The business benefits of network convergence are clear: fast, dependable, real-time communication, unprecedented information mobility and worker flexibility, and the ability to instantly transmit a variety of data types to almost any device, anywhere in the world. And that’s just the beginning.

Not surprisingly, enterprises everywhere want to quickly prepare their IT infrastructure to take full advantage of convergence. Is your company one of them? If so, you need a strategy that helps you quickly achieve these benefits, with minimal investment and impact to your business processes. This white paper is a great place to start.

**Building the right convergence strategy for you**

To successfully transition to a converged network, you must have the appropriate IP telephony applications, system components and bandwidth to manage voice and video communication. The following six questions can help you assess your current infrastructure and determine how to deliver the rich functionality business users demand without compromising network security or performance.

**Question 1: Is your network ready for IP telephony?**

The first step in assessing network readiness is determining whether your current bandwidth can support future VoIP deployments. If not, can you borrow bandwidth from less critical applications, or will you have to add capacity? Second, what will be the impact to your existing applications? You need to ensure your existing networks and the service levels established for data traffic can support the additional demands placed on them by IP telephony.

**Question 2: Can your data and IP telephony traffic co-exist on your network?**

If left unchecked, the additional bandwidth required for voice and video traffic on a converged network will impact the performance of business applications whose data shares that bandwidth. But you don’t necessarily need to purchase new bandwidth to deliver it all. By prioritizing your applications, you can make room for latency-sensitive business applications, such as SAP or Oracle, as well as the new voice and video traffic.
To ensure optimum performance, you need to distinguish between essential, non-essential and harmful traffic on your network such as:

- Bandwidth-hungry applications (sometimes called bursty) like e-mail, file transfers, backup and distributed storage
- Time-sensitive applications that use voice and video
- Recreational or malicious traffic

To identify the difference between business and non-business activity, your infrastructure solution must enable you to:

- Apply partitions and policies to protect critical applications and contain or block recreational and malicious traffic.
- Use bandwidth management to smooth bursty traffic and reduce end-to-end congestion, improving overall network performance and efficiency.
- Take advantage of session guarantees, which will ensure the performance of video and voice applications.

**Question #3: Do you have enough network visibility to ensure consistent voice and video performance?**

To evaluate your current voice and video traffic and calculate your future requirements, measure your current bandwidth usage and determine how many concurrent users you want to support. You can establish a rough estimate of your bandwidth requirements by multiplying the number of users by the amount of bandwidth measured. For voice, ten concurrent sessions at 25Kbps each would equal about 250Kbps in each direction. For video, a 384 codec may require two concurrent sessions of 420Kbps each (headers and control information are included).

If you’re not sure how to generate these metrics, consult with a solutions provider with proven expertise in this area. Either way, don’t skip this step — it’s absolutely critical to insulating your budget from unanticipated bandwidth expenditures down the road.

**Question 4: Can you differentiate between sanctioned and unsanctioned voice and video traffic?**

Bandwidth-intensive voice and video traffic originates from many types of recreational applications, and poses an increasing threat to network performance — even in large organizations. If your company relies on
IP telephony to support critical business activities, you need a way to differentiate between sanctioned and unsanctioned voice and video traffic. Your infrastructure solution must be able to discover and monitor each of these applications before you can separate and control potentially disruptive traffic from the legitimate voice and video communications your business relies on.

**Question 5: Can you minimize jitter, delay and packet loss?**

Jitter, delay and packet loss can cause significant degradation in quality and overall reliability in real-time services. Here’s why:

- **Jitter** causes unpredictable and variable delays in the delivery of each voice packet.
- **Delay** is the end-to-end latency in delivering the voice stream from the speaker to the listener.
- **Packet loss** drops individual packets when the network is too congested.

Together, these disruptions can take an entire service offline. To protect and optimize voice traffic, your infrastructure solution should be able to monitor key metrics designed specifically for real-time protocol (RTP) traffic like IP telephony, including R-Factor and Mean Opinion Score (MOS), and provide alarms to signal performance degradation and automate preemptive troubleshooting. Finally, to accelerate voice and video traffic across your network, you should use only application-aware protocol acceleration technology to ensure that bandwidth is not wasted on non-essential recreational applications.

Without these controls, you can’t determine what to accelerate and what to block or sequester. As a result, acceleration without control can actually increase latency 50-100%, increase jitter to 140ms and almost double your packet loss. To avoid these problems, you need to differentiate between applications.

**Question 6: Can you handle a rapid increase in network traffic without adding bandwidth?**

Network convergence has many proven benefits, but increased voice and video traffic also puts additional pressure on the network. While it can be tempting to simply add more bandwidth to address slow performance, this approach is both costly and ineffective. Many recreational and peer-to-peer (P2P)
Voice, Video and Data Convergence

Voice, Video and Data Convergence applications will actually consume any additional bandwidth they encounter, so this approach rarely improves business application performance.

To maximize available bandwidth for legitimate transactions and discourage recreational traffic the best approach is to integrate compression and control capabilities. Combining compression and control can help prevent recreational traffic from dominating bandwidth while allowing acceptable levels of access to these sites and applications.

Blue Coat: A comprehensive solution for video and voice convergence

Blue Coat offers a comprehensive solution to ensure your critical business applications get the bandwidth they need to perform at their peak. By integrating visibility, acceleration and control technologies, Blue Coat helps you see everything on your network, monitor for potential performance issues and accelerate business applications while controlling recreational use. Best of all, you can make the most of your existing infrastructure and avoid expensive investments in additional bandwidth.

See how data flows across your network

Blue Coat helps you safely determine how to optimize data flow across your network. You can test-run voice calls or video conferences to measure the bandwidth needed to support each of these activities during times of peak demand or when there is little competition on the network. You can then determine an appropriate minimum and maximum amount of bandwidth needed for voice and video traffic.

You can also establish service-level reporting to set thresholds and measure compliance. Simply set performance thresholds against a known set of quality metrics, and configure Blue Coat to proactively send alerts or react immediately. For example, you can reduce bandwidth for applications that are not time- or business-critical when thresholds are reached.

Monitor your network for performance bottlenecks

In a converged network, VoIP traffic and business applications often compete for bandwidth, creating performance problems for both. With Blue Coat, you can determine where and how to allocate bandwidth to ensure optimum performance for all your business transactions.
Blue Coat simplifies this allocation process by helping you identify, classify and monitor all the applications on your network. For instance, you can separately group time-critical applications such as voice and video, business processes like SAP and Oracle, bandwidth-intensive applications such as email and file transfers, and non-essential recreational traffic that can clog your network. Once you classify these applications, you can then prioritize how to manage them according to their business impact.

Accelerate with control

Real-time business communication depends on a highly secure and optimized network. To ensure adequate bandwidth and quickly move applications across your network, you have to distinguish between each application and even between different types of voice and video traffic. Blue Coat delivers the right combination of acceleration and control to get the right content to the right people at the right time, even when network demand is at its peak. Here’s how:

Manage spikes in network usage

On any WAN, there is a finite amount of bandwidth. So when demand spikes threaten your business applications you need to intervene and ensure that business activity, such as voice calls and video sessions, remain uninterrupted.

Blue Coat helps you easily allocate bandwidth during times of peak demand. You can set a rate policy on each of your voice and video data classes (RTP or others) to:

- Indicate the relative importance of voice and video traffic and distribute bandwidth accordingly.
- Insulate voice and video users from each other to gain the benefits of rate control.
- Reduce retransmissions that waste bandwidth and introduce latency.
- Guarantee bandwidth on a per-session basis.

Blue Coat allows you to assign a rate of minimum bits-per-second required to deliver acceptable voice call or video session quality. But you don’t simply prioritize voice and video over other business activity. With Blue Coat, you are able to maintain expected service levels for all business-critical applications.
**Distinguish between personal and professional use**

Recreational voice and video applications, such as Skype™ and IM, are almost as commonly used as email. But these bandwidth-intensive applications can tie up even the highest bandwidth links. So if your company relies on IP telephony for business communication you need to know when it’s being used for business or personal reasons.

With Blue Coat, you can manage voice and video applications by monitoring the network to control recreational use and proactively block malicious traffic before they disrupt the performance of critical business applications. You can then apply granular policies to distinguish between essential voice and video use and non-essential traffic and allocate bandwidth to support quality-of-service (QoS) requirements.

**Recognize and resolve MPLS limitations**

If you are using an MPLS-based IP subscription, you need to assign voice and video with real-time priority classes of service. However, there are limitations in the queuing and packet-based QoS features inherent in MPLS.

For example, if you provision a class of service for four calls, each packet of each of these four calls will be given the highest priority. In an oversubscription situation — such as too many calls in a class of service — the network subscription will process more of that class of traffic than it can support. So when calls 5, 6 and 7 occur, all packets are downgraded to a lower class of service category. As a result, all calls suffer a reduction in quality.

Recognizing this limitation, Blue Coat allows you to integrate with MPLS to control traffic and route each transaction into the proper service class across your MPLS network connection. So real-time voice and video traffic that requires immediate bandwidth is tagged with the correct MPLS class, but only after Blue Coat has managed traffic at the flow level to prevent oversubscriptions.

When you assign an MPLS label to ensure special traffic gets the prescribed performance, you can also configure Blue Coat to classify the traffic separately. Then you can apply analysis techniques or assign partitions or policies to each class to control performance.
Measure for quality

Blue Coat helps you monitor and control voice and video performance throughout your distributed enterprise by establishing service guarantees for every user regardless of location. Blue Coat delivers detailed reports on critical factors for real-time data flows, including MOS, R-Factor, jitter, delay and more. You can also configure performance thresholds for each session to ensure you’re meeting designated service levels. More importantly, you get real-time alerts when performance levels are threatened so you can automatically respond to competing demands for bandwidth. By continually measuring and monitoring network performance, Blue Coat helps you proactively resolve problems before they impact your users and your business.

Key factors for reporting on real-time data flows like voice and video traffic.
**Deliver the service and quality your users expect**

With Blue Coat, you can seamlessly transition to a converged network with solutions that help you plan and execute the right strategy for your business. Our goal is to help you quickly achieve the benefits of convergence with minimal impact during all the stages of execution.

To start the transition process, Blue Coat provides the intelligence you need to optimize essential business applications, including time-sensitive voice and video transactions. Our solutions help you establish and enforce service levels for quality and availability, and give you the tools to anticipate and resolve network problems before they impact your end user.

More specifically, Blue Coat helps you measure jitter, loss and delay for RTP traffic so you can better monitor call quality for IP telephony and video conferencing. You can also leverage monitoring and reporting tools to better understand and manage bandwidth usage across your network. The result is a successfully converged network that delivers the highest level of security, acceleration and control for your business.

---

**About Blue Coat:** Blue Coat Application Delivery Network solutions provide intelligent control with visibility, acceleration and security technologies that optimize application and network performance for any user, anywhere, across a distributed enterprise. Blue Coat’s application performance management, WAN optimization and Secure Web Gateway solutions enable IT to provide greater business efficiency, effectiveness and competitiveness. Additional information is available at www.bluecoat.com.