Fabric Connect: The Quiet Revolution

With Fabric Connect, Extreme Networks is redefining the delivery of communications solutions to match the expectations of businesses operating in the digital age. Long wait times and design constraints can be things of the past; Extreme leverages simplicity to create agility. Network simplification, empowered by a fully integrated communications infrastructure, delivers rapid application deployment and seamless service provisioning. Further up the value chain, organizations can quickly deploy business application solutions with right-sized turnkey packages.

At Extreme Networks, we certainly make some quite bold claims for our Fabric Connect technology, and understandably, we get challenged about these. People will often ask how can be Fabric Connect be that much better than every other offering in the market. Even internally, especially amongst our very experienced technical professionals, there is a sense that, at times, we might be hitting the edge of the envelope in terms of credibility. Perhaps, but the reality is that because Fabric Connect is so fundamentally different to the conventional technology alternatives we need to take the conversation to a different place. Because Fabric Connect is redefining networking, expectations also need to be redefined.

Eliminating Complexity: From 10+ Protocols to 1

When looking at conventional networks built over the last 20 years, it can easily be observed that successive layers of complexity have accumulated, principally in order to meet evolving applications needs. VLANs create Layer 2 virtualization, and aggregation is enabled by MLT (Multi-Link Trunking) and LACP (IEEE Link Aggregation Control Protocol). Then there's dynamic IP Routing that utilizes either RIP or OSPF, often combined with ECMP to provide Layer 3 load-sharing/aggregation across multiple links. Additionally, we need to need to add IGMP (Layer 2) and DVMRP or PIM (Layer 3) to support Multicast, and going further afield there's BGP to provide peering to Internet providers.

Obviously, the legacy network architecture has reached a very high level of complexity. More ominously, all of these protocols also have very high levels of interdependency. For example, if there are problems, failures, or bugs at Layer 2 then all the upper layers – and crucially, business applications – will also be impacted. Hence, the "House of Cards" analogy that we sometime use, a stack that could, and frequently does, collapse, triggering costly business outages that are exacerbated by the slow and unsynchronized re-convergence of multiple inter-dependent protocol layers.

So, can we really claim a reduction of 10 protocols to down to one? Well, here is the list of protocols that are made redundant and unnecessary when migrating from a conventional design to Fabric Connect: STP, MSTP, RSTP, RIPv1, RIPv2, OSPF, EIGRP, ECMP, PIM-SM/PIM-SSM, DVMRP, LSP, GMPLS, TRILL. Occasionally, additional protocols are needed to satisfy sophisticated requirements.

Some argue, quite reasonably, that not every protocol will always be used simultaneously in every network, but that misses the point. Fabric Connect – uniquely – makes this cocktail of complexity redundant for the mainstream, and businesses can now build a robust, reliable, scalable and virtualized architecture that is also free of complexity.

What is equally powerful though, is that we can also run any or all of these legacy protocols in parallel with Fabric Connect. This provides a very smooth migration to a Fabric-centric architecture and ensures that any design-specific requirements, however niche or sophisticated, can be seamlessly accommodated.

Faster Time-to-Service: 11x Better with Edge-Only Provisioning

In 2015, independent research was commissioned to verify exactly what Fabric Connect customers were experiencing in their real-world deployments[1]. The results are genuinely eye-catching: including a 11x improvement (or 91% reduction) for implementation time and a 7x improvement (or 85% reduction) in both configuration and troubleshooting times. Similarly, Fabric Connect delivers enhanced resiliency with failover times more than 2,500x better, and outages caused by human error are now virtually eliminated.

Metric	Before	After	Times Better	% Less	% Seeing Improvement	Paraphrase
Implementation Time	14 Days	1.3 Days	11x	91%	68%	Weeks to Days
Configuration Time	4.6 Days	0.7 Days	7x	85%	86%	Days to Hours
Troubleshooting Time	39 Hours	6 Hours	7x	85%	41%	Days to Hours
Failover Time	>13 Minutes	0.32 Seconds	>2,500x	100%	70%	Minutes to Milliseconds
Outages (Human Error)	3/Year	0/Year	-	100%	74%	De-Risk
Wait Time	31 Days	1 Days	31x	97%	-	Month to a Day

This research reinforces an earlier report that measured the impact and significance of the age-old network-versus-business conundrum: how to make network adjustments, improvements, and corrections without disrupting the business[2]. It explored what happens when changes need to be made to the corporate network and what happens when things go wrong, and looked at the consequences of such activity, including the financial implications.

Again, the results are dramatic: most network changes necessitate a maintenance window, IT networking professionals have had to wait – on average – 31 days before they could make the changes necessary to the corporate network. One company had to wait 9 months for such a maintenance opportunity to arrive.

As can clearly be seen, our solutions provide 11x faster time-to-service/market. This is a direct outcome of a unique capability that Fabric Connect delivers; Edge-only provisioning that can be done in real-time. This delivers radical improvements to service agility. With no requirement for maintenance windows, the time that a business is forced to wait to make a significant change in the network can be dramatically reduced. Instead of an average of about one month, changes can now typically be made the same day. Once the decision to make a change is taken, IT can simply get on and deliver service to the Business.

Even in a purely "manual" Fabric Connect provisioning model, service activation is transformed from a risky and time-consuming process – typically involving multiple lines of configuration, executed on multiple devices – to the simplest of everyday IT tasks. Quite literally, it will take the Technician longer to boot their PC than it will for them to complete a service provisioning operation courtesy of the Fabric Connect Edge-Only capability. Typically, it's one line of CLI or a handful of clicks in the GUI. No delay, no risk, no dead-of-the-night change window, and – crucially – no having to push-back on the needs of the Business.

Not resting on our laurels, things get even better when you consider the possibilities and capabilities of the Fabric Attach technology. This is an open technology that has already been adopted by Open vSwitch[3]. It delivers an ability that facilitates the fully automatic attachment, "auto-attach" in standards verbiage, of endpoint devices, empowering businesses to dynamically deploy services and devices in a highly virtualized world. Businesses can leverage Fabric Attach to dynamically deploy endpoints, temporarily extending unique networking services to the Edge, as required: Fabric Attached endpoints connect to the appropriate network resources: this would typically be a Fabric Connect Virtual Service Network (VSN), or it could be a conventional VLAN.

So, whether it's extending Campus Wi-Fi services or supporting dynamic VM activation in a busy Data Center, the unique differentiation that Fabric Connect delivers – superbly complemented by Fabric Attach – revolutionizes the entire dynamic of service agility and delivery.

Better Time-to-Repair: Eliminating Hop-by-Hop Gives 6.5x Improvement

The Fabric Connect Customer Experience Report highlights another, sometimes overlooked, differentiation that is unique to Extreme: improved service availability driven by efficient troubleshooting if/when an outage does occur. Customers report improvements in the time consumed troubleshooting network outages, with – on average – experiencing a massive 6.5x better (or 85% improved). The highest reported improvement, so far, has been 8.5x or 92%.

Even more interesting perhaps, is the very sizable group (41%) of deployments that could not easily quantify a TTR improvement; simply because they have not yet experienced network issues since the implementation of Fabric Connect.

The basis for this unique differentiation can be attributed to a characteristic of the underlying protocol that powers Fabric Connect: the IEEE's 802.1aq Shortest Path Bridging, enhanced with crucial extensions. This single, hyper-intelligent, unified protocol builds a robust and resilient topology that facilitates every aspect of inter-nodal communication and service delivery. Not only does this provide a huge advantage in terms of service provisioning, but also when it comes to troubleshooting.

Crucially, services are only "presented" at the Edge, and then only on those nodes that specifically interface these specific services to local endpoints. Core or Distribution nodes that are only involved in data forwarding never terminate services. This translates into a truly minimized "fault domain" that can be viewed and debugged on a per-service basis; no longer is it the case that every node in the entire network has to be evaluated and potentially analyzed. In its simplest form, troubleshooting a Fabric Connect service involves the direct analysis of just two nodes, regardless of how many intervening and interconnected nodes may exist.

To add visibility at the SPB layer, additional tools have been introduced (for example: L2 Ping and L2 Trace-Route), and there is an entire standardization effort – IEEE 802.1ag – to develop new and advanced operational, administrative, and management capabilities.
However, what is certain, is that the days of Operations laboriously troubleshooting – hop-by-hop FDB, ARP, and IP Route tables are over.

Anecdotally, Fabric Connect deployments are reporting that the vast majority – 95% by some measures – remain free from an outage or significant problem even after more than a year in production. In a direct contrast with networks designed along conventional lines, those networks leveraging Fabric Connect generate 28% fewer support requests.
Although somewhat unscientific, this data is another outstanding proof-point that Extreme Networks solutions convert proactive simplification into a tangible business benefit: a more reliable and available network helps to optimize business productivity.

Fabric Connect Customer endorsements:

"It has made identifying issues much easier, but there are hardly any issues these days anyway."

Operational since July 2013

"Touching wood, we haven't really had any problems to troubleshoot since implementing Fabric Connect, so that number is a bit of an estimate."

Operational since Oct. 2013

"The 'since implementing' figure I have given you is a guess, as we haven't had to troubleshoot as yet."

Operational since July 2014

Enhanced Business Continuity: 13 Minutes to 320 Milliseconds

Network availability – or more precisely, unavailability – is probably the most important metric to the Business, and clearly the most visibility. When the network or major parts of it go down there's no place to hide.

Again, looking to the real-world experience of our Fabric Connect deployments, three-quarters of our Customers report significant improvements, compared directly to their legacy network. On average, an improvement of more than 2,500x was observed, more than 99.999%. No, that's not a typographical error: more than 2,500x or 99.999% better.

Just to be clear, this is a measure of how quickly networks recover – failover – if and when there's some sort of outage. And the root cause does not have to be a Fabric Connect or an Extreme Networks Switch failure, and could conceivably be a fiber fault or power outage. This capability delivers tangible business benefit; on average the recovery times went from 817 seconds to 0.32 seconds. As we can all appreciate, 817 seconds – more than 13 minutes – is a lifetime in terms of application state-awareness and end-user experience, whereas, by contrast, 0.32 seconds is hitless.

These results were genuinely staggering, and crucially they put science to what everyone close to the technology had believed for a long time: Fabric Connect is, by far, the most bullet-proof networking technology ever created.

Incredibly, however, the story gets even better. Again, a significant portion of respondents (22%) were unable to provide an actual number, either because they have not experienced network issues since their implementation of Fabric Connect, or because their previous design didn't provide a failover capability.

What's highlighted here is the knock-on effect that network outages and extended failovers have on business applications. While any of the conventional Layer 2/Layer 3 redundancy protocols can theoretically be tuned for sub-second failover, real-world deployments, in large and complex environments, mean that much higher figures are typically seen. Something like 40 seconds (or more) is not unusual, but that is only for network recovery. In that time, applications databases have gone out of synch, end-users are seeing applications failure (browsers report pages not found), Contact Center Agents have had Customer calls drop, IP Desktop Phones are rebooting due to the loss of connectivity with their Call Servers. The list simply goes on and on. There is a domino effect happening, one that causes a very costly impact to the Business.

In contrast, Fabric Connect consistently delivers sub-second recovery; that's full network recovery, Layer 2, Layer 3, and IP Multicast. And because the network has – effectively – never gone away, upper layer communication protocols are totally unaffected; just like individual end-users and the Business as a whole.

Fabric Connect has been extensively tested, in a wide variety of scenarios, for failover/recovery. A good example is some recent testing specifically undertaken at a Customer's request, to empirically measure performance and continuity of both Unicast and Multicast traffic flows across a series of failure scenarios. The table below provides detailed results, in terms of times and also the end-to-end impact on the test application (Pelco's Endura IP Video Management System).

These results are, again, outstanding, clearly demonstrating the superior always-on application availability that Fabric Connect's unified protocol stack delivers. It's quite simple really: one integrated technology running all Layer 2, Layer 3, and IP Multicast services works better than multiple disaggregated but interdependent protocols. Testing with traffic generators is one thing, but running genuine applications such as a very high-density, high-definition IP CCTV solution is quite another. Obviously, Unicast tests showed equivalent or better numbers.

Fabric Connect Customer endorsements:

"We've not had a failure yet."

Operational since July 2013

"We haven't seen one (a failover)."

Operational since Oct. 2014

"Prior to Fabric Connect we did not have a failover route, so I can't really answer the question for previously. Now it is 10 milliseconds."

Operational since Aug. 2014

"We haven't measured it since (implementing)… it was 15 seconds before, but it probably is in milliseconds."

Operational since Aug. 2014

"We had one [a redundancy capability will our former design, but] which was particularly long so, to be honest, it wasn't a good benchmark."

Operational since Nov. 2013

"The figure I have given you is a guess, as we haven't had to troubleshoot as yet."

Operational since July 2014

Multicast Flows	Observed Time (Milliseconds)									
Failover Testing	185	121	233	187	117	140	165	202	349	183
Recovery Testing	210	59	146	50	102	109	99	164	135	228
Fabric Connect Node Failure	151	131	227	169	337	57	157	294	322	114
Application-Level Recovery Time	Average Recovery Time = 667									
Impact to Application	0	0	0	0	0	0	0	0	0	0

Although this sort of scenario may be a little dramatic compared to mainstream requirements, it is the sort of challenge that Extreme Networks excels at and an excellent way to highlight our unique capability. Besides, who can tell what is around the corner for any individual network, what new application will need to be deployed and supported. Businesses demand flexibility from their information technology investments, and IT must proactively integrate agility, scalability, and – of course – superior application availability.

Invisible Core: Simplified Security

Fabric Connect delivers significant differentiation, and business advantage, when it comes to network visibility and traffic transparency. The basis for this is the distinctly different approaches taken by conventional networking and Fabric Connect's Shortest Path Bridging.

Just to set the scene, conventional networking has progressively evolved, driven by a number of factors, to what is essentially a collapsed, routed backbone with multiple virtual interfaces that provide connectivity to a variety of user segments. In practice, we configure this as multiple Virtual LANs (VLANs) that service groups of users, each with a routed interface (terminating on Virtual Routers). The Layer 3 engines at the heart of the network populate tables with all known routes and communications are established, creating a situation where any-to-any connectivity is the default behavior.

This technique works – obviously – but it also introduces some undesirable characteristics:

- In larger networks, end-to-end connectivity is, in fact, a series of hop-by-hop forwarding decisions; configuration can become very complex, especially when Layer 2 VLANs need to span beyond a single physical location. Configuration scripting can aid bulk changes but is also prone to input error which can induce loops and network outage.
- Being IP-centric, the conventional network topology is very easily and quickly mapped; good for network management purposes, but a double-edged sword insofar as it also presents an effective attack platform for hackers. Again, being IP-centric, attacks can be launched from any point within or external to the network.
- In an effort to control the default any-to-any behavior – rarely practical in and of itself – businesses often chose to lock-down connectivity to selective paths so that any-to-any doesn't simply become a vehicle used by attackers. Options include using Access Control Lists (ACLs) or distributed physical or virtual Firewalls to limited, for example, users-to-application, not users-to-users. These measures can be expensive and are always complex to plan, deploy, and maintain.

As previously alluded to, Fabric Connect delivers a distinctly different administrative experience. Rather than any-to-any, the entire basis of connectivity, in a Shortest Path Bridging context, is one-to-one, or a series of multiple ones-to-ones. Services, our Layer 2 and Layer 3 "Virtual Service Networks" (VSNs), are a function of explicit provisioning, and communication between different Services is blocked unless specifically enabled. In its simplest form – two devices communicating with each other over the backbone – connectivity is established by both being configured, only at the Fabric Edge, as members of the same VSN, using one of up to 16 million unique Service IDs.

The Fabric Connect philosophy delivers a number of crucial benefits:

- Edge-only provisioning completely removes any need for Service-specific configuration in the Core or any other intermediate Fabric Connect node; if a Service terminates of two nodes, this configuration appears on these two nodes only, not on any other regardless of the network topology or size. This completely changes the configuration paradigm, from hop-by-hop to end-to-end; configuration is vastly simplified and change is de-risked.
- Being Ethernet-centric, the Fabric Connect network topology is invisible from an IP perspective; there are no inherent hop-by-hop IP paths to trace, therefore the network topology cannot be traced using remote IP-based tools. Network management is fully supported – indeed, additional Layer 2 tools are delivered – however, an individual host will only ever see, at most, the other hosts on their specific VSN. Individual SPB nodes are not, by default, visible to any host on any VSN; if enabled, ICMP would only show the VSN Edge nodes, but nothing of the inner network.
- Built natively as a series of isolated VSNs that interconnect specifically provisioning endpoints, Fabric Connect handles traffic forwarding in a fundamentally different way.
  Traffic belonging to a specific Service is encapsulated with the appropriate header at the Edge and remains isolated from every other Service/traffic, and opaque to intermediate nodes. This mitigates the need for intra-network ACLs and Firewalls; VSNs are oblivious to each other, as are hosts on different VSNs, and there is no risk of traffic blurring between VLANs or seeping through generic routing tables.

Hence, Fabric Connect fully addresses the major security pitfalls that conventional networking introduces; however, it actually goes further and delivers even more.

- Individual endpoints and complete Services are transported, fully isolated from each other, delivering a true "ships- in-the-night" capability that we call "stealth networking". This unique capability is very complementary to specialist service overlay, supporting the likes of PCI for financial transactions, and data protection in the healthcare, legal, and financial sectors.
- Deployed in concert with an Enterprise-class access control broker, Fabric Connect leverages authentication to create a very effective policy enforcement point; no connectivity is provided without hosts first proving their bona fides. Failed or suspect hosts are always completely isolated and can be mapped to quarantined or remediation zones.

- Fabric Attach facilitates the automatic attachment of authenticated end-point devices directly into their appropriate VSNs. Equally beneficial at both the Wiring Closet and Data Center edges, Fabric Attach supports dynamic service attachment and removes the delays and risks associated with manually configuring conventional networks, yet seamlessly maintains Fabric Connect's enhanced security posture.

The stealth capability that Fabric Connect delivers is a hidden gem. These benefits are truly unique and when correctly positioned they represent compelling differentiation.

Automated IoT: Plug and Play through Elastic Networks

Extreme Networks has pioneered the concept of "network elasticity", and we're uniquely positioned – by virtue of our differentiated technologies – to deliver solutions that make this a reality. The "elastic network" stretches network services to the Edge, only as required and only for the duration of a specific application session. As applications terminate, or end-point devices close-down or disconnect, the now-redundant networking services retract from the Edge. This elasticity as two obvious benefits: it simplifies and expedites provisioning for the ever-increasing number of network devices, and it has the added benefit of reducing a network's exposure and attack profile. After all, we don't walk about with our wallet in our hand, open, with our cash exposed; no, we produce it only when specifically needed.

First thing to say is that it's neither feasible nor desirable to attempt to pre-provision every possible application segment at every Edge node. The business environment never achieves finality, there's never a point at which evolution stops. Therefore, it's unrealistic to declare a "final" network configuration, for universal deployment, to every Access Switch. Equally, such as configuration would be extremely complex, prone to error, difficult to troubleshoot.

Crucially, it would expose every network segment at every network Edge node, and doing so would be a highly undesirable act. In a variation on the time-honored "need to know" maxim, network access should be elastic, only extended to the Edge as required, and retracted once the genuine need has passed. Replacing static network device configuration with dynamic programming reduces overall complexity in the network and has a corresponding benefit in reducing the risk of outage due to misconfiguration or attack.

In the context of the Internet of Things (IoT), end-point devices – often unattended devices – need to be deployed in real-time, without the requirement for IT intervention or manual configuration, with a centralized policy engine defining and policing device connectivity in compliance with business policy.

Leveraging these capabilities, devices request application-specific network assignment during start-up. Existing techniques for device recognition, authorization, and authentication – i.e. MAC- and/or RADIUS-based, 802.1X, and 802.1AB – can be leveraged and integrated with network provisioning and policy enforcement. Network connectivity – VLAN, QoS, Policy, whatever is needed to deliver this service – are then dynamically extended to the Edge.

This networking session may last only minutes, or hours, or perhaps days. Regardless, the key attribute is that service is automatically provisioned – "spun-up" if you will – without manual intervention or pre-configuration. Similarly, once the session terminates, the same-said networking configuration is now automatically undone, removed from the Access node, and consigned to history.

In addition to supporting the flexible deployment of obvious network endpoints such as IP Phones, Wireless APs, and IP CCTV Cameras, network elasticity plays a crucial role in facilitating IoT solutions.

Multicast Made Easy: 28x Scalability

In the early days of networking, Multicasting was a major innovation. But the ready availability of an IP Multicasting configuration option belies its complexity. The technologies needed to make Multicasting work in a traditional Ethernet environment are complicated, involving protocol overlays that must be kept rigorously in synch with underlying network topologies. Current approaches are ill-suited to next-generation IP Multicasting applications such as video surveillance, as well as emerging Data Center transport models such as VXLAN and NVGRE. Many of these applications involve not just one source to multiple destinations, but multiple sources to multiple destinations.

Conventionally, IP Multicasting relies on a Distribution Tree built by a Multicast Routing protocol, typically Protocol Independent Multicast Sparse mode (PIM-SM), to deliver packets from the sender/source to the receivers that reside on different IP subnets. Multicast Routing protocols need to operate in overlay mode with an underlying Unicast routing protocol such as OSPF. This dependency commonly results in issues where packets transmitted by a sender do not reach receivers due to improper building of the Multicast Tree. In the case of PIM-SM, there is additional dependency on a device called a Rendezvous Point (RP) to build the Tree for a Multicast Group. Improper configuration of these protocols and functions can result in packet delivery issues.

Another common cause of non-delivery of packets to receivers is a Reverse Path Forwarding (RPF) check failure which can occur when the Unicast forwarding path and the Multicast Tree are not sufficiently congruent.

The pseudo-state established by PIM-SM must remain in exact correlation with the underlying Unicast routing topology. If this state is lost or becomes ambiguous, all bets are off. Any change to the network topology can adversely affect the stability of the IP Multicast service. Additions, deletions, sudden outages for any reason (e.g., a faulty link, port or module) can all wreak havoc; the Tree truncates and the distribution service for that length of the Tree is effectively lost.

PIM-SM overlays are also very dependent on timers for the operating protocols and these timers must be fine-tuned. Mutual dependencies like these are difficult and time-consuming to troubleshoot, which means longer repair cycles and higher operational expenses.

Anyone that has been involved in deploying and maintaining large-scale Multicast environments probably has the mental scars to prove it. Indeed, many have found it simply too problematic and have reverted to Unicast, despite the downside of inefficient bandwidth utilization. However, IP Multicast is making a come-back, often out of necessity rather than choice. Many technologies such as next-generation video surveillance, IPTV, digital signage, desktop imaging, financial applications, and some network overlays are reliant on Multicast.

By contrast, Fabric Connect offers a scalable, reliable and efficient way of supporting IP Multicast Routing, without the onerous requirement of configuring, deploying, and maintaining a complex overlay such as PIM. Imagine a Multicast network without RPF checks, Rendezvous Points, and complex configuration. Fabric Connect delivers IP Multicast with the simplicity of Edge-only configuration while offering vastly enhanced scale, performance, and reliability, and eliminating PIM-induced headaches forever.

The unified, single-protocol technology that underpins Fabric Connect – Shortest Path Bridging – is naturally extensible. Extreme has leveraged this extensibility to integrate support for IP Multicasting directly into the stack. This creates a seamless IP Multicast capability, enabling the network to instantiate services on demand, whether they are one-to-many, many-to-few, or many-to-many. Sources are announced throughout the network using extensions in the IS-IS control plane (through defined TLVs). Receivers join a source group (a unique I-SID), by requesting membership using traditional IGMP.

A big advantage of this IP Multicast solution over traditional approaches is the absolute simplicity in provisioning: a single command-line or GUI checkbox. Additionally, Fabric Connect reduces operational burden, increases availability, improves performance, enhances security, and – crucially in an IoT world – delivers all-important scalability.

In most conventional network designs, the practical limit is 500 Multicast Streams. Beyond this number, things get "extreme" very quickly, and it's normally deemed safer to build parallel networks to spread the load and risk. But imagine a Smart City environment where 10,000 or more IP video surveillance cameras are required; this sort of workaround is simply not appropriate.

A recent ZK Research IP Video Surveillance paper is unequivocal on the subject: 75% of all IP CCTV challenges are directly related to the network[4].

Listing the ideal network requirements that IT leaders should seek reads like a checklist of Fabric Connect benefits: network simplicity, reduced number of provisioning points, consistent support for Unicast and Multicast, and reduced number of protocols.

Extreme Networks is uniquely positioned in being able to scale above and beyond any alternative. In truth, the only problem that we face is building test environments large enough to measure the limits of our capabilities. For example, in validating Fabric Connect with Pelco's IP CCTV solution we have been able to demonstrate scalability well beyond 14,000 Streams; an incredible 28x improvement!

Being able to deliver scalable, reliable, and efficient IP Multicast is a genuine differentiator.

Resource Efficient: 1/10th of the Resources, 1/10th of the Time

Even from the very beginning of Fabric Connect, we knew that this was the technology that organizations really needed and would heartily embrace. The critical mass of benefits delivered by the underlining technology – Standards-based Shortest Path Bridging, enhanced with extensions – means that our solutions can provide revolutionary benefits.

A great example of this differentiation is InteropNet, the backbone that provides network and Internet connectivity for every exhibitor at the annual Interop trade shows. The 2013 event was chosen to showcase Fabric Connect to the industry, including interoperability with other SPB implementations. In the run-up to that year's Las Vegas show we liaised with Interop organizers to establish a design and bill of materials, and to schedule our participation in the mandatory pre-show staging build. It was during this exercise that we became privy to some of the horror stories associated with past events; epic failures, incredible inventories, over-the-top engineering requirements, last-minute crisis meetings, and lots of late nights.

In spite all of this, and despite the organizer's scepticism, we remained positive, approaching the staging activity in much the same way that we approach every Fabric Connect deployment; exuding quiet confidence.

Suffice to say, the event was a huge success, and this is a direct quote from the InteropNet's lead architect[5]:

"Fabric Connect performed flawlessly as the InteropNet backbone provider. The fact that they were able to get the backbone network up and running very quickly with minimal staff, is a true testament to the power of the Fabric Connect technology and the quality of the engineers. We were pleased to be able to showcase this technology as a new way to architect and design networks to deliver for unparalleled simplicity, reliability, and agility."

What's not explicitly stated – given the obvious commercial sensitivity– is that just three (3) network engineers were used, rather than the typical 30 engineers, and took only 1/10 of the time typically required to complete both the staging and the final rollout. After the first day, our guys were– quite literally – finished, operational, and sitting around waiting for everyone else. Needless to say, the InteropNet also performed faultlessly, delivering above-and-beyond expectations in terms of provisioning agility and stability.

Equally obvious, we were immediately asked to return in 2014 to again provide the InteropNet backbone. Given a major commitment in the Sochi 2014 Winter Olympics, there was concern that this might be something of a logistical challenge, but we were confident that Fabric Connect would again be up to the task; and, of course, it was.

Over the years, the efficiency factor has been a recurring theme for businesses that have deployed Fabric Connect. There's the likes of the Dubai World Trade Center, with over million square feet of multi-purpose space and hosting more than 500 events across international trade fairs, mega consumer shows and prestigious conventions every year. The DWTC are now proud operators of a Fabric Connect solution:

"We worked together to plan and build a network that would allow exhibitors to use a simple plug-and-play capability for their equipment, ensure that other network users are all connected, and reduce the requirement for highly skilled people to manage the provisioning process. With Fabric Connect, we've achieved all three goals."

Another example is the Blue Springs School District in Kansas City, Missouri. The District employs some 1,000 teachers and 2,000 staff, to support 14,700 students. With such a large user community, the IT team was stretched thin operating its distributed systems spread out over 23 locations:

"Our Fabric Connect backbone was one of the reasons to go to a centralized Data Center model. I knew we had a backbone that could handle it, we could bring all the data and services back to one centralized location. We felt very confident we weren't going to have any issues as far as connectivity…now we're managing one Data Center, not 21 Data Centers,"

And then there's the Westpac deployment in Australia. As part of a Data Center consolidation project, Westpac wanted to relocate a disaster recovery (DR) Data Center from a city center location to a new site in Western Sydney. Westpac also wanted to establish a high-speed Ethernet connection between their Data Centers to replicate the existing applications and services across the sites before gradually relocating the physical servers. Westpac had attempted to achieve their goals with a design from a major industry player, however, things did not turn out well:

"The established vendor's solution was attempted, but it required multiple iterations of code with only varying degrees of success and subsequent unplanned outages."

Westpac requested a revised design from this vendor. However, the updated proposal presented the bank with substantial financial risk: it was much more complex, required double the hardware and would fail to meet deadlines for commitments relating to staging and provisioning equipment and ongoing maintenance resources. Westpac realized that conventional approaches would do what they needed to do and so they turned to Fabric Connect.

"Fabric Connect's main strength has been its straightforward, fast and low-risk deployment capabilities for DC-to-DC migration…activities have been significantly easier than anticipated, which has reduced design costs, labor requirements, project complexity and operational risk."

These are just a tiny sample of the great testimonials that we are gathering, all speak to the agility and efficiency that the Extreme Networks' Fabric-centric solutions deliver to businesses. In delivering a solution that saves time, effort, and money to plan, build, and operate, Extreme is empowering companies to divert their efforts to more profitable and business-centric activities. Recently, a customer operating in the Healthcare vertical presented back on their business outlook, including details on how their deployment of Fabric Connect is expected to help realize 5-year savings in the region of $25 million in capital spending and $15 million in operational expense.

Fabric Connect can deliver revolutionary benefits because, in part, we're revolutionizing the technology and philosophy of networking. It's sometimes overt, sometimes subtle, but in virtually every deployment you will see that the Customer took a different, better path than that permitted by convention.

Workflow Automation: Accelerating Business Outcomes

Integrating with workflow automation middleware, Fabric Connect enables an application development environment that places the Customer in the driver's seat, letting them decide which capabilities they need and how to most effectively integrate existing solutions and processes. It's all about streamlining and accelerating the delivery of business outcomes.

Potential use-cases are numerous, for example: dynamically creating, from scratch, an example business process that detects a device failure (e.g. IP CCTV Camera), and goes on to trigger an operations workflow that initiates a service ticket, schedules the field service technician, queries the status of replacement parts, and provides detailed notification to the system administrator. Obviously, process workflow such as this can be expanded and integrated at multiple stages, delivering great versatility.

The scope of possible use-cases knows no bounds. For example, in healthcare, there is a concept of automating ad hoc team engagement. Ostensibly this would be to facilitate short-term collaboration between expert skill sets, squarely aimed at improving patient outcomes. The scenario is that of complex surgery that requires real-time "second opinion" consultation. The current practice is to pause surgery, make use of conventional communication tools such a phone, if required to exit theater than a lengthy re-sterilization is also required; all the while extremely precious theater staff and resources are being wasted, and the patient remains in limbo. In the "perfect world", both the operating theater and key theater staff would leverage communications-enabled wearable tech to dynamically spin-up procedure-specific media-rich engagement sessions. With simple gestures, high-definition audio and video could be shared with appropriate colleagues, regardless of location. Dynamic team formation turns what can be a risky, expensive, and intrusive exercise into a seamless, streamlined, and immensely productivity activity. Patient outcome is expected to dramatically improve, and the ability to easily collaborate specialist skill sets will deliver higher levels of knowledge transfer.

All of these futuristic scenarios are, however, dependent upon an agile and programmable networking infrastructure that can be dynamically manipulated by higher-level software systems and applications. Fabric Connect is, uniquely, just such a technology.

In Summary

The intent of this paper is to go a little deeper into the characteristics and benefits that Fabric Connect delivers, placing these in the context of more than 1,400 real-world deployments. Increasingly, organizations are crying out for a network virtualization technology that provides linearly dependable scaling, high-reliability, one that actively promotes simplicity, and a solution that lowers their costs and delivers the agility that the businesses crave. Fabric Connect from Extreme Networks is that solution.

[1] Dr Cherry Taylor, Fabric Connect Customer Experience Research Report, Dynamic Markets, 2015.

[2] Dr Cherry Taylor, Network Agility Research, Dynamic Markets, 2014.

[3] Auto-Attach using LLDP with IEEE 802.1aq SPBM Networks (IETF, July 2014), and more recently this technology has commenced IEEE standardization as 802.1Qcj Automatic Attachment to Provider Backbone Bridging Services.

[4] Zeus Kerravala, IP Video Surveillance: The Network is Critical, ZK Research, June 2014.

[5] InteropNet 2013: Unbreakable! Fabric Connect Delivers on All Fronts.

Extreme®
Connect Beyond the Network

http://www.extremenetworks.com/contact / Phone +1-408-579-2800