



2900 West 10th Street
Sioux Falls, SD 57104
605.334.7185
605.334.4782 - Fax
1.800.247.1442 - Toll Free
www.sdncommunications.com



profitability.

A graphic of a paper airplane made of US dollar bills is shown flying upwards and to the right, with a green line trailing behind it, symbolizing growth and profitability.

Introduction

SDN offers a comprehensive MPLS network encompassing both layer 2 and layer 3 services with end to end quality of service. SDN prides itself on the capabilities the MPLS network can offer to increase the client's productivity and network efficiencies. For the client to make an informed decision when choosing a network provider, the remainder of this document will explain SDN's MPLS network and its services.

Contents at a Glance

I.	Core MPLS Connectivity	Page 2
II.	Layer 2 VPN Services	Page 3
III.	Layer 3 VPN Services	Page 10
IV.	Quality of Service	Page 15
V.	Network Management	Page 17

I. Core MPLS Connectivity

The core of SDN's MPLS network consists of twenty-four routers located across the state of South Dakota, Iowa, Nebraska and planned deployments in Minnesota. These routers are owned and operated by SDN and its member companies. By locating multiple routers across SDN's footprint, it allows for provisioning circuits in the most cost effective and redundant manner. If the client wishes to minimize potential outages by the loss of a single SDN MPLS router, the client's circuits can be distributed across multiple SDN routers.

SDN's use of multiple MPLS routers also allows for a lower amount of latency by being able to provision circuits that are close to the client's location. SDN doesn't have to "back-haul" circuits to major metropolitan cities like Minneapolis and Omaha. By having these circuits stay local within a smaller geographic area, network response times are faster.

The routers are interconnected by using SDN's vast statewide fiber network with redundant links utilizing a failover technology called resilient packet ring (RPR). Through the use of redundant links and RPR, SDN is able to provide service in the event of a core link failure or fiber cut. In the event of a core link failure or fiber cut, RPR will switch to the alternate path within 50 milliseconds.

SDN's MPLS routers incorporate internal redundant capabilities. These capabilities include multiple DC power supplies and multiple power sources (A and B feeds). In addition these routers have redundant CPUs, switch fabrics, and the use of any and all redundant interfaces that are possible within the device.

The routers are located in hardened and secured facilities. These facilities offer the best environment in regards to temperature control and power service to ensure maximum uptime for these core devices. SDN's facilities are monitored for environment variables such as temperature and moisture. If these parameters fall outside of acceptable levels SDN's Network Operations Group is notified immediately. These locations also have batteries and generators to ensure the uninterrupted flow of power in the event the commercial power feed to the building is disrupted.

II. Layer 2 VPN Services

SDN is able to offer layer 2 VPN services via the MPLS network. Layer 2 VPNs are the traditional WAN circuits in addition to more current layer 2 services such as WAN Ethernet and interworking circuits.

The following layer 2 circuits are available:

- Point to Point Ethernet
- Transparent LAN Services
- 802.1q Ethernet Trunked Circuits
- Point to Point T1/DS3 Circuits
- Multilink Frame Relay (FRF.16)

- Interworking Circuits
 - Ethernet to Frame Relay
 - Ethernet to ATM

Point to Point Ethernet

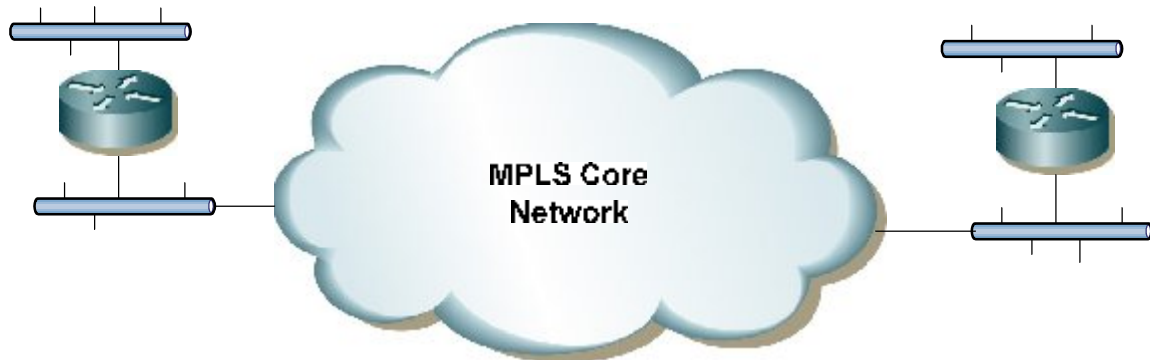
Through the use of SDN's regional MPLS network, SDN's Metro Ethernet network and SDN's member companies, it is possible to get a point to point Ethernet within SDN's large service area. Ethernet service availability is determined by the client's geographic location.

SDN offers multiple client hand-offs, such as copper 10/100/1000, multi-mode fiber and single-mode fiber connections. The bandwidth available on these point to point circuits start in the single megabits per second, and go all the way to full port speed.

SDN offers the use of Q-in-Q (802.1ad) services allowing the client to transport multiple VLANs across a single circuit and SDN is totally transparent to the client's terminating equipment. SDN is really just a long Ethernet cable.

Please refer to the following Figure 1 for a simple graphic displaying a point to point Ethernet circuit:

Figure 1 Point to Point Ethernet



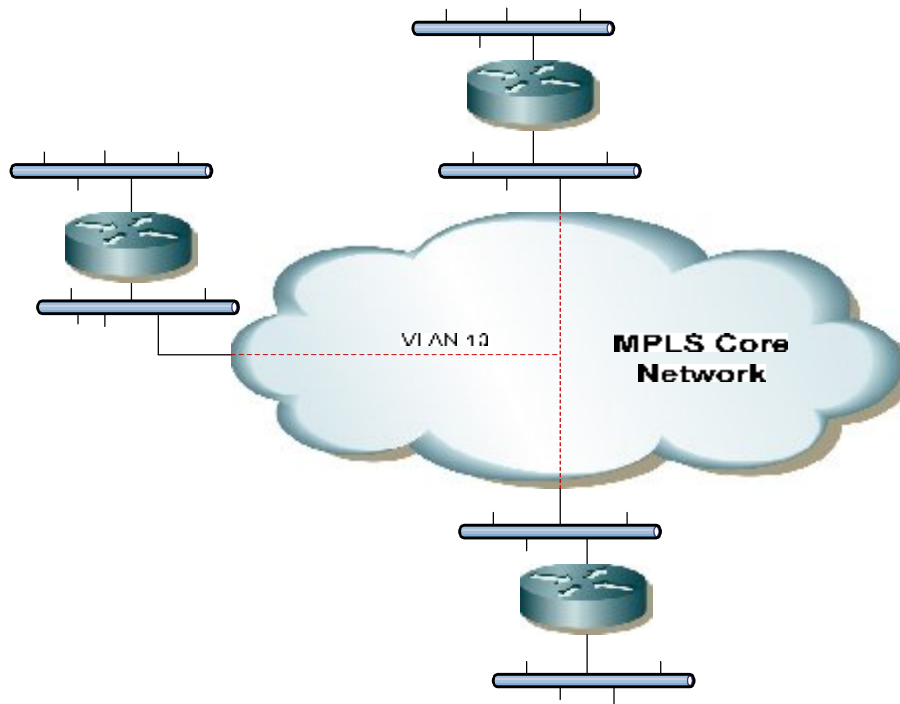
Transparent LAN Services

SDN also offers transparent LAN services which is sometimes referred to as virtual private LAN services (VPLS). This offering is simply a multipoint Ethernet service. This type of circuit is required when three or more sites need any to any connectivity, with a single VLAN amongst all the locations. Transparent LAN services acts as if all the client terminating devices are plugged into a “single switch”.

SDN offers multiple client hand-offs, such as copper 10/100/1000, multi-mode fiber and single-mode fiber connections. The bandwidth available on these point to point circuits start in the single megabits per second, and go all the way to full port speed. If the design dictates, each site could have a different amount of provisioned bandwidth.

Please refer to the following Figure 2 for a representation of transparent LAN services.

Figure 2 Transparent LAN Services



802.1q Ethernet Trunked Circuits

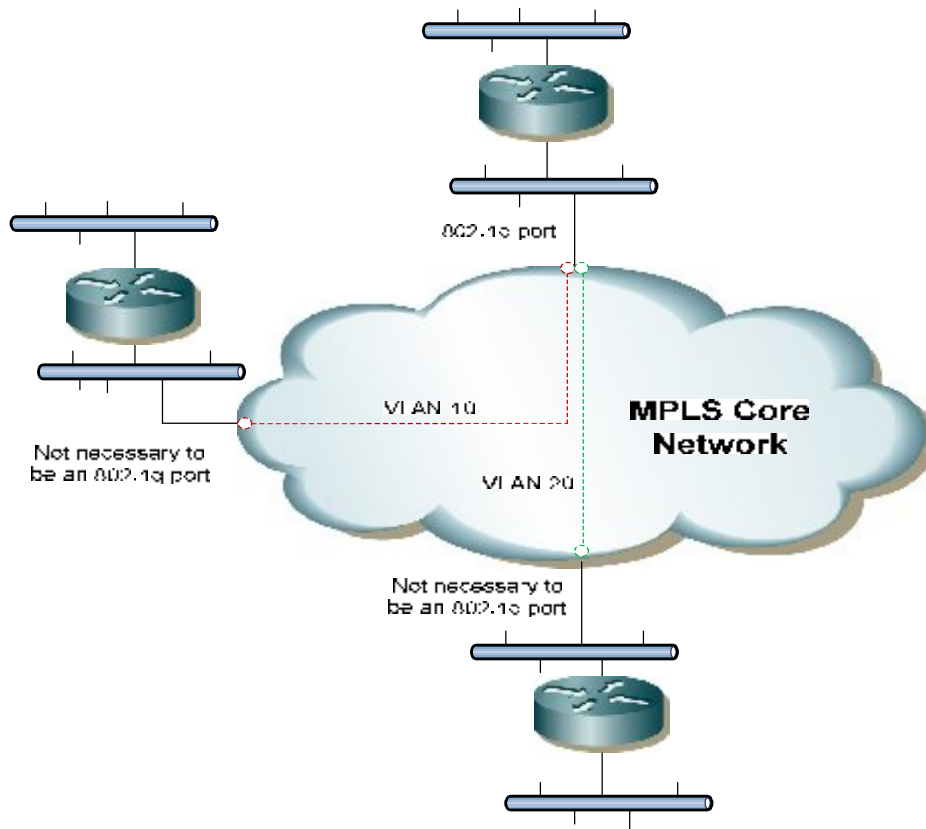
SDN offers 802.1q services if multiple VLANs are needed between two or more Ethernet locations.

SDN offers multiple client hand-offs, such as copper 10/100/1000, multi-mode fiber and single-mode fiber connections. The bandwidth available on these point to point circuits start in the single megabits per second, and go all the way to full port speed. If the design dictates, each site could have a different amount of provisioned bandwidth.

Q-in-Q (802.1ad) is available on SDN's transparent LAN services, but is recommended only if all the same VLANs terminate at all locations. Otherwise, unwanted VLAN traffic could traverse across the core MPLS network and be dropped off at a client's remote location that doesn't terminate a particular VLAN. If multiple and unique VLANs are needed at certain remote client locations, standard VLAN trunking (802.1q) is recommended. SDN will work with the client to determine VLAN numbers that don't cause conflicts.

Please refer to Figure 3 for a representation of 802.1q trunked circuits.

Figure 3 802.1q Ethernet Trunked Circuits

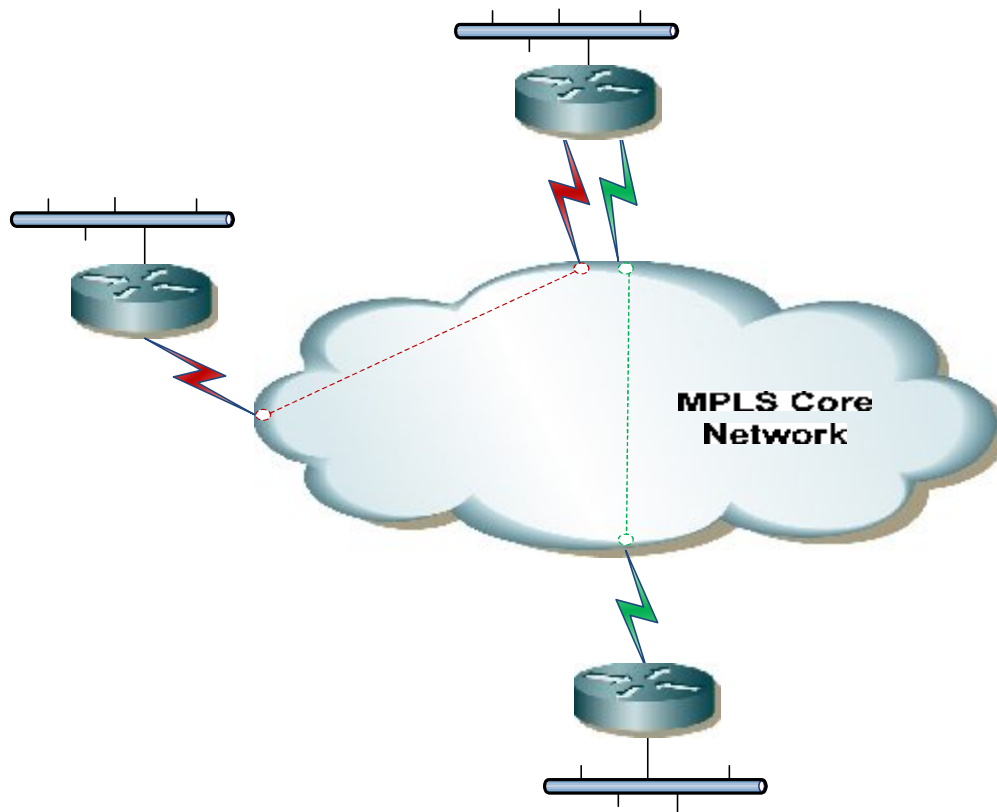


Point to Point T1/DS3 Circuits

SDN is capable of providing T1 and DS3 based circuits across the MPLS network as long as the client terminating devices supports "router-type" encapsulations of HDLC, PPP, frame-relay and ATM. With this service SDN is able to provide point to point, frame-relay and ATM layer 2 services.

Please refer to Figure 4 for a representation of point to point T1/DS3 circuits.

Figure 4 Point to Point T1/DS3 Circuits

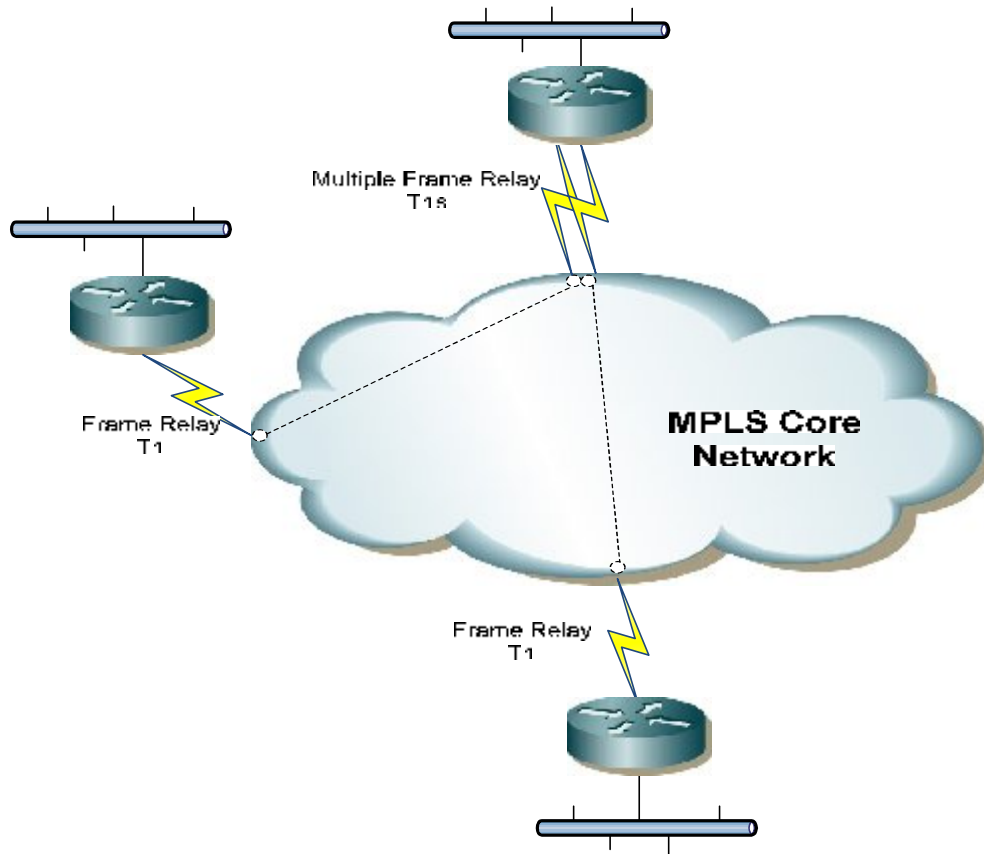


Multilink Frame Relay (FRF.16)

SDN offers multilink frame-relay which allows the bonding of multiple T1s at a client's location to increase the bandwidth beyond a single T1. This service is useful when a single T1s bandwidth isn't sufficient at a client's location.

Please refer to Figure 5 for a representation of a multilink frame-relay service.

Figure 5 Multilink Frame Relay (FRF.16)



Interworking Circuits

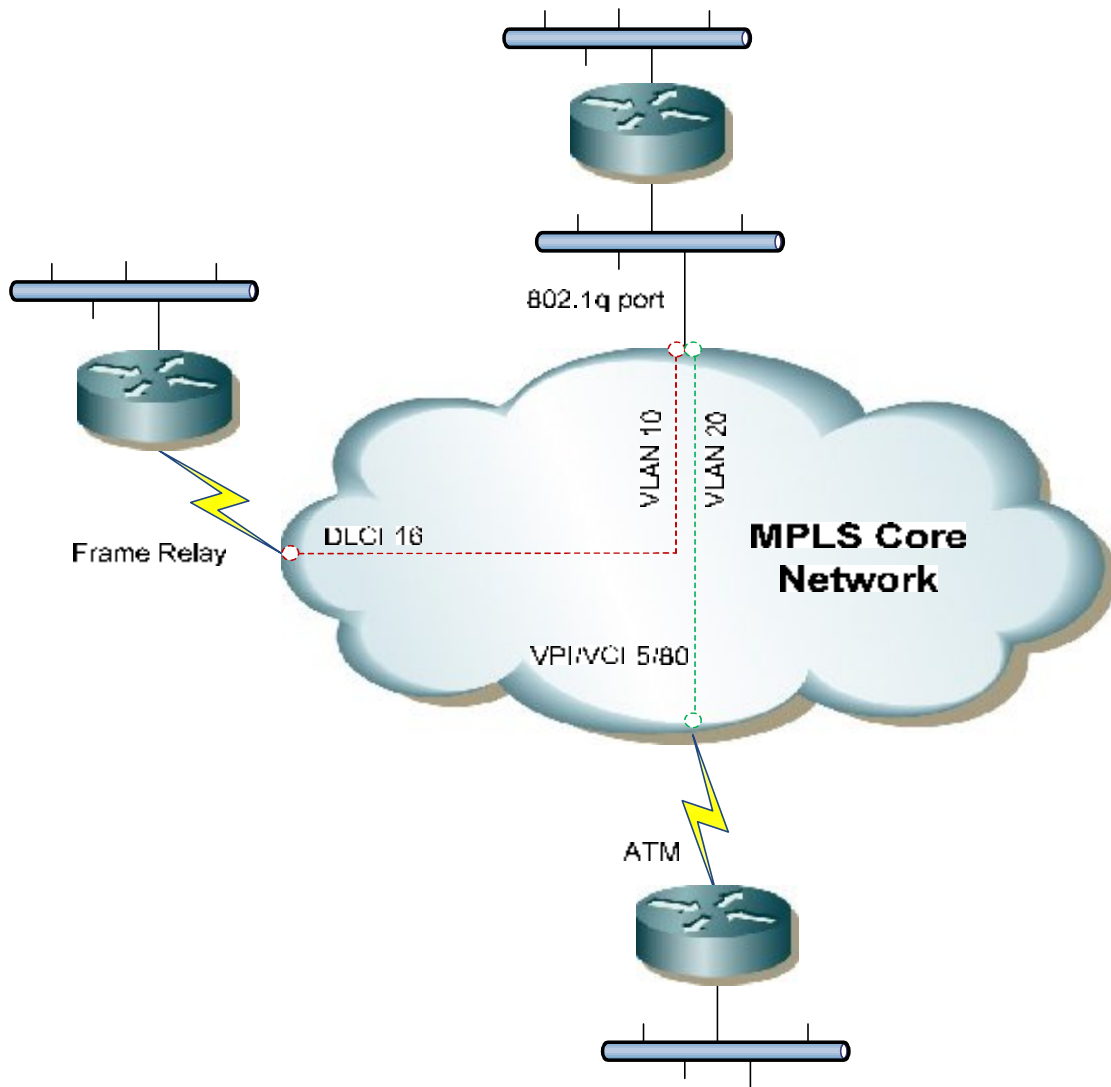
SDN has the capabilities to offer dissimilar layer 2 topologies on opposite ends of a connection and interwork these unlike topologies into an end to end connection. Interworking is simply the ability of SDN's MPLS network to "swap" one protocol type to another.

SDN can interwork (convert) an Ethernet VLAN to frame relay and interwork an Ethernet VLAN to ATM.

With these capabilities it allows the client to choose the best network transport that is available in a geographic region. It also allows the client to utilize legacy hardware as the need dictates.

Please refer to Figure 6 for a representation of an interworking service.

Figure 6 Interworking Circuits



III. Layer 3 VPN Services

SDN is able to offer layer 3 VPN services via the MPLS network. Layer 3 VPNs are where SDN becomes an active IP participant at layer 3. SDN appears to the client's routers as if the SDN routers are part of the client's private network. Actually, SDN is truly part of the client's private network. Through the use of Virtual Routing Forwarding (VRF) technology, SDN is able to keep every client's network private and secure within their respective VRF.

Every client's routing table is kept separate and unique via the use of VRFs. SDN assigns the individual client's interfaces to their own VRF routing table, thus keeping the separation between different client networks.

The transport from the client's location to SDN's MPLS network can be achieved by all the transport technologies that have been previously discussed within this document.

Below is a summary of the available transport methods:

- Point to Point Ethernet
- 802.1q Ethernet Trunked Circuits
- Point to Point T1/DS3 Circuits
- Multilink PPP T1 Circuits
- Multilink Frame Relay (FRF.16)
- Frame Relay
- ATM

By SDN allowing such a wide variety of transport methods where geographically allowed, it gives the client the flexibility to choose the best transport based upon availability and budget. It also allows the client to use legacy hardware as the need dictates.

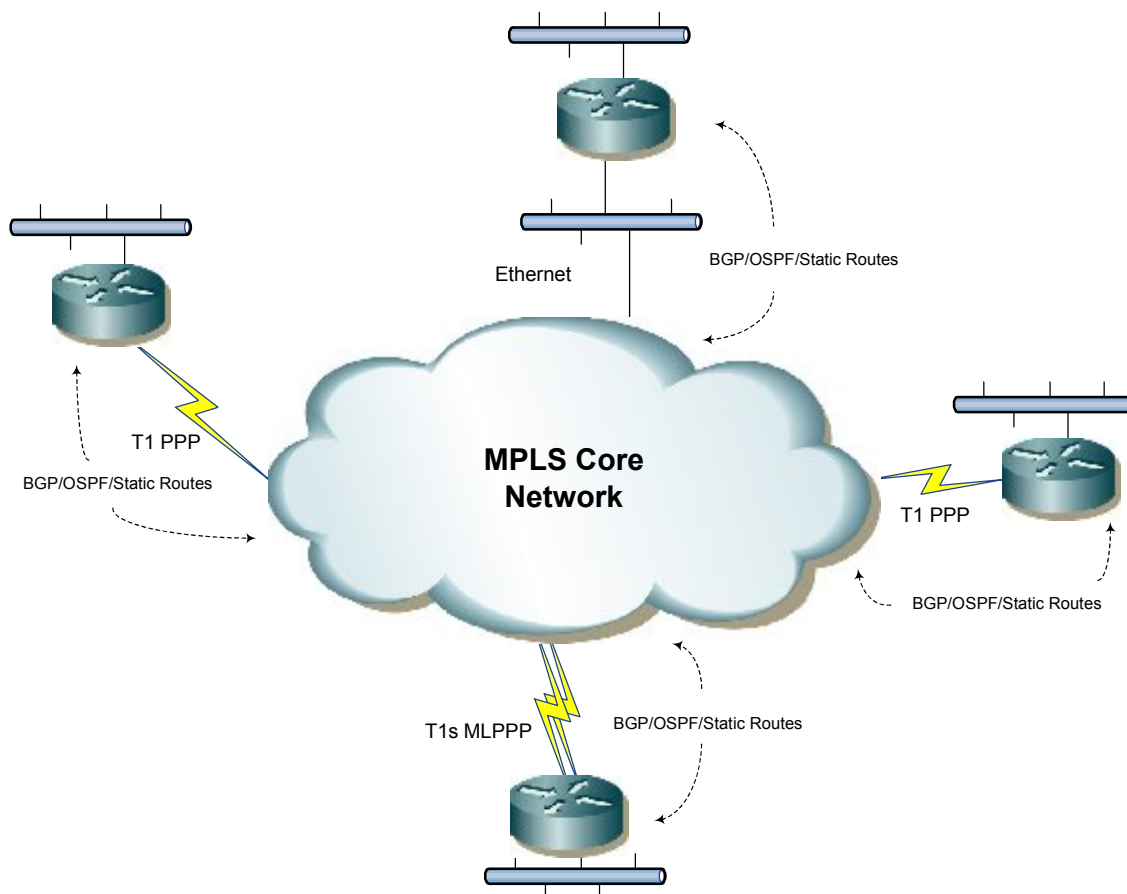
Layer 3 VPNs give many benefits to the client. One of the leading advantages is the inherent any-to-any connectivity amongst client locations. This ability is achieved by running a routing protocol between the client's routers and SDN. SDN prefers to run BGP as the routing protocol, but is more than willing to run OSPF if the client's router or needs dictate. SDN could also perform IP static routes, but due to the management and lack of flexibility this option is not advised.

The below gives a complete list of advantages that a Layer 3 VPN offers:

- Inherent any-to-any connectivity
- Ability to easily deploy a disaster recovery site
- End-to-end QoS capabilities
- Layer 2 agnostic for connectivity to MPLS core
- End to end QoS if point to point circuits are utilized
- Redundant failover capabilities within the MPLS core

Please refer to Figure 7 for a representation of a Layer 3 VPN service.

Figure 7 Layer 3 VPN Services



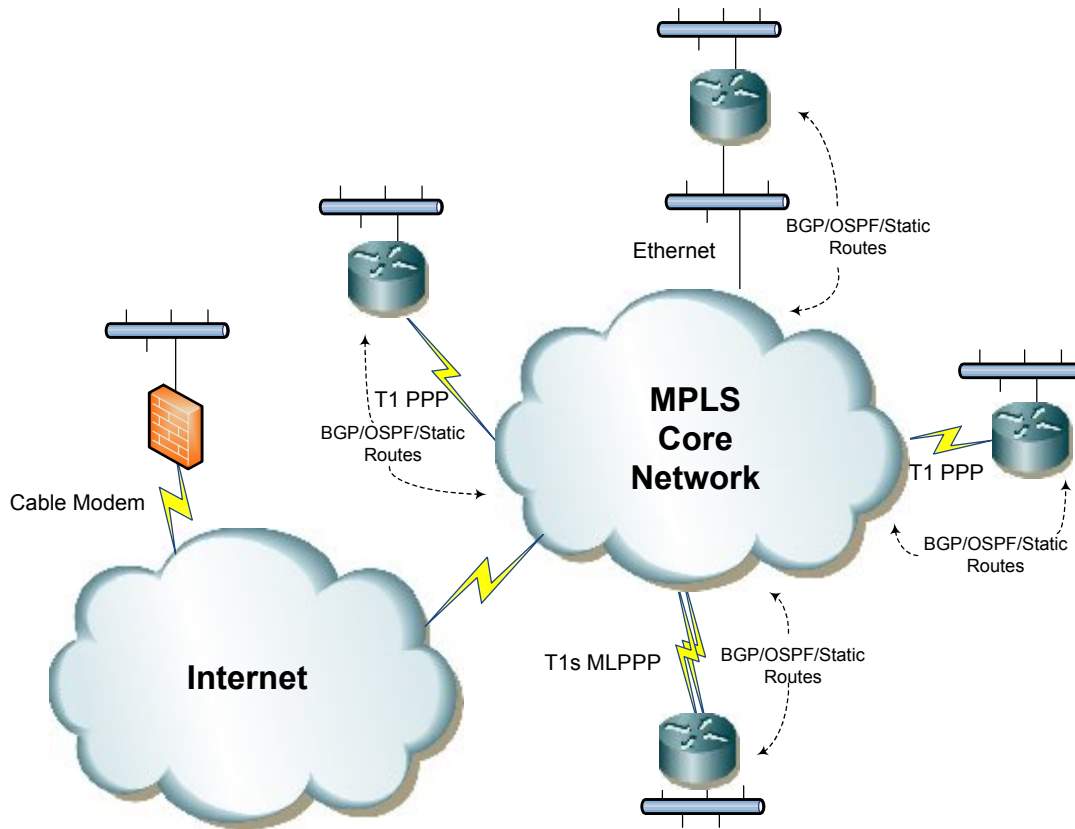
Broadband Remote Access Gateway (BRAG)

SDN offers the ability to connect an encrypted IPSEC tunnel that originates from a standard Internet connection into a client's existing private MPLS network. In this configuration the client purchases a standard Internet connection such as a cable modem or DSL from a local Internet Service Provider. This remote location also needs a firewall that has IPSEC capabilities, in addition to the local Internet Service Provider connection. The client's firewall then creates an IPSEC tunnel back to SDN's VPN concentrator. SDN then connects this Internet originated IPSEC VPN tunnel into the client's existing Layer 3 MPLS VPN. The net result is that the Internet remote site appears to the other client's MPLS sites as if it is a "private" type of connection. Through the use of the previously discussed VRF technology and IPSEC, this BRAG connection is completely secure.

The client should choose this type of connection based upon the type of applications and reliability that is required at the remote site. If real time applications such as voice and video are being used, a BRAG connection would not be advised due to the increased latency, increased router hop, and lack of quality of service that is inherent with a BRAG connection. If maximum reliability is required at the remote location a BRAG connection might not be the right choice. In these situations a private type of transport (I.E... T1, Ethernet) should be chosen over BRAG. However, if the fit is correct a BRAG connection can be a very cost effective solution for interconnectivity.

Please refer to Figure 8 for a representation of a BRAG Layer 3 VPN service.

Figure 8 Broadband Remote Access Gateway (BRAG)



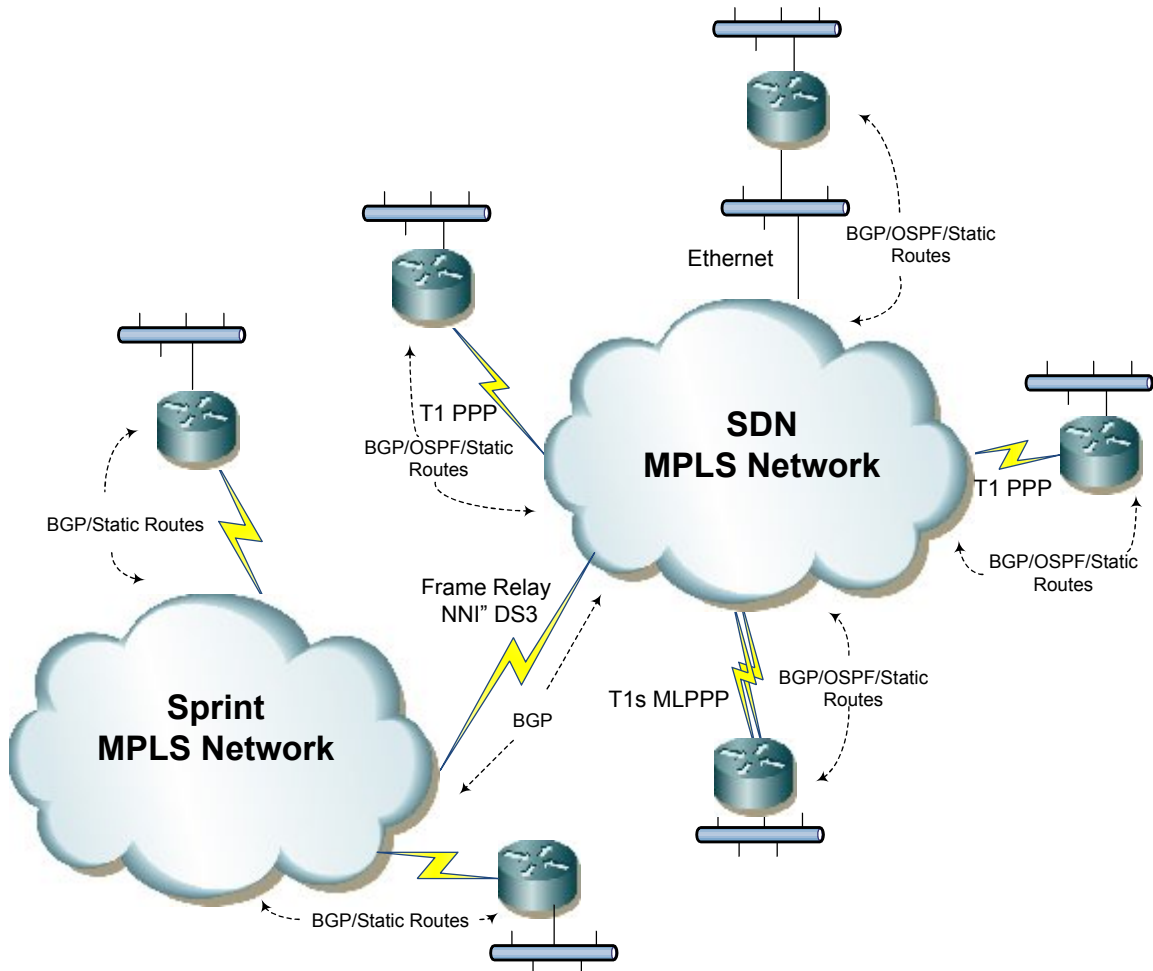
Layer 3 VPN Interconnect to Sprint's MPLS Layer 3 VPN

SDN has a network interconnect into Sprint's MPLS network. This allows all the advantages that have been previously discussed about Layer 3 VPNs, with the additional footprint that Sprint offers outside of SDN's normal service area. This is advantageous if the client has sites that are outside of SDN's region that would normally be cost prohibitive to interconnect. This option allows all sites, no matter if they are on Sprint's or SDN's network to be seen as one cohesive network.

It must be noted that the Sprint Layer 3 VPN sites only support BGP and static routes. OSPF is not an option for the Sprint Layer 3 VPN locations.

Please refer to Figure 9 for a representation of SDN's interconnect into Sprint's Layer 3 VPN network.

Figure 9 Interconnect between SDN and Sprint's Layer 3 VPN Network



IV. Quality of Service (QoS)

SDN's MPLS network offers end-to-end quality of service (QoS) capabilities. The charge for this service is in 1 megabit increments. QoS is activated on an individual circuit level. QoS is only active during times of congestion on the circuit.

SDN offers 3 queues; Real Time, Mission Critical and Best Effort. SDN will need to know from the customer how the traffic is being marked. The customer markings can be DSCP and/or IP Precedence. SDN will honor these markings and place the traffic into the appropriate queue. SDN collaborates with the customer to determine these markings and what traffic type gets placed into the corresponding queue. SDN also works with the customer on determining the size of each queue.

The amount of bandwidth purchased for QoS is distributed amongst the Real Time and Mission Critical queues and the remaining circuit's bandwidth is allocated to the Best Effort queue. For example, if a 10 megabit Ethernet circuit is purchased with 1 megabit of QoS traffic, the 1 megabit of QoS can be evenly dispersed with 500 kilobits for Real Time and 500 kilobits to Mission Critical, or any combination up to the purchased value. In this previous example the entire 1 megabit could be allocated to the Real Time queue. The remaining 9 megabit (non-QoS purchased bandwidth) is automatically allocated to the Best Effort queue.

The Real Time queue is a strict priority queue. When this queue is active it will be serviced until the queue is completely empty. Once the Real Time queue is empty the remaining two queues will be serviced. Due to the Real Time queue having a higher precedence and being serviced until it is completely empty, it is generally used for time sensitive applications like voice and video. This queue has a "hard ceiling", meaning when this queue is active it cannot take available bandwidth from the remaining two queues. While this queue is active and if the customer's router attempts to send more bandwidth than what is currently allocated, the excessive bandwidth is discarded. For example, if the size of this queue (hard ceiling) is set at 500 kilobits and the network needs to send 600 kilobits of real time data, the excess of 100 kilobits is completely discarded.

The Mission Critical queue is a class based queue. A class based queue allocates a specific amount of bandwidth per the agreed upon markings. During times of congestion traffic that meets the agreed upon markings are guaranteed this minimum amount of bandwidth. The Mission Critical queue can use available bandwidth from the Real Time and Best Effort queues, thus it is possible this

queue can transmit above the minimum defined value. For example, if 500 kilobits are allocated to the Real Time queue and 500 kilobits to the Mission Critical queue and there currently isn't any traffic in the Real Time queue, the Mission Critical queue can use the entire 1 megabit of QoS purchased bandwidth. In this example the Mission Critical queue can also take from the Best Effort queue if excessive bandwidth exists. However, traffic taken from the Best Effort queue it isn't guaranteed a specific amount of bandwidth. Only traffic within the Real Time and Mission Critical queues are guaranteed. Excessive bandwidth taken from the Best Effort queue will not be discarded if the bandwidth is available, it just won't be guaranteed.

The Best Effort queue treats all data allocated to this queue the same. The queue is a "catch all" for traffic that doesn't adhere to the Real Time and Mission Critical markings. The customer should ensure the Best Effort queue is large enough to provide service to applications that aren't assigned to the Real Time and Mission Critical queues.

SDN doesn't mark-down traffic that exceeds the specified queue sizes. In the event of excessive traffic in the Real Time queue it is completely discarded. In the situation of exceeding the traffic size of the Mission Critical queue, the Mission Critical queue can "steal" bandwidth from the other queues if it exists. If no free bandwidth is available from the other queues, the Mission Critical queue will drop any bandwidth needs that exceed its specified value. Due to these reasons it is important that the sizes are chosen correctly and periodically monitored by the customer for dropped packets within the queues.

Depending upon the MPLS circuit type that the customer purchases QoS is handled differently. If the customer purchases a layer 3 VPN, QoS is very granular. It is granular down to the individual IP flow. With a layer 3 VPN and the corresponding DSCP and/or IP Precedence markings, any packet that is tagged with the agreed upon markings will be treated independently. This allows the customer to give preference down to an application level, or for that matter down to an individual IP address. If a layer 2 VPN is purchased SDN can only give preferential treatment to the Ethernet VLAN or Frame Relay/ATM private virtual circuit (PVC). With a layer 2 VPN, SDN is unable to give preferential treatment down to an individual IP flow. However, multiple layer 2 circuits (VLAN/PVCs) can be provisioned on the same physical circuit and preference can be given to one VLAN or PVC versus another.

V. Management

SDN manages and monitors the core MPLS network 365 days a year, 24 hours a day. This is to ensure maximum uptime and to be able to proactively expand the core network as the needs arise. In addition to the internal managing that SDN does for its own network, SDN will give web portal access to clients who purchase a Layer 3 VPN at no additional charge. This web portal access will allow the client to see graphically how much each circuit is utilized from a bandwidth perspective. The client simply logs into a secure web portal utilizing any web browser. From this web browser the client can run "ad hoc" graphic reports to see what the total utilization was for a specific timeframe.

If additional management needs are needed, SDN does offer a complete suite of management capabilities at an additional charge. This service is provided through the Network Surveillance Center (NSC). The NSC can provide 24x7 monitoring so the client will be alerted when there is a failure on the client's network. Very detailed reporting can be provided for circuit errors, networking equipment errors/failures and server errors/failures. The NSC can also provide security services for firewalls and detection and prevention of network attacks/intrusions. The complete realm of the NSC services is outside of this document. If there is interest in the NSC services, SDN would be more than willing to discuss these capabilities in detail.