Provisioning Multiple ISPs For Multiple Cable Operators

Lessons Learned from Solving this Complex Cable Internet Challenge in Israel

Special to *Cable Datacom News* by Mike Stone, Artnet Experts Ltd.

In November 2001, our company, Artnet Experts, was asked to provide the Internet customer provisioning solution for Tevel Telecom, Israel's cable TV infrastructure provider. Unlike independent MSOs in the U.S., Tevel Telecom provides the hybrid fiber coax (HFC) infrastructure and common Internet infrastructure for Israel's three dominant cable service providers: Tevel Digital, Golden Channels and Matav. This article shares some of our more interesting experiences in setting up the solution to provision cable modem services supporting multiple Internet service providers (ISPs) for multiple cable operators.

Network Requirements and Architecture

When entering the cable Internet business, Israeli operators Tevel Digital, Golden Channels and Matav decided to leverage common HFC and IP infrastructure through Tevel Telecom, while keeping their commercial and IT operations separate. Tevel Telecom, in turn, decided that it did not want to compete with ISPs and certainly did not want to invest in submarine trunks and satellite links required for IP connectivity to and from Israel. The plan was to offer cable access services to any ISP the end customer wanted to use, and to offer customers the option to use multiple service providers, as well as access corporate virtual private networks (VPNs) for telecommuting.

To create its broadband data network, Tevel Telecom deployed Cisco UBR 10000 CMTSs compliant with Euro-DOCSIS 1.1, as well as Cisco GSR 12000 backbone routers. In total, eight Cisco routers were installed, one for each of the largest Israeli ISPs. Artnet partner Netcom created MPLS VPNs from each CMTS to each ISP router. In addition, a non-provisioned MPLS VPN was installed to allow new cable modem customers to access only the provisioning system to activate service. Artnet implemented the provisioning system to provide IP addressing (DHCP) and quality of service (TFTP) for cable modems and customer PCs, integrating it with central LDAP directories to hold technical customer profiles. Cisco CNR software was used for DHCP and TFTP services, and iPlanet Directory supplied the LDAP solution.

Multi-Cable Operator and ISP Provisioning

Provisioning multiple ISPs for customers of multiple cable operators offered a unique technical challenge for Tevel Telecom. Here is how we helped address it.

The provisioning system was configured to allow each cable operator's Customer Relationship Management (CRM) system to update its own LDAP directory with subscriber profile data and service configuration parameters. To provision service for a subscriber, the DHCP server looks up the subscriber's profile in the LDAP directory, based on his or her cable modem MAC address, and then allocates the proper IP address and DOCSIS quality of service (QoS) configuration file.

In a multiple ISP environment, cable modem subscribers must be provided with an IP address from their ISP of choice to ensure their traffic traverses that ISP's network. To support this requirement, each ISP provided Tevel Telecom with IP address subnets for each CMTS servicing residential cable customers. Artnet configured the ISP subnets for each CMTS into DHCP address pools with tags corresponding to the LDAP ISP codes. Cable modem boot files and option values were also configured corresponding to the LDAP QoS code attributes.

How It Works

Here's how it works in practice. The cable modem is turned on or reset so that it can issue a DHCP request for an IP address and the QoS options it needs. The DHCP request is broadcast up to the CMTS router. The CMTS records its IP address in the DHCP request packet and forwards it to the DHCP server for the cable modem address (based on the Option 82 contents). The DHCP server uses the cable modem MAC address from the DHCP request to perform an LDAP query, which returns the customer's ISP and QoS codes. The ISP code tells the DHCP server to allocate an available IP address from the ISP's subnet. The QoS code points to the cable modem boot file and the option values required by the cable modem. The DHCP server packs some other information into the response packet, such as the default gateway address (the sub-interface for the selected ISP) and the DNS pointer. The DHCP server returns the DHCP response packet to the cable modem. If the cable modem is satisfied, it accepts the allocated IP address, downloads the boot file via TFTP and then reboots. The DHCP server address pools use RFC 1918 addresses because their only use is to establish MPLS VPN tunnels within Tevel Telecom.

Then the customer's PC boots up and issues its own DHCP request for an IP address. The DHCP request is broadcast to the CMTS router's sub-interface. The CMTS records its IP sub-interface address in the DHCP request packet and forwards it to the DHCP server for customer premises equipment authorization (based on the Option 82 contents). The DHCP server allocates an available IP address for the PC from the ISP's subnet. The DHCP servers maintain logs and statistics telling how many and which IP addresses have been leased.

Problems and Solutions

When moving this concept from the drawing board to the field, challenges were of course encountered. The first problem we faced was that there was no mechanism designed to force a cable modem to reboot as soon as a CRM agent changed the customer's service settings in the LDAP directory. It would not be acceptable for the CRM agent to make a change for the customer, such as increasing access speed or switching ISPs, and then wait for the cable modem to reboot because the modem would only reboot if it lost electrical power or its DHCP lease ran out.

In working to resolve this first problem, we encountered another: The LDAP standard does not provide triggers to execute stored procedures that relational databases, like Oracle, provide. As a matter of fact, Oracle provides an LDAP interface for its RDBMS, which would have given us LDAP and triggers. But Oracle's performance benchmarks were slower than iPlanet's.

To get around this, Artnet wrote a routine called Cable Modem Reset to accept trigger files transmitted by each CRM system whenever a critical change was made for a customer. The trigger file contained only the cable modem MAC address. When Cable Modem Reset received a trigger file, it used the cable modem's MAC address to look up the corresponding CMTS IP address in the LDAP directory and then transmitted a cable modem reset command. The reset command caused the cable modem to reboot and request a new IP address, QoS boot file and option values.

The next problem was that Cisco's CNR DHCP only supported multiple LDAP directories for fail-over purposes or for separating LDAP reads from writes. Tevel Telecom required three separate and different LDAP schemas, one for each cable provider. Artnet came up with a virtual LDAP design, based on OpenLDAP with back-end shells, to provide this functionality.

At this point, it would be both wise and truthful to state that Artnet would not have been able to accomplish what it did without Cisco providing us with deep access to its CNR gurus. We were able to tap into their abundant brain cells for work-arounds and fixes for LDAP and cable modem configurations.

What's Next?

Because this is an ongoing project, it might be pertinent to describe what's under development and what's under consideration.

Both cable operators and ISPs are interested in tracking use and abuse of Internet services by their customers. Because Cisco CNR DHCP version 5.5 provides a fairly detailed lease log, containing IP address allocated, date and time allocated, and MAC address receiving the allocation, we developed a solution that leverages this intelligence. Essentially, it parses the CNR lease log, using the CMTS addressing and the cable modem MAC address from the DHCP Option 82 field to look up customer details from the appropriate LDAP directory. Additionally, we extracted the date and time and stored the data together in a MySQL relational database. We then created a Web routine to provide secure customizable views of the MySQL data for cable providers and ISPs so that each could only look at their own data. Thus, an ISP or cable provider can query MySQL with an IP address and time period to obtain the associated customer's details. As an option, the system could export MySQL data for each ISP into a RADIUS accounting log.

Another desirable function is to provide a captive portal site for unprovisioned PCs attempting to browse the Internet over cable. This site would capture all Web requests and redirect them to a site explaining why they cannot access the Internet and how to subscribe to the service. The solution could be extended to provide customers free content and services, pre-provisioned assistance and customer self-provisioning.

The latest project under consideration is the integration of Multi-ISP access with MPLS-DHCP based cable Internet service. The challenges are great and there is no tried-and-true template solution for it. Broadband cable services differ from DSL services, which use encapsulation tunnels to carry traffic, and RADIUS to identify users and track usage. Cable customers get their IP addresses via DHCP, while DSL and dial-up ISP customers get their IP addresses via RADIUS. In any case, MPLS VPNs are not inherently flexible enough to allow cable customers to switch VPNs from one ISP to another ISP or to their corporate networks.

To allow this, Artnet came up with a solution in which cable customers who opted to do so would be assigned to a shared MPLS VPN. This VPN would direct them to a portal, where they could log in with a user name and password and then select from a menu of access options, such as available ISPs and corporate networks. After selecting an option, the portal transmits a trigger file to the Cable Modem Reset system (described above), which would cause the customer's cable modem to reboot with the new configuration parameters required for the selected access option.

About the Author: Mike Stone is a senior network consultant for Artnet Experts Ltd., in Israel. Mike has been intimately involved with bits and bytes for over 30 years and has been consulting in all areas of networking since 1993. Mike's clients include several Israeli government ministries and municipalities, the police, the army, the major ISPs, cable operators, high-tech industries and several start-ups. He can be reached via email at s_mike@artnet.co.il.

Taken from Cable Datacom News – October 2003

http://www.cabledatacomnews.com/oct03/index.html