ARRIS

TECHNICAL PAPER

Implementing Layer 2 Virtual Private Network (L2VPN) Over DOCSIS®

With the ARRIS C3™ Cable Modem Termination System (CMTS)

Re-Written March 22, 2007

By: Tom Dadds, Richard Rommes

The ARRIS C3 Cable Modem Termination System (CMTS) enables advanced Layer 2 Virtual Private Network (VPN) services in DOCSIS cable networks worldwide. With support for secure, high performance Layer 2 VPNs, the ARRIS C3 CMTS gives the cable operator compelling market advantages over the Local Exchange Carrier (LEC) offering Transparent LAN Services (TLS) to the same customer base. The ARRIS C3 CMTS is currently deployed by Top MSOs in networks with complete traffic separation between residential and business customers.

Layer 2 VPN Model

The C3 CMTS implements a Layer 2 VPN model that makes it simpler to provision and maintain secure data services. Customers can be provided with one or multiple VPNs per facility. This combined with point-to-point and multipoint-to-multipoint connectivity gives the cable operator a service offering that is in high demand by business, government and educational institutions.

Layer 2 VPNs are established by the ARRIS C3 CMTS to segregate different classes of traffic. Traffic segregation may be based on the type of traffic and defined groups of users. A user group can be provided with their own virtual network for secure and private communication within the group. The appropriate Quality of Service (QoS) is provisioned for each VPN to comply with service level agreements.

Layer 2 VPNs make it easier for an enterprise to communicate across a network without the need to coordinate address space. Communication is done securely over the CMTS because each VPN can be individually encrypted.

The Layer 2 VPNs provided by the ARRIS C3 CMTS are based on the industry-standard IEEE 802.1Q VLAN protocol. The Ethernet packet structure supporting 802.1Q frame tagging is shown in Figure 1. In the “EtherType” field, 8100 indicates an 802.1Q tag in the extended Ethernet header. The header contains a 12-bit field for VLAN ID which allows up to 4,095 unique VLANs in the operator’s network.

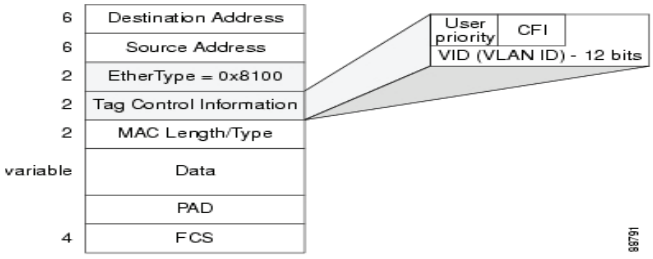

Figure 1 Packet Structure Supporting 802.1Q

The Layer 2 VPN approach is noteworthy for its ability to support non-IP protocols, which simplifies networking for enterprise customers the operator may wish to serve. The operator can also more easily meet requirements to implement franchise-dictated networks. Municipalities that issue cable franchises typically require the operator to provide an Ethernet, Layer 2 or fiber-based network as part of the franchise agreement. Layer 2 VPNs are well suited to fulfill these requirements.

Layer 2 VPN Configuration and Provisioning

The ARRIS C3 CMTS’s flexible design actually implements multiple 802.1Q-based configuration options: CPE-based Q-tagging, ARRIS C3 CMTS CLI-provisioned tagging and Vender-Specific-Encoding (VSE) based tagging via cable modem configuration files. Each implementation has its uses; however, the most common customer deployment method involves VSE-tagging via the cable modem configuration file.

VSE tagging eliminates the need to provision each member of a VLAN ID group and provides secure, private network functionality by configuring multicast encryption on the cable side sub-interface.

With VSE encoding, subscriber devices connected to the ARRIS C3 CMTS are assigned to a particular VLAN based on a vendor-specific Type Length Value (TLV) that is placed in the configuration file for that particular cable modem or group of cable modems (see Figure 2). The Value of the TLV identifies the device as a member of a particular VLAN.

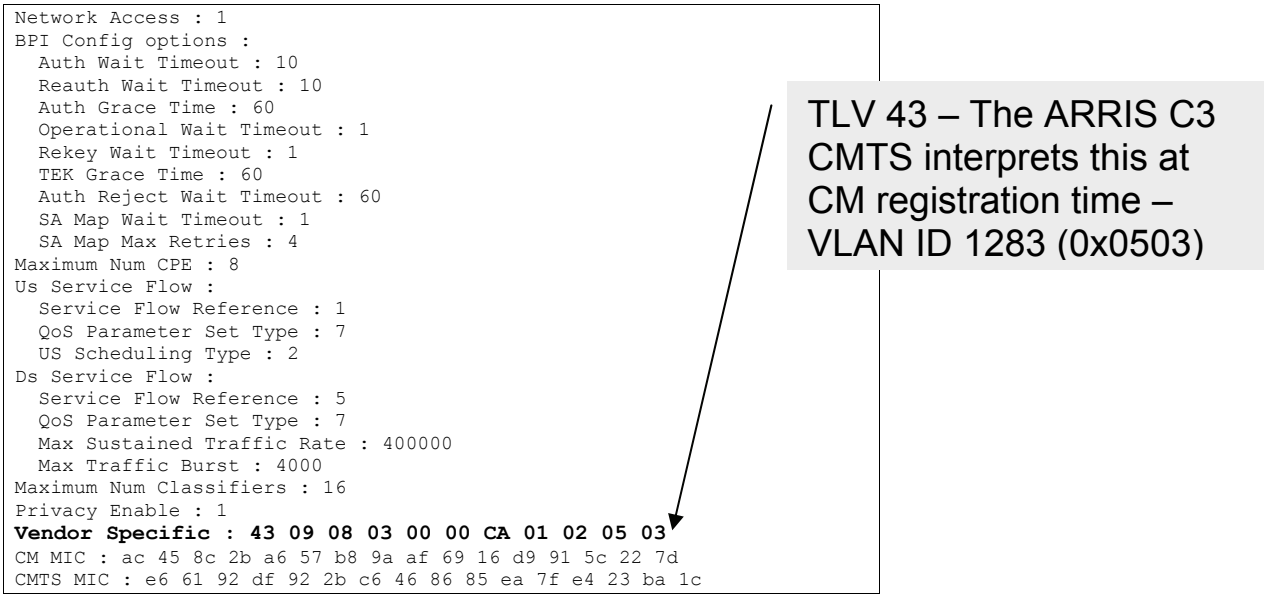

Figure 2 Cable Modem Configuration File Containing a VLAN ID

While the cable modem itself actually ignores the Vendor Specific Encoded 43 syntax, configuration files containing VLAN IDs allow cable modems to self-provision on a particular VLAN with the ARRIS C3 CMTS. Self-provisioning based on TLVs gives the MSO a major advantage. This technique parallels the normal configuration and provisioning process that most MSOs use now. Assignment to the appropriate VLAN is fast, secure and automatic. Once assigned to a VLAN, the traffic frames generated by individual members of a VLAN are tagged with the appropriate VLAN ID by the ARRIS C3 CMTS prior to exiting the Ethernet WAN interface.

As part of the general cable modem registration process, the cable modem tells the ARRIS C3 CMTS to automatically add this modem to a particular VLAN. The addition of a cable modem to a VLAN does not require extra action by a technician at the ARRIS C3 CMTS itself and does not require client-based software. This eliminates the provisioning hassles associated with having to know which ARRIS C3 CMTS will support which of the many cable modem endpoints. The cable modem can be moved from ARRIS C3 CMTS to ARRIS C3 CMTS with no need to re-provision. The cable modem simply needs access to the configuration file with the appropriate TLV and VLAN ID.

In addition to static configuration files, new provisioning systems allow for "group" configuration files, which are files that share common criteria or profile. A set of cable modems belonging to "Company A" can be defined by a group called “Companya”. This group will associate the MAC addresses of the respective cable modems with the proper TLV for the VLAN ID and auto-populate the TLV into that file on a per group basis. Subsequently, all of the modems in the group will boot using the same TLV even though there is only one file, thus simplifying provisioning. No matter where the modems in the group are moved, the VLANs will always be properly provisioned at the CMTS level.

It is important to note that the configuration file VSE technique to assign cable modems to existing VLANs involves no CLI command entry at the CMTS. Once a VLAN is established on the CMTS, cable modems are assigned to that VLAN by simply giving them the correct configuration file.

Some MSOs choose to have cable modem configuration files under centralized control at their headquarters location. In such circumstances, where configuration file editing is not possible or is difficult to do at the regional/local system level, there is a CLI command to map a particular modem's CPE traffic to a VLAN. The format for this command is:

[no] cable modem A.B.C vpn VLAN-TAG

When a cable modem with MAC address A.B.C registers, the effect of the above command is the same as if there had been a VSE tag of value VLAN-TAG in the cable modem's configuration file. All CPEs behind the cable modem with MAC address A.B.C will be mapped to a VLAN that has an ID with value VLAN-TAG.

Logical Sub-Interfaces and Bridge Groups

All subscriber devices are physically connected to the RF interface of the ARRIS C3 CMTS. The RF physical interface is in Slot 1 of the ARRIS C3 CMTS as shown in Figure 3. Slot 0 contains two physical Fast/Gigabit Ethernet interfaces.

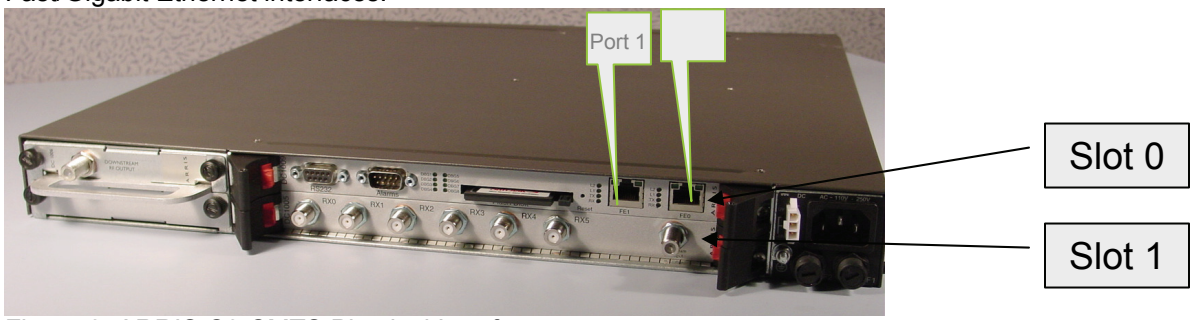

Figure 3 ARRIS C3 CMTS Physical Interfaces

Each of the three physical interfaces (one RF and two Ethernet) can be divided into up to 250 logical sub-interfaces. Nomenclature for sub-interfaces is "Slot/Port.Sub Interface." Traffic on the same physical interface can be treated differently depending on the sub-interface to which it is assigned.

When configured for Layer 2 operation, the logical sub-interfaces on the ARRIS C3 CMTS are then provisioned into Bridge Groups as shown in Figure 4. The ARRIS C3 CMTS supports up to 250 unique Bridge Groups. Each Bridge Group acts as a MAC layer bridge that is isolated from other Bridge Groups. An incoming packet is treated according to its respective sub-interface provisioning and then forwarded to its destination based upon the respective bridge-group assignment.

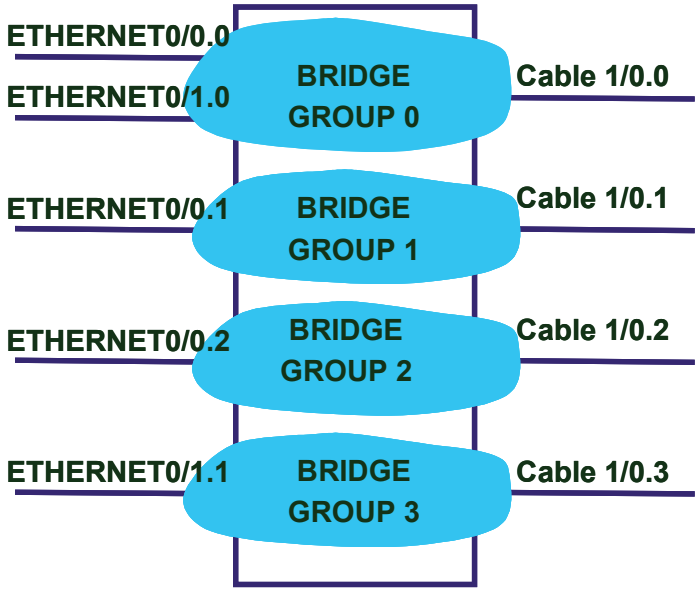

Figure 4 Sub-Interfaces Assigned to Bridge Groups

Traffic arriving at the ARRIS C3 CMTS on the RF upstream can be mapped to a cable sub-interface based on the cable modem MAC address and the VLAN ID contained in the configuration file for that cable modem at the time of provisioning. The traffic is then bridged to the Ethernet sub-interface contained within the same Bridge Group. The 802.1Q tagged Ethernet header with the respective VLAN ID is placed onto the packet by the ARRIS C3 CMTS prior to Ethernet egress.

Traffic arriving at the ARRIS C3 CMTS Ethernet ports may or may not have 802.1Q tags applied to it. This traffic is mapped to the cable side sub-interface based upon the arriving VLAN ID and respective MAC address.

Provisioning of sub-interfaces and bridge-groups is performed with the ARRIS C3 CMTS Command Line Interface (CLI). The example below shows provisioning of a cable sub-interface using a Vendor Specific Encoding (VSE) VLAN ID in a cable modem configuration file. The use of the key word “native” in this instance tells the ARRIS C3 CMTS that packets on the RF side of the interface should not be arriving or leaving the ARRIS C3 CMTS with Q-tags on them. The ARRIS C3 CMTS will in fact strip the Q-tags as they arrive on packets from the Ethernet side interface prior to transmitting them on the RF-side interface. Packets arriving on the RF side interface will show up without Q-Tags applied and the ARRIS C3 CMTS will insert the Q-Tags prior to exiting at the Ethernet sub-interface.

```
conf t
bridge 1

interface cable 1/0.1
      ! VSE tag of 1283 will map here
      encapsulation dot1q 1283 native
      bridge-group 1
    exit
exit
```

The next example shows provisioning of the Ethernet sub-interface with 802.1Q VLAN ID identified as part of the configuration. Note that the key word “native” is not used here as the ARRIS C3 CMTS is expecting to map incoming packets with the respective VLAN ID to the sub-interface and forward based

upon bridge-group association.

```
conf t
bridge 1

interface fastethernet 0/0.1
      ! VSE tag of 1283 will be added here
      encapsulation dot1q 1283
      bridge-group 1
    exit
exit
```

Double Tagging and Bridge Tunneling

Quite often, business subscribers will operate more than one VLAN on their internal network with CPE devices behind the cable modem generating their own VLAN tags. These VLAN tags must be preserved by the cable modem and the CMTS. Traffic with CPE-generated VLAN tags arriving to an RF-side sub-interface is bridged by the C3 CMTS to an Ethernet sub-interface where a second tag is applied before egress. In the reverse direction, ingress packets arriving on the network side may be double tagged with the outer tag being used to associate the packet with a logical Ethernet sub-interface. This outer tag is stripped off; the inner tag is retained, and packets with the inner tag are transmitted downstream. The command to enable/disable double tagging within a bridge group is:

[no] bridge {bridge-group #} double-tagged

When double tagging is used, bridge tunneling must be established between the RF side and Ethernet side of the C3 CMTS. With bridge tunneling enabled, packets with VLAN tags can arrive to and leave from the RF side of the C3 CMTS. Effectively, the “native” mode of operation is ignored allowing the inner tag in a double tagging scenario to be retained. Optionally, no bridge table learning is done. The available options are no source MAC learning on the RF side, Ethernet side or in the bridge table. The command to enable/disable bridge tunneling is:

[no] bridge {bridge-group #} tunnelling [no-learning | no-cable-learning | no-ethernet-learning]

Downstream Broadcast Traffic and Privacy

In a shared medium like coaxial cable, subscriber cable modems are tuned to the same downstream RF channel and thus have access to all downstream RF packets as they are transmitted by the ARRIS C3 CMTS. However, the bearer channel traffic in each packet may or may not be encrypted to prevent viewing by unintended receivers. With unicast traffic (ARRIS C3 CMTS to one cable modem or one cable modem to the ARRIS C3 CMTS), DOCSIS® BPI (or BPI+) provides 56-bit DES encryption of a packet’s contents. Only the ARRIS C3 CMTS and the destination cable modem have the private “keys” and thus the ability to encrypt/decrypt the packets. However, residential subscriber downstream multicast or broadcast traffic is typically sent in the clear even when BPI is enabled. If this were permitted in a business-service Layer 2 VPN, it would result in instances where downstream multicast or broadcast traffic from a VLAN group is communicated to non-VLAN members. This situation and associated provisioning is depicted in Figure 5.

Fortunately the ARRIS C3 CMTS design has taken multicast VLAN traffic into consideration and provides optional Layer 2 VPN functionality where even broadcast traffic can be encrypted so that only members of the respective VLAN group have access to a packet’s contents. In addition to supplying a unique Security Association Identifier (SAID) or “key” for unicast traffic, the ARRIS C3 CMTS will also supply a unique “key” per VLAN group for VLAN-associated broadcast traffic. Both unicast and broadcast keys

are handed out to respective cable modems as part of the CMTS-to-cable modem BPI security negotiation that occurs after cable modem registration. Each VLAN group and the associated cable modems have a unique SAID to enable 56-bit DES decryption of downstream broadcast traffic associated with that group. Thus, only members of a respective VLAN group can decrypt multicast traffic related to that group. Security issues with unencrypted downstream traffic are effectively eliminated.

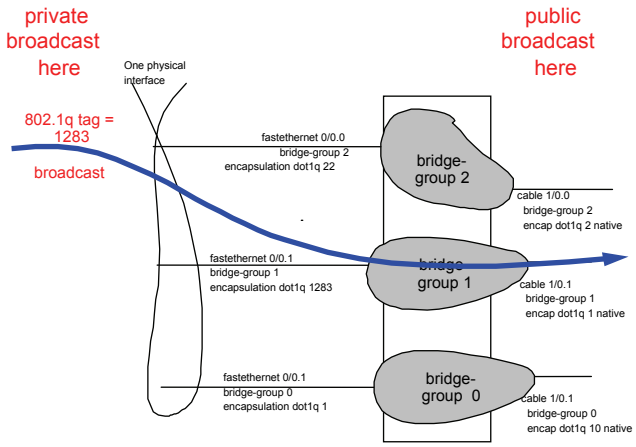

Figure 5 Downstream Broadcast

To insure privacy of downstream RF broadcasts, the key-word “encrypted-multicast” must be provisioned on the appropriate cable sub-interface. With such provisioning, only VLAN members assigned to a particular cable sub-interface with “encrypted-multicast” provisioned can decrypt the downstream broadcast/multicast traffic. Now, both unicast and broadcast/multicast traffic privacy is maintained.

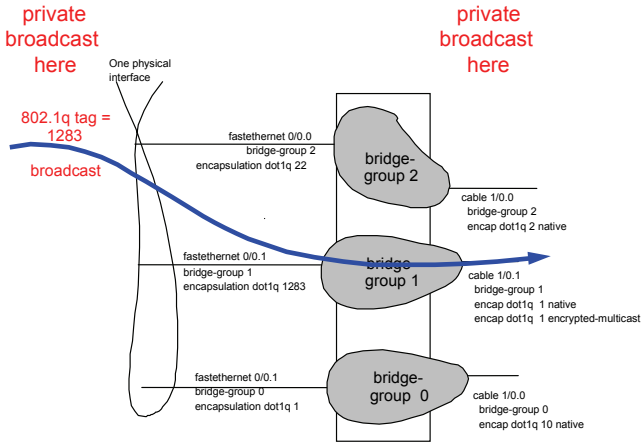

Figure 6 Downstream Broadcast Privacy Using “encrypted-multicast”

An example of how to provision “encrypted-multicast” on a cable sub-interface is shown below. BPI must be enabled on the ARRIS C3 CMTS for “encrypted-multicast” to work.

```
conf t
default cm-subinterface cable 1/0.0
interface cable 1/0.0
        ! For all modems
        bridge-group 0

interface cable 1/0.1
        bridge-group 1
        ! VSE tag of 1283 will CPE map here
        encapsulation dot1q 1283 native
        encapsulation dot1q 1283 encrypted-multicast
        exit
exit
```

Managing Layer 2 VPNs

Large-scale Layer 2 VPN networks over DOCSIS are deployed today, and for at least one cable operator, the Layer 2 VPN network has expanded to include more than 50 ARRIS C3 CMTSs. As the network size grows, cable operators need to be able to access information on how the Layer 2 VPNs are configured. Special “show” commands and a proprietary MIB are provided to simplify the management of Layer 2 VPNs.

The “show” command with a read out of the cable and Ethernet sub-interfaces belonging to a particular bridge group and the VLAN ID number for that bridge group is:

show bridge-group [bridge-group #]

If the cable modem IP address or MAC address is know, the “show” command to output the VLAN ID number, bridge-group ID number and cable sub-interface the cable modem’s CPE traffic is assigned to is:

show cable modem [IP address | MAC address] detail

Additionally, a proprietary SNMP MIB provides the sub-interface and VLAN to which a cable modem’s CPE traffic is assigned. This information can be accessed by element management and network management systems.

Network Architecture

Figure 7 shows a VPN network architecture as provisioned in one customer network. High-speed traffic from administration workstations is bridged locally and securely across the Layer 2 broadcast domain provided within the CMTS. Each of the three respective VLANs represented in this diagram have their cable modem traffic tagged by the ARRIS C3 CMTS according to the 802.1Q specification as the packets leave the ARRIS C3 CMTS and pass into the routed IP/MPLS network. Packets arriving on the Ethernet interface of the ARRIS C3 CMTS are mapped to the logical sub-interface based upon the VLAN ID present with each packet. The Q-tags are stripped as the packets are mapped from Ethernet to RF sub-interface and transmitted out the physical cable interface. Stripping the Q-tags in downstream traffic eliminates cable modem and CPE compatibility issues as none of the devices on the RF side of the network are required to support 802.1Q-tagged traffic – only the ARRIS C3 CMTS. If CPE devices do support 802.1Q tagging, double tagging is used with the outer tag being stripped when packets arrive at the Ethernet interface.

Numerous routers allow 802.1Q tagged packets to be mapped to MPLS. Thus Q-tagged traffic supported by the ARRIS C3 CMTS can be mapped North of the ARRIS C3 CMTS to an MPLS tag for Virtual Private Network and end-to-end QoS treatment across the IP network. Such an implementation allows for the simpler 802.1Q protocol to be provisioned and supported at the edge of the network while more complex protocol implementations like MPLS are configured and supported in the core network.

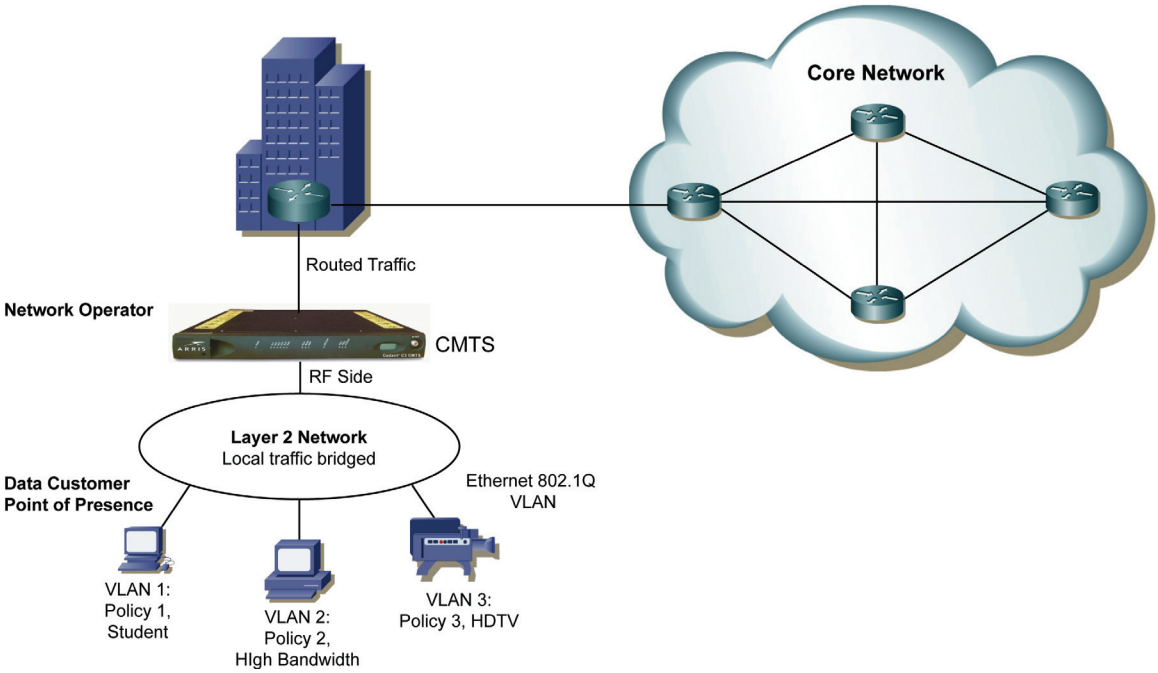

Figure 7. An operator serves dozens of business and educational sites with high speed data traffic using the ARRIS C3 CMTS and L2 VPN technology. Traffic is bridged locally on the Layer 2 network provided by the CMTS. Traffic destined for the Internet is sent to the Northbound router where it can be mapped to MPLS.

It should be noted that each and every C3 CMTS Ethernet sub-interface can be provisioned to forward traffic in Layer 2 or Layer 3 regardless of whether 802.Q tagging is being used. On a per Ethernet sub-interface basis, traffic can be forwarded in Layer 2 or in Layer 3 using static, RIP, or OSPF routing. For example, the operator can choose to have the traffic from VLAN A / Bridge Group A forwarded in Layer 2 from an Ethernet sub-interface belonging to Bridge Group A while traffic from VLAN B / Bridge Group B is forwarded in Layer 3 from a different Ethernet sub-interface belonging to Bridge Group B. Provisioning Layer 2 and Layer 3 forwarding on a per sub-interface basis gives the cable operator maximum flexibility in configuring the network side of the CMTS.

RF Spectrum Allocation for Business Services

A common practice in HFC networks running both residential and business services is to segregate these two traffic types. A set of upstream and downstream RF channels not being used for residential services is reserved for business services. Cable operators find this to be a convenient method for meeting service level agreements committed to residential and business subscribers.

Some cable operators have no usable RF spectrum less than 1 GHz that is not already allocated to residential video, voice and data service. This situation is often referred to in the cable industry as “channel locked”. To get past this problem, many cable operators are planning to convert analog video

channels to digital and use switched digital video (SDV) to free up RF spectrum below 1 GHz. Other cable operators are considering the use of frequency up-conversion / down-conversion devices. Typically, these devices are placed between the fiber node and coax plant and between the coax plant and the cable modem. Additionally, bi-directional amplifiers that operate at higher RF frequencies are co-located with existing amplifiers in the coax plant. By employing spectrum overlay techniques, cable operators can run downstream and upstream channels for business services at RF frequencies above 1 GHz.

Layer 2 VPN Service Delivery

The ARRIS C3 CMTS supports a Layer 2 VPN strategy that allows cable operators to deliver point-to-point and multipoint-to-multipoint business-class service quickly and easily. This unique service delivery technology gives the operator numerous benefits and advantages over competitive offerings, including:

• Flexible Deployment Options: The ARRIS C3 CMTS supports multiple 802.1Q provisioning and deployment options including: CPE-based Q-tagging, ARRIS C3 CMTS CLI-provisioned tagging, Vender-Specific-Encoding (VSE) tagging based on cable modem configuration file editing, double tagging and bridge tunneling.

• Easy Provisioning and Maintenance: To ensure scalability, cable operators need a fast and easy method to install new devices and provision services. With Vendor Specific Encoding (VSE) of VLANs, new devices attached to the network are automatically configured and provisioned with no client-based software required.

• Traffic Isolation and Security: Security is a critical "must-have" requirement of the business subscriber. The ARRIS C3 CMTS makes it simple to set up a secure Layer 2 VPN for each location. With “encrypted-multicast” enabled, security issues with unencrypted downstream traffic are effectively eliminated. VPN group members can communicate with each other in a secure manner knowing that non-group members are not receiving unencrypted traffic from the group VPN.

• Quality of Service (QoS): The ARRIS C3 CMTS makes it easy to set up a Layer 2 VPN for different classes of users. Many routers support 802.1Q to MPLS VPN mapping – thus enabling end-to-end QoS treatment if necessary.

• Lower equipment and OAM&P costs: The ARRIS C3 CMTS delivers competitive services at a much a lower cost structure than the traditional telecom architecture. Typically, Local Exchange Carriers (LECs) provide managed Transparent LAN Services (TLS) that provide the customer with an Ethernet interface. To deliver TLS, operators link sites together using copper T1 lines (1.5 Mbps) and T3 lines (45 Mbps) that are expensive to install, provision and maintain. Equipment is required in the T1/T3 POPs (e.g. add-drop muxes, channel banks and inverse muxes) and at the customer premise (e.g. Channel Service Units/Data Service Units or CSU/DSUs and routers). The LEC is very often responsible for maintaining the router operation at the customer site, which is often a point of failure requiring technical and on-site maintenance. This infrastructure is far more expensive to install, provision and manage than a Layer 2 VPN infrastructure that leverages the Hybrid Fiber Coax (HFC) plant.

With the ARRIS C3 CMTS, the equipment and infrastructure cost is lower allowing the MSO to tap into an incremental revenue opportunity which tracks closely with capital expenditures (CAPEX). With its ease-of-use, the ARRIS C3 CMTS supports lower provisioning costs than managed native Ethernet services offered by traditional telecommunications operators. The simplicity that Layer 2 VPNs bring to provisioning and maintenance also reduces the number of truck rolls required and maintenance costs.

• The ARRIS C3 CMTS supports desirable high upstream speed capabilities: The DOCSIS® 2.0 qualified ARRIS C3 CMTS is capable of transmitting data upstream at speeds of 20 Mbps with 16QAM and 30

Mbps with 64QAM (6.4 MHz channel), which meets the demanding needs of multimedia applications. Data communication at these higher speeds is expensive to provision and maintain using the telecom operator's traditional private data networking paradigm.

The ARRIS C3 CMTS At-A-Glance

- Operator-selectable Layer 2 or Layer 3 IP forwarding
- 802.1Q to support multiple ISPs & Layer 2 VPNs
- T1/E1 Service when used with ARRIS circuit-emulation equipment
- Flexible upstream channel configurations (2, 4 or 6)
- Multiple RF operational modes: DOCSIS and Euro-DOCSIS
- 30 Mbps upstream capable with 64QAM
- Full DOCSIS 2.0 Qualification - A-TDMA and SCDMA operation
- Superior RF performance including a digital receiver and ingress noise cancellation
- Compact size (1 rack unit)
- 3,000 registered cable modems supported
- Scalable and Reliable VoIP (NCS or SIP)
- Bandwidth on Demand using PacketCable™ Multimedia COPS DQoS
- Bandwidth Aware Periodic Load Balancing
- Interoperation with ARRIS Spectrum Analyzer