sMAT – A Simplified MAC Address Translation Scheme

Stephan Kubisch, Harald Widiger, Dirk Timmermann
University of Rostock, Institute of Applied Microelectronics and CE
18051 Rostock, Germany
stephan.kubisch@uni-rostock.de

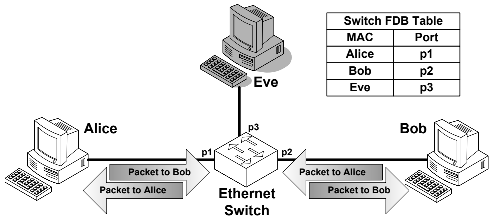
Daniel Duchow, Thomas Bahls
Nokia Siemens Networks
Siemensallee 1, 17489 Greifswald, Germany
daniel.duchow.ext@siemens.com

Keywords—Broadband Access, Security, Scalability

I. Introduction

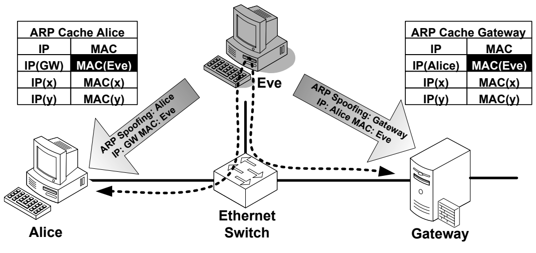
In Ethernet-based access networks, network security plays a more significant role than in ATM-based access environments. We assume that in the foreseeable future Internet access can be established *without* using the conventional Point-to-Point protocol. Various scenarios already envisage straightforward delivery of selected IP services over Ethernet, e.g., forwarding of multicast services in Ethernet-based DSL access networks [1]. Traffic will be switched on Layer 2 without any further traffic separation by protocol encapsulation (Figure 1). Thus, access segments will be prone to typical Layer 2 attacks: MAC Address Spoofing & Flooding and Address Resolution Protocol (ARP) Spoofing as illustrated in Figure 2. Furthermore, customers demand newfangled services. Providers satisfy these wishes with modern multimedia services. New technologies provide the required bandwidth, e.g., GDSL [2]. Thus, increasing traffic and workload must already be handled in the first aggregation levels of an access network. It is necessary to move functionality towards the customer edge and to decentralize.

Following, an approach for a *simplified* MAC Address Translation (sMAT) scheme for Ethernet-based DSL access networks is introduced. It addresses several relevant issues as discussed in [3]. sMAT focuses on security and scalability issues in Ethernet-based DSL access networks. We also propose its implementation in hardware due to performance reasons. All considerations refer to a generic Layer 2 Ethernet network model without VLANs, which would inherently eliminate certain Layer-2 attacks. But in given network scenarios, VLANs cannot be applied or are not suitable for customer separation purposes [3]. The limited number of VLAN-IDs leads to scalability problems in cascaded and aggregated networks with an increasing number of connected customers. Other mechanisms would also be feasible for port isolation but sMAT offers significant improvements compared to pure Layer 2 traffic segregation. Section 2 presents sMAT and Section 3 highlights important advantages before concluding the paper.



Switch FDB Table	
MAC	Port
Alice	p1
Bob	p2
Eve	p3

Fig. 1. Basic network scenario before attack


Eve
ARP Spoofing: Alice IP: GW MAC: Eve
ARP Spoofing: Gateway IP: Alice MAC: Eve
Alice
Ethernet Switch
Gateway

ARP Cache Alice	
IP	MAC
IP(GW)	MAC(Eve)
IP(x)	MAC(x)
IP(y)	MAC(y)

ARP Cache Gateway	
IP	MAC
IP(Alice)	MAC(Eve)
IP(x)	MAC(x)
IP(y)	MAC(y)

Fig. 2. Basic network scenario after ARP spoofing attack

II. sMAT – Simplified MAC Address Translation

sMAT is used to translate Layer 2 addresses (MACs). Thereby, client MACs (CMACs) are replaced with provider MACs (PMACs) and vice versa. Individual 1:1 translation targets security reasons. Flexible n:1 translation targets scalability. sMAT's mapping tables are of static nature to eliminate security leakages of dynamically updated ARP caches and Forwarding Database (FDB) tables (Figure 3). Each single PMAC is trustworthy and truly distinct across the whole access network. In principle, pure Layer 2 address translation can be applied at different positions in the access segment, e.g., behind the DSLAM's uplink-port as previously proposed in [4] and [5]. Here, we focus on a simplified, adapted, and local implementation (sMAT) on the DSL line cards. Port information, which exists only at this position, is used to limit the maximum legal number of MACs per port to a configurable value. Each line card manages an assigned pool of unique PMACs. Each CMAC is going to be translated. No MACs will be filtered or bypassed. Besides, certain protocols require a special treatment to ensure consistency because address information also exists within their payload, e.g., ARP and DHCP. PMAC assignment uses a static key consisting of MAC and IP. Additional key information like VLANs may also be considered in other scenarios. This way, CMACs and PMACs can unambiguously be translated in a 1:1 or n:1 manner in the up- and downstream. All in all, sMAT targets three goals:

Security (Un)intended attacks of subscribers against other subscribers within the same Layer 2 domain or against the (access) network are prevented. Using sMAT is not only restricted to the access area. It can be applied in all Ethernet LAN environments. Furthermore, security issues on higher layers, which base upon antecedent Layer 2 attacks, are *indirectly* suppressed. The uniqueness of MAC addresses is ensured due to the explicit mapping of CMACs and PMACs and vice versa.

Scalability With an n:1 mapping, the total number of MACs in the access and core segments is reduced. Thus, the number of addresses and therewith the workload in network equipment scales as well as the size of switching devices' FDBs. Table explosions and the likelihood of running into failopen modes, which may also be enforced by MAC flooding, are prevented.

Performance Due to its simple structure, sMAT is feasible for hardware implementation. A sample FPGA implementation of an MAT mechanism [4] shows high, non-blocking performance of up to 1 GBit/s and inserts only a negligible additional delay. On a typical line card, only small memory resources are needed for the MAT mapping tables (e.g., 72 ports*16 MACs/port*256 bit/entry=36 KB), which are available on low-cost FPGAs.

III. Summary of Advantages

Important advantages of sMAT are listed below.

Security:

- MAC Address Spoofing prevention: Source MACs will already be translated at network ingress
- MAC Flooding prevention: limiting the number of valid CMACs per port
- Prevention of failopen mode through MAC table explosions: see MAC Flooding
- Active ARP Spoofing prevention: ARP information will also be translated (Figure 2)
- Prevention of higher layer attacks, e.g., DNS Spoofing
- No duplicate MACs after translation
- sMAT mechanisms are fully transparent and thus not directly addressable or vulnerable.

Scalability

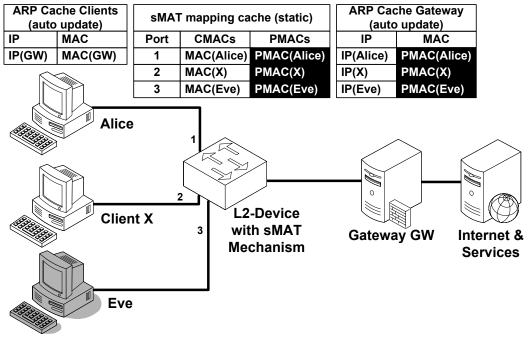
- Reducing the total number of MACs in the network by n:1 mapping
- No FDB overflow in subsequent network segments
- No overflow within sMAT module due to limiting the number of CMACs per port
- PMACs can be built using simple, structured schemes, e.g., a device-ID (line card ID) combined with an incremental part or more advanced structures.

Standard-compliant to IEEE 802.3

- Similar encapsulation schemes like MAC address stacking [6] or MAC-in-MAC [7] exist but modify the frame size and structure. sMAT does not modify size and structure.
- No functional extensions required in existing switching hardware

Miscellaneous

- Seamless integration due to transparency
- Unattended & maintenance-free
- Configuration at synthesis time
- Feasible for hardware implementation on DSL line cards, e.g., in ASICs or existing FPGAs (low costs)



ARP Cache Clients (auto update)	
IP	MAC
IP(GW)	MAC(GW)

sMAT mapping cache (static)		
Port	CMACs	PMACs
1	MAC(Alice)	PMAC(Alice)
2	MAC(X)	PMAC(X)
3	MAC(Eve)	PMAC(Eve)

ARP Cache Gateway (auto update)	
IP	MAC
IP(Alice)	PMAC(Alice)
IP(X)	PMAC(X)
IP(Eve)	PMAC(Eve)

Fig. 3. Basic network scenario with sMAT mechanisms

- Operation at wire speed with very low latency

IV. Conclusion

This paper presented sMAT, which is a simplified MAC address translation mechanism. sMAT is intended to be integrated as a small hardware module on DSL line cards. At this peripheral position, it decentralizes core functionality, purifies and preprocesses traffic for the further access network and core segment, and provides an extensive set of features and advantages with just little effort and at low costs. A sample implementation in an FPGA showed high performance and low additional latency. Currently, sMAT is implemented as a maintenance-free mechanism configured at synthesis time. If desired, the functionality can be enhanced with a configuration interface. Future considerations also comprise the use of hierarchically structured PMACs. Therewith, the required memory can be reduced, memory operations can be accelerated, and MACs can be associated with their origin in the network environment without further information.

We look forward to interesting discussions of the pros and cons of sMAT on the poster, which will give further information.

Acknowledgment

We thank Nokia Siemens Networks, location Greifswald, Germany, for support and cooperation in this project.

References

[1] S. Ooghe, "IPTV Architecture Overview," in *TSB Director's Consultation Meeting on IPTV Standardization*, Geneva, Switzerland, April 4-5 2006.

[2] J. Cioffi et al., "Vectored DSLs with DSM: the road to ubiquitous gigabit DSLs," in *Proc. of the World Telecommunications Congress 2006 (WTC06)*, Budapest, Hungary, April 30-May 3 2006.

[3] DSL Forum, "Migration to Ethernet-based DSL Aggregation," April 2006, Technical Report TR-101.

[4] S. Kubisch, H. Widiger, D. Duchow, D. Timmermann, and T. Bahls, "Wirespeed MAC Address Translation and Traffic Management in Access Networks," in *Proc. of the World Telecommunications Congress 2006 (WTC'06)*, Budapest, Hungary, April 30-May 3 2006.

[5] H. Widiger, S. Kubisch, D. Timmermann, and T. Bahls, "An Integrated Hardware Solution for MAT, MPLS-UNI, and TM in Access Networks," in *Proc. of the 31st IEEE Conf. on Local Computer Networks (LCN)*, Tampa, FL, USA, November 2006.

[6] G. Chiruvolu, A. Ge, D. Elie-Dit-Cosaque, M. Ali, and J. Rouyer, "Issues and Approaches on Extending Ethernet Beyond LANs," *IEEE Communications Magazine*, pp. 80–86, March 2004.

[7] Nortel Networks, "Service Delivery Technologies for Metro Ethernet Networks," 2003, White Paper.