

Qwest iQ Networking[®]

Evolution to a Private IP Core Network

Overview

Have you ever wondered why networking companies talk about converged network solutions only to learn the provider still maintains separate networks for voice, private data and Internet? Qwest has always been a leader in Internet protocol (IP) network technology and extends that position another step with the completion of our third-generation converged Private IP Core Network.

Qwest has consistently led the industry by offering top-performing public Internet access services, virtual private network (VPN) services and voice over IP (VoIP) telephony. Qwest continues an IP leadership position with a third-generation core network design that adds security enhancements to isolate public and private services over a common core transport system. In other words, Qwest runs a converged network that carries voice, private data (VPN traffic) and Internet on one secure, robust Private IP Core Network.

Based on multi-protocol label switching (MPLS) standards, our converged network delivers both IP security and performance over a reliable, flexible platform unique to Qwest. Qwest's Private IP Core Network creates completely isolated public and private IP network switching domains, delivering both speed and security, over a single network infrastructure designed for future growth and stability.

Qwest's network engineering organization embarked on a multi-tiered network design strategy to create a highly flexible and secure environment to accommodate current customer applications and to prepare for anticipated future advancements in IP, VoIP and MPLS. Qwest's Private IP Core Network provides a hardened physical security barrier at the edge between public and private IP services, running over the IP network while harnessing the flexibility and efficiency that a single, private core network offers. The tiers of the architecture are:

- Shared layer:
 - Core: A secure, MPLS-only and IP-unaware transport infrastructure for all service types to traverse.
- Layers dedicated to a single security domain:
 - Aggregation: Deployed as needed to aggregate traffic from edge devices serving customers with smaller port sizes with traffic from customers with very large ports for delivery to the core.
 - Edge: Used for specialized service connectivity to customers.

The first and second generation Qwest IP backbone designs focused on offering high-end best-effort IP service, primarily for Internet access. Since the second-generation network was operationalized, additional services have become more common for commercial, government, and wholesale customers. These prevalent services include Layer 3 VPNs, Layer 2 VPNs and VoIP.

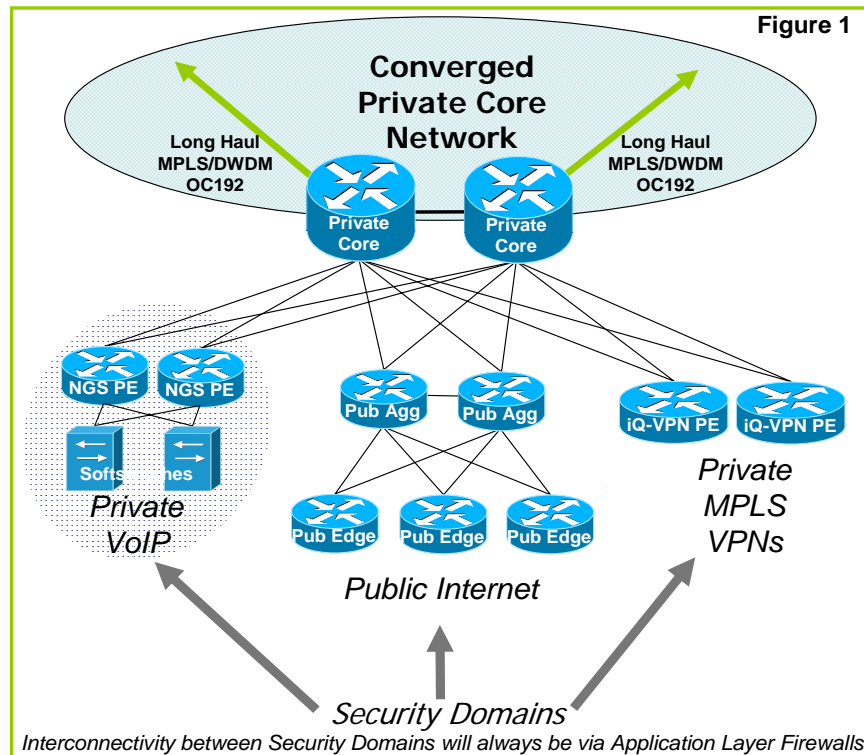
In addition, as the Internet has become a defacto business asset to complete transactions and coordinate communications, the reliability and security requirements of networks have steadily increased. Qwest completed incremental changes to the network over the past few years to enable services and to increase security. In concert with the continuously increasing focus on security posture, Qwest network engineering proposed a third-generation design using security domains—now referred to as the Private IP Core Network.

The secure domain architecture isolates each specific service type Qwest offers customers from all other service types. In other words, each service type is fully contained in its own security domain. Each security domain is encapsulated in MPLS and switched inside dedicated MPLS label-switched paths (LSPs) through the IP core network routers. Each IP core network router functions with uninterrupted performance, completing the movement of traffic across Qwest's

long-haul OC-192 fast re-route-enabled backbone using the efficiency and stability of MPLS technology.

This third-generation design truly allows Qwest to live convergence by allowing multiple service types to share a single core network securely. This converged core provides (Figure 1) an increase in the security and reliability of the Private IP core Network against malicious attacks, increases the capacity and reliability of the network and allows Qwest remarkable flexibility in offering compelling converged solutions.

Qwest's Private IP Core Network provides Qwest iQ Networking® these important characteristics to allow customers to operate highly secure and reliable private MPLS WANs, to get reliable Internet access and implement high-quality VoIP:



A. Cutting edge and fast

- Qwest's core network runs at OC-192 speed.
- Uses the latest technology from Cisco® and Juniper® in the Private IP Core Network.

B. Scalable

- New hardware supports total link capacity between core routers greater than OC-192 using fully redundant, bonded OC-192.
- Can handle backbone growth by upgrading the pair of routers that are exceeding acceptable capacity levels without requiring changes to the security domain.
- Qwest's research and development efforts are focused on OC-768 transport performance evolution.

C. Flexible

- The addition of new services becomes significantly easier by creating new security domains, allowing more rapid deployment.
- For potential future integrated services, such as Qwest iQ Networking® Enhanced Port with Internet access and network security services, the security domains would be interconnected through separate provider-edge network connections that run through appropriate application layer firewalls and rate limiters before reaching the non-public IP interfaces of the Private IP Core Network.

D. Reliable

- Security domain separation and containment of IP routing to each security domain means the core of the Private IP Core Network is more stable by virtue of more limited signaling requirements.
- Multiple, redundant devices at each tier: edge, aggregation and core.
- Multiple, redundant connections from each device to the next tier and multiple connections from each core router to other core routers.

E. Secure

- Private IP Core Network routers do not participate in Layer 3 routing of traffic – they only “know” MPLS.
- Qwest iQ Networking® services are separated into two different security domains:
 - Qwest iQ Networking Internet Port.
 - Qwest iQ Networking Private Port and the Enhanced Port VPN segment.

F. Other benefits

- Additional security domains can be deployed as needed for new services.
- Signaling from a security domain is confined to that security domain.
- Separate MPLS LSP mesh per security domain: Private IP Network Core only forwards traffic inside LSP dedicated to each security domain.
- Separate edge and aggregation routers used for each security domain.
- Those separate edge routers use separate connections into the private core.
- Planning for a dedicated security domain for Qwest Voice long-haul traffic on our Next Generation Switch platform.

Conclusion

Qwest separates VoIP, Private VPN and Internet traffic across a Private IP Core Network. Qwest's third-generation networking design combines secure and flexible converged core networking fundamentals to assist customers run the most advanced applications for their business. When it comes to convergence, Qwest not only talks about what to do, but shows how to do it every day on Qwest's Private IP Core Network.

Qwest iQ Networking® is a suite of WAN services with domestic and international availability depending on services selected. Recurring fees vary depending on services ordered. Additional equipment may be required.