CARRIER-GRADE ETHERNET AS A FOUNDATION FOR CAMPUS ACCESS NETWORKS

Introduction

Existing campus access networks are constrained by dissimilar and often stressed data networks—typically using numerous legacy technologies such as ATM and Frame Relay. These disparate networks are becoming increasingly difficult to manage, leading to higher operational and maintenance costs. Additionally, these legacy networks do not cater to the kinds of emerging real-time applications that are crucial for an effective Information and Communications Technology (ICT) environment, including VoIP, video, and cloud-based data processing. These applications are all IP/Ethernet based, requiring a next-generation, highly resilient, scalable, and packetized campus access network.

To this end, many government agencies have embarked upon modernization efforts that intend to transform ageing and legacy communications infrastructure into a consolidated, next-generation network. This usually includes refreshing the desktop environment to provide a more efficient and cost-effective method to transport packet-based applications to a high density of end-users.

There are several approaches available that attempt to provide a cost-effective access network. These include a pure Layer 2 Ethernet-based solution, otherwise known as “carrier-grade Ethernet;” Passive Optical Networking (PON), which uses a shared medium to distribute traffic; and a Layer 3 IP/Multi-Protocol Label Switching (MPLS)-based solution.

This paper will examine how a Layer 2 switching capability based on carrier-grade Ethernet offers the most scalable, reliable, and secure networking solution for a campus-based access network, and provides the lowest Total Cost of Ownership (TCO).

Carrier-grade Ethernet as a Network Layer

Carrier-grade Ethernet leverages well-known Layer 2 networking principles to provide standards-based transport for packet-based applications. Carrier-grade extensions to Ethernet increase overall network reliability, targeting five- or six-9s availability using classic telecommunications equipment supplier specifications to produce network elements with ultra-high reliability. In addition to increased reliability, the scalability of carrier-grade Ethernet is several orders of magnitude higher than traditional Local Area Network (LAN) designs.

Carrier-grade Ethernet technology has become widely adopted in the carrier and enterprise environments because of its ability to offer differentiated service at a highly attractive cost. Standards-based carrier Ethernet is defined by the Metro Ethernet Forum (MEF) and the Optical Interworking Forum (OIF) as a connection-oriented Layer 2 service. Carrier-grade Ethernet enables the ability to offer bandwidth-assured, Layer 2 Virtual Private Networks (VPNs) with up to eight layers of Quality of Service (QoS), allowing differentiated service offerings for voice, video, and data IP networks.

It is important to note that the carrier-grade Ethernet standards and frameworks mentioned above are built on the well-known, existing networking principles defined by IEEE 802.3. When applied to Carrier-grade Ethernet, the benefit of this adherence to established principles is that the technologies still use standards-based Ethernet components to realize the lowest-cost solution per bit, delivered by leveraging the millions of ports of Ethernet deployed around the world.

For an optical LAN or campus environment, carrier-grade Ethernet provides the following benefits, described in detail below:

- Increased network flexibility
- Flexible deployment options
- High levels of resiliency
- Network and user scalability
- Service security
- Carrier-grade Operations, Administration, and Maintenance (OAM)
These attributes are critical for an effective campus network, especially in an environment that requires a highly available, scalable, and secure network. Carrier-grade Ethernet is the best option for a campus-based access network, compared to alternative technologies such as PON.

**Network Flexibility**

Ethernet is inherently a multi-point technology routinely characterized as “plug and play” when adding devices to the network. With well-established mechanisms such as MAC flooding and learning, Ethernet can automatically discover paths through the network to enable communication. With this high level of built-in intelligence and adaptability, Ethernet can be deployed in any physical topology. Topologies include mesh, partial mesh, ring, and hub-and-spoke, or any mix of these architectures. Because Ethernet networks can adapt to growth and change, these topologies can expand easily or change over time.

All of these topologies have advantages depending on their application. With the flexibility Ethernet provides, there is no
restriction on how fiber can be rolled out to accommodate the network. This increased flexibility reduces overall installation cost.

Additionally, Ethernet standards provide for the use of bidirectional optics, where both transmit and receive are performed on a single fiber, from 100 Mb/s to Gigabit Ethernet (GbE). This efficiency greatly maximizes the use of fiber—often cutting fiber costs in half.

Along with flexibility in physical topology, Ethernet provides flexibility in “logical” topology. This refers to how services (Layer 2) are routed in the network. Traditionally, Ethernet networks were completely auto-learning, as mentioned above. This is still a valid premise in a campus environment, but enhancements have been made to Ethernet that allow for connection-oriented switching, with paths defined by identifying specific connections during route provisioning. This arrangement allows deterministic path identification, letting network operators choose the network path services take to better manage latency or maximize fiber and bandwidth utilization. This becomes more relevant as network topologies change and grow. Connection-oriented switching gives the network operator the ability to offer network security on par with circuit-based applications, yet with the flexibility and robustness of packet switching. Combined with carrier-grade Ethernet’s OAM tools, a network operator can define and monitor network performance while providing assured information technology infrastructures for critical missions.

Finally, because Ethernet is a well-defined standard, new vendor equipment can be interconnected to existing networks with minimal testing. This ease of transition makes Ethernet a risk-free option with minimal lag time.

**Ethernet Configurations and Equipment Flexibility**

Ethernet has widespread global deployment and can be thought of as the de facto data link standard for carrying TCP/IP-based traffic. Deployments are ubiquitous in the user appliance connection to the edge, campus networks, and the Wide Area Network (WAN). As such, equipment manufacturers have created a large range of devices with varying options for port type, speed, density, and multiple form factors. Ciena offers a wide breadth of carrier-grade Ethernet devices in its Packet Networking Portfolio, as shown in Figure 1.

Ciena’s Ethernet product portfolio is particularly robust in the campus environment, which was the initial design target, so these options effectively meet the requirements of medium to large enterprises. Included are options for high-density, low-footprint switches, high port count (48 Ethernet ports or more) for high-density fan-out, and small, single-port desktop devices. A variety of physical interfaces are available, including multi-speed copper RJ45 or fiber-based options, which can be changed with the simple addition of an SFP module.

**Resiliency**

Networks carrying mission-critical information require high tolerance to network disruptions such as fiber cuts or equipment outage. Network resiliency is essential to the ability to support critical command and control applications, data center connectivity, and even desktop applications.

Due to Ethernet’s ability to be deployed in various topologies, it is possible to set up multiple physical paths to specific network elements. This flexibility allows network operators to provide resilient paths in the network. Traditionally, Ethernet LAN technology used spanning tree to manage failures in a network, often taking up to a minute to reconverge after a...
failure. This lag is not acceptable in today’s highly demanding networks. Operators are looking for failover rates closer to the TDM gold standard of 50 ms to ensure applications such as VoIP are not impacted. The MEF utilizes standards such as IEEE 802.1Qay Provider Backbone Bridging – Traffic Engineering (PBB-TE), MPLS-TP, and ITU-T G.8032 Ethernet Ring Protection (ERP) to ensure reconvergence times below 50 ms in the event of failure. These failover times are applicable to any network topology—mesh, ring, or linear—yet this configuration does not preclude using unprotected hub-and-spoke architectures where redundancy is not required.

Bandwidth Scalability and Granular Bandwidth Control

Today’s Ethernet networks provide interfaces from 10 Mb/s to 100GbE interfaces. Because Ethernet hardware enjoys such large-volume deployments, even 10GbE connections are becoming reasonably priced. The change from lower to higher speeds is basically seamless; in many cases, the equipment’s basic configurations support multiple connectivity options. This means that GbE and 10GbE ports exist on the same hardware, the latter of which does not need to be used until it is required. Additionally, it is now possible to upgrade from GbE to 10GbE with the simple addition of a software license. This option is becoming a more popular trend among Carrier-grade Ethernet switches.

Ciena’s solution provides unprecedented levels of service classification. Ciena’s service aggregation switches provide up to 64 class-of-service levels, allowing greater flexibility than the typical eight found within competitive offerings. In addition, operators can configure certified MEF-compliant Committed Information Rate (CIR), Excess Information Rate (EIR), and burst parameters.

An example of a Ciena innovation is the use of service templates defining QoS parameters. For instance, a provider’s “Silver” service can be easily changed from 40 Mb/s to 50 Mb/s. Every service configured to Silver is automatically changed, dramatically reducing the number of configuration/provisioning steps required by the operator.

Flexible bandwidth scaling and granular bandwidth control are important in a campus environment where there is a high density of users with a dynamic mix of traffic requirements, and increasingly higher traffic usage as more bandwidth-intensive applications are introduced. Specific links or portions of the network can be upgraded seamlessly as required, without impacting the entire network. No rip-and-replace of an entire network is required, as all data rates can co-exist on separate links.

Service Security

To support critical enterprise applications, assured networking solutions are critical to provide required levels of service. Assured networking refers to all aspects of the network lifecycle, including network architectures, product features, network services, and the supply chain.

Beyond network firewalls, gateways, and other mechanisms aimed at defending the borders of a network, security also can be enhanced by incorporating protection into the network architecture itself. The core structures of the Ethernet extensions built into the frameworks by the MEF let the Ethernet standard scale to carrier networks, allowing robust security architectures to be built in the campus environment. Layer 2 VPNs can be used to segregate traffic, limit the potential for contention and congestion to affect critical traffic, and ensure traffic prioritisation decisions remain private.

Secure services are classified in the Ethernet standards defined by the MEF by appending VPN tags, which differentiate the VPN service type and priority, to an expanded Ethernet frame. This service can be scaled by consecutively adding layers of VPN tags to create network VPNs that are logically isolated from edge VPNs.
The ability to stack VPN tags was crafted by IEEE 802.1ah to enable both the customer and the network operator to set up VPNs independently, with no possibility of mixing between the domains. This technique, also known as MAC-in-MAC, can be added as a security element in the Ethernet network. By establishing a customer VPN inside a particular security zone or sub-network and then using PBB in the network, details of the internal topology of the sub-network can be isolated from other elements of the network.

Ciena also has implemented a patented technology, virtual switching, into its carrier-grade Ethernet portfolio. Virtual switching logically partitions a physical Ethernet switch into separate switching domains; each virtual switch forwards traffic independently of the others, providing a unique mechanism for isolating user traffic that is superior to other available techniques.

These core elements of the Ethernet standard, when used in conjunction with Layer 2 encryption, provide powerful tools to enable network operators to build assured network security architectures into their networks. Internal network addressing, traffic prioritization and QoS targets, and data are best kept private for mission-critical applications. Judicious application of encryption and VPN tag-stacking provide these key assured networking benefits. Ciena’s Ethernet products have undergone extensive interoperability testing with the SafeNet Layer 2 encryptor and will support all of these security features.

In addition to PBB-TE, there is a variety of encapsulation mechanisms such as MPLS-TP available to create these VPN tags; in each case, user traffic is separated and there is a clear segregation between end-user traffic and core network traffic. The selection of encapsulation mechanism depends on a number of factors, including the need to interact with Layer 3 infrastructure, the extent of the security requirements, and the need for robust segregation in the network.

With carrier-grade Ethernet, Ciena can build a network architecture that offers the benefits of a segregated network on a common infrastructure, thus maintaining security principles at the lowest possible cost.

**Operations and Maintenance**

A key element of MEF standards development was to build a framework that allows Ethernet networks to operate in manner similar to legacy TDM transport networks, including high-level or OAM capabilities. This factor includes “the ability to monitor, diagnose, and centrally manage the network, using standards-based, vendor-independent implementations.” Ciena has been a pioneer in introducing and pushing relevant OAM protocols in standards bodies.

| Turn-up Acceptance and SLA Conformance Testing | RFC 2544 Generator/Reflector  
| ITU-T Y.1564 Generator/Reflector |
| Layer 3 SLA Monitoring & Metrics: Delay, Jitter | IETF RFC 5357 TWAMP  
| Two-Way Active Measurement Protocol |
| Layer 2 SLA Monitoring & Metrics: Delay, Jitter, Frame Loss | ITU-T Y.1731 Ethernet OAM |
| Service Heartbeats, End-to-End & Hop-by-Hop fault detection | IEEE 802.1ag CFM  
| Connectivity Fault Management |
| Enhanced troubleshooting, rapid network discovery | IEEE 802.3ah EFM  
| Physical Link |

*Figure 4. Ciena’s virtual switching*  
*Figure 5. OAM toolkit implemented in carrier-grade Ethernet solutions*
With the addition of comprehensive OAM capabilities, Ethernet offers a complete feature set that allows network operators to troubleshoot networks effectively to ensure Service Level Agreements (SLAs) are met. IEEE, IETF, ITU-T, and MEF now describe mechanisms that allow an operator to poll the status of a given end-to-end service, link, or beyond to provide detailed metrics around each. These mechanisms are essentially proactive monitoring tools. The OAM tools also provide the ability to reactively troubleshoot the network. Upon discovering a network fault or service degradation, the operator can rapidly isolate and correct the issues, thus providing higher availability for business-critical services.

OAM encompasses the ability to rapidly turn up services and devices. Ciena’s solution provides a truly automated provisioning paradigm. All carrier-grade Ethernet devices shipped from the factory have the intelligence by default to request specific software and configuration templates from the Network Operations Center (NOC).

In addition to the operational benefits, the OAM tools are another pillar of the assured networking strategy. The ability to generate real-time situational awareness, rapidly respond and reconstruct after network disruptions, and monitor expected performance is vital to supporting critical government applications. The ability to detect and quickly respond to a threat to the network is a key part of the network security strategy, especially with respect to actions by an insider. By maintaining a current network baseline and using the OAM tools to monitor the network for anomalies, network threats can be detected and quickly addressed.

The templates are extensible and incredibly powerful, allowing many customizable parameters to be pushed down when the device is turned on.

Ciena has deployed automated solutions at many carriers and campus networks for Ethernet-based services and demonstrated that the time to turn up a service was reduced by up to 75 percent.

**Carrier-grade Ethernet vs. PON/GPON**

Although this white paper focuses on the benefits of carrier-grade Ethernet as a technology, alternatives are available within the access space for campus networks. PON and Gigabit PON (GPON) have gained good traction within the residential access market for many years due to their commercial benefits in that market segment.

PON is a shared medium in which a fiber is “passively” split into many end-user connections. The term “passive” refers only to the optical splitter, which does not require external electrical power. Each end-user has an active Optical Network Unit (ONU), and the fiber terminates at a central office in an Optical Line Terminal (OLT), which also requires electrical power. Studies by the U.S. Army have shown that an enterprise’s total power requirements for PON solutions and carrier-grade Ethernet are similar. Between the OLT and the ONU, there may be one or two stages of passive splitters that split the connection to multiple endpoints. PON is a shared medium and typically uses a two-stage splitter, where each OLT is connected to a 1:4 splitter, followed by four 1:8 splitters, to accommodate 32 users. In addition, since it is a shared...
medium, GPON makes each user dependent on the other users, so the optical budget of the PON has to be divided among the users of the network. Therefore, the service provider must have early, accurate, and granular planning data about the user requirements for each campus area and the distance of each of its users from the campus. The splitter architecture limits the reach of the fiber from each of the splitters, so even a small serving area has to be planned to accommodate expected user requirements, and any variation results in decreased efficiency. Under-predicting user requirements results in users who cannot be serviced without more investment; over-predicting results in investment that goes unused.

PON systems automatically balance signal power to account for disparate transmission distances between user drops in a network environment. This fluctuation creates an inherent security vulnerability; a user can intentionally or unintentionally affect the service delivery to other users by changing the losses on their connection and potentially flooding the bandwidth.

Carrier-grade Ethernet networks typically use an aggregation switch located in the campus network control center, closer to the end-user. PON uses a passive splitter at this aggregation point. The use of a passive splitter is listed as a capital cost advantage for PON, since it does not require electrical power and has a small form factor. This difference can provide a substantial advantage in the residential access environment; however, these advantages largely disappear in the campus and enterprise environments.

The table in Figure 7 provides an overview of the different technology approaches.
Carrier-grade Ethernet as an Enabler of Assured Campus Environment Communications

Carrier-grade Ethernet is a technology that could be deployed within the campus and desktop environments to provide an alternative to shared-bandwidth solutions. As discussed earlier, carrier-grade Ethernet will enable and facilitate a full-bandwidth service that gives enhanced security, greater deployment flexibility, and better resiliency.

Interconnecting a campus-wide Layer 3 network would utilize an architecture that connects Provider Edge (PE) routers at each sub-network boundary with a set of Layer 2 VPN tunnels that provide an A-to-Z connection with another PE router at the destination sub-network. Each of these tunnels will assign a deterministic amount of bandwidth to the IP flows from that router. Network operators can assign flows based on classification, data type, priority, or any other logical separation that meets the application needs. In this way, VoIP traffic can be segregated from video and other data traffic via assured bandwidth tunnels. This segregation can be accomplished on a customer-by-customer basis or in any logical grouping, according to the security sensitivities of the end-users. This is a particularly useful architecture for maintaining assured network security when interconnecting geographically dispersed campuses and sub-networks that are interconnected over a common carrier service.

Equally importantly, if the required application is a dedicated Layer 2 connection (similar to a leased line), a carrier-grade Ethernet solution is ideal for campus networks, providing the lowest latency, highest bandwidth, and most cost-effective solution.

What Ciena Delivers

Ciena's solutions focus on four areas: Assured Networking, Ethernet for Branch and Base Connectivity, Grid and Cloud Computing, and Data Center Networking. Many elements combine to form these solutions—including technologies such as Optical Transport Network (OTN), Carrier Ethernet, software reconfigurable platforms, and data encryption—augmented by services such as network design, analysis, deployment, and operation. The solutions utilize elements of a broad networking portfolio that includes powerful optical transport and Layer 2 carrier-grade Ethernet switching functionality. These hardware elements are managed by a unified, automated control plane that simplifies operation. Additionally, Ciena offers comprehensive network services to aid in the design, deployment, and operation of any network.

Optical networking

Ciena's assured optical networking solutions comprise switching, transport hardware products, software components, and services. Our 5400 Reconfigurable Switching Systems are the industry’s first multi-terabit-class optical switching systems that utilize intelligent mesh networking to automate the provisioning and dynamic bandwidth control of high-capacity services. These core and metro core products support any mix of Carrier Ethernet/MPLS, OTN, Wavelength Division Multiplexing (WDM), and SONET/SDH switching to facilitate the transition to a service-enabling infrastructure.

Ciena’s optical transport products address any transport network requirement or application and offer a variety of service and interface options. With the company’s WaveLogic coherent optical processor technology, Ciena platforms automatically accommodate a wide range of existing fiber plants, making 40G and 100G as easy to deploy as 10G. In addition, the platforms leverage common management and control plane interoperability to make each network scalable.

Carrier Ethernet access

Ciena provides carrier-grade access solutions based on Ethernet service aggregation and delivery. Ciena’s Packet Networking portfolio combines intelligent devices and software to create low-touch, high-velocity carrier-grade
Ethernet access and metro networks—resulting in a common, consistent means to deliver the full range of Ethernet services that significantly accelerate and automate service creation and activation. Assured networks built on Carrier Ethernet access allow operators to build highly reliable networks that scale easily and offer service diversity with a high degree of inherent security and economy.

The Packet Networking portfolio includes aggregation and service delivery switches that are sized to match the needs of a specific application. Service delivery switches are available with a range of 10/100 Ethernet, GbE, and 10GbE physical port counts to fit small, medium, and large customer sites, with placement in customer premises, on the sides of buildings, or on utility poles. Service aggregation switches provide 10/100 Ethernet/GbE/10GbE aggregation to better fill the transport facilities within both the metro access and aggregation tiers and ultimately minimize the number of IP/MPLS router ports with which they interwork. These switches can be deployed in a wide variety of locations, including business parks, outside plant cabinets, and in central offices.

**Conclusion**

Ciena collaborates with government customers to unlock the strategic potential of their networks and fundamentally change the way they operate. Ciena’s carrier-grade Ethernet solutions allow organizations to optimize IP and Ethernet services for campus locations onto a converged service delivery and aggregation network based on a broad, integrated family of purpose-built Carrier Ethernet switches with low-touch operations. Our Ethernet service delivery solutions combine the low cost and high capacity of Ethernet with the reliability, manageability, and service quality usually associated with SONET/SDH networking solutions. Ciena employs advanced OAM features and the latest innovations in Ethernet switching technology to deliver sophisticated QoS capabilities, superior Virtual LAN (VLAN) and virtual switching functions in scalable, cost-effective products that address the performance and capacity needs of any enterprise—large or small.

Security is critical in government networks. The emergence of carrier-grade Ethernet standards has given network operators the ability to introduce segmentation and provide enhanced security. When combined with Layer 2 encryption, these capabilities offer improved performance at a lower cost. Carrier-grade Ethernet solutions offer the ability to isolate user sets based on their authorization levels, offering implicit protection to adjacent VPNs. The use of Layer 2 switching offers significant reliability improvements in the event of a major security break or catastrophic event. Robust OAM tools allow efficient network operations and rapid response and remediation for network disruptions. By utilizing modern architecture concepts and equipment, the appropriate amount of security may be embedded in each layer, allowing operators to construct an assured network that yields trusted, reliable, and secure services to all user classes.

Ciena understands that governments need a variety of options to create efficient next-generation networks. As the worldwide leader in coherent technology for 40G and 100G deployments, OTN and mesh networking, and packet transport with cell tower deployments, Ciena also is leading the packet transport evolution by offering comprehensive data, transport, and OAM products. Furthermore, MPLS-TP, Carrier Ethernet, OTN, and coherent technology will help the industry move toward the packet-optical integration Ciena has been advocating for years.