The Keys for Campus Networking: Integration, Integration, and Integration

Introduction

Internet Protocol (IP) is considered the working-horse that the vast majority of current and future applications use as the key technology for information exchange, and the demand for more bandwidth is driven by IP-centric applications. These applications are generally characterized by the need for large bandwidth, robustness, flexibility, and scalability. Therefore, our network architectures have to evolve to keep up with evolving requirements of such applications. It has become clear within the networking community that the present mode of operation (PMO) of our networks while relying on legacy technologies such as SONET, ATM, and Frame Relay cannot keep up with these demanding requirements. As a result, the future mode of operation (FMO) requires cost-efficient, intelligent, robust, and packet-centric architectures.

Campus network is an example of an application that saw tremendous changes over the past years. By examining the evolution of our campuses, one can see the urgent need for reliable and scalable networking architectures to support this evolution. Today's academic institutions like universities and schools are using the latest technological innovations to improve the quality and the outcome of the academic process. Almost any school or university is providing facilities that merely depend on its network infrastructure. Campus network must provide several services including but no limited to Internet connectivity, managed internetworking among departments and colleges, reliable access to a campus's high-performance Information Technology (IT) which normally houses important resources such as data servers with large volumes of critical information, video conferencing services, and voice services. Generally speaking, today's campus network has gone long way beyond its legacy function of providing simple and very limited services and evolved into a complex network-of-networks carrying many bandwidth-hungry services and applications just like any service provider's network. However, unlike service provider networks, campus networks are not built to generate profit and they are limited by stringent cost constraints. Therefore, cost of ownership, i.e., capital expenditure (CapEx) and operational expenditure (OpEx) of these networks must be carefully considered without jeopardizing their reliability and scalability requirements.

This white paper discusses key technologies for building campus networks with particular focus on Ethernet over fiber optic DWDM transport. It provides an overview on other packet-based solutions such as IP and MPLS. It also shows how integrated and intelligent solutions can achieve superior performance and cost savings in a campus network.

Campus Network: Packet Layer Transport

Like other applications, campus networks require quality of service, scalability, security, traffic protection and obviously total cost of the solution. Therefore, the different solutions must be discussed and compared within these requirements to assess their pros and cons. Next, we consider various transport technologies for packet forwarding in a campus network. These technologies are Layer-2 Ethernet-based, Layer-3 IP-based, and MPLS-based.

1) Layer 3 Solution – IP Transport

Service providers have been successful in offering IP-based multi-point services, i.e., IP VPNs. In this scenario, end-users are connected to routers instead of switches, creating secure private IP circuits on a shared backbone, see Figure 1. The use of routers further improves scalability because broadcast storms are limited to individual LAN segments and the VLAN limit does not exist.

However, IP VPNs are costly and complex to manage and require routers to connect to customers. Because of that many service providers have recognized that IP-based transport is not suitable for a campus network compared to the simplicity and low cost of Ethernet-based services.

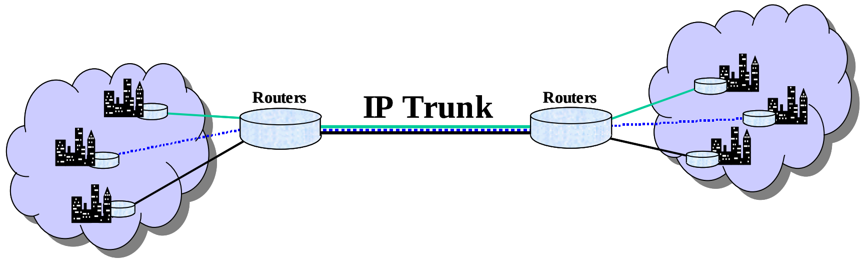

Figure 1: IP-based solution

2) MPLS Solutions – VPLS

In recent years, MPLS has become a de-facto technology that many service providers use in the core of their IP networks. MPLS offers scalability, quality of service, traffic engineering tools and reliability. Because of these attributes, MPLS-based transport is moving from the core towards the WAN and MAN in packet centric infrastructure. This network is an example network

IP VPN Service

Initially, IP-based VPN services where offered because of the many attractive features of MPLS. However, the same disadvantages exist as described for native IP VPNs. So while service providers are rolling out IP/MPLS VPN services aggressively, that approach is not seen as the best suited for campus networks.

Virtual Private LAN Service – VPLS

VPLS is an improvement of MPLS pseudo-wires, both Layer 2 solutions. VPLS offers all the advantages of MPLS pseudo-wires but adds multi-point connectivity capabilities. VPLS is a promising emerging technology and many service providers are committing to adopt VPLS to offer Layer 2 VPNs.

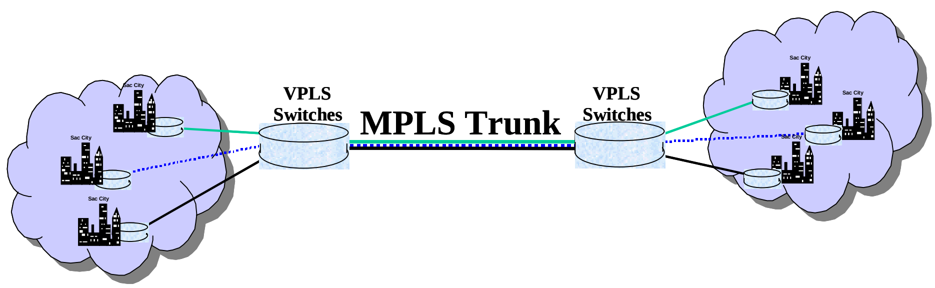

Figure 2: MPLS-based solution

Despite all the advantages of VPLS, MPLS awareness is still required of all switches. Although that is less expensive than the use of routers, which can also be used for VPLS, MPLS switches still add cost as compared to non-MPLS switches. Furthermore, given that a Campus network is limited in size as compared to a MAN, it is not clear that the advantages of MPLS are needed in this part of the network. It is therefore questionable whether this approach is right for a cost-sensitive application like a Campus network. It should also be noted that VPLS is still under development at IETF and it is therefore likely that proprietary solutions will be implemented until it is clear what service providers prefer.

Given the attractive features of MPLS and its already widespread adoption, it is likely that many MAN networks will be MPLS-based. In such cases, a gateway function can be implemented that translates traffic between the Campus network and the MPLS-based MAN. However, it is important to point out that in most campus applications, the campus network will not have the size nor the requirements that would justify the extra cost incurred by extending the service providers MPLS-based MAN all the way into the Campus network.

3) Layer-2 Ethernet Solutions

Ethernet is a mature technology that has long benefited form the massive volume production which has driven equipment prices to very low levels compared to other technologies. This trend has been most significantly witnessed in LANs. This trend is being pushed for use in other larger networks such as large campus. However, Ethernet must scale to the requirements of these networks. Next, we discuss various Ethernet solutions and explain their pros and cons.

Ethernet Solution Based on IEEE 802.1D Switches – Native Switched Ethernet

While probably the most cost-effective solution, it has long been recognized that IEEE 802.1D-based Ethernet, or switched Ethernet, in itself does not offer a scalable and secure solution in a campus-wide application. Broadcast storms and the use of network-wide STP limits network scalability and security is virtually non-existing.

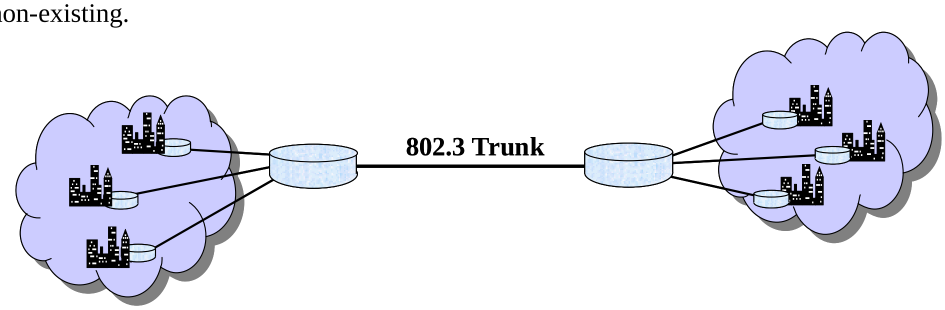

Figure 3: Ethernet-based solution: IEEE 802.3 trunk

Ethernet Solution Based on IEEE 802.1Q Switches – VLAN Aware Switches

To overcome the security issues as well as to some degree the scalability issues, the VLAN concept was introduced in IEEE 802.1Q (Fig. 4). VLANs allow the creation of Layer 2 VPNs, where traffic from different users can be aggregated while maintaining traffic separation, see Figure 3. Scalability is improved by limiting broadcast storms to VLAN domains and security is added because of logical traffic separation.

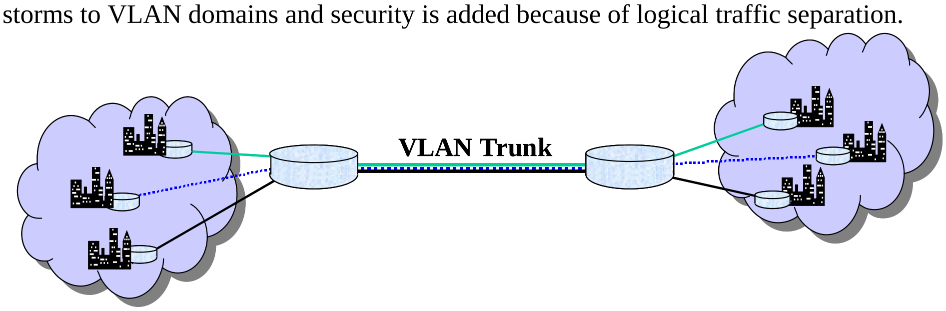

Figure 4: Ethernet-based solution: VLAN trunk

This is also a simple and low cost approach and has been widely adopted by service providers. Additionally, users on different VLANs can use the same IP addressing scheme, which improves service transparency and removes the need for central IP address management. Also, the introduction of RSTP and MSTP improves on key limitations of STP, i.e., hop limit of 7, much faster convergence times and support of per VLAN protection. Finally, the use of priority tagging enables traffic differentiation improving QoS.

Still, important limitations restrict the use of this approach for campus networks. Scalability is still limited by the fact that only 4094 VLANs are available for use – there are 4096 VLANs but two are reserved – and that one VLAN has to be used per user per service. Also, the STP (in any flavor) utilized in the users LAN can conflict with that used on the campus backbone. A major concern resulting from this is that if the end-users LAN required a topology change then the whole campus network would have to participate in process.

Ethernet Solution Based on IEEE 802.1ad Switches – VLAN Stacked Aware Switches
A solution that maintains the low cost and simplicity of Ethernet but solves the limitations of VLAN enabled Ethernet is based on IEEE 802.1ad – also known as VLAN stacking. The concept expands upon 802.1Q VLAN concept. End-users can use their own VLAN scheme but when traffic enters the service provider's domain, a new VLAN tag is added, hence the name VLAN stacking. Service providers benefit from this because they can use their own VLAN tagging scheme in the backbone without being impacted by end-users VLAN scheme, which means that network scalability is improved. End-users benefit because they can use their own VLAN scheme without regard to other end-users or the service provider. CPE boxes can used to define a clear demarcation point between the end-user domain and the service provider domain and it is at the demarcation point that service provider VAN tags are added and traffic priority is set. These CPE boxes should be placed at the end-user sites as shown in Figure 5.

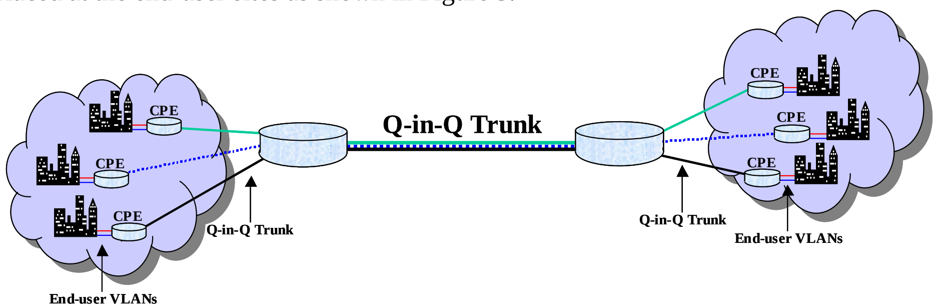

Figure 5: Ethernet-based solution: Q-in-Q (double tagging/stacking) trunk

Table 1 summarizes the different packet-based solutions for campus networks and shows their performance in terms of cost, security, scalability, resilience, transparency, and management. Clearly, Ethernet based on IEEE 802.1ad solution provides an ideal solution for the campus network application.

	802.1D	802.1Q	IP	VPLS	802.1ad
Cost	Low	Low	High	Medium	Low
Security	Poor	Good	Good	Good	Good
Scalability	Poor	Poor	Good	Good	Good
Resilience	Poor	Poor	Poor	Good	Good
Transparency	Poor	Medium	Poor	Good	Good
Management	Simple	Simple	Complex	Medium	Simple

Table 1: Comparison of various transport technologies for use in a Campus environment

Physical Layer Transport – DWDM

Now that we agree that Ethernet is the best choice of packet-level networking technology in a campus network, let us discuss physical layer transport.

For long time, wavelength-division multiplexing (WDM) has been viewed as technology that has use only in large-scale networks, e.g., backbone networks, that aggregate traffic flows coming from different access networks and aggregate into a second layer of transport such metro networks which are in turn aggregated and transported into the network's backbone. Hence, large-capacity pipes are required and WDM is the best fit for such environments with what it offers of huge bandwidth with relatively low cost.

Traditionally, campus networks have been used primarily to provide simple and basic connectivity services with small bandwidth requirements. However, the explosion of today's bandwidth-intensive applications such as video has completely changed this view. WDM is the only cost-efficient and flexible technology that can provide large pipes of capacity as needed to meet the ever-increasing demand for capacity in a campus. As a result, campus networks can benefit from the tremendous capacity offered by a DWDM optical fiber technology to meet this demand. In fact, fiber optic based on DWDM can be the only cost-efficient technology to serve for this task. Next, we discuss how campus networks based on DWDM can be realized.

Present Mode of Operation (PMO) – Layers of Networking

Figure 6 shows PMO campus network architecture with access switches connecting different campus facilities to the network's DWDM backbone ring. Using the present mode of operation, campus networks are built using layers of networking: aggregation layer using an Ethernet-based ring and a transport Layer using a DWDM ring as the backbone of the campus network. Even though Ethernet-over-DWDM (EoDWDM) seems to be the efficient solution in a campus network, today's EoDWDM solutions are not optimized for campus networks since they significantly lack the required functional integration which complicate these solutions and make them costly. These systems are based on large and expensive platforms originally designed for metro and core networks and therefore, using them for campus networks brings several drawbacks. First, the bandwidth requirement of a campus network seldom requires the full capacity of such large systems. As a result, it ends up being partially utilized forming "idle capacity" laying around in the network without any use. Second, these systems have poor capacity-allocation flexibility, i.e., if additional capacity is required, this has to be done using large capacity increments. For example, if the campus DWDM ring requires capacity expansion equivalent to single DWDM wave, current platforms demands using multi-wave (e.g., four) line cards as they lack granular capacity augmentation capabilities. This leads to additional massive costs. In addition, because these networks are built using several layers, this further complicates their architectures and makes their management even harder. In fact, today's solutions

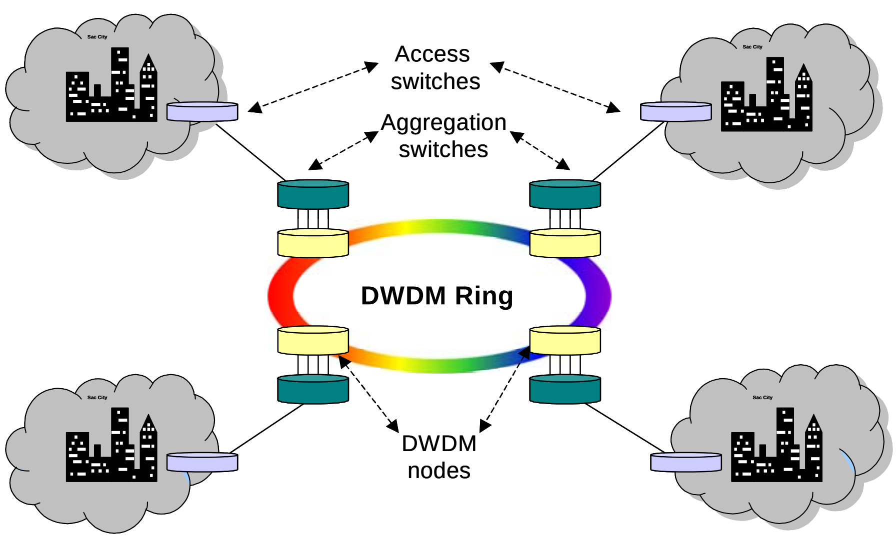

Figure 6: Campus network using layers of networks (PMO). Different nodes are shown in different colors since they have different functions with each node belonging to specific layer of networking.

Future Mode of Operation (FMO) – The Role of Integration

Figure 7 shows FMO campus network architecture. Designing efficient solutions for campus networks must start from understanding the drawbacks of today's mode of operation and understanding their requirements. An efficient approach must eliminate the complexity originating form the fact several layers are being used. Instead, campus network must be built using a single layer of networking where an Ethernet switch must also integrate DWDM capability to realize a single Ethernet-over-DWDM ring. This brings huge cost savings by consolidating two layers into one single layer. Also, for this integration to further reduce the costs, it must reduce the size of the EoDWDM platforms. This is particularly important in a campus environment where space required of these systems is a bottleneck. Another major element for further simplifying the network architecture is functional integration. In this case, the switch must provide all functions required in the network such as access, aggregation, and transport. This integration is equivalent to consolidating three separate platforms into one solution which leads to tremendous CapEx and OpEx savings. Integrating functions and systems in one platform has additional advantage of simplifying thenetwork architecture and therefore, simplifying its management. In PMO campus networks, since the several networking layers are used, multiple management elements are also used. This is particularly hard and costly since it requires inter-layer coordination requires expertise in different platforms and networking paradigms. Also, unlike PMO, FMO solution must enable capacity expansion in fine increments to exactly match bandwidth requirement as the network grows. This saves resources by fully utilizing the network's capacity and avoiding the idle capacity and reduces CapEx by paying only for what is needed and OpEx by eliminating the need for maintaining un-used extra capacity.

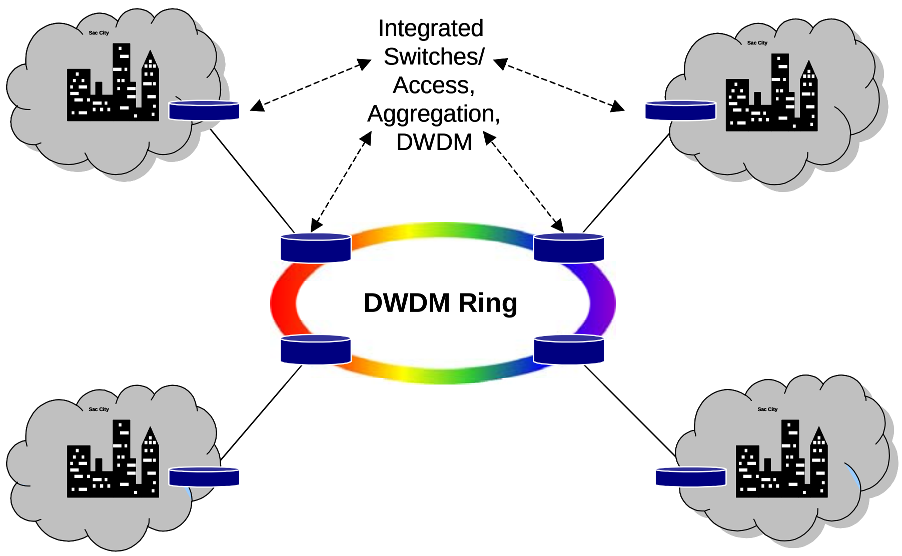

Figure 7: Campus network using single layer of networking (FMO). All nodes are shown using one color since they are fully integrated and belong to one specific networking layer.

Table 2 summarizes the different cost elements of a campus networks and shows the performance of PMO and FMO modes on CapEx, OpEx, or both. By quickly looking at the table, we can see how huge cost savings can be achieved when integration is efficiently exploited. This is true for all domains of networking, but is articulately necessary in campus where budget and cost constraints are the most stringent among all other applications.

Cost Elements (CapEx/OpEx)	PMO	FMO
Price (CapEx)	High	Low
Platform Size/Power (OpEX)	Large	Small
Transport Integration (OpEX)	Low	High
Functional Integration (OpEx)	Low	High
Management (CapEx/OpEx)	Hard	Simple
Capacity Flexibility (CapEx/OpEx)	Low	High

Table 2: Comparison of campus network mode of networking.

Summary

This white paper has described various approached to creating a Campus network. Solutions have been focused on packet transport, in particular Ethernet, because it is believed that with the advances experienced in the last 5 years, packet-based networks are much more flexible and cost-effective than TDM implementations. Compared to PMO-based campus network, it discussed how FMO-based campus network achieves superior performance gain and cost savings. Thanks to integration, integration, and integration.