered.

In the age of the digital transformation these timeframes are no longer acceptable.

The line between business and IT is becoming increasingly blurry and the loss of systems and their associated data for more than just a few hours can have a significant impact on productivity and revenue.

Key Problems with Backup and Replication

- Both backup and replication transfer large amounts of data between sites.
- This data must be transferred within a pre-defined time window in order to meet RPO/RTO requirements – the *Backup Window*.
- Often the links have insufficient bandwidth, or for large organizations, the latency is too great for this data to be transferred within the time required.
- By optimizing this traffic with Riverbed SteelHead appliances these times can be significantly reduced, allowing backup windows to be reached and ensuring business continuity plans are met.

Recovery Point Objective (**RPO**)

- How old can the (recovered) data be?
  - Credit card transaction RPO = 0
  - CEO on \\homes\users RPO = 1 day
  - Email RPO = 1 hour
- Lower is better

Recovery Time Objective (**RTO**)

- How long does it take to get the data back to the primary site?
  - 10 seconds for recovery from snapshot
  - 5 minutes to an hour for recovery from on-site disk
  - 1 day to 1 week for recovery from off-site tape
- Lower is better

What is the Difference Between Backup and Replication?

- Backup
  - An application-consistent copy of data stored as a backup file
  - Typically:
    - All data backed up weekly (*Full Backup*)
    - Incremental changes backed up daily (*Incremental Backup)*
  - One copy of the data normally stored off-site
- Replication
  - Regular copies of the data stored in the same format in a secondary location
  - Two main types of replication:
    - *Host-based replication*
    - *Array- or Storage-based replication*
  - Can replicate *Synchronously* or *Asynchronously*

What is the difference between backup and replication?
The difference is subtle but important, especially when we consider how SteelHead appliances can help.

Backup
The process of backup takes a copy of your data and stores it as a backup file in a secondary location, typically in a deduplicated and compressed format.

Backup also has the concept of *backup cycles*:
- *Full Backup* - backing up all of your data once a week
- *Incremental Backups* - backing up the daily changes

The key thing here is that, as the full backups contain a lot of data, which has been backed up before, these particular backups benefit greatly from SDR. Even your incremental backups should be copied over more quickly as the block size used by common backup applications is typically in the order of KB rather than the average block size used in SDR, which is 128 bytes, giving ample opportunity for SDR.

Replication
Replication involves taking a copy of your data and then storing it in the same format in a secondary location. There are lots of flavors of replication. Two common ones are:

- *Host-based replication* - Replication occurs at the server level and is typically performed by either software running on the server or some type of proxy. Two good examples of this are Veeam and Zerto where a virtual machine is quickly copied from one VMware/Hyper-V host to another, irrespective of the underlying physical storage.
- *Array- or storage-based replication* - Replication is built into the underlying storage system and is performed independently of the host. Two good examples of this are NetApp's SnapMirror and EMC's SDRF.

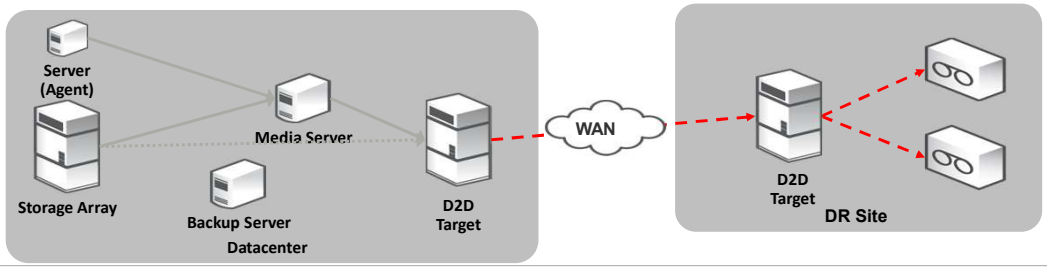
There is also synchronous and asynchronous replication. Most of the situations that you will encounter when optimizing using Riverbed will probably be asynchronous.

Again, Riverbed can help with all of these, using our unique blend of bandwidth and transport optimization.

Optimize Backup and Replication Traffic

Key Considerations

- Are there existing SteelHead appliances?
  - If so, how were they sized?
  - Optimizing replication traffic that is different from user data
- Would generally want a dedicated pair of appliances
- Watch out for encrypted and compressed backup traffic
- How much data needs protecting?
- What is the backup window?



There are a number of issues to be aware of when optimizing backup/replication traffic.

One of the most important concerns is whether there are existing SteelHead appliances and what size they are. SteelHead appliances are normally sized based on number of connections and will typically have a datastore/segstore, which is too small for replication traffic.

This will result in the datastore ‘wrapping’ (i.e., filling up and then over-writing the existing references with new data). You will also be replacing all of your lovely user data with backup/replication traffic. The solution is to have a dedicated set of SteelHead appliances, just for the replication traffic, and sized appropriately.

In terms of sizing appliances in this type of environment you first of all need to know how much data is being copied and how quickly this needs to take place – the so, called *backup window.* You also need to know, roughly, what type of data is being optimized: file video, general, etc.

Backup and Replication Types

- Software-based backups and replication over WAN
  - Include backups with Veeam, NetBackup, replication with DoubleTake, CA XOSoft as well as standard protocols like CIFS and FTP
- NAS replication
  - Primarily file data like NetApp SnapMirror, EMC Celera, HDS HNAS, and BlueArc
- SAN replication
  - High-end SAN replication like EMC SRDF/A, HDS TrueCopy and HUR, IBM PPRC, HP EVA
  - Other SAN replication technologies like Dell EqualLogic, Compellent
- Power Office use
  - Sites exhibiting very heavy file and mail usage that causes sustained and high rates of traffic
- For replication requirements it all boils down to desired LAN throughput
  - Low: < 10Mbps
  - Med: 10Mbps - 75Mbps
  - High: 75Mbps - 200Mbps
  - Med High: 200Mbps - 622Mbps
  - Very High: > 622 Mbps

riverbed 34

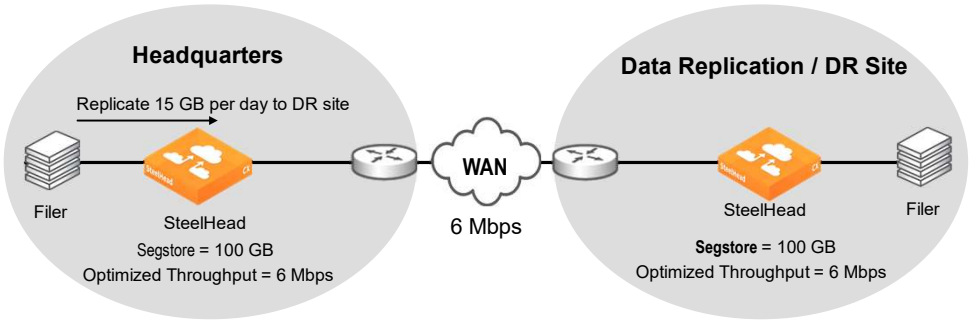
Problem: How to protect data with an effective DR strategy covering storage growth, network limitations, and many sites.

Solution: Protect more data, recover faster, and reduce costs with DR specific optimizations – Simple! ☺

Centralize backup:
- Backup over WAN
  - Off-site backups of data direct to disk to eliminate local tape libraries
- Consolidate servers and backup within datacenter
  - Centralize storage operations, without impacting branch user performance

Improve replication:
- Branch to datacenter, or datacenter to datacenter
  - Defer network bandwidth upgrades by reducing utilization and overcoming latency
  - Shorten time required, which lets you shorten windows or protect more data
  - Reduce impact on other WAN application by freeing up bandwidth

Sizing Example: Data Backup



Scenario	Data Redundancy	Data Type	Disk Efficiency (Approx.)	Actual Segstore Used Per Day	Days of Warm Data	Notes
1	Best Case	Logs, text, full backup	1:5	3 GB	33 days	(Segstore size 100 GB)/(3 GB per day)
2	Typical	Mixed data (MS Office), database, text/logs	1:3	5 GB	20 days	(Segstore size 100 GB)/(5 GB per day)
3	Worst Case	Images, compressed files	1:2	7.5 GB	14 days	(Segstore size 100 GB)/(7.5 GB per day)

So, for example, imagine we were optimizing 15 GB of data per day across a 6Mbps link with a smallish SteelHead with a 100 GB datastore. The above table shows how many days of warm data you could expect.

The key point here is that, for the best case, we can expect a month of warm data, and even for the worst, we will still have two weeks. We would want a bare minimum of at least a week, so this datastore size is OK.

An Exercise in Expectations

- "I want to copy 1.8 TB of nightly database dumps over my OC-3 within a 10 hour window."

$$\frac{1.8\ TB}{10\ hour} * \frac{1000\ GB}{1\ TB} * \frac{1000\ MB}{1\ GB} * \frac{8\ mbit}{1MB} * \frac{1hour}{60\ min} * \frac{1\ minute}{60\ sec} = 400\ \text{mbit/sec}$$

  - Hmm… 400 / 155 = 2.6:1… I could probably do that with just LZ!
- "My daily SnapMirror update of home directories is usually about 4 TB, and I've got a designated DS3, and we can safely be as much as 24 hours behind."

$$\frac{4\ TB}{24\ hour} * \frac{1000\ GB}{1\ TB} * \frac{1000\ MB}{1\ GB} * \frac{8\ mbit}{1MB} * \frac{1hour}{60\ min} * \frac{1\ minute}{60\ sec} = 370\ \text{mbit/sec}$$

  - 370 / 45 = 8.2:1… so we'll likely need disk-based SDR, and I hope their data reduces well… and that LAN-side throughput is high enough to probably need more than one Steelhead.
- "The incremental Veeam backup from a remote T1-attached site is typically 600 GB, and the backup window each night is 8 hours."

$$\frac{600\ GB}{8\ hour} * \frac{1000\ GB}{1\ TB} * \frac{1000\ MB}{1\ GB} * \frac{8\ mbit}{1MB} * \frac{1hour}{60\ min} * \frac{1\ minute}{60\ sec} = 167\ \text{mbit/sec}$$

  - 167 / 1.5 = 110:1 *…for eight hours?!!? Sometimes the best bandwidth between two sites is a freight truck!*

Encryption in Backup & Replication Environments

Be Careful Attempting to Optimize Encrypted Data!

- No bandwidth nor application optimization benefits if encrypted
- Many backup products encrypt data
- Most products offer the following options; the first two causing the greatest issues with optimization:
  a. Encryption at source
  b. Encryption across the network
  c. Encryption at rest
- Most have the option to disable encryption at source/network.
  - If encryption is important, you could encrypt at rest, pass network traffic unencrypted, then optimize and re-encrypt with the SteelHeads using the *Secure Inner Channel &/*or *Secure Transport* features.

Another crucial aspect when dealing with backup and replication environments is that of compression and encryption.

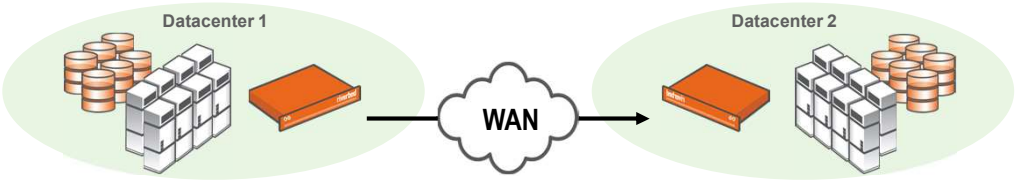
You will not see very much, if any, optimization benefit if the data is encrypted so ensure that, if there is the option to encrypt, that this option is disabled across the network.

Most enterprise solutions allow you to configure this with the following options:
- Encryption at source
- Encryption across the network
- Encryption at rest

It is the first two that will cause problems, but if the customer really does want encryption across the network then one solution is to enable encryption at rest, ensure the native network traffic is unencrypted, and then SSL encrypt the inner channel using the SteelHead *Secure Inner Channel* feature.

DR Deployment: Data Protection Features

- Backup & replication traffic can be quite high-throughput for extended periods
- Optimization can allow much greater throughput, with faster completion
- Compatible with all major vendor hardware and software DR products



- Adaptive Data Streamlining
  - Per Flow SDR-M
  - SDR-Adaptive
- Network integration and management
  - QoS, HS-TCP, MX-TCP
- CPU offload for higher throughput
  - Multi-core balancing
  - Adaptive compression
  - Tunable LZ

Firstly, for the vast majority of situations these settings are not an issue and the default SteelHead settings are fine.

However, there will be occasions, when a large amount of data is transferred across a relatively wide pipe where the default SDR and LZ compression settings might want adjusting.

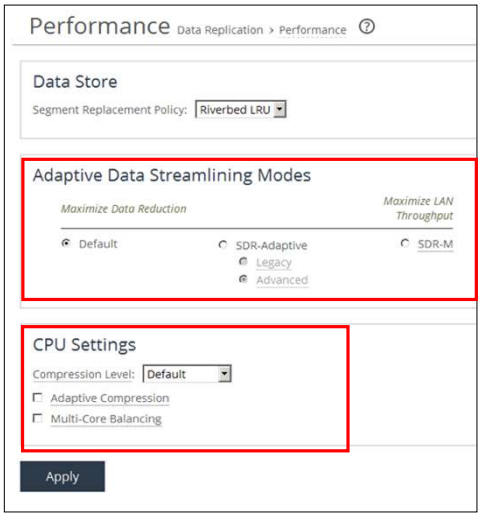
Bear in mind that when we are doing this we are striking a balance between, on the one hand, data reduction, and on the other, throughput.

So in other words, for very high throughput environments the SDR and/or LZ processes might actually be providing a bottleneck and thus might be preventing the throughput from being as high as it could be.

DR Deployment

Data Protection Features

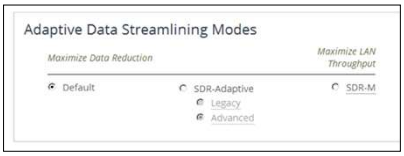
- Corollary/relevant features include:
  - Network integration and management: QoS, MX-TCP, HS-TCP
  - Security, scalability and HA: IPSec, segstore encryption and synchronization, SteelHead clustering solutions, Interceptor



- Performance is normally lower or less than optimal with pre-compressed or pre-encrypted data.
- Databases like Exchange, SQL, and Oracle lend themselves well to SDR, but normally in high throughput environments we may need to turn on the DR knobs per the toolbox.
- SAN replication environments like SRDF/A (especially with high bandwidth) usually equates to starting with the SDR-M option and the same SteelHead model on each side.
- High throughput DC-DC replication scenarios should always have the compression level set to 1 (Low Compression = Increase LAN Throughput).
- Adaptive compression should normally be enabled in high throughput DC-DC replication scenarios.
- For less than four connections multi-core balancing is very useful.
- If the Disk Load report shows 100% for a sustained time or multiple times a day that coincide with periods of lowered performance then turn on SDR-Adaptive mode.
- If the average cost of the segstore is greater than 10000 and the disk load graph for the same period shows high utilization then it is symptomatic of disk performance issues and we should switch to SDR-Adaptive mode.

Data Streamlining Modes

- Data Streamlining Modes
  - Default – SDR & reading/writing data to disk, coupled with compression
  - SDR Adaptive – shift between default SDR and compression-only
  - SDR-M (Memory) – Memory based SDR, increases LAN throughput



- Adaptive SDR & Per Flow SDR-M
  - Focused on high throughput DR environments like SRDF/A
  - Dynamically uses SteelHead appliance resources (disk, CPU, memory) to provide maximum performance for disaster recovery operations
  - Data streamlining in either memory (higher throughput) or on disk (greater reduction) uses both data deduplication and compression

```
datastore sdr-policy ...
```


Database log files should typically use LZ-only as there is not too much common data that one can leverage and LZ-only gives great results.

SDR-Adaptive options:

- Legacy: Monitors disk I/O response times, and based on statistical trends, employs a blend of disk-based de-duplication and compression-based data reduction techniques.
  Important: Use caution with this setting, particularly when optimizing CIFS or NFS with pre-population. For more information, contact Riverbed Support.
- Advanced: Monitors disk I/O response times and WAN utilization, and based on statistical trends, employs a blend of disk-based de-duplication, memory-based de-duplication and compression-based data reduction techniques.

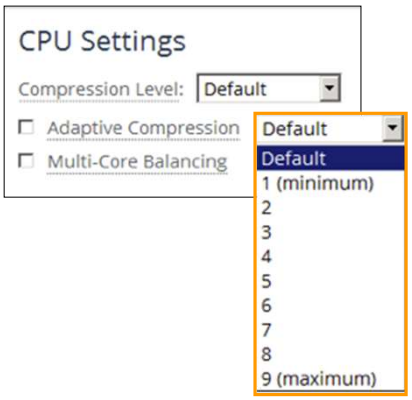
Replication environment example:
Maintaining high throughput while providing data de-duplication over LFN for random workloads or disk-seek-heavy workloads (like database replication).
Solution:

- SDR-M mode allows SteelHeads to de-dupe and accelerate data at high throughput
- Might want to consider Multi-core Balancing with minimal LZ
- Typically used when time to completion is the primary goal
- Used with random workloads like database, SAN replication environments

CPU Settings

- Compression Levels
  - Levels 1 – 9: the higher the number the more LZ & CPU effort; the lower the number the less LZ is applied
  - Default Level = 6
- Adaptive Compression
  - Per connection, switches to LZ level 0 if compression is “not effective”
  - Periodically (sample rate) re-checks data
- Multi-Core Balancing
  - Better spreading of load across available CPUs
  - Useful for applications that use few connections (SRDF/A, etc.)

```
# datastore codec multi-core-bal
```



Problem

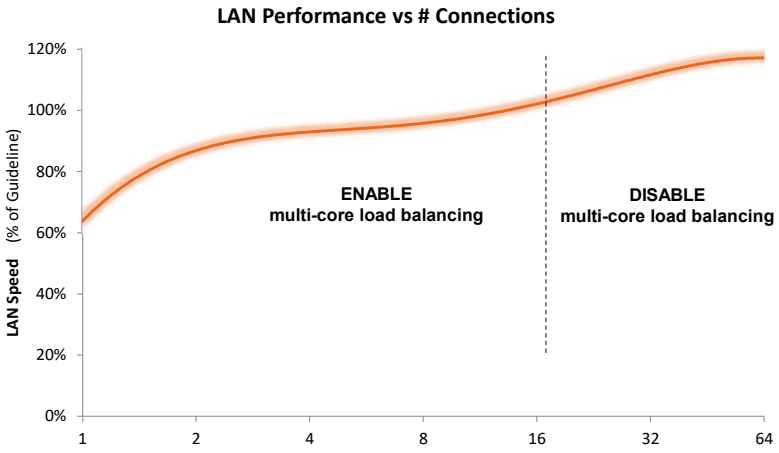
- Time to completion is primary objective with maximum LFN utilization
- Single stream job on a multi-core CPU bottlenecked on the single CPU
- CPU pressure issues

Solution: CPU offload features

- Adaptive compression
- Dynamically disables LZ compression when not effective
- Multi-core balancing
- Balance single stream processing across available CPU cores
- Tunable LZ Levels (1-9) can be tuned, the lower the number the higher the LAN throughput

Together, these CPU offload features can increase throughput by 30% or greater, enabling higher throughput and hence better RPO/RTO (Recovery Point Objective, Recovery Time Objective).

Multi-Core Balancing



- 64+ connections delivers maximum performance
- 16 or less connections, ENABLE multicore balancing
- 16 or more connections DISABLE multicore balancing

riverbed 43

Multicore balancing distributes the load across all CPUs, which maximizes throughput. Multicore balancing improves performance in cases where there are fewer connections than the total number of CPU cores on the SteelHead. Without multicore balancing, the processing of a given connection is bound to a single core for the life of the connection. With multicore balancing, even a single connection leverages all CPU cores in the system.

Continuous code improvements to the performance of single connections has made it unnecessary to enable multicore balancing in RiOS 8.0 or later when 8 or more connections are used. Enabling multicore balancing in these conditions will cause a lower throughput.

Under normal optimization scenarios this feature should be disabled. SteelHead Multi-Core Balancing may be appropriate after careful review of the environment by a Riverbed Sales Engineer.

Performance Tuning Summary

- Understand the data protection environment.
- Find and eliminate bottlenecks at all levels.
  - End hosts – CPU and disk
  - Undersized network buffers on SH appliances and routers
  - Tackling packet loss environments
- SteelHeads offer *multiple* knobs and dials that could be used in data protection / data replication scenarios.
  - Riverbed strongly recommends reading the appropriate sections in the SteelHead Appliance Deployment Guide, and complete the Predeployment Questionnaire.
  - Riverbed also recommends consultation with Riverbed Professional Services or an authorized Riverbed Delivery Partner when planning for a data protection deployment.

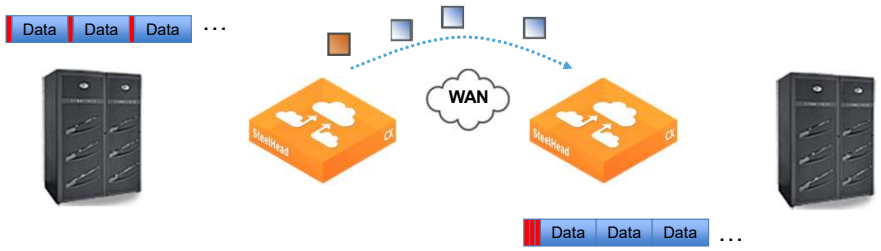
To identify and resolve SteelHead performance issues:

- Check to see if there is a slowdown in time but great data reduction.
- Take sysdumps and provide throughput charts to support.
- Work with your SE or Riverbed support to confirm your findings.

Optimize Array-Based Replication

Array-Based Replication
SRDF and FCIP Optimization

- Use protocol knowledge to improve WAN utilization and performance.
- De-duplicate data, not random protocol headers
  - V-MAX SRDF/A – 8 bytes of DIF for every 512 bytes of data
  - FCIP – 68 bytes of FCIP/FC header for every ~2100 bytes of data
  - SteelHead can auto detect the header size



Riverbed is the only WAN optimization vendor to provide both network AND application optimizations for FCIP and SRDF protocols.

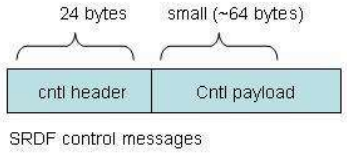
Just like TCP includes header information, which should be excluded from de-duplication algorithms, FCIP and SRDF has the same.

This is depicted here, where the blue “Data” areas are interrupted by the “red” pieces of header information, which is essentially random. Due to Riverbed’s application-fluent architecture, the SteelHead is able to intelligently apply de-duplication to the data areas only. Prior to de-duplication, the random headers are set aside, then reinserted at the destination. We then de-duplicate the data, not the random headers.

There are also specific settings for both NetApp and EMC.

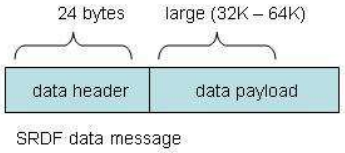
SRDF and FCIP Data Formats

- SRDF and FCIP use a header / payload format
  - Headers are “escaped”: no SDR
  - Control messages are also escaped



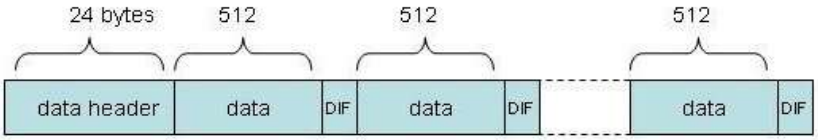
SRDF control messages

- Data streams are rearranged
  - Headers put to one side
  - Data aggregated and SDR’d



SRDF data message

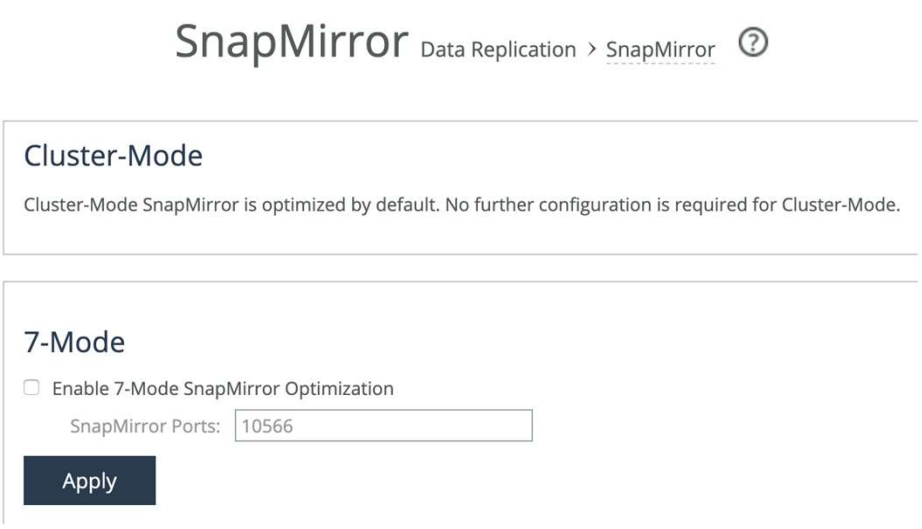
- Data Integrity Fields hate SDR!
  - DIFs treated just like headers



SRDF data message with DIF

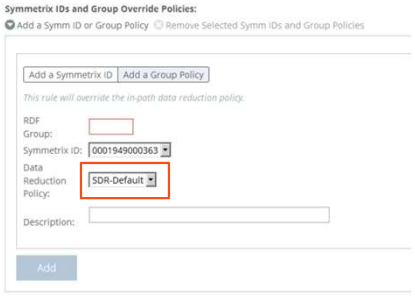
SnapMirror and SRDF Optimization

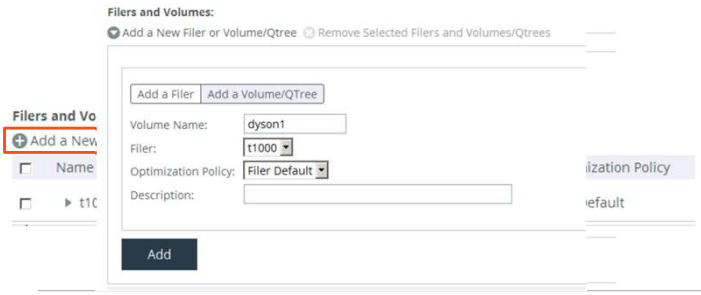
- Cluster-Mode SnapMirror is optimized by default.
- 7-Mode SnapMirror optimization needs to be enabled.
  - **Data Replication > SnapMirror**



SnapMirror and SRDF Optimization (Continued)

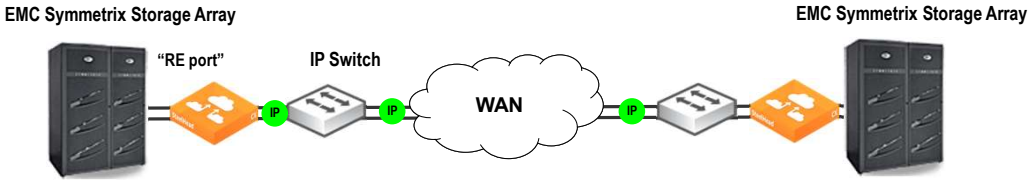
- SRDF and SnapMirror can set per flow SDR policy
- Examples:
  - "None" on the "daily random image" archive
  - "LZ-Only" text file directory with lots of turnover
  - "SDR-Default" on the email archive
- SRDF uses "RDF groups" (remote data facility)
- SnapMirror has volumes and Qtrees





For NetApp, you can add a specific filer with a default optimization policy: *SDR-Default, LZ-Only or None.* You can then specify rules for particular Volumes with specific optimization policies for each. In this way, you can target volumes with particular types of data and give them the data reduction mode most suitable for them. e.g., Files/Documents could have *SDR-Default* and Video could have *None.*

Sizing and Best Practices for EMC SRDF/A



- Symmetrix GigE Ports called “RE ports”
- Full mesh of connections between src and dst RE ports
  - 2 src ports and 2 dst ports → 2 x 2 = 4 connections
  - 4 src ports and 4 dst ports → 4 x 4 = 16 connections
- Symmetrix array can create more than 1 connection per pair.
  - Up to 4 connections per pair can be configured
  - But, 32 is max supported between Symmetrix arrays
- Best practices
  - Maximize SRDF connections
  - Disable speed limit, let SH figure out throughput

For the Symmetrix array, try and get the max number of 32 connections going end-to-end.

Symmetrix – High-end family of monolithic storage arrays. Everything in pairs/redundant.
DMX – Name of actual arrays. Come in “series”, e.g., DMX-4 is current and what Riverbed owns.
SRDF – Symmetrix Remote Data Facility. App-level protocol to replicate data between DMX arrays.
Fibre Channel – Storage networking protocol. Not IP.
RA port – “Remote Attach”. Describes any kind of port used for SRDF transport.
RE port – “Remote Ethernet”. Describes an RA port that’s GigE.
FA port – “Fibre attach”. Describes a Fibre Channel port through which host communications occur.

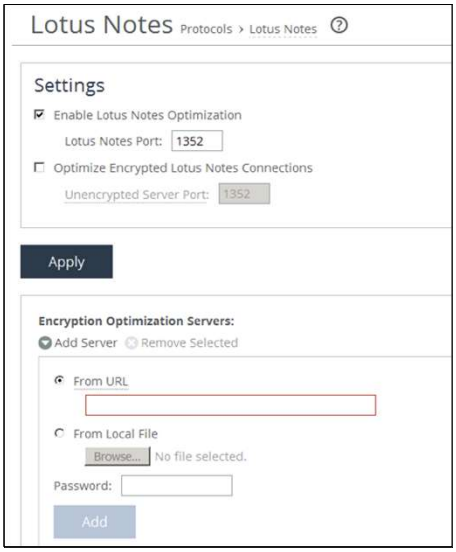
By default, Symmetrix will create 1 connection for each pair of RE ports between the source and destination arrays. For example, a 2 RE port sym talking to another 2-port sym will create 4 connections. However, symmetric can be configured to create up to 4 SRDF connections per pair, with 32 maximum per array. That number of connections will improve the LAN throughput of the SteelHead. They should be able to configure up to 32 per Symmetrix array with 4 RE ports. Also, disabling "speed limit” on the RE ports will be necessary.

Optimize Lotus Notes

Lotus Notes Optimization

- Enables latency and bandwidth optimization for both non-encrypted and encrypted Lotus Notes traffic
- Supports Notes Client and Domino Server version 6.0+
- Improves both client-to-server and server-to-server traffic
- Requires enabling, and in-path rule

```
[no] protocol notes enable
protocol notes port <port-num>
```



RiOS provides latency and bandwidth optimization for Lotus Notes v6.0 and later traffic across the WAN, accelerating email attachment transfers and server-to-server or client-to-server replications. To ensure that the SteelHead appliance can accelerate Lotus Notes traffic, the data must be available in unencrypted and uncompressed form. Lotus Notes and Domino servers have the ability to perform encryption and compression at the port level and compression on a per-attachment basis. These features must be addressed to ensure the SteelHead appliance can perform optimally.

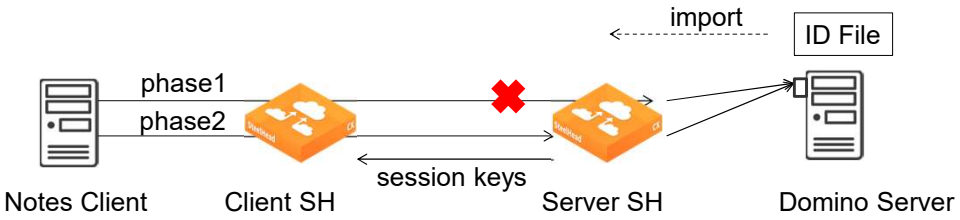
RiOS saves bandwidth by automatically disabling socket compression, which makes SDR more effective. It also saves bandwidth by decompressing Huffman-compressed attachments and LZ-compressed attachments when they are sent or received and recompressing them on the other side. This allows SDR to recognize attachments that have previously been sent in other ways (such as over CIFS, HTTP, or other protocols), and also allows SDR to optimize the sending and receiving of attachments that are slightly changed from previous sends and receives.

To enable optimization of encrypted Lotus Notes connections:

- Both client-side and server-side SteelHead appliances must be running RiOS v7.0
- The Domino servers ID file(s) must be imported into the server-side SteelHead appliance(s)
- The Domino server(s) must be configured with a port on which it will accept unencrypted

Lotus Notes Encryption

- Notes / Domino server uses ID files to exchange encryption information
- Domino server must be configured with “unencrypted port”
- SteelHead must have a copy of the Server ID file
- Phase 1: client connects and server SH redirects to unencrypted port
  - Server SH preserves the authenticated, unoptimized connection to server
  - Server SH drops connection to client
- Phase 2: client reconnects and server SH acts as server to get encryption keys
  - Client SH encrypts and decrypts client traffic
  - SSL/secure peering must be enabled for WAN encryption



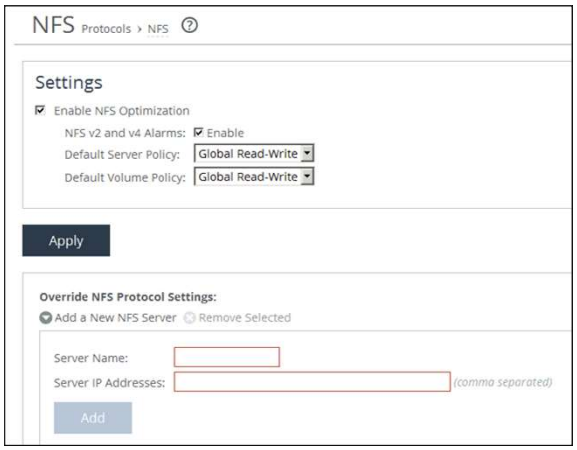
In Phase 1, we redirect to an unencrypted port because the server SH does not have the client ID file and so it cannot authenticate to the server or take part in encryption while acting as a client.

Forcing to the unencrypted port means the client and server will establish an authenticated, plain txt connection.

In Phase 2, because the SH has the server ID file, it can pretend to be the server and authenticate to the new connection that comes in from the client. This client-to-server SH connection will be encrypted.

NFS Optimization

- Provides Latency& Bandwidth optimization for NFS v3
  - NFS v2/TCP & v4/TCP receive bandwidth optimization
- Settings can be global for all servers & volumes (the default), or per-server and/or per-volume



NFS optimization provides latency optimization improvements for NFS operations by prefetching data, storing it on the client SteelHead appliance for a short time, and using it to respond to client requests.

NFSv3 has broad popular adoption by a number of software vendors and is the dominant network file sharing protocol for Unix systems.

RiOS supports NFS application optimization for TCP NFSv3 only. Bandwidth optimization (SDR and LZ compression) still applies to the TCP-based NFS v2 or NFS v4 traffic.

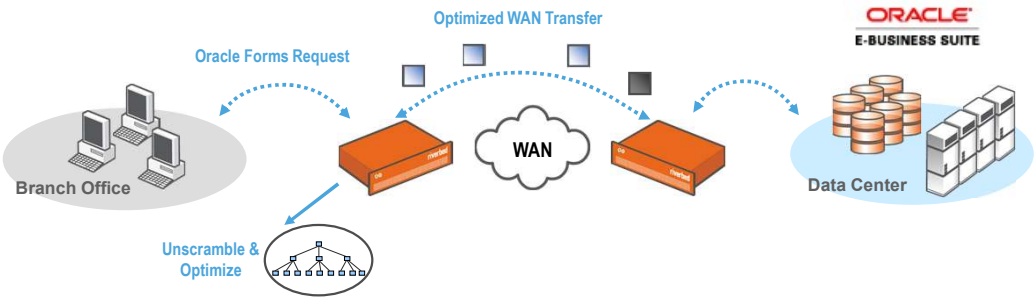
Considerations when optimizing NFS:

- Module does not work with server-side out-of-path (SSOOP) because direction is only from client to server.
- In serial clusters only global read/write and read-only policies are supported
- The client OS is most important for compatibility, when using clients not in our tested list, be extra sensitive for problems (Linux 2.4/2.6, NetApp, Solaris 8-10, IBM AIX 5.1/2)

  Solaris 10 defaults to v4 and TCP
  Linux 2.4 defaults to v2 and UDP
  Linux 2.6 defaults to v3 and UDP
- There are some internal variables which can be tuned if needed.

Optimize Oracle Forms

Oracle Forms HTTP Optimization



- Oracle Forms request is seen by client-side SteelHead
- Client-side SteelHead intercepts and decrypts request
- SteelHead applies RiOS streamlining to optimize WAN transfer
- Server-side SteelHead decodes optimized traffic and sends to Oracle e-Business servers
- Both socket / native and HTTP modes supported

riverbed 57

You can display and modify Oracle Forms optimization settings in the **Optimization > Oracle Forms** page.

Oracle Forms is a platform for developing user interface applications to interact with an Oracle database. It uses a Java applet to interact with the database in either native, HTTP, or HTTPS mode. The SteelHead appliance decrypts, optimizes, and then re-encrypts the Oracle Forms traffic. You can configure Oracle Forms optimization in the following modes:

Native - The Java applet communicates with the backend server, typically over port 9000. Native mode is also known as socket mode.

HTTP - The Java applet tunnels the traffic to the Oracle Forms server over HTTP, typically over port 8000.

HTTPS - The Java applet tunnels the traffic to the Oracle Forms server over HTTPS, typically over port 443. HTTPS mode is also known as SSL mode.

Use Oracle Forms optimization to improve Oracle Forms traffic performance. RiOS v5.5.x and later supports 6i, which comes with Oracle Applications 11i.

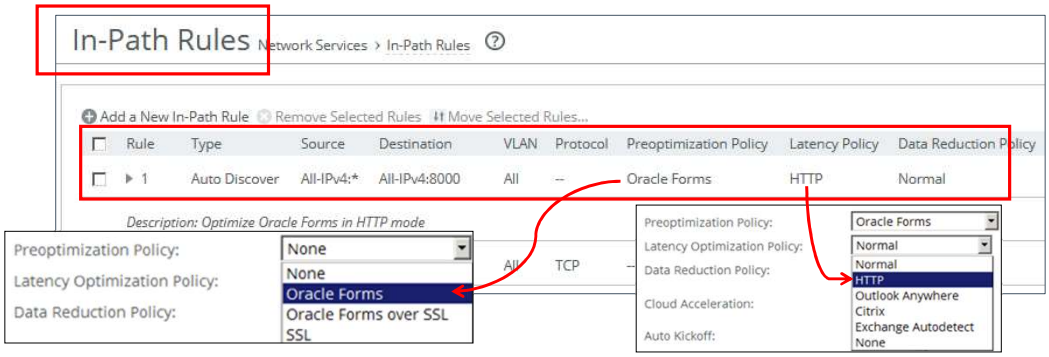
RiOS v6.0 and later supports 10gR2, which comes with Oracle E-Business Suite R12.

This feature does not need a separate license and is enabled by default. However, you must also set an in-path rule to enable this feature.

Oracle Forms Configuration

- Two steps to configure
  - Enable the optimization feature, and HTTP Mode if applicable

  - Add in-path rule(s) to identify and correctly handle Oracle Forms traffic



Before enabling Oracle Forms optimization, you must know the mode in which Oracle Forms is running at your organization. To determine the Oracle Forms deployment mode:

- Start the Oracle application that uses Oracle Forms.
- Click a link in the base HTML page to download the Java applet to your browser.
- On the Windows taskbar, right-click the Java icon (a coffee cup) to access the Java console.
- Choose Show Console (JInitiator) or Open <version> Console (Sun JRE).
- Locate the “connectMode=” message in the Java Console window. This message indicates the Oracle Forms deployment mode at your organization: for example,
  - connectMode=HTTP, native
  - connectMode=Socket
  - connectMode=HTTPS, native

Note: Optionally, you can use the Secure Inner Channel to protect optimized Oracle Forms traffic between two SteelHead appliances over the WAN. This can done in In-Path rules but note:

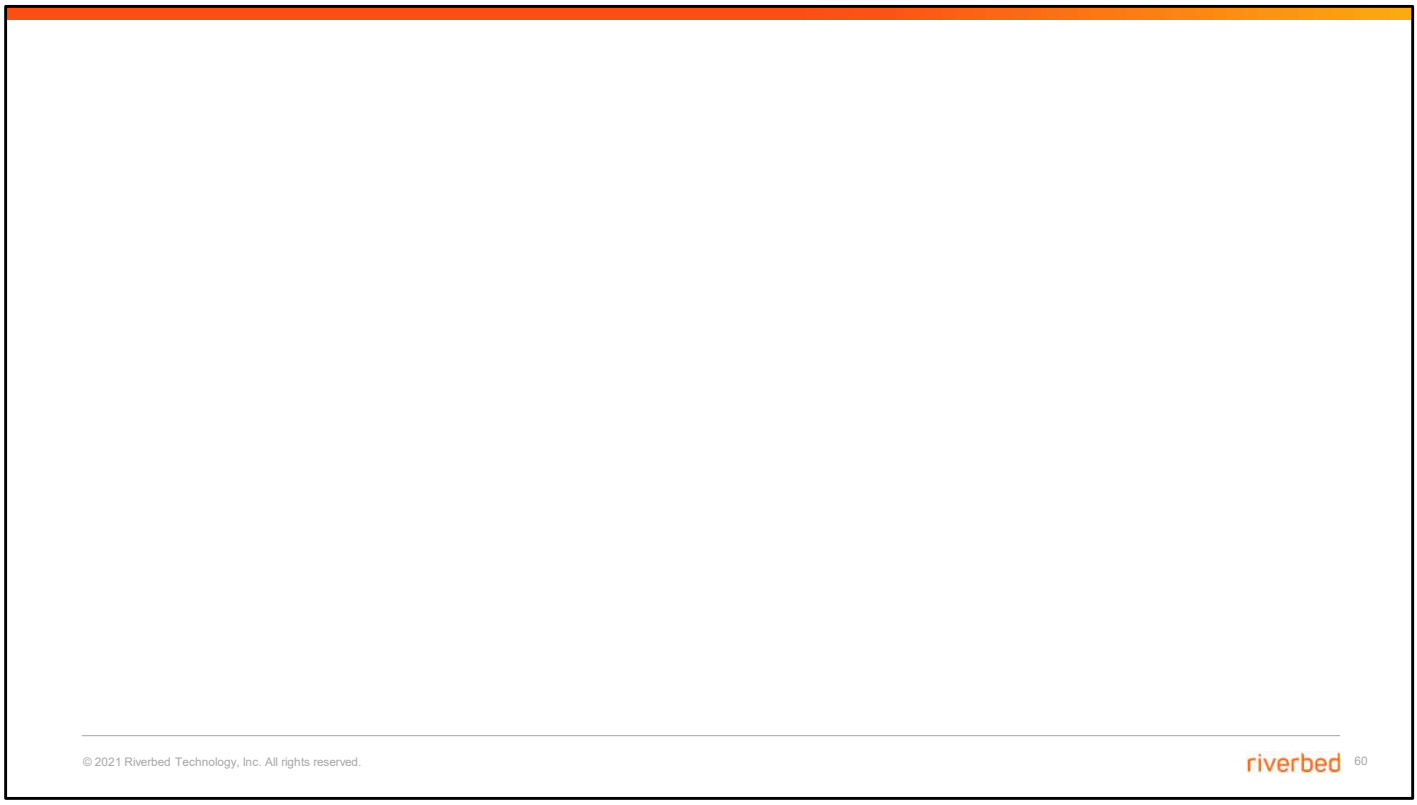
- Preoptimization Policies - Special handling required for Oracle Forms over SSL support.
- Latency Policies - Set to normal, none, or HTTP to support HTTP traffic. Special handling required for Oracle Forms over SSL support.

Module Review

You should now be able to:

- Describe the Virtual Desktop Infrastructure.
- Optimize Citrix ICA.
- Verify optimization of Citrix traffic.
- Describe the requirements of backup and replication traffic.
- Tune SteelHeads for throughput.
- Optimize array-based replication.
- Optimize Lotus Notes.
- Optimize NFS.
- Optimize Oracle Forms.

riverbed
The Digital Performance Company



This slide intentionally left blank.