Application Note
Use of Access Control Lists (ACLs) on EDS500 family
Table of Content

1 Introduction ......................................................................................................................... 3
   1.1 Motivation ..................................................................................................................... 3
   1.2 Classification of Network Traffic ............................................................................... 3
   1.3 Technical Considerations .......................................................................................... 3

2 Configuration ....................................................................................................................... 4
   2.1 Setup ............................................................................................................................ 4
   2.2 Technical Background ............................................................................................... 4
   2.3 Applying Incoming Filters ........................................................................................ 5
   2.4 Configuring Incoming Access List .............................................................................. 5
   2.5 Assigning Incoming Access List ................................................................................ 6
   2.6 Optional: Applying Outgoing Filters ......................................................................... 6
   2.7 Optional: Configuring Outgoing Access List ............................................................ 6
   2.8 Optional: Assigning Outgoing Access List ............................................................... 7
   2.9 Configuration File ...................................................................................................... 7

3 Verifying operation ............................................................................................................. 8
   3.1 Verification of configuration and operation .............................................................. 8

4 Ordering Information ......................................................................................................... 9

5 References ........................................................................................................................... 10
Introduction

This document describes the settings required to configure packet filtering using access control lists. The feature is available on all EDS500 managed Ethernet products, namely 500NMD and 560NMS series of DIN rail and rack mount Ethernet products.

1.1 Motivation

Operators of networks used in critical infrastructure applications like the energy grid experience a growing demand of security functions. This includes physical protection of premises but also electronic measures to monitor and regulate access to local and wide area networks. ABBs Ethernet and SHDSL switches of the EDS500 series help to protect the network not only by access control for users and end devices, the switches also allow to filter traffic where it is generated – at the edge of the network.

1.2 Classification of Network Traffic

Network traffic in EDS500 switches (500NMD and 560NMS series) can be filtered by different user-defined criteria. This includes layer 2 properties like MAC addresses or protocols as well as layer 4 port numbers. Table 1 shows a list of properties supported.

<table>
<thead>
<tr>
<th>ISO/OSI Layer</th>
<th>Properties (filter criteria)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Layer</td>
<td>Source MAC, Destination MAC, Ethertype, VLAN</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Source IP, Destination IP, Protocol</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>TCP Source Port, TCP Destination Port,</td>
</tr>
<tr>
<td></td>
<td>UDP Source Port, UDP Destination Port</td>
</tr>
</tbody>
</table>

Table 1: Traffic Classification

The classification is realized via white- or blacklists that can be applied to one or more ports in incoming or outgoing direction. Source IP and destination IP can also be networks. If no subnet mask is given during configuration a host address is assumed.

1.3 Technical Considerations

If access control lists are enabled on a port all traffic is inspected by the CPU and checked against the rules defined. Depending on these rule(s) the packet is either discarded or forwarded. The implemented packet filtering technologies does exactly what is defined by the user. There are no implicit assumptions. This significantly increases security and controllability; however, it also means that if you whitelist a certain IP based protocol make sure to include ARP (IP to MAC address resolution) for communication to work (refer to chapter 2.2 and following).
# 2 Configuration

## 2.1 Setup

Chapter 2 describes the limitation to IEC-104 traffic on a 500NMD device. The RTU is connected to 500NMD via Port 1. The uplink to the control center using an TCP/IP network can be done via any of the other ports including optical fiber or SHDSL.

![IEC conversion setup](image1.png)

**Figure 1: IEC conversion setup**

The IEC 60870-5-104 standard defines TCP server port 2404 for communication. In Figure 1 the RTU therefore listens on port 2404 for IEC-104 messages while the control center may use any TCP port available.

## 2.2 Technical Background

For the filtering to work proper knowledge of the working fundamentals of TCP/IP is required. Figure 2 shows a typical abstracted logical setup. In the connection establishment phase to the RTU the router needs to resolve the IP address of the RTU to a MAC address to start communication. This is done via the Address Resolution Protocol (ARP); ARP is not an IP protocol, it is encapsulated directly in an Ethernet frame and is based on a broadcast mechanism.

![TCP Connection process](image2.png)

**Figure 2: TCP Connection process**

After address resolution is complete the IP connection phase starts. The initial packet is sent from the control center to IP 192.168.10.56, TCP port 2404 of the RTU. After the RTU has answered and the control center has acknowledged, the connection is established, and IEC messages can be transferred.

If a router does not exist in the network the ARP function would be performed directly by the control center.
2.3 Applying Incoming Filters

The access control list to be applied is configured as whitelist (all traffic conforming to the list allowed, all other traffic is denied). Elements within one rule are connected by a logical AND, while different rules are connected by a logical OR.

- **Rule 1**: Allow if
  IP source is 192.168.10.56 (RTU IP address)
  AND IP destination is 192.168.1.4 (Control center IP address)
  AND TCP source port is 2404 (IEC 60870-5-104 port number)

- **Rule 2**: Allow if
  protocol is ARP (Address Resolution for IP)

The rules can be set more restrictive e.g. by adding MAC address filtering. If a second control center is present an additional rule (rule 3) is required containing the second control center IP. The operation performed in the example is:

If rule 1 OR rule 2 is matches the packet is forwarded, otherwise it is discarded

During configuration the rules are linked to an access list number. The access list itself must finally be applied to a certain port or interface in incoming or outgoing direction. In the example the access list is applied in incoming direction to the port the RTU is connected to.

2.4 Configuring Incoming Access List

The configuration of the access list is performed by the following tasks. The access list number has been defined to be “1”.

**Tasks**

<table>
<thead>
<tr>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set first condition of rule 1 within access list 1.</td>
<td>access-list 1 permit-rule 1 ip source 192.168.10.56</td>
</tr>
<tr>
<td>Set second condition of rule 1 within access list 1.</td>
<td>access-list 1 permit-rule 1 ip destination 192.168.1.4</td>
</tr>
<tr>
<td>Set third condition of rule 1 within access list 1.</td>
<td>access-list 1 permit-rule 1 tcp src-port 2404</td>
</tr>
<tr>
<td>Set first condition of rule 2 within access list 1.</td>
<td>access-list 1 permit-rule 2 ethertype arp</td>
</tr>
</tbody>
</table>
2.5 Assigning Incoming Access List

Finally, the access list is assigned to Port 1 (the RTU is connected to Port 1) in incoming direction, meaning that all traffic originating from the RTU is filtered.

Tasks

<table>
<thead>
<tr>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign access list 1 to Port 1.</td>
<td>set switch port1 acl 1 in</td>
</tr>
</tbody>
</table>

2.6 Optional: Applying Outgoing Filters

Usually a network can be protected by filtering any inbound to traffic to the network at the edge and use firewalls at the core or distribution area. In some configurations and topologies, also outgoing access lists at the edge are used to protect end devices from misconfiguration or to prohibit connectionless unicast traffic. In this example an outgoing access control (whitelist) is configured. In general, the structure and syntax of the rules is identical to incoming elements. Moreover, an access list can also be applied to multiple interfaces or ports in incoming and/or outgoing direction.

- Rule 1: Allow if
  - IP destination is 192.168.10.56 (RTU IP address)
  - AND IP source is 192.168.1.4 (Control center IP address)
  - AND TCP destination port is 2404 (IEC 60870-5-104 port number)

- Rule 2: Allow if
  - protocol is ARP (Address Resolution for IP)

The rules can be set more restrictive e.g. by adding MAC address filtering. If a second control center is present an additional rule (rule 3) is required containing the second control center IP.

The operation performed in the example is:

If rule 1 OR rule 2 is matches the packet is forwarded, otherwise it is discarded

During configuration the rules are linked to an access list number. The access list itself must finally be applied to a certain port or interface in incoming or outgoing direction. In the example the access list is applied in incoming direction to the port the RTU is connected to.

2.7 Optional: Configuring Outgoing Access List

The configuration of the access list is performed by the following tasks. The access list number has been defined to be “2”. In the example access list number “1” is already in use by the incoming access list.

Tasks

<table>
<thead>
<tr>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set first condition of rule 1 within access list 2.</td>
<td>access-list 2 permit-rule 1 ip destination 192.168.10.56</td>
</tr>
<tr>
<td>Set second condition of rule 1 within access list 2.</td>
<td></td>
</tr>
</tbody>
</table>
Set third condition of rule 1 within access list 2.

```
access-list 2 permit-rule 1 ip source 192.168.1.4
```

Set first condition of rule 2 within access list 2.

```
access-list 2 permit-rule 2 ethertype arp
```

## 2.8 Optional: Assigning Outgoing Access List

Finally, the access list is assigned to Port 1 (the RTU is connected to Port 1) in incoming direction, meaning that all traffic originating from the RTU is filtered.

### Tasks

<table>
<thead>
<tr>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign access list 1 to Port 1.</td>
<td>set switch port1 acl 1 in</td>
</tr>
<tr>
<td>Assign access list 2 to Port 1.</td>
<td>set switch port1 acl 2 out</td>
</tr>
</tbody>
</table>

## 2.9 Configuration File

The listing below represents the configuration file.

```
! version 2.0
! common
access-list 1 permit-rule 1 ip destination 192.168.1.4
access-list 1 permit-rule 1 ip source 192.168.10.56
access-list 1 permit-rule 1 tcp src-port 2404
access-list 1 permit-rule 2 ethertype arp
access-list 2 permit-rule 1 ip destination 192.168.10.56
access-list 2 permit-rule 1 ip source 192.168.1.4
access-list 2 permit-rule 1 tcp dst-port 2404
access-list 2 permit-rule 2 ethertype arp
set switch port1 acl 1 in
set switch port1 acl 2 out
set system gateway 192.168.10.1
set system ip 192.168.10.46
set system subnetmask 255.255.255.0
! interface state
set switch port1 no shutdown
set switch port2 no shutdown
set switch port3 no shutdown
set switch port4 no shutdown
```
### 3 Verifying operation

There are several commands to verify the operation of packet filtering using access control lists conversion.

#### 3.1 Verification of configuration and operation

<table>
<thead>
<tr>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display access list assignments to ports and interfaces.</td>
<td>show access-list</td>
</tr>
<tr>
<td>Display access list rules and match statistics.</td>
<td>show access-list &lt;number&gt;</td>
</tr>
</tbody>
</table>
## Ordering Information

For order numbers regarding 500NMDxx the table below can be used.

<table>
<thead>
<tr>
<th>Product</th>
<th>Ident No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>500NMD01</td>
<td>1KHW025096R0002</td>
<td>4xRJ-45, 1xSHDSL, 1xRS-232</td>
</tr>
<tr>
<td>500NMD02</td>
<td>1KHW025097R0002</td>
<td>4xRJ-45, 2xSHDSL, 2xRS-232</td>
</tr>
<tr>
<td>500NMD11</td>
<td>1KHW027869R0002</td>
<td>4xRJ-45, 1xSHDSL, 1xSFP, 2xRS-232</td>
</tr>
<tr>
<td>500NMD20</td>
<td>1KHW025098R0002</td>
<td>4xRJ-45, 2xSFP, 2xRS-232</td>
</tr>
<tr>
<td>500NMD30</td>
<td>1KGT038890R0002</td>
<td>4xRJ-45, 1xRS-232</td>
</tr>
<tr>
<td>500NMD40</td>
<td>1KGT038891R0001</td>
<td>4xRJ-45, 1xRS-232, POE 280W</td>
</tr>
<tr>
<td>500NMD40</td>
<td>1KGT038891R0002</td>
<td>4xRJ-45, 1xRS-232, POE 36W</td>
</tr>
<tr>
<td>500NMD41</td>
<td>1KGT038892R0001</td>
<td>4xRJ-45, 1xSHDSL, 1xRS-232, POE 280W</td>
</tr>
<tr>
<td>500NMD41</td>
<td>1KGT038892R0002</td>
<td>4xRJ-45, 1xSHDSL, 1xRS-232, POE 36W</td>
</tr>
<tr>
<td>500NMD42</td>
<td>1KGT038893R0001</td>
<td>4xRJ-45, 2xSHDSL, 2xRS-232, POE 280W</td>
</tr>
<tr>
<td>500NMD42</td>
<td>1KGT038893R0002</td>
<td>4xRJ-45, 2xSHDSL, 2xRS-232, POE 36W</td>
</tr>
<tr>
<td>500NMD43</td>
<td>1KGT038894R0001</td>
<td>4xRJ-45, 1xSHDSL, 1xSFP, 2xRS-232, POE 280W</td>
</tr>
<tr>
<td>500NMD43</td>
<td>1KGT038894R0002</td>
<td>4xRJ-45, 1xSHDSL, 1xSFP, 2xRS-232, POE 36W</td>
</tr>
<tr>
<td>500NMD44</td>
<td>1KGT038895R0001</td>
<td>4xRJ-45, 2xSFP, 2xRS-232, POE 280W</td>
</tr>
<tr>
<td>500NMD44</td>
<td>1KGT038895R0002</td>
<td>4xRJ-45, 2xSFP, 2xRS-232, POE 36W</td>
</tr>
<tr>
<td>500CAB03</td>
<td>1KGT038909R0001</td>
<td>Serial configuration cable DB9-F</td>
</tr>
<tr>
<td>500CAB05</td>
<td>1KGT038911R0001</td>
<td>Shielded serial cable DB25-F</td>
</tr>
<tr>
<td>500CAB06</td>
<td>1KGT038912R0001</td>
<td>Shielded serial cable DB9-F</td>
</tr>
<tr>
<td>500CAB09</td>
<td>1KGT038916R0001</td>
<td>RTU500 connection cable RJ-45</td>
</tr>
<tr>
<td>500NMA01</td>
<td>1KGT038909R0001</td>
<td>Configuration stick</td>
</tr>
</tbody>
</table>
5 References

<table>
<thead>
<tr>
<th>Product</th>
<th>Reference(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>500NMDxx</td>
<td>Presentation</td>
</tr>
<tr>
<td>500NMDxx</td>
<td>Brochure</td>
</tr>
</tbody>
</table>

Contact

Technical questions: de-eds-sales-support@abb.com
Comercial topics, orders: substationautomation-products@de.abb.com
We reserve the right to at all times make technical changes as well as changes to the contents of this document without prior notice.
The detailed specifications agreed to at the time of ordering apply to all orders.
ABB accepts no responsibility for possible errors or incompleteness in this document.
We reserve all rights to this document and the topics and illustrations contained therein. The document and its contents, or extracts thereof, must not be reproduced, transmitted or reused by third parties without prior written consent by ABB.
All rights reserved.