

# THE IMPORTANCE OF TRANSPARENCY, VISIBILITY AND CONTROL

Over the past fifteen years the delivery of IT functionality over Wide Areas has come full circle. A decade and a half ago all IT was fully consolidated in a thin-delivered, dumb-terminal, and mainframe environment moving only the required efficient traffic to make remote users productive. Then, as application design became more complex, we were forced to distribute client-processing power, storage, and even the very mainframe functionality out to remote data centers, users and servers. The result was IT sprawl that was unsecure, hard to manage, and expensive. Enterprise IT budgets quickly ballooned and data loss became commonplace. As a result infrastructures quickly collapsed again to consolidated storage and application servers in well staffed, secure, and central datacenters. This solved the immediate cost and risk challenges but lack of application design progress created a new and difficult network load on severely limited Wide Area Networks. In these competitive environments, each application needs to be identified and controlled as it requests network resources. Today these mixed use networks present a challenging environment that requires powerful visibility and control to provision correctly. In the future, as entire enterprises consider migrations to server-based computing and possibly Virtual Desktop Infrastructures, the distributed IT enterprise will resemble something closer to it's mainframe days, delivering the thin presentation layer to users, centralizing all the end-user processing, storage, and data security. This will come with major benefits in IT efficiency, but with those advances will also come with some new and some old challenges as IT delivery methods once again create new application and productivity obstacles and dependencies to the distributed enterprise.

As Service providers and IT organizations leverage more effective delivery services, network traffic must remain transparent to function. Next generation networks inspect packets to determine their data types, refusing traffic they don't recognize, and categorizing the rest into specific levels of service. Organizations have standardized and grown accustomed to wide area data collection and reporting like NetFlow, which are dependent on identifying traffic over the WAN.

As the IT methods of application discussed have delivered a new consolidated WAN traffic. These consolidated traffic types result in WAN use that is undistinguishable by application or user

## DIFFERENT DELIVERY – DIFFERENT CHALLENGES

Traditional monitoring, data collection, and network control over WAN's are challenged or completely disabled by consolidated traffic flows. As applications are consolidated, visibility for probes like Netflow are completely lost. Even traditional WAN Optimization's method of encapsulating and tunneling traffic can disable all network visibility for an environment.

behavior, removing the ability to police and provision limited network resources to the right user and use. As a result WAN Optimization, visibility, and control play a larger, more difficult role than ever before in enabling branch office delivery of IT. But the right solution must be future focused, affordable, and easy to integrate and optimize these new challenging environments. Over the past decade these IT trends and developments on Wide Area Networks have demanded WAN Optimization for efficiency and performance. Ironically, most of today's required WAN Optimization technologies themselves create an un-identifiable and uncontrollable consolidated traffic. Furthermore, the growing popularity of shared and meshed wide area network technologies prove extremely challenging environments that demand visibility.

What used to be taken for granted is now a key challenge for IT delivery over WAN's. While application delivery and network technologies adapt, so must our methods to monitor and control these resources. It's clear as dependency on the WAN grows once again, WAN Optimization plays a paramount role in successful deployments. The key to WAN optimization today and in the future is to transparently supply benefits to these new traffic types while not losing visibility for monitoring or control over your applications.

### Transparency

While ways to deliver applications were maturing, the very technologies delivering and controlling Wide Area connectivity were also advancing. WAN technologies like meshed MPLS (Multi-Protocol Label Switching) and WAN based QoS (Quality of Service)

# THE IMPORTANCE OF TRANSPARENCY, VISIBILITY AND CONTROL

delivered higher performance and guaranteed resources for business critical applications. With them providers implemented strong control over their limited WAN resources deciding which customers, applications, and traffic received their resources and when. However, WAN based QoS is out of the customer's control, service levels are imposed on traffic without their input, and in large generic categories, lacking true application granularity. Simultaneously, customers began firewalling these business critical links to protect

## WAN BASED QOS CHALLENGES

Today's service level WAN resources are partitioned by several broad use cases. However these broad categories of use require fully visible packets (Transparency) in order to inspect and categorize. Un-identifiable traffic is refused and dropped or degraded, causing the traffic to delay or fail altogether.

their valuable data on these higher risk distributed deployments. The cost for these performance and security returns was a loss of control to the customer and an unprecedented requirement for transparent optimization capabilities.

While these new WAN based services can assist performance and raise security on a service provider's network, most of the overall performance and control loss occurs before traffic reaches their network. The siphon where the very high bandwidth LAN traffic must be transferred into the bandwidth constricted WAN is the biggest challenge and the right place to solve these problems. Here WAN based services can't provide a benefit, it must be managed through dispersed powerful WAN Optimization technology.

A truly transparent WAN Optimization solution like Expand's can provide significant benefits without difficult configuration

## TRADITIONAL WAN OPTIMIZATION CHALLENGES

Most WAN Optimization solutions encapsulate the original traffic's packet payload and header. If the original packet header is not visible, traffic is not identified and WAN based services fail.

while adhering to these new WAN visibility requirements. Even better, new and granular application level control, even inside and in addition to service provider WAN based provisioning can be

achieved as long as the traffic remains visible to the provider based inspection and provisioning.

Traditional WAN Optimizations create 'optimization tunnels' between sites. Typically refused and blocked at firewalls, these tunnels mask the original packets' IP headers, completely preventing MPLS networks and WAN QoS from providing benefit. This usually means choosing between traditional dispersed WAN Optimization and a secure and best-in-class WAN based service – sacrificing visibility, performance, and your control over your resources.

### Expand's Multiple Layers of Transparency

In order to truly integrate into today's distributed enterprises; powerful and transparent WAN Optimization technologies must be implemented. Expand's best-in-class solutions deliver the required benefits of WAN Optimization while new WAN based services and requirements can be met and complimented instead of disabled or handicapped.

Expand's extensive commitment to transparent deployment ensures enterprises can leave existing WAN based services (Monitoring, WAN based QoS, Netflow, and security) in place and functional. It also means benefiting from best-in-class WAN optimization doesn't require any changes to user systems or infrastructure.

### Router Transparency Mode:

In order to enable Expand's powerful WAN optimization transparently over these complex WANs, Expand pioneered Router Transparency Mode (RTM). RTM ensures that each IP packet header is preserved for inspection and identification. Expand's optimization technologies will perform powerful optimizations on packet payloads but leave each packet's header untouched for complete MPLS, WAN Router, and WAN QoS functionality.

- WAN and edge routers can classify, shape and mark traffic and IP flows
- Network probes and collectors can report data on the actual IP flows
- Encryption can be applied to sensitive traffic
- Threats (like SYN attacks) can be identified and prevented
- Unauthorized traffic can be blocked

### Firewall Transparency Mode:

Only a secure network is a productive network. Expand encourages the use of intrusion detection, security, and firewalls to protect valuable resources, but these technologies can cripple

# THE IMPORTANCE OF TRANSPARENCY, VISIBILITY AND CONTROL

and disable most WAN optimization solutions. Only Expand's Firewall Transparency Mode (FTM) can seamlessly provide security friendly optimized WANs.

- Completely transparent and compatible to Firewalls and Intrusion Detection systems
- Encapsulates all optimized traffic in efficient UDP flows
- Full featured WAN optimization across deep packet inspected networks.
- Secures networks from malicious use while optimizing business traffic
- Eases implementation, configuration and management

## User and Server Transparency:

At the application layer transparent optimization is a must. Expand's Virtual Branch Office solution offers completely transparent virtual servers and local services to your remote users. No changes are required to end-user systems, infrastructures, or networks to provide local Microsoft File Server, DNS, DHCP, Print, and IPsec VPN services to your remote offices.

- Transparently deliver local services to end-users without local servers
- No changes to end-user systems
- Transparent distribution of data to remote offices
- Seamless support of Distributed File Services
- Transparent high-availability

## Visibility and Control

As businesses continue to attempt to deliver functional IT to distributed enterprises they are faced with many varied performance and cost challenges. To overcome them they've adapted old technologies and implemented new. At the application layer, under-performing applications, originally delivered traditionally, were migrated to thin server-based computing and

## LOSS OF VISIBILITY

As applications are webified and delivered under consolidated HTML traffic, we lose the ability to identify which application is which. Unable to identify specific applications, the entire consolidated stream is all that can be controlled and monitored.

"Webified" environments to increase performance and lower WAN network loads. At the hardware layer, remote office server consolidations have delivered on the promise of cost-savings and control, but now that critical remote office traffic is forced over the WAN inducing new problems.

And now, future focused organizations are investing in the potentially exponential cost-savings of consolidating actual desktops and delivering end-user functionality through a Virtual Desktop Infrastructure (VDI). VDI promises unprecedented delivery, control, availability, and performance to end users, but at the same time in many ways represents a challenging return to the mainframe and thin-terminal delivery environment. Users will be working on thin-clients, with absolutely no productivity without a connection to the VDI hosting server. With a WAN outage or WAN performance problem, the entire user's session is impacted. Unlike just one or two server based computing applications degrading, the user is entirely un-productive and your IT organization has failed to deliver its core services. Furthermore, all VDI traffic looks alike over networks and is entirely encapsulated into VDI streams, all un-distinguishable by application, action, or user. However great the enhancements and benefits from VDI – it's a new world – one entirely dependent on the WAN and more

## IMPACTS OF NO CONTROL

While yesterday's WANs were easily inspected and controlled, today Server Based Computing and other consolidated delivery has masked use and traffic type information. It is impossible for instance, to determine non-priority bulk printing traffic from business critical payroll, CRM, or accounting applications. The result is greedy print jobs squeezing out business critical application traffic creating a non-productive and erratic user experience. With the advent of VDI, it will be the entire user's desktop functionality, all encapsulated into one traffic type!

consolidated than ever.

While all these application delivery advances have come through on cost savings, the byproduct is this new consolidated network traffic. Instead of multiple independent applications, one application's traffic delivers multiple business critical feature and function en-mass. Without the right tools consolidated application environments resemble a single application to the WAN with no visibility, nor the ability to inspect and control them. Business consolidation and IT efficiency has created today's new WAN; one that is more complex, less visible, and harder to control than ever before.

Lastly and most importantly, it's the future challenges that are of the most concern. Along with growth in consolidation, server-based computing, and VDI, corporations are seeing unprecedented

# THE IMPORTANCE OF TRANSPARENCY, VISIBILITY AND CONTROL

use of peer to peer applications for business but, more often recreational use. It's imperative that business gain visibility into these applications to ensure resources are used for productive business priorities, not non-business recreational use. Peer to peer traffic may have amazing implications for business productivity in the future, but without visibility into these application's usage, corporations are left with no control of the use of their expensive network resources. Limited networks can be completely saturated and rendered useless by just one rogue or non-business related peer-to-peer session. These traditionally efficient applications open multiple threads to complete their role, causing extremely high traffic loads that randomly change its characteristics. These active and scalable applications have been impossible to monitor and more importantly limit as they randomly create new connections as needed and hop ports making traditional monitoring methods ineffective.

## VDI – PRODUCTIVITY DEPENDENT ON THE WAN

Any user running VDI will have absolutely no functionality without network connectivity to its host server. In this brave new world, a WAN outage will spell an entire loss of productivity. Users will be unable to continue functioning whatsoever as the entire end-user desktop session is hosted at the centralized VDI Server and non-functional without it.

The key to gaining visibility and control on current and future WANs supporting these new traffic types is a powerful set of inspection, identification, and classification technologies to enable provisioning of the WAN. Next generation Layer 7 application visibility enables inspection of the consolidated network traffic delivering invaluable application, user, and environment details. These details can be used to categorize and classify traffic that originally was unclassifiable, enabling the visibility and control of business resources and aligning them with business critical productivity and functionality.

### Expand's Unprecedented Visibility and Control:

#### Ensure, Protect, and Provision any WAN Traffic

Bi-Directional Layer 7 Quality of Service (QoS):

Expand provides extensive bi-directional QoS, which is a key requirement for effective WAN Optimization. Expand's QoS is

fully application-aware, auto-recognizing application traffic and provisioning, shaping, and conditioning the limited WAN resource by business criticality. It provides visibility into and beyond application type; breaking through the new consolidated WAN traffic and giving back powerful provisioning to the enterprise. Expand's industry leading QoS engine enables extremely granular provisioning in addition to ISP provided service levels.

- Over 400 applications immediately identified and controlled.
- NetFlow reporting and integration.
- Layer 7 visibility for:
  - Citrix
  - Web
  - Peer to Peer: (bitTorrent, Gnutella, eDonkey, Kazaa, Napster, WinMX, SoulSeek, DirectConnect),
  - Instant Messaging: AOL, ICQ, Jabber, MSN Messenger, Skype, Qq, Yahoo Instant Messenger
  - Audio/Vidio: sip\*, h323\*, rtp\*, rtp-sip\*, rtp-h323\*, rtsp, h225, mms, q931, sccp, rtcp-sip, rtcp-h323
  - Email: MS Mapi (Exchange), Lotus Notes
  - Printing: Cups

### Summary

The present day and future Wide Area Networks are providing new levels of service and performance as IT migrates yet again to new delivery methods over them. However these changes bring with them limited control, visibility, and scalability. These new WAN environments require and can never replace the unique benefits provided by distributed WAN Optimization. In fact, these new managed networks demand the very best-in-class transparent WAN Optimization technologies in order to functionally deliver optimized IT resources to distributed enterprises. As IT organizations continue to find ways to thin and consolidate the delivery of services, new applications emerge as business enablers, and new WAN based services are leveraged; the result is consolidated, complex, and obscured WAN traffic resembling an un-identifiable single monogamous traffic type. In order to truly optimize these challenging new environments it is clear that a fully transparent solution that provides next generation visibility into network use and powerful application-aware control of these resources is a necessity.