Open Access Technologies and MPLS-VPNs

The SCTE Cable-Tec Expo, June, 2002.
Presented by:
Joel T. McKelvey, Technical Marketing Engineer and
Cable Communications Specialist
Cisco Systems, Inc.

Abstract:

Open Access, the opening of cable IP networks to third-party ISPs, is of increasing concern among MSOs. In some countries and regions legislation exists mandating Open Access. Business models are being developed which indicate Open Access may supply new revenue streams to the MSO. Several technologies exist to suppy Open Access across the MSO network.

Technological requirements for Open Access include traffic identification, marking, and transport. Routing considerations must be taken into account, as well as QoS, security, caching, provisioning, and management. Particularly difficult issues arise for the MSO with regards to demarcation of responsibility for support and customer service, achieving the technological knowledge to deploy Open Access, and changes to the MSO's core network.

Some of the technologies available for Open Access are tunneling and VPN protocols. IP-Sec VPNs, MPLS-VPNs, Policy Based Routing, and L2TPv3 tunneling are all possible solutions to the challenge of Open Access. Each technology offers its own benefits and challenges and no one technology is totally effective. It is probable that MSOs will need to deploy more than one technology to adequately meet all their Open Access needs.

Introduction

Open Access (OA) describes the ability of a cable Multiple System Operator (MSO) to give access to its cable modem subscribers to multiple third party Internet Service Providers (ISPs). MSOs have traditionally either provided Internet service themselves or partnered with a single ISP. With the decline of @Home, a large cable-associated ISP in the United States, MSOs find themselves increasingly faced with the issue of providing Internet access using new partners and technologies.

While the legal battle over Open Access legislation continues in the US, other countries and regions have already begun to mandate the opening of cable IP networks. Brazil and Canada are among the countries with mandated Open Access at the time of this writing. US MSOs understand that by voluntarily opening their networks to third party ISPs they may be able to avoid costly and complicated legislation.

Legislative concerns aside, there are potentially important business reasons to implement one or more Open Access technologies on the cable IP network. Partnering with ISPs may improve cable modem penetration rates. Third party companies may be able to more quickly offer new services on the cable IP network. Partnering with ISPs can also help reduce subscriber support and management costs associated with Internet access subscribers.

The purpose of this paper is to review the technological requirements of Open Access technologies. It will also cover the ongoing operational and management issues of an Open Access environment. Finally, this paper will cover the most common Open Access technologies, discuss their status in the industry, and attempt to describe the scenarios in which each technology is best utilized. Included will be portions on IP-Sec VPN, MPLS-VPN, Policy Based Routing, and L2TP/UTI technologies.

Technological Requirements for Open Access

Regardless of the technology used to supply Open Access on the cable IP network, all OA architectures share some basic characteristics. Traffic traversing the MSO network must be identified as associated with a specific ISP and it must be transported between the subscriber and the ISP in question. The ideal open access solution would incorporate most if not all of the features addressed below.

Traffic Identification

Open Access environments by their very nature must include the ability to associate cable modem traffic with an ISP. Without this ability, it is impossible to

determine the manner in which traffic should be transported across the MSO's network. Traffic identification is based on a set of characteristics associated with the traffic. Usually, the mechanism involves the layer-two and layer-three information included in all IP packets. Although frequently called packet classification, this process is also called identification or differentiation.

Inherent in the DOCSIS 1.0 protocol is an identification process, which associates a single modem's traffic with a unique SID. SIDs are by definition associated with a DOCSIS MAC domain and thus a physical port on the CMTS. Many Open Access technologies use the DOCSIS 1.0 modem-SID-port association mechanism to identify traffic. One limitation of this method is that a single traffic stream can be associated with any given modem.

With DOCSIS 1.1 the ability to differentiate traffic streams from a single modem becomes increasingly possible. As Open Access technologies mature they are evolving to utilize the DOCSIS 1.1 traffic classification mechanisms as the way of identifying traffic streams. This involves the mapping of DOCSIS 1.1 Service Flow IDs (SFID) to VPNs or tunnels.

Some identification mechanisms do not utilize the CMTS for traffic differentiation. Some Open Access technologies, specifically Policy Based Routing (PBR), can be implemented at different areas within the MSO network and still supply Open Access. However, it is recognized that an optimal Open Access solution identifies traffic streams before the traffic enters the MSO network and therefore protects valuable MSO network resources from waste or misuse.

Traffic Marking

Once traffic is classified and associated with a specific ISP, it can be marked with an identifier to simplify subsequent classification. Each Open Access technology performs marking in a unique way. Some simpler technologies do not propagate the marking across the network at all.

Some complex Open Access technologies, such as MPLS-VPN, include a marker in every packet that identifies it as requiring a specific type of traffic handling. These mechanisms enable every device on the network to quickly and properly apply QoS and other behaviors based on the packet type.

Some tunneling technologies do not necessarily contain markers in the classic sense of the term. These types of technologies encapsulate packets within new packet headers and footers to allow for differential packet transport.

Traffic Transport

Transport is the act of moving differentiated and marked packets across the network. In the case of many Open Access technologies this is accomplished via well-established destination-based IP routing protocols. Some Open Access technologies use advanced mechanisms to improve the speed and latency characteristics of transport.

Routing Considerations

Frequently cable modem subscribers will generate traffic that is destined for another cable modem subscriber. With the increase of file sharing and Voice over IP (VoIP) on the Internet, modem-to-modem communication is increasing significantly. An efficient Open Access technology will allow modem-to-modem traffic to remain on the CMTS and will not necessitate the transport of modem-to-modem traffic back to the affiliated ISP. Traffic which remains within the CMTS does not consume valuable MSO network resources. However, for purposes of billing and management, it is important that the technology include functionality that allows for metering and troubleshooting of such traffic streams.

Virtual routing is a feature offered with some Open Access technologies that allows for total or partial route isolation between subscribers associated with different ISPs. Routers with virtual routing features hold multiple route tables, one for each ISP with attached subscribers. In the cable IP network, every CMTS holds a routing or forwarding table for each ISP. While it increases routing complexity, virtual routing allows modem-to-modem communication between two subscribers of the same ISP to remain on the DOCSIS portion of the network. Modem-to-modem communication between subscribers of two different ISPs may remain on the DOCSIS link or may be forwarded beyond the MSO network before returning.

Caching

Caching of network content, such as web content, is another way in which an MSO may reduce load on valuable network resources. An efficient Open Access technology should allow for the caching of content close to the subscriber to reduce traffic on the MSO core network and network interconnects.

QoS End-to-end

MSOs partnering with ISPs must be able to offer certain levels of service quality. ISPs will require Service Level Agreements (SLAs) guaranteeing throughput and latency across the MSO network. Open Access technologies must take into account the Quality of Service (QoS) needs of traffic streams and be able to utilize industry standard QoS mechanisms to achieve these goals. In the case of an MSO partnering with an ISP to offer interactive service such as VoIP or Video on Demand (VoD), QoS agreements across the IP network become vital.

Security Requirements

Subscribers and enterprise customers are becoming increasingly concerned about perceived security risks on the shared cable IP network infrastructure. Open Access technologies must not only assist in supplying a basic level of network and data security

to subscribers but must also support efforts to combat Theft-of-Service (ToS) and Denial-of-Service (DoS) attacks.

In an environment where multiple ISPs share a single network infrastructure it is also important to isolate traffic streams between ISPs. Traffic from one ISP should be unable to detect traffic from another ISP. ISPs must remain unable to learn routes to other ISPs unless they are deliberately and publicly advertised routes.

Provisioning

The complex Open Access environment necessitates an efficient provisioning solution capable of elegantly handling complex provisioning issues. Many ISPs will require control over the provisioning and management of subscriber hosts. Some Open Access technologies require specialized provisioning of cable modems to operate. It is important that Open Access technologies interoperate with all required cable modem and host provisioning systems.

Open Access technologies themselves are complex and often difficult to provision and manage across the many devices on the MSO network. An additional level of provisioning systems may be useful in the deployment and management of Open Access enabled CMTSs and other network devices.

Management and Troubleshooting

Operational expenses associated with an Open Access technology should be as low as possible. Provisioning, management, and troubleshooting tools should be readily available to help reduce these costs. Management tools must scale enormously to handle massive Open Access deployments if necessary.

Additional Challenges for Open Access

Beyond the technological requirements, an Open Access environment brings new challenges for the MSO. In addition to the financial aspects, there are a number of business model concerns that must be addressed. These are typified by a number of policies, which must be negotiated between the subscriber, MSO, and ISP.

Subscriber Management and Support

In an Open Access environment a subscriber frequently relies on both the MSO and an ISP for network access. As a result, issues of subscriber management and support arise. Some ISPs insist on full provisioning and control of the subscriber host systems and subsequently are responsible for all subscriber support. In other models, management, support, and provisioning are shared duties between the MSO and the ISP. It is vital that a support model be developed that will enable excellent service, support, and management to attract and retain subscribers.

Core Network Configurations

Established IP networks may need some minor modification to operate in an Open Access environment. In particular, some routers or other network components may require software or hardware upgrades. Before deploying Open Access an MSO must identify those areas of the network that will require additional investment.

Some Open Access technologies require configuration of core network elements. Ramifications of these configuration changes must be well understood. An ideal Open Access technology will require little or no change to the MSO core network configuration. However, in networks where overall QoS features are not enabled or in which basic IP routing is not enabled, Open Access technologies are likely to be less effective. These types of network configurations may be required, even when using the most simple of Open Access technologies.

Technological Readiness

It is difficult to attract and retain staff with a high level of networking expertise. MSOs may find it challenging to identify and hire the appropriate talent for deploying an Open Access solution. Technologies involved should therefore be as simple as possible and based on industry standards.

MSOs should be careful to purchase networking equipment from an experienced vendor. Vendors should be experts in the required Open Access technology and should have excellent customer support and consulting services departments in the case such services are required.

Open Access Technologies

Based on the considerations listed above, several technologies are currently being used or considered for Open Access. Among these are IP-Sec VPNs, MPLS-VPNs, Policy Based Routing, and L2TP/UTI tunneling. Each has its own benefits and challenges.

IP-Sec VPNs

IP-Sec is a point-to-point encryption and tunneling protocol. Packets entering a configured interface on an IP enabled device are encrypted using algorithms as secure as 3DES. Encrypted packet content is encapsulated into new packets with new headers. These IP-Sec packets are then routed using regular destination-based routing protocols to an endpoint where they are decrypted. Because packets are hidden between encryption and decryption, IP-Sec is called a tunneling protocol. Because IP-Sec is often used to transparently connect remote networks, IP-Sec tunnels are often called IP-Sec Virtual Private Networks (VPNs).

IP-Sec is widely deployed throughout the world, primarily as a means of allowing telecommuters to connect to enterprise networks. Several MSOs have deployed IP-Sec

enabled cable modems as a form of Open Access. In these cases, IP-Sec supplies secure connections across the MSO network between remote sites. IP-Sec is relatively easy to configure and secure cable modem configurations are usually managed by the enterprise and not the MSO. Several companies offer IP-Sec enabled Customer Premises Equipment (CPE) and at least two models of IP-Sec enabled cable modem are currently available. IP-Sec VPN configuration, management, and accounting software is available.

IP-Sec does not require any changes to the core MSO network configuration except for requiring pre-existing QoS configurations and other typical core routing configurations. Most IP-Sec implementations support QoS using the IP Type of Service (ToS) bit in the IP packet header. This ToS value can be propagated to the header of the encapsulating packet to ensure end-to-end QoS across the MSO network. The 3DES encryption available with IP-Sec is extremely difficult to compromise. IP-Sec is an excellent Open Access technology for small numbers of hosts connected across the MSO network in simple hub-and-spoke or meshed configurations.

Connecting large numbers of sites via IP-Sec may cause issues of scalability. IP-Sec encryption and decryption require a large amount of processing power at the tunnel endpoints. Because IP-Sec is a point-to-point protocol, a fully meshed topology between a large number of devices quickly becomes cumbersome with the number of required tunnels growing exponentially with the number of attached hosts. In a hub-and-spoke topology with many attached IP-Sec tunnels, the central IP-Sec aggregation device is easily overloaded. Some issues of demarcation can occur with an IP-Sec enabled cable modem managed by both the ISP (IP-Sec configuration) and the MSO (provisioning and troubleshooting). Also, IP-Sec is an Open Access technology that is unable to supply modem-to-modem communication without the configuration of a tunnel between the two modems. However, as long as the number of connected devices remains low, IP-Sec is one of the simplest Open Access technologies to configure and deploy.

Case Study: a small US municipality wished to connect several remote sites to a centralized location. These sites included multiple fire and police stations as well as other government and administrative buildings. The municipality already used a leased-line for Internet access, but required a method to connect and share the leased line between sites. Because of the nature of the attached sites, security needed to be exceptional. Because of the small scale of the subscriber operation, a simple and inexpensive solution was a must.

This municipality, in conjunction with a local cable operator, deployed IP-Sec enabled cable modems at remote sites. An IP-Sec aggregation device was deployed at the location with the leased line. All sites were connected and all traffic was routed through the centralized Internet connection. The municipality has experienced excellent results from their IP-Sec VPN configuration and is expanding services to other government offices.

MPLS-VPNs

Multi-Protocol Label Switching (MPLS) is an industry standard published by the Internet Engineering Task Force (IETF) and based on Cisco Systems tag switching technology. Many MSOs are using MPLS-VPNs in Open Access tests and trials. MPLS includes a single forwarding mechanism that supplies layer-two forwarding speeds with layer-three routing intelligence. MPLS includes a forwarding plane wherein traffic is quickly and efficiently forwarded based on packet labels, and a control plane used to identify label switch paths and supply necessary QoS guarantees. The MPLS standard includes provisions for traffic engineering, Class of Service parameters, throughput guarantees, resource reservations, differential routing, and VPNs. Using MPLS, an MSO can offer SLAs to multiple ISPs and monitor the status of ISP traffic to ensure the SLA is met.

Upon entering an MPLS enabled network a packet is sorted and labeled. This label is used to forward the packet through the network. Once the packet reaches the far network edge, the label is removed and the packet exits the network. This labeling process can be used to associate packets with specific ISPs. Each router in the MSO network, however, must have MPLS label switching enabled.

MPLS-VPN technology relies on a set of Virtual Routing and Forwarding tables (VRFs) configured on each MPLS-VPN edge router. These VRFs contain and isolate routing information for each connected VPN. Because routes can be individually permitted or denied propagation between VRFs, routing isolation can be completely managed by an administrator.

MPLS-VPNs are widely accepted as an extremely flexible and elegant solution to the many requirements of Open Access. Using VRFs, a virtual routing/forwarding environment is built for each ISP allowing route isolation and security. Traffic Engineering policies can ensure optimal traffic distribution and improve overall network performance. Class of Service (CoS) parameters enable the transport of interactive traffic such as VoIP. MPLS is a robust and powerful technology.

However, with multiple ISPs, multiple VPNs, multiple CMTSs, and even minor changes to core router configurations, MPLS-VPNs are undeniably complex to deploy. Of particular concern is the potential need to upgrade the software images on core routers to support the MPLS-VPN feature set. Overall management of the routing protocols involved for MPLS and the initially difficult configuration of each CMTS to support MPLS-VPNs are important gating factors in MSO deployment. Although vendors now offer software that significantly reduces the management burden for MPLS-VPN, the knowledge level required for deployment is often disconcerting.

Case Study: an MSO wished to deploy an Open Access solution to partner with a third-party ISP as well as to connect telecommuters to enterprise networks. Initial deployment was relatively painless because the MSO network was already configured with an OSPF routing overlay. Subsequent MPLS-VPN routing requirements (BGPv4

overlay on the CMTS and edge routers) went relatively smoothly. However, configuring multiple VRF on each device as well as determining which routes should be shared between all VPNs and which should be isolated was complex. Management software helped alleviate this issue, but a degree of operational overhead remains as the network management staff comes up to speed on the new technologies involved.

This MSO currently has over 80,000 subscribers attached via MPLS-VPNs with approximately 6,000 additional customers attaching to the MPLS network each month. At the time of this writing no issues with MPLS scaling have been identified.

Policy Based Routing

Policy Based Routing (PBR) is a mechanism used to differentially forward traffic on a single router. PBR consists of a number of easily configured routing rules. Using PBR, a router will forward traffic out specific ports based on values in the packet headers. These values can include source IP address, source port, destination port, source MAC address, and others. Because PBR forwards sorted traffic out specific ports, it is best deployed on the router directly connected to peering ISPs. Traffic from cable modems traverses the MSO network until it reaches the edge router where it is identified by a set of packet header values and forwarded to the appropriate ISP. Packets destined for a specific cable modem are received by the edge router and forwarded across the MSO network to the appropriate modem. PBR is in use by many MSOs as an early way to supply Open Access to a limited number of ISPs.

PBR is also useful in conjunction with tunneling or VPN technologies as a method for differentiating traffic and forwarding it into the appropriate tunnel or VPN.

Because PBR is a mechanism for traffic sorting and forwarding that is localized to a single router, it has difficulty scaling in a large Open Access deployment. With the potential for many attached ISPs, the amount of configured PBR rules increases at the same rate as the number of ISPs. Issues with router redundancy also arise because PBR is configured on a single device. If a redundant router is configured, a second PBR configuration must also be configured and a redundant set of connections between all ISPs must also be created. Monitoring modem-to-modem traffic or even traffic between CMTSs is a challenge with PBR as in some configurations the traffic never leaves the DOCSIS network.

PBR is, however, easy to understand and simple to deploy. It is primarily because of its operational simplicity that it is used for Open Access at this time.

Case Study: PBR was deployed in a trial in conjunction with MPLS-VPN technology. In the trial architecture, multiple CMTSs were aggregated onto a layer-three aware switch and the switch was connected to an MPLS-enabled router. The switch supported PBR functionality and was intended to allow for multi-vendor CMTS aggregation.

Traffic entering the switch was policy-based routed to a specific port. That port was directly connected to an MPLS port on the router. Traffic was effectively sorted using PBR into MPLS-VPNs.

This architecture was determined to be rather expensive due to the need for a switch and a router with full layer-three functionality. More efficient means were attempted to provide sorting and transport such as PBR on the remote network edge and MPLS-VPNs initiated at the CMTS.

L2TPv3/UTI

Layer-two Tunneling Protocol (L2TP) is an extension to the PPP protocol based on features from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco Systems Layer-two Fowarding (L2F). L2TP allows for the creation of tunnels between two endpoints and enables VPN-like functionality. An emerging version, L2TPv3 may also combine Cisco's Universal Transport Interface (UTI) to provide a more robust VPN architecture.

Vendors intend L2TPv3 with UTI as an intermediate step between simpler tunneling architectures and a full MPLS-VPN architecture. However, developments in L2TP may make it robust enough to supplant MPLS-VPN as the final goal of Open Access deployments. Nevertheless, in its current state of refinement it appears to have the same set of scaling issues as IP-Sec tunneling. As L2TPv3 develops there is sure to be more interest in this standard for use in Open Access.

Conclusions

There is no simple answer to the question of Open Access – several technologies exist and each has its on benefits and challenges. Because of this, it may be true that an MSO will deploy more than one technology on the cable IP network. One technology may simply be more appropriate for certain uses than another. It is important that each technology, as well as technologies which are in their infancies, be evaluated thoroughly. Testing and trials are necessary in every event and vendors and MSOs must work together to develop and deploy these Open Access technologies.

As new or exiting as these Open Access technologies may be, however, it appears that the technological challenges for Open Access are relatively well understood. As vendors race to implement flexible and powerful features to benefit the MSO, business ramifications of Open Access remain unanswered. Business models simply don't exist to explain the potential benefits of Open Access to the MSO. Due to the relatively recent push towards Open Access, business case studies remain rare, too. It remains uncertain if ISPs will even benefit from the opening of the cable IP network in any measurable way.

While the future of the technologies seems relatively clear, the future of Open Access is significantly less so.

References

Almquist, P. Type of Service in the Internet Protocol Suite (RFC 1349).

Cable Television Laboratories, Inc. (CableLabs). Data Over Cable Services Interface Specifications (DOCSIS) -- http://www.cablelabs.com

Configuring Head-End Broadband Access Router Features – Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/mcprt3/mcdhubr.htm

Managed Broadband Access Using MPLS-VPNs for Cable MSOs – Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/cablsol/mplscabl.htm

Pepelnjak, Ivan, Guichard, Jim. MPLS and VPN Architectures. Cisco Press. Indianapolis, 2001.

Policy Based Routing -- Cisco Systems, Inc. http://www.cisco.com/warp/public/cc/techno/protocol/tech/plicy_wp.htm

Universal Transport Interface (UTI) -- Cisco Systems, Inc. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s18/uti.htm

Vegesna, Srinivas. IP Quality of Service. Cisco Press, Indianapolis, 2001.