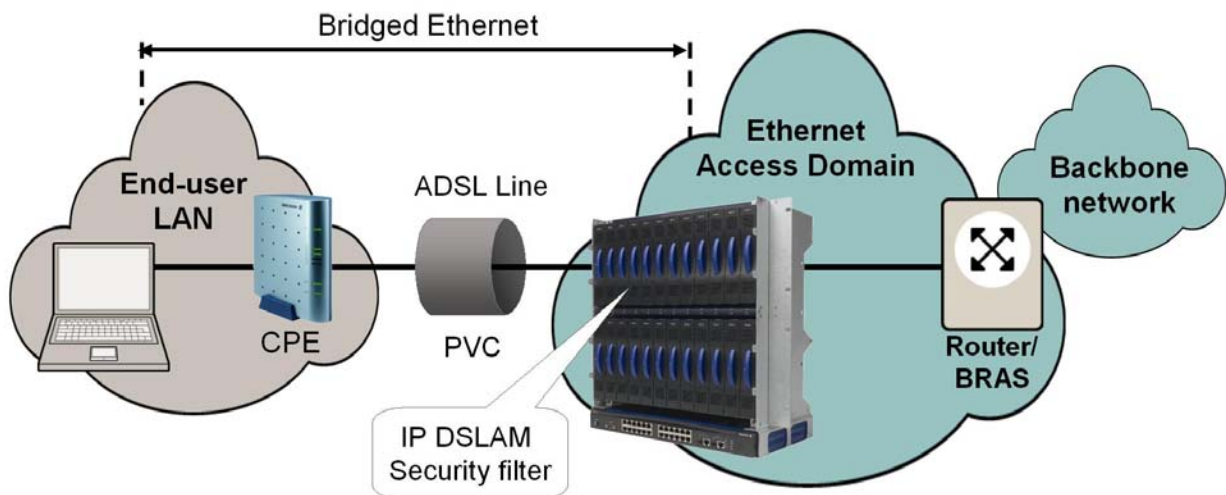


# SECURITY IN THE EDA NETWORK

EDA 2.2



## Introduction

The ability to protect information and communication systems from various types of attacks has become increasingly important. As the use of the Internet spreads, hackers become more and more skilled and are now equipped with numerous tools to perform a multitude of attacks on data networks.

## Ethernet security issues

The EDA concept is based on Ethernet as the transport media in the Access Domain between the IP DSLAM or IP MSAN node and the Router/BRAS in the backbone. In addition to threats imposed to general IP networks, security issues are imposed by the use of Ethernet.

The bridging functionality of the IP DSLAM creates a common virtual LAN covering both the Ethernet Access Domain network and the end-user's network. As this creates simple and flexible network architecture, it also introduces some potential security issues to be addressed by the EDA system.

The nature of a broadcast media like Ethernet implies that information is distributed to multiple entities connected to the media, including some that are not the intended receivers. This may be acceptable in a corporate LAN environment, but in an access scenario like EDA, it must be ensured that end-users will only receive information that is explicitly intended for them.

Sharing Ethernet as media for management traffic as well as traffic for all end-users requires that the system provides security mechanisms that ensure the privacy and integrity of the transported data. Consequently, the EDA concept includes mechanisms to handle any type of attack on the system, including attacks on EDA system nodes within the Ethernet Access Domain and on data conveyed via the EDA network.

### Filtering in the IP DSLAM

EDA IP DSLAMs are able to perform filtering and other functions that ensure security and privacy. Filtering makes it possible to control the traffic to and from ADSL end-users by restricting the types of frames/packets forwarded by the IP DSLAM. The filtering is done on top of Layer 2 based on Layer 2 (Ethernet) and Layer 3 (IP) information as shown in the figure below.

The filtering policy can be based on a wide set of possible rules. Consequently, a filter tailored to a specific deployment scenario can later be updated on the fly if a security risk is discovered via the EDA management system, the Public Ethernet Manger (PEM). The filters are individually configurable per PVC on the ADSL line.

### Broadcast and multicast traffic

In general, broadcast and multicast traffic can be filtered out. This filtering prevents end-users from loading the Ethernet access network with broadcast traffic from their LAN networks. It also prevents that network broadcast messages in an Ethernet access network are sent to the end-users.

### Source MAC/IP address

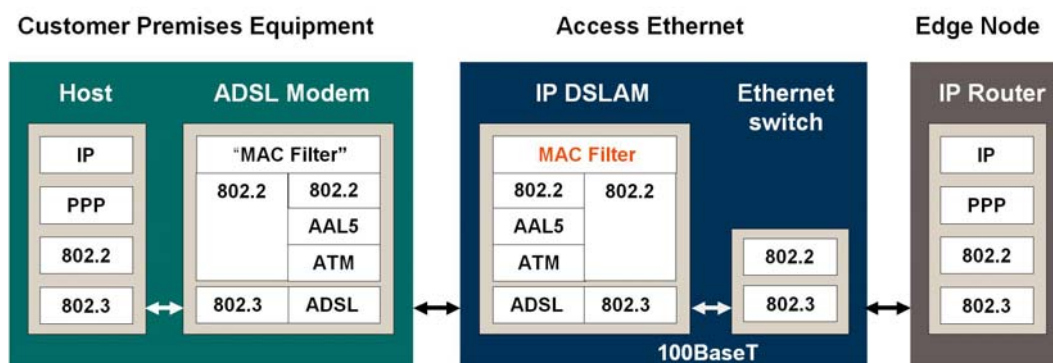
To prevent end-users from spoofing the source MAC and IP address in upstream traffic, each end-user can be verified as belonging to a set of addresses. The IP DSLAM stores the valid combinations of MAC addresses and IP addresses for each end-user in a MAC table. Entries can be created based on the DHCP responses from the DHCP server. A specific end-user MAC address is then stored as belonging to a specific IP address assigned from the DHCP server, and only this combination is allowed access through the filter.

### Destination MAC/IP address

To prevent attack on EDA system nodes it is possible to filter out upstream packets towards illegal addresses.

### Ethernet frame type

Ethernet frame type can be limited to acceptable frame types in both directions, for example to Ethernet frames carrying IP traffic.



## Layer 2 separation

The Ethernet Access Domain traffic is separated by use of VLANs according to IEEE 802.1Q. The figure below shows a basic use of VLAN for separation of traffic types in order to enhance the security and offer service selection of the EDA system.

The Ethernet Access Domain enables direct Layer 2 communication between EDA subscribers if they are using the same VLAN. This is considered an advantage in some scenarios, but normally it is necessary to prevent direct Layer 2 communication between subscribers. Management traffic is isolated from the end-user traffic by use of a separate VLAN for management of the EDA system.

Without any Layer 2 separation, hosts connected to the same VLAN can communicate directly with each other if they know the other party's MAC address. The host can see if the other party is on the same VLAN by looking at the subnet mask. If the other party's IP address is located within the same subnet, then the sender can obtain the destination MAC address by an Address Resolution Protocol (ARP) request.

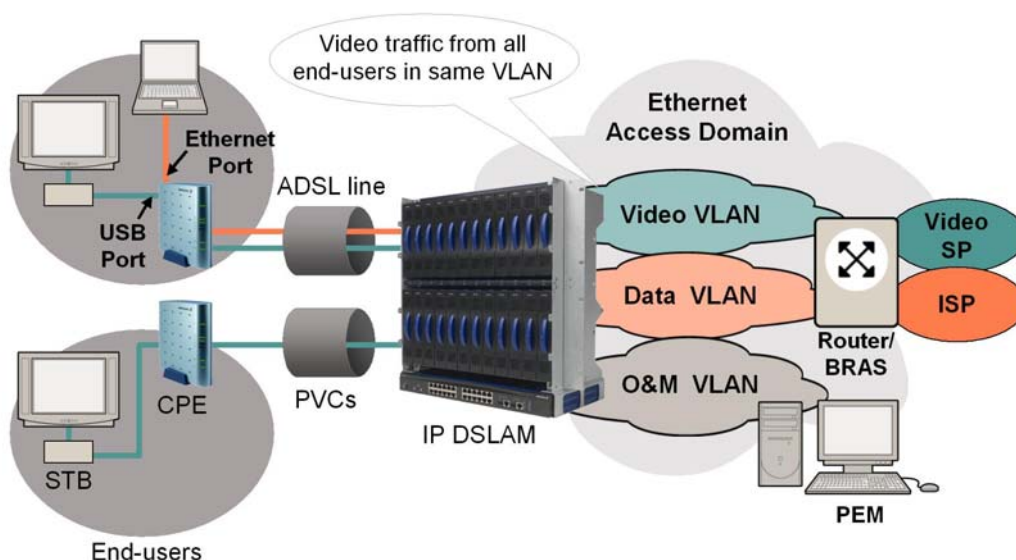
## Forced Forwarding

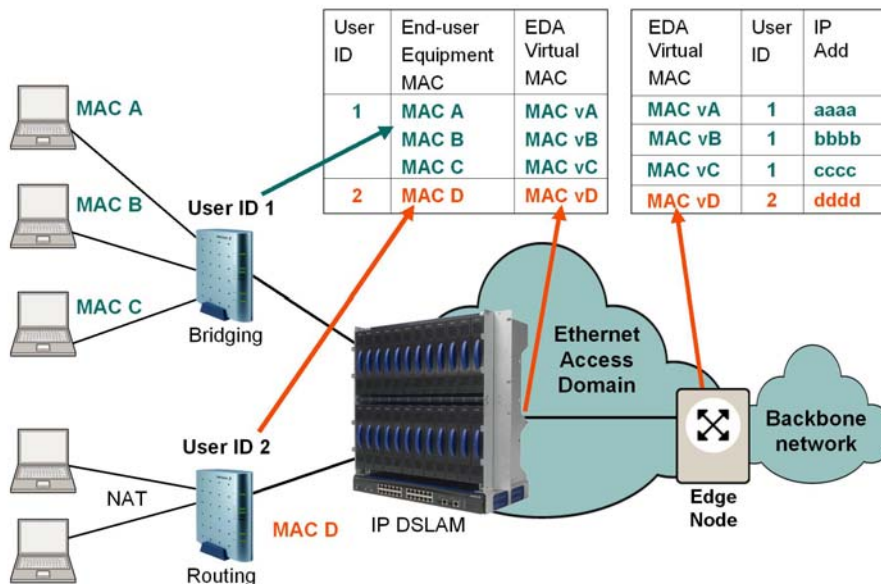
To create Layer 2 separation, the EDA system offers a feature called Forced Forwarding that prevents visibility between the end-users. Forced Forwarding is an EDA-specific technique in which the end-user is forced to use the router as default gateway for all upstream traffic.

The Layer 2 separation is done by an ARP proxy function in the IP DSLAM. If End-user 1 tries to communicate with End-user 2 within the same VLAN, End-user 1 will issue an ARP request to get the destination MAC address. However, the ARP proxy will respond to the ARP request with the MAC address of the default gateway instead of the MAC address of End-user 2. In this way, the requesting End-user 1 will now forward the traffic via the default gateway, believing that it is in fact End-user 2.

For this mechanism to work properly, the default gateway must be configured to accept and forward (or actually return) traffic between hosts within the same subnet. The IP DSLAM will verify that the upstream traffic actually uses the returned MAC address of the default gateway as destination address in Ethernet frames.

The ARP proxy functionality implementing Forced Forwarding is an optional security feature that ensures Layer 2 separation (rules for Forced Forwarding is configurable through the EDA management system).





### Virtual MAC address

To prevent MAC spoofing and to be able to uniquely identify an end-user in the EDA access system, the EDA solution offers an optional security feature called Virtual MAC address.

The basic principle of Virtual MAC address is that the IP DSLAM performs address translation of MAC addresses. The IP DSLAM pre-assigns a number of potential MAC addresses to be associated with the real MAC address of the end-user's equipment (such as a computer for data services or a set-top box for video services).

The IP DSLAM maps between the MAC addresses received from the end-user's equipment and the locally administered MAC (Virtual MAC) address used in the Ethernet Access Domain as shown in the figure below.

For upstream traffic, the source MAC address from the end-user is replaced with its corresponding locally administered address and forwarded to the aggregation switch. For downstream traffic, the locally administered address is replaced with its corresponding end-user MAC address and forwarded to the ADSL line.

In this way, it makes no difference if multiple end-user equipment is configured with the same MAC address (spoofing); these addresses are never used within the Access Domain.

The Virtual MAC addresses are of the category "Locally administered", that is, bit 2 of the MAC address is '1'. The remaining 46 bits (~70,000 billion addresses) are free to be used for the internal MAC addresses. The actual address value is in principle unimportant, as long as two different IP DSLAMs cannot assign the same internal MAC address to different subscribers.

The use of the Virtual MAC address function in the EDA solution is implemented in a way that makes it very easy to use and manage. Virtual MAC addresses are statically assigned by the IP DSLAM and allow the operator to control and limit the number of equipment that the end-user is able to connect to the ADSL line (per PVC).

The Virtual MAC function gives the ability to uniquely identify the end-user traffic in the EDA access network by looking at the Virtual MAC address in the Ethernet frame, as this is traceable to the specific PVC on the end-user's ADSL line.