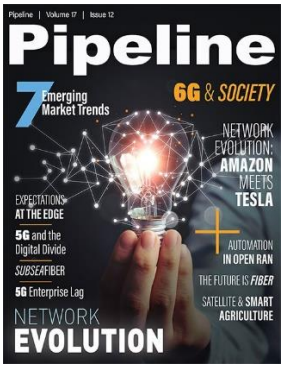
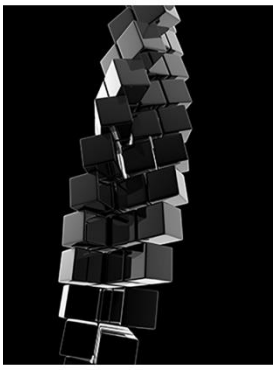


www.pipelinepub.com
Volume 17, Issue 12

Network evolution? Think Amazon meets Tesla!

By: Prayson Pate



We admire Amazon for its low costs and business efficiency, as well as its AWS cloud unit. Tesla is a leader in technology and performance. Both are very innovative and agile. What if we could bring all these concepts together to drive network evolution?

Why network evolution is important

Before we get to the **how** of network evolution, let's look at the **why**.

Today, networks are under tremendous stress. The drivers are numerous and include the COVID-19 pandemic and lockdowns. Expanded use of videoconferencing. Working from home. The semiconductor crisis. The desire for faster service innovation. These have all contributed, and enterprises and operators have been trying to keep their heads above water responding to the changes.

The pandemic and the semiconductor crisis may be temporary situations. But increased videoconferencing, working from home, and rapid innovation are here to stay. Now it's time to look forward, toward network evolution. Operators must plan for networks with higher bandwidth, better security, and lower latency. And they must design with innovation in mind. This means thinking differently about how they build these networks.

Amazon and Tesla are not known as telco suppliers, but they can still be useful models. They display the attributes that can help drive network evolution and provide a lesson for working in new ways.

Technology is great – but can you get it?

In the networking world we tend to focus on technical specifications—speeds and feeds, bandwidth, processor speed, and disk size. But the most important aspect of any product is availability. The best and fastest widget does you no good if you can't get it.

Amazon has been a marvel at rapid delivery of orders and at suggesting alternatives when your choice is unavailable. But this focus on supply chain and availability hasn't always been a driver in the telco world. Sure, we talked about second sources and continuity of supply—but an awful lot of the network was single-sourced, and much of the supply chain was fragile.

The pandemic and semiconductor crisis have highlighted the folly of this approach. We're now seeing the essential nature of reliable supply chains and the imperative to change suppliers when they can't meet demand.

Network operators are looking much more closely at the supply chains behind the products they buy. And they want the resilience of a diverse set of suppliers. They are insisting on standards and interoperability to support multi-vendor networks. Nobody wants a disruption of one supplier to stop their network evolution.

Technology is still important

Network innovation is about more than technology. But we still need technology innovation to support network innovation. And sometimes we must come at the problem in a completely different way.

Tesla is a great model for this. Electric cars have been around for as long as their gas-powered counterparts. And electric motors have incredible power and torque. This is why we use them in applications like diesel-electric locomotives. But electric cars were limited by cost and battery capacity. Now, Tesla has applied the latest technologies to make electric cars practical and affordable. With performance that meets or exceeds most gas-powered equivalents, they changed the game.

We're seeing the same thing in technology to support networking evolution. The move to open and multi-vendor systems has changed the networking game. We now see a division of functional building blocks, such as separating terminals from line systems in optical transmission systems or separating hardware from software. We call this disaggregating network elements, and it enables faster development of hardware and the utilization of a global software community, including open source. Users can select best-of-breed technology at each layer. This open model is spurring innovation everywhere. Here are some examples we're seeing:

Open line systems. Operators can build optical transport solutions where the line system remains largely independent from the terminals. This is critical as the endpoints evolve much faster than the line systems, which may not change for years.

Pluggable optical modules optimized for short-range or mid-range systems. The advent of coherent pluggable optical modules (also known as transceivers) such as 400ZR can simplify applications such as data center interconnect and metro access. They can plug into switches, routers, and optical shelves, eliminating the need for external optical terminal equipment.

Disaggregated switching. The Telecom Infra Project (TIP) has defined the disaggregated cell site gateway (DCSG) application. It includes a network operating system from one supplier that runs on a standard switch from another supplier. Operators can pick best-of-breed software and hardware to meet their needs.

Post-quantum encryption. Quantum computers are rapidly evolving. They can't yet break today's encryption, but experts predict they will be able to do so soon. It's essential that sensitive data be protected today to prevent a cryptographic assault tomorrow. This is why communications systems are already deploying cryptographic protocols that should withstand quantum attacks.

Network functions virtualization (NFV) and universal CPE (uCPE). These technologies implement a similar model to disaggregated switching. But in this case, the hosting hardware is a standard server (not switch). The NFV or uCPE model delivers the benefits of the cloud to the telecom world.

Open RAN. The move to 5G cellular is about much more than towers, radio technology and handsets. It's a complete overhaul of how radio access networks are built and used. An essential part is open, disaggregated, and software-centric approaches. This is where Open RAN comes in. It defines an architecture built on an ecosystem of suppliers using standard interfaces. Its software is cloud-native and it runs wherever required by latency, scale, security, or other requirements.

Cost and efficiency matter

I'm old enough to remember when air travel was very expensive. True, people were polite and well-dressed, and the airline fed you. But it was too expensive for most people. We complain about today's flights, but they really are a miracle. Our air transport system is incredibly large and complex, and it delivers safe end economical travel. Likewise, Amazon can deliver an amazing variety of goods, often overnight, at great prices. And their AWS group is the leader in cloud infrastructure. How do airlines and Amazon deliver these results?

A big part of the answer is massive automation driving a self-service model. You can book an airline ticket, select your seat, check in, and monitor flight status—all from your smartphone app. There is no need for human intervention.

Likewise, you can go to AWS, select a compute model, networking allocation, storage capacity, see the price, and charge it to your credit card. It's cloud computing on demand, under user control. Now contrast these situations with the usual networking model of "hurry up and wait."

It's clear that the telco world needs to evolve. The telco world makes heavy use of automation, but much of it is internal. Users must be able to shop and compare prices online, and then order, modify and monitor their telco services without human intervention.

Fortunately, some of the technologies mentioned above can help. They are designed to support automated deployment, and they have standard control interfaces to connect into customer portals. Will today's telco operators use these technologies to deliver a higher level of automation and user control?

What about trust?

I previously talked about post-quantum cryptography in the context of data security. But trust goes beyond securing data in transit. Let's talk about trust between end users, telcos, and suppliers.

The old telco model was adversarial. Enterprises and telcos would beat up their suppliers on price and then buy a single-source product. Once entrenched, the supplier would then milk the customer for all they could get. Not a pretty sight. And even worse, there was no way to see how the traffic was processed and monitored.

Now everyone is taking a different view. Multi-vendor systems mean that the operator must collaborate with multiple suppliers. And those suppliers must cooperate with each other, even when they compete in other applications. Doing so requires a standardized architecture with open interfaces. This provides full transparency at every part of the system. What's more, this approach ensures competition for the best features at the best price.

On the service side, innovation means that end users want customized services delivered in short order. Getting that means partnering with service providers and suppliers. Everyone must trust each other enough to work together.

Before concluding, let's go back to the security of data. There is a push to remove some suppliers from the network based on suspicion of snooping on user data. How can customers know their data is secure? There are government approvals and certifications for sensitive applications, but they don't cover the full range of networking equipment. This means that we need suppliers to be open and transparent so that they can build trust with the customer. Doing so may be uncomfortable for some suppliers, but it will be a requirement going forward.

Can we really emulate Amazon and Tesla in the network?

I think so. These juggernauts have shown how to apply technology and efficiency to drive cost and performance—and provide a high level of customer satisfaction at the same time. Applying those tenets to network evolution means stepping back to think hard about what we want to do and being willing to try new and different approaches. If we do this, we can drive network evolution to provide a faster, cheaper, and better version of what we have today.