Advanced Security Management in Metro Ethernet Networks*

Ammar Rayes
Cisco Systems
255 West Tasman Drive
San Jose, CA 95134, U.S.A.
rayes@cisco.com

Abstract

With the rapid increase in bandwidth and the introduction of advanced IP services including voice, high-speed internet access, and video/IPTV, consumers are more vulnerable to malicious users than ever. In recent years, providing safe and sound networks and services have been the zenith priority for service providers and network carriers alike. Users are hesitant to subscribe to new services unless service providers guarantee secure connections. More importantly, government agencies of many countries have introduced legislations requiring service providers to keep track and records of owners of IP and MAC addresses at all time.

In this paper, we first present an overview of Metro Ethernet (or Ethernet-To-The-Home/Business (ETTx)) and compare with various IP broadband access technologies including DSL, wireless and cable. We then outline major security concerns for Metro Ethernet networks including network and subscriber/end user security.

Next we introduce state-of-the-art algorithms to prevent attackers from stealing any IP or MAC addresses. Our proposal is to use network management in conjunction with hardware features for security management to provide a secure and spoofing-free ETTx network. The key idea behind our proposal is to utilize network management to enforce strict (port, MAC, IP) binding in the access network to provide subscriber security.

The paper then proposes an adaptive policy-based security controller to quickly identify suspected malicious users, temporarily isolate them without disconnecting them from the network or validating their contracts, and then carry the required analysis. The proposed controller identifies malicious users without compromising between accurate but lengthy traffic analysis and premature decision. It also provides the ability to make granular corrective actions that are adaptive to any defined network condition.

Keywords: Internet Security, Network Management, Network Security Management

1 Introduction

The flexibility of broadband and Internet Protocol (IP) networks introduce new challenges to hardware vendors as well as service providers. Broadband access to the Internet is becoming ubiquitous. Emerging technologies such as Ethernet access and VDSL offer increasing access link capacity. Access speed exceeding 1 Gbps is becoming a reality. At the same time, it introduces new challenges to hardware vendors as well as service providers.

---

*This work as presented in part at the International Conference on Security and Management in Las Vegas, Nevada, USA.

The most important challenge is perhaps the network and service security. Business and residential customers are reluctant to subscribe to services unless service providers guarantee that their transactions and online activities are completely secure. That is, no one else has access to the contents of their applications, no one can spoof their IP address, etc. Service providers are extremely concerned about network security especially when the network utilization and latency are high. As a result, effective and efficient detection of malicious activities is critical. However, this requires detailed traffic analysis to determine if certain suspicious activities are indeed malicious. Once an activity is determined as malicious, the service providers can then perform the corrective actions, e.g., disable the user port. Incorrectly identifying a proper activity as malicious will cause, at the minimum, unnecessary service interruption and may result in loss of revenue and subscriber dissatisfaction. At the same time, detailed traffic analysis is complicated and time-consuming. As a result, before the analysis is completed and the results are understood, a malicious activity may cause grave harm to the network. Thus, in order to ensure the network integrity, it is critically important to prevent suspicious users from further inflecting damage to the network while detailed traffic analysis is being carried out.

The success of comprehensive security prevention solution depends greatly on delivering and implementing secure and protected networks. Providing such capabilities in the hardware alone is a daunting task. Security is often being addressed at the device hardware level, e.g., implementing certain security features in the switch [2]. In this paper, we focus on the overall hardware and software / control (network management) solution. The combined solution shall preclude anyone from using someone else's identity (e.g. an IP address other than the one being assigned by the service provider), network element's identity (e.g. claim to be the default gateway) or unassigned but valid identity (e.g. using a valid IP address not yet assigned).

The basic idea behind the solution is to maintain a binding relationship [6] between the device Layer 2 identifier (i.e. MAC (Medium Access Control) address or Ethernet address) with the Layer 3 identifier (i.e. IP address of a user) and implement strict rules to enforce such a relationship at the port level. The solution minimizes dependency on hardware enhancement and provides easy mechanism to support subscriber traceability.

Next, we propose a policy-based security controller (PSC) which allows service providers to isolate the suspicious users so that actual malicious activities will not cause damage to the network while allowing effective traffic analysis to complete and take granular level of actions against attackers based on the network condition.

The rest of the paper is organized as follows. Section 2 gives an overview of Metro Ethernet / ETTx networks. Section 3 describes security issues that are specific to Metro Ethernet networks. Section 4 discusses spoofing prevention techniques via port isolation. Section 5 presents a spoofing free environment for Metro Ethernet networks. Section 6 defines the policy based security controller. Concluding remarks are given in Section 7.

2 Network Architecture

Residential or business customers have several broadband technology options to access the Internet including digital subscriber line (DSL), cable, wireless, and most recently Metro Ethernet / fiber-to-the-home or business (FTTx or ETTx). DSL uses the current twisted copper pairs in the Plain Old Telephony systems (POTs) to provide Internet access. The actual speed depends on the specific implementation and the distance between the customer premise and the central office, i.e., the loop length. Today's DSL deployment is limited in speed and can be very expensive to deployed and provisioned. Cable access can provide connection speed up to 6 Mbps. Being a shared medium, cable access can be extremely slow when traffic increases.

Multiple flavors of broadband fixed wireless have been deployed including Local Multipoint Distribution Service (LMDS) and Multi-channel Multi-point Distributed System (MMDS). The ATM transport based

LMDS solution, which is based on the SpectraPoint technology, is a regulatory designation for broadband fixed wireless systems that operate in the 28 GHz band and offer up to several Giga-Hertz of licensed spectrum (1.3 GHz in the United States). It is designed for line-of-sight coverage over a range of 3 to 5 kilometers and has the capacity to provide data and telephony services for up to 80,000 customers from a single node.

ETTx offers the highest access speed due to the use of fiber technology. It supports up to the Giga bits per second (Gbps) range. However, it entails laying fibers to the customer premises, which may be difficult and expensive. As a result, Ethernet is often used in the last mile and it drives down the cost significantly. ETTx is an emerging access technology as an alternative to DSL and cable.

Figure 1 shows the network architectures for these broadband access technologies. In general, at the customer premise, there will be an access gateway. The main purpose of this access gateway is to convert the packets into the technology-specific format and medium. For example, in a cable access environment, the access gateway will be the cable modem, while in the DSL environment it will be the DSL modem. In ETTx, such conversion is unnecessary, and the access gateway in this case (if presence) will play the role of a concentrator for different services, e.g., Internet access, VoIP (Voice over IP) and video. The user traffic is then aggregated at the aggregator before entering the backbone network into the ISPs (Internet Service Provider).

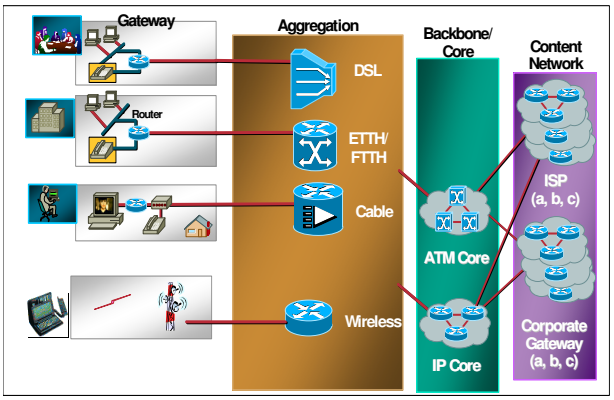

Figure 1. Broadband Access Technologies

Regardless of the access technology, the security requirements are common. Customers are unwilling to subscriber to new services unless the network is secure. Service and network providers need to implement protocols to prevent unauthorized users from stealing a legitimate customer's identity, network element identity, and/or unassigned but valid identities such as IP address, MAC address, log-in IDs and passwords, cable cards, or connecting directly to access switch. Security in ETTx poses a challenging problem because of the lack of operating standard similar to DOCSIS (Data-over-Cable Service Interface Specifications) in the cable access technology. In addition, the architecture of ETTx is like extending the LAN (Local Area Network) technology to a public network. The openness of such architecture and the infancy of this technology in the public access domain pose another level of difficulty to the security problem. In addition, in ETTx, it is not uncommon to see large subnet spanning across multiple access switches to conserve IP addresses. As a result, we often see a large number of subscribers sharing the same IP subnet. This makes the security problem more interesting. In this paper, we will focus on the security issues that arise in ETTx and introduce a solution which is a combination of hardware and software (network management). The combined solution shall preclude the most common spoofing problems and at the same time minimize the dependency on hardware enhancement and provide easy mechanism to support subscriber traceability.

3 Security Issues in ETTx Networks

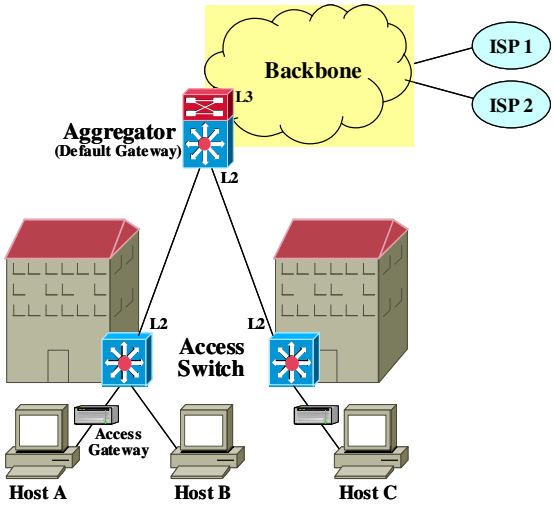

Figure 2. Typical ETTx network architecture

In ETTx environment, the network consists of access switches, aggregation switches and the backbone network connected into different ISPs, as shown in Figure 2. Typically, there is an access switch residing in the basement of a building aggregating user traffic within the building. In a typical ETTx deployment, a building often consists of business users (in the ground floor) and residential users (in the upper floor). Several access switches are then aggregated before entering the backbone network into the ISPs. The access switch is the provider network delimiter. An Ethernet link goes from the access switch in the building basement to an Ethernet outlet in each unit providing network access. Inside the building unit, one either connects the Personal Computer (PC) through the Network Interface Card (NIC) to the Ethernet outlet, or connects a sort of access gateway to aggregate different devices such as PC, set-top-box, phones for simultaneous data, voice and video services. For the purpose of security discussion, the presence of access gateway is irrelevant. We shall consider the simpler case where the PC connects directly to the access switch port through the NIC.

In the sequel, we will consider the access switch is a Layer 2 device. The aggregator is the first hop of Layer 3 device. That is, the aggregator is operating at Layer 2 on the access switch facing side and at Layer 3 on the backbone facing side. The aggregator is also serving as the default gateway of an IP subnet, consisting of a number of access switches.

From the user's point of view, the paramount importance is the service being delivered securely in the sense that it is spoofing-free. The bottom line is nobody should be able to tap into anyone's communication path, and that nobody should be able to steal an identity that he/she is not supposed to be using. That being said, from the user perspective, there are three main security problems: 1) a malicious user is stealing someone else's identity, e.g., an IP address other than the one being assigned by the IP address assignment server, 2) a malicious user is stealing a network element identity, namely the identity of the default gateway, 3) a malicious user is stealing unassigned but valid identity, e.g., using a valid IP address not yet assigned.

To utilize someone else's identity or a network identity, the malicious user needs to corrupt the Address Resolution Protocol (ARP) table at the first hop of Layer 3 device. The purpose of ARP is to resolve the MAC address of a device from a given IP address. An ARP packet consists of the 2-tuple (MAC, IP) of a device. Within the IP subnet, two communicating devices need to know each other's MAC addresses. For example, if Host A needs to communicate with the default gateway, Host A will issue an ARP request with (NULL, $IP_{\text{default gateway}}$), usually broadcast within the IP subnet. The default gateway will reply through unicast to Host A ($MAC_{\text{default gateway}}$, $IP_{\text{default gateway}}$). Host A will then store the ARP information in the local ARP table.

If the default gateway is replaced, the default gateway can broadcast an ARP request with ($MAC_{\text{new default gateway}}$, $IP_{\text{default gateway}}$). All the hosts within the subnet will then update the local ARP table to take into account the fact that the default gateway device is replaced. Such an ARP operation was originally designed for a trusted friendly network environment. In public IP network, ARP can be abused for malicious use.

Consider in Figure 2 where Host A is the malicious user, intending to steal Host C's identity. To steal Host C's identity, Host A needs to corrupt the ARP table at the default gateway, which is usually the aggregator. The ARP table at default gateway stores all the MAC-IP address relationship for all devices within the IP subnet (or Virtual LAN (VLAN)). So the ARP table at the default gateway will have the following entries:

MAC_A	IP_A
MAC_B	IP_B
MAC_C	IP_C
…	…

To corrupt the ARP table of the default gateway, Host A sends a unicast unsolicited ARP request claiming the (MAC_A, IP_C) association to the default gateway. Without knowing the malicious intent, the default gateway thinks that Host C has been replaced by a new PC and will modify the ARP table to the following:

MAC_A	IP_A
MAC_B	IP_B
MAC_A	IP_C
…	…

Such an attack can be easily carried out by using some widely available tools, such as dsniff [3] and ettercap [4]. All traffic destined to Host C will then be directed to Host A. If Host A turns on the IP forwarding feature (available in many modem Operating Systems), he will then able to forward Host C's traffic back to Host C. As a result, Host A steals the Host C's identity. If the service is being measured by the amount of traffic associated with an IP address, Host A is in fact stealing Host C's service.

Host A can steal the default gateway identity in a similar fashion. To sniff Host C's traffic, Host A will send an ARP request to Host C, claiming the (MAC_A, $IP_{\text{default gateway}}$) association. Host C will then happily update the ARP table, thinking that the default gateway is replaced and has a new MAC address. By turning on IP forwarding, Host A now sits in the middle of the communication path between Host C and the default gateway. Host A is then able to monitor Host C's traffic and obtain passwords transmitted both in clear-text and as part of a SSL (Secure Socket Layer) transaction.

Besides doing ARP spoofing, Host A can also simply configure its PC to bear MAC_C and IP_C to steal Host C's identity. Similarly, Host A can also configure its PC with an unassigned but valid IP address. Either way, Host A will be able to use services without paying the service provider.

Users are concerned about such security issues and are reluctant to sign up for services until these are being addressed by the service providers. These security issues also translate to loss of revenue for the service providers. As a result, service providers are extremely apprehensive about subscriber security.

4 Spoofing prevention

4.1. Port Isolation

Port isolation isolates endpoints within the same IP subnet or VLAN. With port isolation, one can specify some unique set of rules governing the connected endpoint's ability to communicate with other endpoints connected within the same subnet. One such rule can be "when a host needs to communicate with another

host, it needs to do so through the Layer 3 device". For example, Host A in Figure 1 needs to go through the aggregator if he wants to communicate with Host B. As a result, a malicious user cannot send unsolicited ARP request directly to another host within the subnet. The ARP request will be relayed to the first hop of Layer 3 device. Protected port and private VLAN are some example of port isolation offered in Cisco switches. Protected port provides port isolation within a switch while private VLAN provides port isolation to a subnet across multiple switches [5]. Port isolation itself cannot prevent any ARP spoofing. However, with the access switch being Layer 2, it is needed so that ARP spoofing can be dealt with in a more centralized place: the first hop of Layer 3 device, i.e., the aggregator.

4.2. ARP Inspection

ARP inspection is another security feature which redirects all the ARP traffic for validity checking [5]. The payload of each redirected ARP packet is inspected by software and the MAC-IP association is checked for consistency. A set of order dependent rules, for example, in the form of Access Control List (ACL) can be specified by the user to check if an ARP payload is legitimate or faked. A simple rule that can prevent the dsniff attack would look like:

permit $IP_{\text{default gateway}}$ $MAC_{\text{default gateway}}$
deny $IP_{\text{default gateway}}$ any
permit any any

If an ARP packet complies with the user rules, then it is forwarded to the destination. A non-compliant ARP packet is dropped, and the event is logged. ARP inspection is implemented in the aggregator. It can prevent spoofing of the default gateway IP address and if used in conjunction with port isolation, it can help prevent ARP spoofing of another host within the same subnet. However, the latter can be cumbersome because all the legitimate MAC-IP association needs to be configured manually in the switch. For a large number of subscribers, it becomes infeasible because it entails configuring thousands of entries of legitimate MAC-IP associations statically in the ARP ACL. In addition, the ARP ACL needs to be updated every time the IP lease of an existing user expires and a new IP address is assigned.

4.3. Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is ARP Inspection in conjunction with DHCP (Dynamic Host Configuration Protocol) gleaning. In DAI, the ARP ACL is built dynamically. The switch gleans all the DHCP traffic. As the DHCP server assigns an IP address to a host, the switch will parse the DHCP packet for the MAC-IP association and create a new ARP ACL entry for ARP inspection. As a result, DAI restricts ARP request access by not relaying invalid ARP requests and responses out to other ports in the same VLAN. Unsolicited ARP requests will be prevented from the network and ARP table of the hosts and aggregator will not be contaminated.

4.4. Port ACL

All of the above aim to avoid malicious users from poisoning the ARP tables of the network switch/router and other hosts in the attempt to steal an identity. It does not, however, prevent someone from changing his/her device configuration, namely MAC and IP address, to a valid association recognized by the network. To prevent this type of malicious users, a Port ACL needs to be set up at the user port. Different levels of security can be configured by restricting access to the user port by only the registered devices or network identity. For example, one can restrict access of user port by only devices with a registered MAC address, or an IP address assigned by the network DHCP server, or a combination of both. Similar to ARP Inspection, setting up the port ACL for a large number of subscribers on a dynamic basis is cumbersome.

4.5. Dynamic Port ACL

Dynamic Port ACL (DPA) is Port ACL in conjunction with DHCP gleaning. In DPA, the Port ACL is built dynamically by the switch by gleaning all the DHCP traffic. With DPA, network identity not being assigned by the network and any MAC-IP association not being expected by the network will be treated as illegitimate.

Table 1 summarizes the capabilities of each the security feature described above. Note that "✓" designates support, "P" designates partial support, and "×" designates not support.

Table 1. Security features summary

	Gateway Spoofing	Host Spoofing	Device Identity Changing
Port Isolation	×	×	×
ARP Inspection	✓	P	×
Dynamic ARP Inspection	✓	✓	×
Port ACL	×	×	P
Dynamic Port ACL	×	×	✓

5 Spoofing-Free Environment in ETTx

Network management system (NMS) can play a pivotal role in providing subscriber security to public IP networks. From Table 1, it is obvious that the more powerful the security feature, the more intelligence it requires on the switch hardware. For example, ARP inspection can prevent gateway spoofing, but to prevent host spoofing, DHCP gleaning feature is needed. Similarly, DCHP gleaning is also needed to prevent device identity spoofing using Port ACL.

In this paper, we propose the use of network management in conjunction with hardware feature to provide a spoofing-free environment in ETTx [6]. The main benefit is to offload the stringent requirement on sophisticated hardware security features to NMS, while at the same time, user traceability requirement can also be satisfied, which is becoming a legal requirements in many countries. It also gives the service providers the ability to pinpoint the malicious user instantly and take appropriate actions, e.g., send a warning or disable the user port.

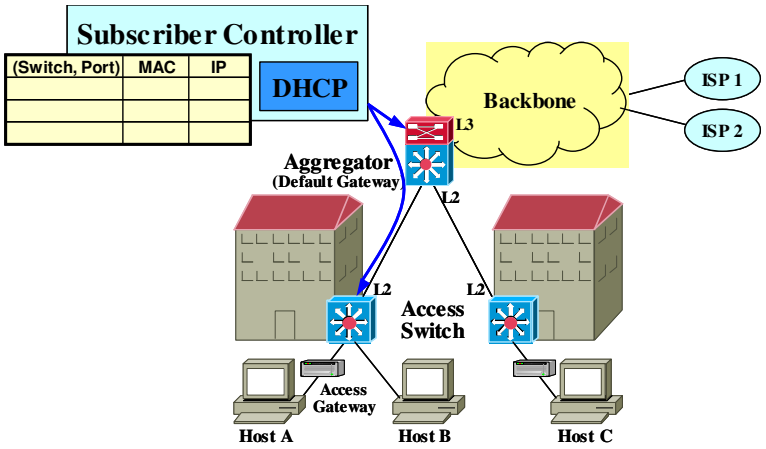

Figure 3. Network Management approach to Subscriber Security

Table 2. Sample Subscriber Service Profiles

Subscriber	Service Profile	Network Attachment Point
Bob	Gold Data (10 Mbps, 5 IP addresses)	Switch SJ_1, Port 5
Tom	Silver Data (5 Mbps, 2 IP addresses)	Switch SJ_6, Port 2
Ken	Gold Data (10 Mbps, 5 IP addresses)	Switch SJ_2, Port 12
…	…	…

The main idea behind our proposal is to utilize network management to enforce strict (port, MAC, IP) binding in the access network to provide subscriber security. Consider a subscriber controller (SC) as shown in Figure 3. SC is typically part of the overall Network Management System (NMS), maintaining the subscriber profiles holding information including the service profiles (e.g., subscriber subscription, number of devices allowed, etc.), and the network profiles described by the subscriber network attachment point, namely the switch and the port that the subscriber is associated with. Table 2 shows an example of the Subscriber Service Profile. SC translates the service profile of each subscriber into a set of authorization policies defining the access right of the user to network and enforces them at the necessary network location, such as an access switch and aggregator. The policies are on a port-level, i.e., each subscriber is associated with a unique port in the access network. At the time of service registration, the SC creates a new subscriber object capturing the service subscription in the Subscriber Service Profiles.

As part of SC, the DHCP server assigns IP addresses to subscriber devices according the subscriber policy defining the subscriber service subscription. As a result, the DHCP server can be considered a trusted network resource. When a subscriber device issues a DHCP discovery to obtain the IP address, the DHCP server will obtain the MAC address and the location DHCP request (which port from which switch). As the DHCP server assigns an IP address to this subscriber device, it will trigger an event in the SC to store the new (port, MAC, IP) association. As a result, the SC will always have the latest up-to-date subscriber network profile, defined as the (port, MAC, IP) associations, for all subscribers. Table 3 shows an example of the Subscriber Network Profiles, which hold the present (port, MAC, IP) associations for all subscribers. The SC creates a new entry in the Subscriber Network Profiles when the SC detects and activates a new subscriber device at a network attachment point.

Table 3. Sample Subscriber Network Profiles

Network Attachment Point	MAC address	IP address
Switch SJ_1, Port 5	01:34:B4:DA:45:6A	123.67.225.13
	01:34:B4:DA:53:31	123.67.168.187
	01:34:B4:DA:55:12	123.67.168.189
Switch SJ_6, Port 2	A2:D4:23:8C:11:B2	123.67.225.19
Switch SJ_2, Port 12	B4:23:60:DD:2F:02	123.67.219.101
	B4:23:50:E0:65:81	123:67.219.189
…	…	…

Note that the Network Attachment Point is the key that relates the Subscriber Profiles and the Subscriber Network Profiles. The Subscriber Network Profiles provide the list of legitimate users and their associated network identifiers, namely, the MAC and IP addresses of the allowable devices.

The Subscriber Network Profiles are used to define the subscribers' network access privilege and will be enforced by the SC. With the DHCP server being a trusted resource, the SC holds the authoritative (port, MAC, IP) bindings in the Subscriber Network Profiles, the SC can maintain all legitimate MAC-IP associations, to be enforced in the ARP ACL and Port ACL. This relieves the need to implement DHCP gleaning at the aggregator and access switch.

A change in the Subscriber Network Profiles, e.g., when a subscriber obtains a new IP address from the DHCP server or when a subscriber installs a new device and obtains a new IP address, an update event will be triggered. The update event will be processed by the SC. SC will then update the new MAC-IP association in the ARP ACL at the aggregator. At the same time, the SC will update the MAC-IP association in the Port ACL at the access switch. As a result, ARP spoofing is prevented and subscribers are unable to perform host spoofing or gateway spoofing by corrupting the ARP tables in any network entities. At the same time, malicious users cannot re-configure their MAC-IP associations at a local device (e.g., a PC) to access the network because the Port ACL ensures the MAC-IP associations are enforced on a port-level. For example, from Table 3, (01:34:B4:DA:45:6A, 123.67.225.13) is a valid MAC-IP association from Switch SJ_1, Port 5 (Bob). If Tom reconfigures his PC to bear this MAC-IP association, he cannot obtain any service because this association is valid only behind Bob's port. Tom's traffic will be blocked by the access port and he would not be able to penetrate through the access port.

In addition to assisting in spoofing prevention, the SC can also be used to pinpoint the origin of spoofing attacks. For example, when a malicious user tries to contaminate the ARP table in the default gateway, it will be caught by ARP inspection. The switch will then generate an alarm, containing the bogus MAC-IP association and the port where the attack is originating from. The SC will capture such alarms and use the embedded information to deduce the user who is launching the attack. Consider the case when the malicious Host A plans to claims Host C identity by sending an unsolicited ARP message with the (MAC_A, IP_C) association to the default gateway. ARP Inspection will stop such an ARP contamination and generates an alarm with the (MAC_A, IP_C) association embedded in it. From the Subscriber Network Profiles, using IP_C, the SC can deduce the associated Network Attachment Point. Using the Network Attachment Point as the key, the SC determines that Host C is possibly under attack. Similarly, from MAC_A, the SC can deduce the associated Network Attachment Point. Then using the Network Attachment Point as the key, the SC determines that Host A is possibly launching an attack. From the Subscriber Service Profiles, the SC also knows the detail of Host A. The network administrator will then be notified and will decide on the appropriate actions. For example, Host C can be notified and prompted to obtain a new IP address. For the attacker (Host A), the network

administrator can, for example, for first time offence, sends a warning. For repeated offences, the user port will be shut down and user will be denied service as a penalty.

Besides spoofing prevention, the Subscriber Service Profiles and Subscriber Network Profiles can be used in combination to provide subscriber reporting and subscriber traceability. By keeping a log of the Subscriber Network Profiles change history, the service provider will have complete knowledge of who has which IP address, from which port, using what device, and at what time. Such a feature is very important legal requirement.

6 Policy-Based Security Controller

The Subscriber Controller proposed in Section 5 enforces an authoritarian (port, MAC, IP) binding. However, it does not fully prevent malicious subscribers from diminishing network sources such as IP addresses by requesting address renewal too any times from the DHCP server. To further augment the security of IP based networks, this section proposes a Policy-based Security Controller (PSC) to manage high risk subscribers as shown in Figure 4. Like to the SC in Section 5, PSC is also implemented in the NMS layer to assure a global view of the entire network. Such view is important for an effective adaptive decision-making controller. The PSC consists of two components: a user quarantine mechanism and an adaptive state dependent decision making controller. The user quarantine mechanism allows service providers to run detailed diagnostics and analysis to the suspected user's traffic behavior so that premature decision can be avoided. The adaptive decision-making controller is introduced to provide granular level of actions against network security attacks depending on the network condition.

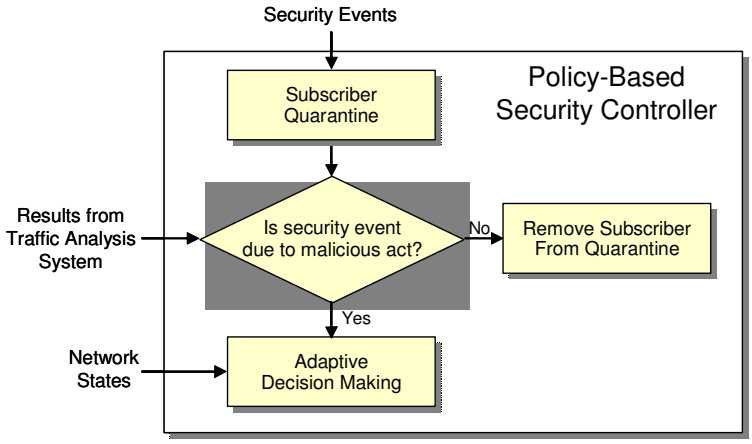

Figure 4. Policy-Based Security Controller

PSC detects malicious activity by monitoring security events generated by the network devices or commercial monitoring applications [7]-[8]. The information is typically correlated with the network inventory to pinpoint the suspected end-points. Examples of security events include traps due to illegal Address Resolution Protocol (ARP) requests or the number of DHCP requests per user exceeds a threshold within a given time window. An early detection of suspicious network activity will cause the user to go into "quarantine". Traffic of users in quarantine will be routed through some traffic analysis system to determine if the suspected users are indeed carrying out malicious acts. Although PSC may be extended to handle traffic analysis, it should be noted that traffic analysis is not the focus of this paper. If a malicious act is concluded by the traffic analysis system, the PSC will use an adaptive state approach to make a corrective action decision.

6.1 User Quarantine Mechanism

The PSC uses the concept of *high alert* user group to provide user quarantine. The high alert user group can be realized by creating a special *high alert* IP subnet, e.g., IP addresses ending between 240 and 255. Intelligent DHCP server can be used to assign IP addresses based on user groups. When the DHCP server receives a DHCP request from a user in the *normal* group (non-high alert group), it will assign an IP address associated with the public subnet. On the other hand, if the DHCP request is from a user in the high alert group, it will assign an IP address associated with the high-alert group.

The user quarantine mechanism is shown in Figure 5. Upon an early detection of suspected malicious activity, the PSC classifies the suspected user as high alert. To force the suspected user into quarantine, the user's device (e.g., a personal computer) needs to get a new IP address corresponding to the high alert IP subnet. This can be achieved by three ways.

1. The PSC triggers the DHCP server to send a DHCPRECONFIGURE message to the suspected host. The DHCPRECONFIGURE message is a unicast *forced renew* message sent by the DHCP server causing the client (user device) to renew the IP lease.
2. The PSC triggers the DHCP server to expire the current IP address lease and prompts the suspected user to perform *ipconfig /release* and *ipconfig /renew* to obtain a new IP address.
3. The PSC triggers a user port reset at the access device [6], e.g., sends a *shutdown* command to the user port. This causes the user device (DHCP client) to interpret that there is a "disconnection from the local network".

Basically, the above three methods force the suspected user device to lose their currently assigned IP address, hence it will issue a DHCPDISCOVERY message to request for new IP address. Since the user is already classified as high alert, upon receiving the DHCPDISCOVERY message, the DHCP server will assign an IP address from the high alert group.

To ensure the suspected user cannot inflict further damage to the network potentially, Access Control List (ACL). For example, MAC ACL and IP ACL can be used to restrict access to the network. For example, the IP ACL at the user port can be used to accept upstream IP packets only with the newly assigned special IP as the source IP address:

permit ip <special IP> any.

The MAC ACL can also be used to allow upstream packets destining to any host, to originate only from the device which a given MAC address that corresponds to the device where the special IP address is assigned:

permit any <user's MAC address>.

Other stringent security measure can also be applied, as long as the user service contract is not violated.

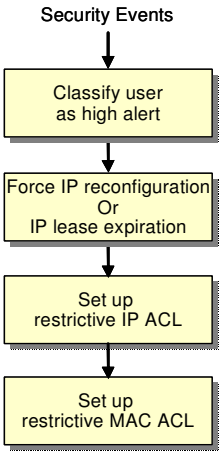

Figure 5. User Quarantine Mechanism

After the next datagram is sent to/from the suspected user or explicitly through DHCP snooping/secure ARP, the ARP table will be automatically updated replacing the original MAC/IP mapping with the new mapping bearing the IP address from the high alert group.

By quarantining all the suspected users by IP subnet, their malicious activities will only affect their isolated subnet, without affecting other *well-behaved* users. Approaches such as policy-based routing can then be used to forward all the traffic from the high alert subnet to the traffic analysis system before being delivered to the final destination.

6.2 Adaptive State-Dependent Decision-Making

In programmable networks, a considerable amount of information regarding the network condition is available. Such information can be taken into consideration when making a decision of the best course of actions against a malicious user. For example, if the traffic analysis system concludes that a user was trying to launch an ARP attack, the PSC may issue a warning message if the network utilization is low while it may disable the user port immediately if the network utilization is critically high. In the literature, the class of events that utilizes the status (or the states) of the network is called *adaptive state dependent*. The PSC uses a programmable adaptive state-dependent decision-making controller against network security attacks.

The adaptive state-dependent decision making controller is a function of n states. In this paper, we propose state-dependent decision making controller using three states: alert state, user risk state, and the network and resource health state, as shown in Figure 6. The decision process can be described as

$$Decision(t,T) = f(Alert\_State(t,T), User\_Risk\_State(t,T), Health\_State(t,T)) \quad (1)$$

where T (e.g. 5 minutes) is the user-defined window of time over which the network alert and health states will affect the decision. In other words, the decision is dependent on the network condition between time t-T and t.

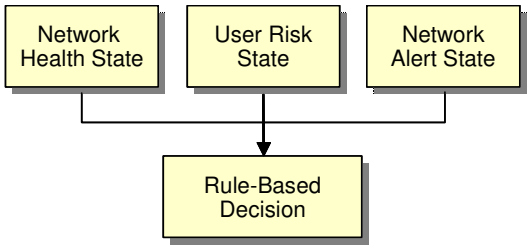

Figure 6. Adaptive State-Dependent Decision-Making

We define the novel term network "alert state", a function of the number of security events captured over the last T units of time. The security events are the set of events that have implications to network security, Examples include (1) DHCP flooding where an event is issued when the number of IP addresses requested per port/user is above an admin-defined threshold. Such parameter is of particular importance when the DHCP resource (IP addresses) utilization is high (very few IP addresses are left for allocation), (2) invalid unsolicited ARP (Address Resolution Protocol) packets, and (3) port ACL (Access Control List) violation. The generation of alert state is not the scope of this application. This can be accomplished by some event correlation engine, which may be part of the PSC.

We also define the novel term "user risk level" which, for instance, associates high risk users with a risk level (e.g. low, medium, high, critical) by keeping historical track of the alerts generated over time. For example, user of port 5 of access switch 25 is of critical risk because s/he has more than x number of invalid unsolicited ARP requests and y DHCP alert levels in the past month.

Further, we extended the industry-known "network health" state to account for resource health (e.g. the utilization of a DHCP sever, the utilization of an ARP table (or the number of entries). Resource and network health state is a function of the parameters that describes the health of the resources as well as network. Example of network health states includes network packet loss probability (PLP), *PLP(t,T)*. For example,

$$PLP(t,T) = (\sum_i y_i \cdot PLP\_Network\_Element\_i), \quad (2)$$

where y_i is the user-defined *PLP* weighting factor for the i^{th} network elements, $\sum_i y_i = 1$. Examples of Resource States includes DHCP server utilization, *DHCP_Util (t,T)*. For example,

$$DHCP\_Util(t,T) = (\sum_i w_i \cdot DHCP\_Util\_Network\_Element\_i), \quad (3)$$

where w_i is the user-defined *DHCP_Util* weighting factor for the i^{th} network elements, $\sum_i w_i = 1$. Based on *PLP(t,T)* and *DHCP_Util(t,T)*, PSC determines the network and resource health state. Other health parameters can include network latency, utilization, and other SLA parameters. In general, there can be m health states. The generation of the network health state is not the scope of this paper. This can be generated by other management applications.

The programmable administrative controller makes use of the alert state, user-risk level, and the network and resource health state and makes a decision when traffic analysis concludes the existence of a user malicious act. The decision is based on a set of programmable rules that maps all combinations of alert state, user-risk level, and network and resource health state into a set of pre-defined actions.

In this example, the network Alert State, *Alert(t,T),* is a function of the number illegal ARP request. The network and resource Health State, *Health(t,T),* is a function of PLP. Note that the threshold values depend on the network size and the type of services.

Alert Rules

Number of illegal ARP requests over *T*	**Alert State**
> 100	Critical
Between 50 and 100	High
Between 10 and 50	Medium
Below 10	Low

Network and Resource Rules

Network and Resource of the network (PLP)	**Health State**
> .01	Critical
Between .01 and .01	Good
Between .001 and .0001	Medium
Below 0.0001	High

User Risk Level

Number of alerts in the last 30 days	**User Risk State**
> 100	Critical
Between 50 and 100	High
Between 10 and 50	Medium
< 10	Low

Decision Rules

Alert State	**Health State**	**User Risk State**	**Decision**
Critical	Critical	Critical	Shutdown the malicious user access (e.g. port) immediately after the very first attack to prevent the network from possible crashing
High	Low	Critical	Send a warning message after the first attack (e.g. "*You have attempted to send an illegal ARP request.*

			Further attempts will cause your access will be terminated. Please call your network administrator if you have any questions"). If another illegal ARP request is attempted from the same port within *T*, the port will be terminated.
Medium	Good	Low	Send a warning message, e.g., "*You have attempted to send an illegal ARP request. Please call your network administrator if you have any questions*").

6 Conclusions

Metro Ethernet or Ethernet To The Home/Business is gaining significant momentum especially in Europe, Middle East and Asia Pacific. Security is a vital factor of success. By providing a secure network which is spoofing-free, it will increase the customer satisfaction and confidence in the service providers. This will ensure the wide acceptance of ETTx.

In this paper, we have used network management in conjunction with hardware features for security management and provide a secure and spoofing-free ETTx network. The key idea behind our proposal is to utilize network management to enforce strict (port, MAC, IP) binding in the access network to provide subscriber security. The main benefit is that the stringent requirement on sophisticated hardware security features is relieved, while at the same time, user traceability requirement can also be satisfied, which is becoming a legal requirements in many countries.

We have also proposed a policy-based security controller consisting of two major components: a user quarantine mechanism and a state-dependent decision making controller. The user quarantine mechanism isolates all users who are suspected of carrying out malicious acts so that accurate but lengthy traffic analysis can be carried out. Since suspected users are isolated, any further infliction will not affect the regular well-behaved users, and premature decisions can also be avoided. The state-dependent decision making controller provides a way to define granular levels of security violation and their corresponding correction actions that are adaptive to any defined network condition.

7 References

[1] "Mobile Services: Performance Management and Mobile Networks Application Note", *TeleManagement Forum, Member Evaluation* Version 1.0, November, 1999.
[2] "Security Workshop - Cisco Customer Summit, Iceland 2002", *Cisco Systems, Inc.*, 2002.
[3] http://www.monkey.org/~dugsong/dsniff.
[4] http://ettercap.sourceforge.net.

[5] "Cisco Catalyst Operating System Software Version 7.5(1) for the Cisco Catalyst 6500 Series and Cisco Catalyst 4000 Family Switches", *Cisco Systems, Inc.*, 2003.

[6] A. Rayes and M. Cheung, "Isolation Approach for Network Users Associated with Elevated Risk," U.S. Patent Application No. CPOL 335670, Issued on October 20, 2009, http://patft.uspto.gov/

[7] Mazu's Profiler, http://www.mazunetworks.com/solutions/white_papers/download/Mazu_Profiler.pdf, December 2003.

[8] Mazu's Enforcer, http://www.mazunetworks.com/solutions/white_papers/download/Mazu_Enforcer.pdf, March 2004.

[9] Y. T'Joens, C. Hublet, P. De Schrijver, "DHCP reconfigure extension", IETF RFC 3203, Dec. 2001.

[10] Policy-Based Security Management Controller," U.S. Patent No. 7,237,267, Issued on June 26, 2007, http://patft.uspto.gov/

[11] Designing Network Security, Mierike Kaeo, Cisco Press.

[12] A. Rayes and M. Cheung, "Security Management in IP Metro Ethernet / ETTx Networks," Proceedings of the 19thInternational Conference on Security and Management, vol. 1, pp. 183-189, June 2004, Las Vegas, Nevada, USA.

[13] A. Rayes and M. Cheung, "Intrusion Detection and Prevention in IP Metro Ethernet / ETTx Networks," Proceedings of the 20th International Conference on Security and Management, pp. 75-79, June 2003, Las Vegas, Nevada, USA.