PCoIP® Protocol Network Design Checklist

TER1105004

Issue 3

teradici®
PCoIP

Teradici Corporation
#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada
phone +1.604.451.5800 fax +1.604.451.5818
www.teradici.com

Revision History

Version	Date	Description
3	7 Mar 2014	Revised bandwidth and network requirements.
2	08 Jul 2011	Added requirement for PortFast and updated bandwidth guideline tables.
1	02 Jun 2011	Initial release.

Contents

Table of Tables

1 PCoIP® Protocol Network Design Checklist

The PCoIP protocol provides a real-time delivery of a rich user desktop experience in virtual desktop and remote workstation environments. To ensure a responsive desktop, the PCoIP protocol must be deployed across a properly architected virtual desktop network infrastructure that meets bandwidth, QoS, latency, jitter, and packet loss requirements.

1.1 PCoIP Protocol Overview

The PCoIP protocol incorporates the following features:

- Uses UDP packets similar to other real-time protocols (VOIP, video conferencing).
- Implements packet reliability and flow control similar to TCP; however, this is done in an intelligent manner consistent with real-time requirements (i.e., USB is always resent, imaging may be resent, but stale imaging/audio is not resent).
- Performs traffic shaping on the PCoIP packet traffic and will dynamically adapt image/audio quality depending on the available network resources.
- Will fairly share the available network resources with other PCoIP sessions on the network.
- Has WAN optimizations already built into the protocol.

For more detailed information, please see techsupport.teradici.com.

2 Network Requirements

The following checklist contains important network requirements to take into consideration.

Table 2-1: General Network Requirements

☐	Consider QoS options such as Class-based Weighted Fair Queuing (CBWFQ) or Low Latency Queuing (LLQ) on switch uplinks and on Layer 3 WAN/LAN links.	
☐	Mark and classify PCoIP traffic the same as real-time interactive traffic according to your QoS marking scheme. (i.e., below VoIP RTP but above all other traffic).	Note: This is necessary for the real-time responsiveness of the protocol.
☐	If using DSCP markings, PCoIP traffic should be marked to DSC AF41 or AF31. This ensures low drop probability inside each queue if WRED must be configured for the queue servicing the PCoIP protocol. The choice of which DSCP value to use is influenced by the presence of possible video and/or VoIP control packets.	Note: Not all switches support the same number of priority queues. Work with service providers to ensure proper end-to-end priority mapping.
☐	Avoid using low latency queuing (LLQ) for PCoIP packets on links that do not carry VoIP and have greater than 1.544 Mbps available. Consider the 33% LLQ rule, which limits the amount of strict priority queuing configured on an interface to no more than one-third of the link's capacity.	Note: The strict priority queue should only be considered if performance is suffering and there are many different types of traffic competing with PCoIP.
☐	Avoid adjusting the MTU on low bandwidth links to decrease serialization time for VoIP packets, as PCoIP protocol packets should not be fragmented.	Note: It may be difficult to guarantee high quality conversations with both VoIP and PCoIP on links with less than 1.544 Mbps of bandwidth.
☐	Consider tuning the hardware transmit ring to 1 to ensure that software queuing takes place if LLQ is not possible and PCoIP or VoIP are experiencing high jitter.	Note: Large packet serialization can sometimes cause high amounts of jitter. This should not be done in most cases as proper CBWFQ usage will allow for acceptable guaranteed session quality.

☐	Increase the queue depth settings in the PCoIP queue if tail drops are experienced. If you are near the maximum recommended queue depths, consider optimizing PCoIP for lower bandwidth or increasing the link bandwidth.	Note: On a Cisco device, look for the drop rate on the "show policy-map interface" command.
☐	Ensure that your classification and QoS schemes work with your WAN carrier's QoS schemes. This is especially applicable to MPLS networks.	Note: Most WAN carriers only offer three or four different classes of traffic on MPLS networks.

☐ Configure Weighted Random Early Drop (WRED) in the path of all PCoIP conversations. On Cisco routers this is the "random-detect" command. The PCoIP protocol incorporates rate limiting and flow control mechanisms optimized for virtual desktops.

Note: Unlike traditional UDP applications, WRED will work with the PCoIP protocol, and gradual packet loss allows time for the PCoIP protocol to adapt. Tail drop does not allow time for the PCoIP protocol to adapt and alleviate the congestion before user experience is impacted.

☐	Confirm that the network interface is not configured for WRED if you have selected WRED for the service policy on that interface.	Note: Configuring WRED on the physical interface overrides all other QoS queuing configurations.

☐ Consider segmenting PCoIP traffic via Layer 2 VLAN and/or COS types at the access layer of your network.

☐	Only use Layer 2 QoS COS prioritization if there is noted congestion at the access layer or between the access and aggregation (distribution) layer.	Note: Consider adding Layer 2 uplink bandwidth before applying Layer 2 QoS, if possible.
☐	Avoid the use of auto-QoS features at the Layer 2 layer for devices that do not explicitly support auto-QoS for PCoIP packets, as this may result in WRED being applied at the switchport layer through the use of Shared/Shaped Round Robin (SRR) queues.	Note: When using the auto-QoS feature, SRR queues are automatically configured on many access layer platforms. By default, these enforce WRED for all but trunked packets marked with COS 5 (generally VoIP packets from a hardphone). Often PCoIP packets are treated as scavenger class traffic, which can negatively impact desktop performance.

- ☐ Avoid traffic shaping unless absolutely necessary. Shaping works to smooth traffic bursts and achieve a defined Committed Access Rate (CAR) by buffering packets. Traffic shaping increases PCoIP packet latency and can impact user experience. If necessary, consider traffic policing as an alternative.

- ☐ Ensure that a full-duplex end-to-end network is used.

  Note: Older switches may incorrectly default to half-duplex when connected to a link with auto-negotiation. In this case, explicitly set the switch link to full-duplex.

- ☐ Ensure that network ports are open for the PCoIP protocol and virtual desktops. For details, see the Teradici Knowledge Base article 15134-114.

- ☐ Ensure that PortFast is enabled on all network ports that have PCoIP end points connected to them.

  Note: If an IP phone is connected between the client and the switch, you may need to set a different PortFast mode because of the internal switch inside the phone. This ensures that the port is immediately configured to forward traffic in the event of a spanning tree recalculation.

- ☐ Ensure Intrusion Protection Services (IPS) in network devices and/or laptop/desktop software have been disabled or configured to allow the PCoIP protocol and other virtual desktop network ports. IPS can block some or all network ports and/or throttle bandwidth for the PCoIP protocol.

- ☐ Ensure that the round trip network latency is within specification. Excessive latency will impact desktop performance.

  - ☐ Latency should be less than 250 ms round trip for virtual desktops and PCoIP remote workstation cards.

- ☐ Ensure the latency variation is less than 30 ms.

  Note: About 1 frame for 30 fps (HD video) is a common default for PCoIP software in virtual desktop products.

- ☐ Minimize packet loss.

  - ☐ Packet loss should be zero for properly configured LAN/WAN deployments. Packet loss within a single PCoIP session should target less than 0.1%.

    Note: Users typically notice performance degradation if the session packet loss is greater than 0.1%, although higher loss may be tolerated.

  - ☐ PCoIP packets that arrive sufficiently out of order may be considered as lost packets by the PCoIP protocol. Avoid packet re-ordering in the network.

    Note: This will show as packet loss in the PCoIP session logs, but not in network device logs.

☐	Avoid gaps in PCoIP protocol traffic. PCoIP sessions will disconnect after 30 seconds of loss in traffic in either network direction or the PCoIP port (4172 UDP).	Note: Intrusion Protection Services (IPS) or Intrusion Detection Services (IDS) should be disabled, or configured to allow (4172 UDP).
☐	Ensure that PCoIP packets are not fragmented at any point in the network path.	
☐	Ensure the MTU in network devices is not below the PCoIP packet MTU size. Defaults are 1200 or 1300 bytes for PCoIP software (depending on the vendor), and 1400 bytes when connecting PCoIP zero clients to PCoIP remote workstation cards.	Note: Increase router MTU before reducing PCoIP packet MTU, as lower PCoIP protocol MTU can impact desktop performance. Keep in mind that network devices may add additional encapsulation and increase the PCoIP packet size.
☐	Ensure that packet order is maintained.	
☐	Do not use per-packet load balancing for any load balancing decisions along the path of traffic, including but not limited to EIGRP load balancing, Static Route load balancing, and MPLS load balancing.	Note: Out of order packets adversely affect the quality of the PCoIP protocol.
☐	For load balancers, ensure affinity (or related) is set to 1.	Note: Ensure that the same SA/DA is sent on the same path.
☐	Configure WAN optimization devices to bypass PCoIP packets unless the devices explicitly support the PCoIP protocol.	Note: Some WAN optimization products can impact PCoIP packets, causing increased latency and packet loss, as well as packet re-ordering.
☐	Ensure that small packets are not prioritized over larger packets.	Note: This can cause PCoIP packet reordering, as small PCoIP packets jump ahead of larger ones.
☐	VPN considerations:	
☐	If a VPN is used, confirm that UDP traffic is supported (IPSEC, or DTLS-enabled SSL solutions).	Note: Do not route PCoIP traffic through TCP-based SSL tunnels.

☐	Avoid VPN overhead. If possible, consider a VPN-less secure remote access solution that supports the PCoIP protocol.	
☐	Use QoS Pre-Classify if CBWFQ or LLQ is necessary on the outgoing interface of the VPN device.	Note: This may not be available on many platforms or in many designs.
☐	Confirm the VMware ESXi virtual switch traffic shaper is turned off.	
☐	Perform a detailed network health check.	
☐	Determine other protocol traffic that exists on the network, especially other high priority traffic that could impede PCoIP forwarding.	
☐	Determine the network characteristics that are key for a successful real-time protocol deployment, including latency, jitter (latency variation), and packet loss.	
☐	Optimize networks for virtual desktop connections.	Note: For details, see the Knowledge Base topics 15134-242 and 15134-880 on the Teradici support site.

3 Network Capacity Planning

The following checklist contains important bandwidth requirements to take into consideration when planning network capacity.

Table 3-1: Network Capacity Planning Guidelines

☐	Ensure sufficient bandwidth is allocated to PCoIP traffic.	
☐	Plan for an *average* of 150–250 Kbps for standard office applications with Windows Experience settings optimized. Or plan for 80–150 Kbps when optimizing the Windows Experience settings and also optimizing PCoIP session variables.	Note: For further details, see Table 5-1 "Mainstream Office Desktop Scenarios".
☐	Consider the bandwidth required for audio input/output.	Note: For further details, see Table 5-1 "Mainstream Office Desktop Scenarios".
☐	Consider the bandwidth required for USB traffic.	Note: PCoIP zero client bandwidth limit will limit USB traffic per PCoIP session.
☐	Plan a minimum of 1 Mbps per simultaneous user watching a 480p video window.	Note: More bandwidth may be required depending on video resolution/user quality requirements.
☐	Ensure network bandwidth analysis includes following network loading guidelines (i.e., 60%–80%).	Note: Hardware interfaces running at over 80% utilization tend to have problems queuing packets due to network burstiness, resulting in packet drops.
☐	Ensure there is sufficient bandwidth headroom for bursts of PCoIP protocol traffic.	
☐	Plan for a minimum bandwidth headroom of 500 Kbps to 1 Mbps.	Note: The actual burst bandwidth required will depend on the user and applications (e.g., the number of pixels changing, the level and complexity of compression, and the display frame rate).

☐	Plan for adequate burst capacity for host card users.	Note: Many workstation applications require a higher burst bandwidth that varies per user and imaging workload. It also depends on how many users are sharing the link.
☐	Over-subscription analysis (optional) can enable efficient link sizing while maintaining a reasonable expectation that burst bandwidth is available per session.	Note: Use of enterprise network loading guidelines is a reasonable basic planning alternative.
☐	Consider bandwidth reduction options when operating in a known constrained network environment.	
☐	Optimize desktop Windows Experience settings (implement this first).	
☐	Optimize PCoIP session variables.	Note: For further details, see Section 4 "PCoIP Session Variables".
☐	Optimize display resolution and/or number of displays.	

4 PCoIP Session Variables

Note: Depending on the version of your software, some session variables can be manually modified (and will go into effect) during an active session.

Table 4-1: PCoIP Session Variables

PCoIP Maximum Bandwidth Limit

- Sets a limit on the bandwidth a PCoIP session can use. Be careful not to set a maximum bandwidth limit too low since the PCoIP protocol needs to burst. Consider setting when operating in a network with known link congestion. The limit set can vary across usage scenarios, such as the following:
  - Single user on a link (i.e., home user on an Internet connection). Set bandwidth limit to 90% of the link rate.
  - Consider setting the maximum bandwidth to **[(available bandwidth for PCoIP packets)/(n users)] + 500 Kbps**.
  - The minimum bandwidth limit should be set between 500 Kbps and 1 Mbps; however, this may need to be increased, depending on the user requirements (see examples in Table 5-1 "Mainstream Office Desktop Scenarios").

PCoIP Bandwidth Floor

- The minimum bandwidth that will be transmitted when the session is attempting to transmit at a rate above the minimum. Consider only if operating on a network with known packet loss (i.e., wireless). Ensure sufficient bandwidth is available: **(n users) * (minimum bandwidth) <= available link bandwidth**

PCoIP Audio Playback Bandwidth Limit

- Configures audio compression. Resulting audio bandwidth will be near or below the limit set.

PCoIP Imaging: Minimum Image Quality

- Trades off display image quality with display frame update rate (i.e., lower image quality for a higher frame rate, etc.).

PCoIP Imaging: Maximum Initial Image Quality

- A lower maximum initial image quality will reduce the peak bandwidth during large screen changes and will also reduce the initial display quality.

PCoIP Imaging: Frame Rate Limit

- Sets a limit on the display update rate. Reduces average and peak bandwidth for high frame rate display content. Only useful when the native frame rate is above the limit.

PCoIP Session MTU

- Option to adjust the PCoIP packet MTU to ensure it is lower than the network MTU.

PCoIP Client PCoIP UDP port

- Option to adjust the PCoIP UDP port that is used at the client.

5 Sample Network and Bandwidth Settings

5.1 Configuration Example

The following example contains marking and CBWFQ with LLQ for VoIP. SIP traffic is not treated. The example assumes a LAN Ethernet interface and a WAN Serial T1 interface. QoS is configured to guarantee the following:

- Strict Priority for four G.729 VoIP calls marked as EF.
- Reserved bandwidth for two "task worker" PCoIP sessions marked as AF41 (500 Kbps minimum peak bandwidth, limited ability for over-subscription).
- The default class gets all the remaining bandwidth and is fair queued.

Sample router configuration settings:

```
!match PCoIP packets

access-list 100 permit tcp any any eq 4172

access-list 100 permit udp any any eq 4172

class-map match-all VOIP-IN
match ip rtp 16384 16383
class-map match-all PCOIP-IN
match access-group 100

class-map match-all VOIP-OUT
match ip dscp EF
class-map match-all PCOIP-OUT
match ip dscp AF41

policy-map ETH-IN
class VOIP-IN
set ip dscp EF
class PCOIP-IN
set ip dscp AF41

policy-map SERIAL-OUT
class VOIP-OUT priority 128
class PCOIP-OUT
bandwidth 1000
class class-default
fair-queue

interface Serial 0/1
bandwidth 1544
no fair-queue
service-policy output SERIAL-OUT
```

```
!trust dscp markings coming into this router from across the WAN

!do this if you need Layer 2 COS QoS and have a DSCP-COS map defined or set
COS on e0/1

mls qos trust dscp

interface Ethernet 0/1
service-policy input ETH-IN
```

5.2 Sample Guidelines

Due to variation in user perception, these general guidelines are only intended to provide a starting point. More or less bandwidth may be needed to satisfy user performance requirements based on application usage. Real world testing in your own environment with realistic workloads is required.

5.2.1 Mainstream Office Desktop Scenarios

The following tables show recommendations for basic virtual desktop users.

Table 5-1: Mainstream Office Desktop Scenarios

Example Virtual Desktop User Categories	General Office			
	Simple Screen Data/Text Entry	Basic Office & Web	Fast Window Switching	Win7 Aero Glass
Task Worker	✓			
	✓			
Basic Office	✓	✓		
Office Productivity	✓	✓		
	✓	✓		
Advanced Office	✓	✓	✓	
	✓	✓	✓	✓

Example Virtual Desktop User Categories	Video Resolution					Video Usage	
	Embedded Web Flash	360p	480p	720p	1080p	Occasional	Frequent
Task Worker							
Basic Office	✓						
Office Productivity	✓						
	✓	✓	✓			✓	
Advanced Office	✓	✓	✓			✓	
	✓	✓	✓	✓		✓	

Example Virtual Desktop User Categories	Audio Quality				
	No Audio	Compressed Mono	Mono	Compressed Stereo	CD Quality Stereo
Task Worker	✓				
	✓				
Basic Office		✓			
Office Productivity			✓		
				✓	
Advanced Office				✓	
					✓

Note: For the following table, the actual average and peak bandwidth required can vary greatly across users and enterprise environments. Your deployment may require more or less than these suggested values.

Note: For the following table, it is recommended that you do not set the PCoIP Bandwidth Limit unless you are in a known constrained and/or WAN environment. It is also

recommended that you do not define a PCoIP Bandwidth Floor unless you are operating on a network with known packet loss (i.e., wireless networks).

Example Virtual Desktop User Categories	Estimated Bandwidth Consumption		Bandwidth Settings	
	Average Bandwidth	Minimum Bandwidth (for bursts)	PCoIP Bandwidth Limit	Audio Bandwidth Limit
Task Worker	<70 Kbps	500	500 Kbps	disable audio
	<100 Kbps	1 Mbps	1 Mbps	disable audio
Basic Office	<150 Kbps	750 Kbps	750 Kbps+	50 Kbps
Office Productivity	<250 Kbps	1–3 Mbps	3 Mbps+	90 Kbps
	<600 Kbps	5 Mbps	5 Mbps+	200 Kbps
Advanced Office	<1.25 Mbps	7 Mbps	7 Mbps+	450 Kbps
	< 2.5 Mbps	10 Mbps+	10 Mbps+	1.6 Mbps

Note: For the following table, adjustments to the initial recommendations for Minimum Image Quality and Maximum Initial Image Quality may be needed for known constrained networks or long latency WAN networks.

Note: For the following table, limited Windows Experience optimization refers to such measures as basic optimization of the desktop background, removing menu fading, etc. Full optimization includes additional steps, such as setting visual effects to the best performance.

Example Virtual Desktop User Categories	Image Settings			Windows Experience Optimization
	Minimum Image Quality	Maximum Initial Image Quality	Maximum Frame Rate	
Task Worker	40	70	8	yes
	50	70	15	yes
Basic Office	40	70	15	yes

Example Virtual Desktop User Categories	Image Settings			Windows Experience Optimization
	Minimum Image Quality	Maximum Initial Image Quality	Maximum Frame Rate	
Office Productivity	50	90	20	limited
	50	90	24	limited
Advanced Office	50	90	30	no
	50	90	30	no

6 Teradici Network Solutions Partner Program (NSPP)

NSPP is a program designed to help network equipment manufacturers optimize PCoIP traffic on their products. The program focuses on increasing the performance of Virtual Desktop Infrastructure (VDI) environments and ultimately providing a richer end user experience.

For more information on network products that are certified for use with the PCoIP protocol, please see Knowledge Base article 15134-756.

You can sign up for the program by going to Teradici Network Solutions Partner Program (Teradici OEM partner access required).