Traffic Measurement and Analysis of Building Automation and Control Networks

Radek Krejčí, Pavel Čeleda, Jakub Dobrovolný

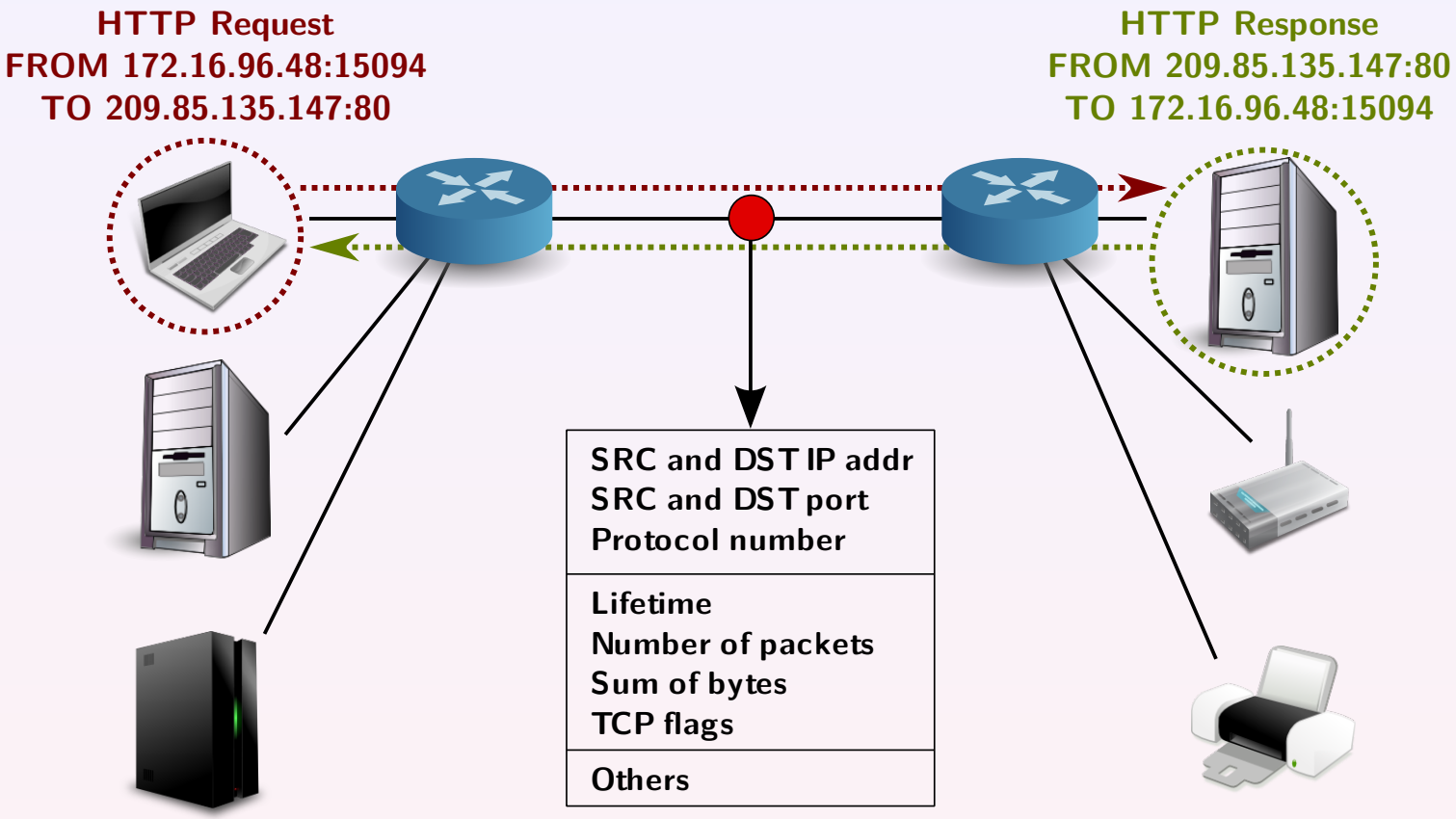
rkrejci@cesnet.cz, {celeda|dobrovolny}@ics.muni.cz

AIMS 2012 - 6th International Conference on Autonomous Infrastructure, Management and Security, 4-8 June 2012, Luxembourg

Part I

Building Automation and Control Network Monitoring

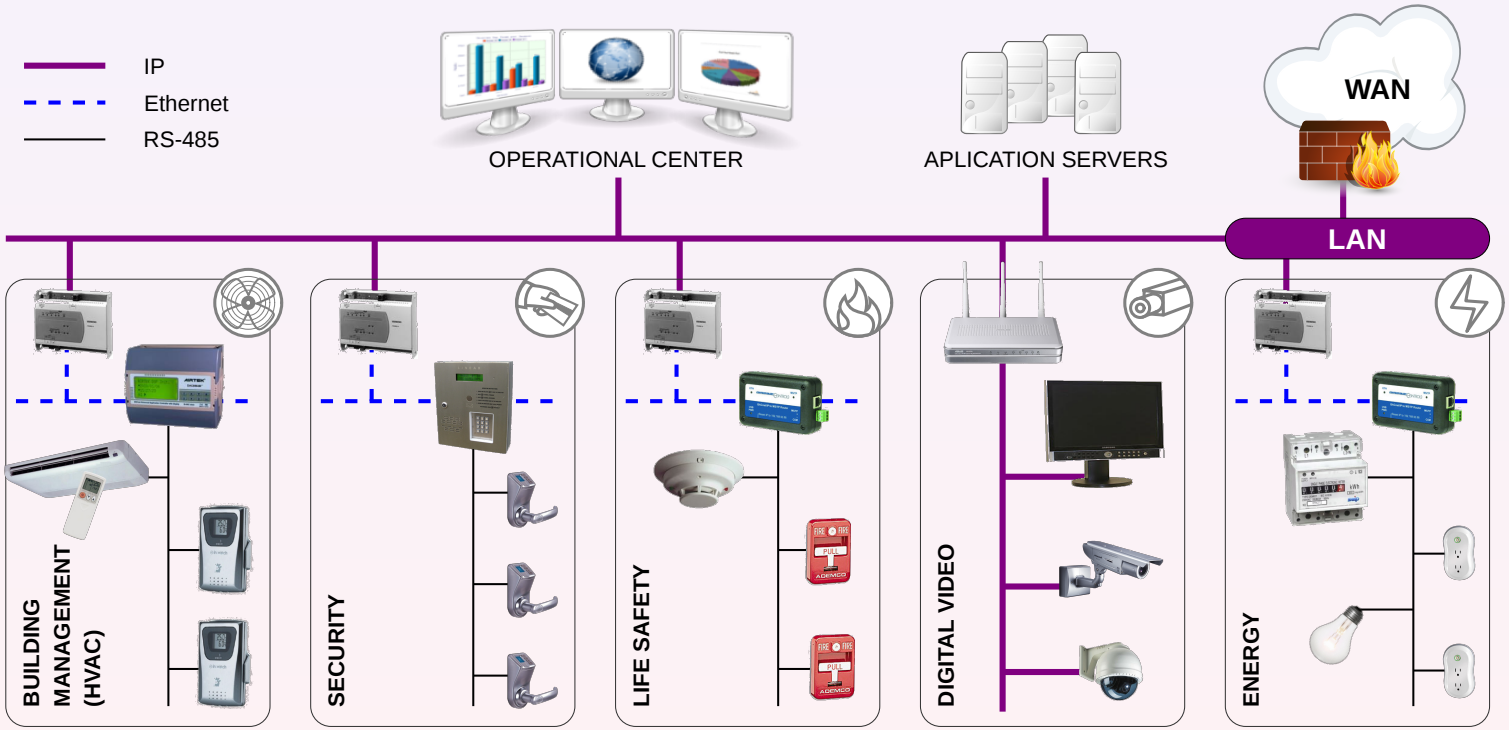
IP Flow Monitoring



Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes
09:41:21.763	0.101	TCP	172.16.96.48:15094	->	209.85.135.147:80	.AP.SF	4	715
09:41:21.893	0.031	TCP	209.85.135.147:80	->	172.16.96.48:15094	.AP.SF	4	1594

What About Special Networks?

- Building Management System (BMS) networks
- Supervisory Control And Data Acquisition (SCADA) networks



Network Monitoring in Special Environment

Active Monitoring – SNMP polling, ICMP ping

- Nagios
- Zabbix

Network Monitoring in Special Environment

Active Monitoring – SNMP polling, ICMP ping

- Nagios
- Zabbix

Deep Packet Inspection

- Specialized Firewalls (BACnet Firewall Router)
- Intrusion Detection/Prevention Systems

Network Monitoring in Special Environment

Active Monitoring – SNMP polling, ICMP ping

- Nagios
- Zabbix

Deep Packet Inspection

- Specialized Firewalls (BACnet Firewall Router)
- Intrusion Detection/Prevention Systems

Flow Monitoring

- Barbosa et al. (University of Twente)
- Using standard NetFlow – limited to IP only.

BMS Network Environment

BACnet Protocol

- Communication protocol for BMS networks.
- ASHRAE standard 135 – U.S. standard, adapted by ISO, EU.
- Various protocols used at transport layer:
  - LonTalk, MS/TP, Ethernet, Ethernet/IP, ZigBee, ...
- Contains key information about BMS network traffic.

BMS Network Environment

BACnet Protocol

- Communication protocol for BMS networks.
- ASHRAE standard 135 – U.S. standard, adapted by ISO, EU.
- Various protocols used at transport layer:
  - LonTalk, MS/TP, Ethernet, Ethernet/IP, ZigBee, ...
- Contains key information about BMS network traffic.

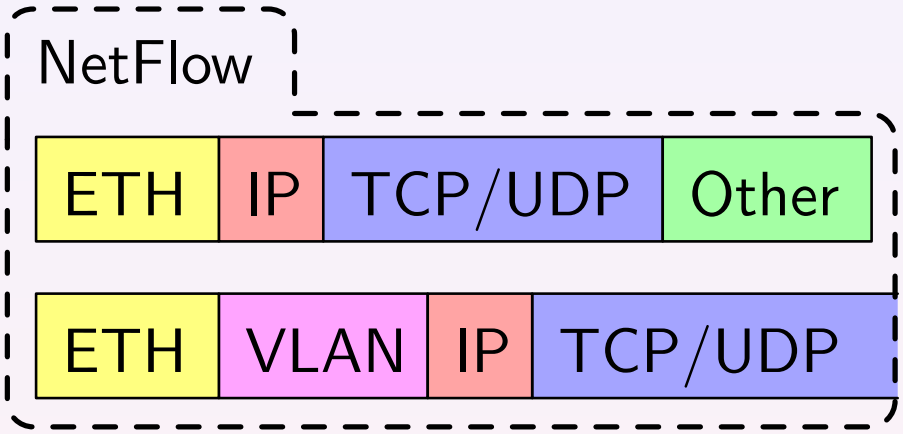
Need of modification of IP flow for the BACnet environment

BACnetFlow

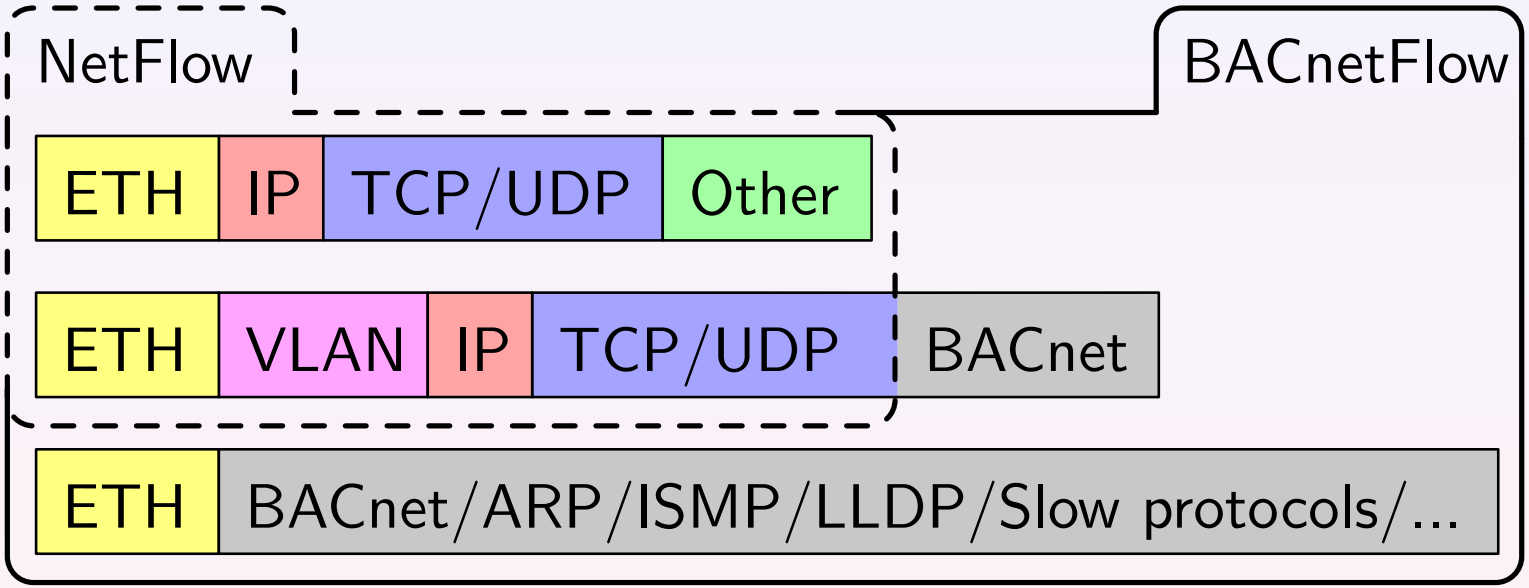
Part II

BACnetFlow

NetFlow vs. BACnetFlow



NetFlow vs. BACnetFlow

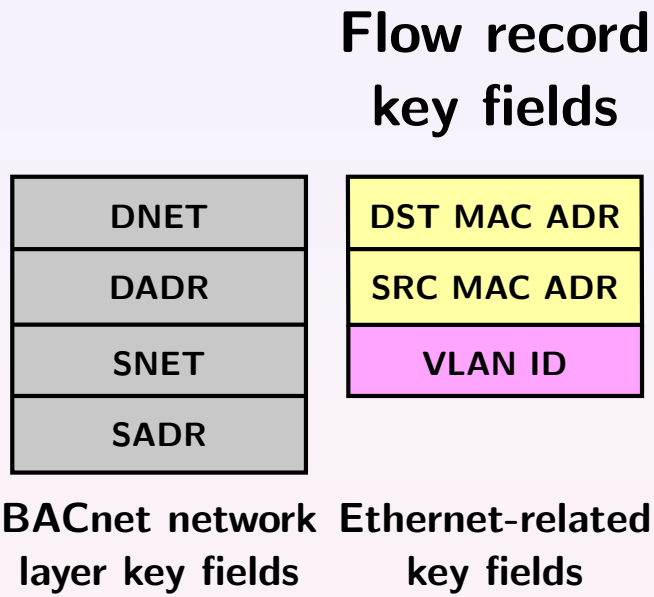


BACnetFlow

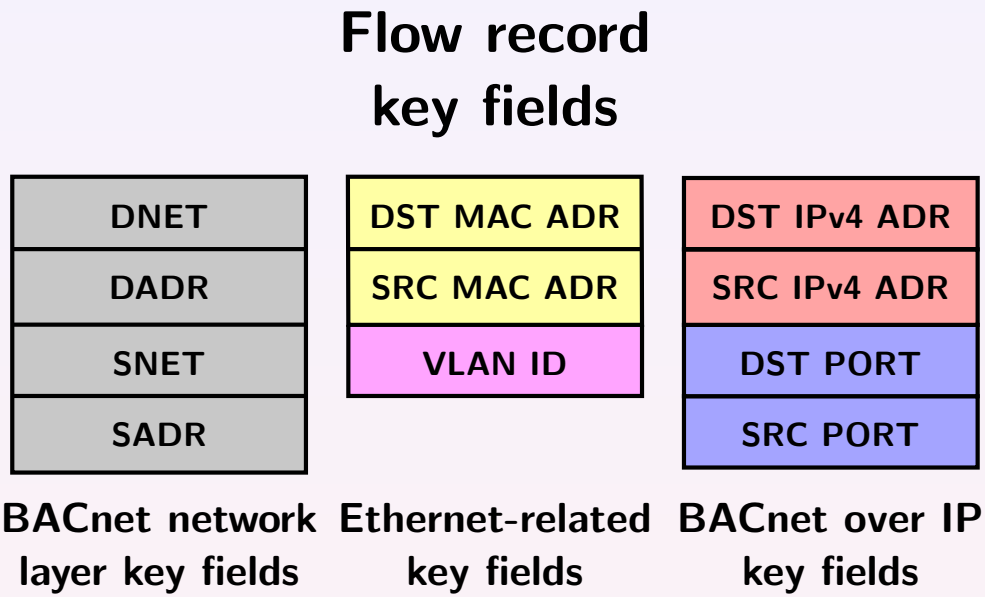
Flow record key fields

BACnet network layer key fields

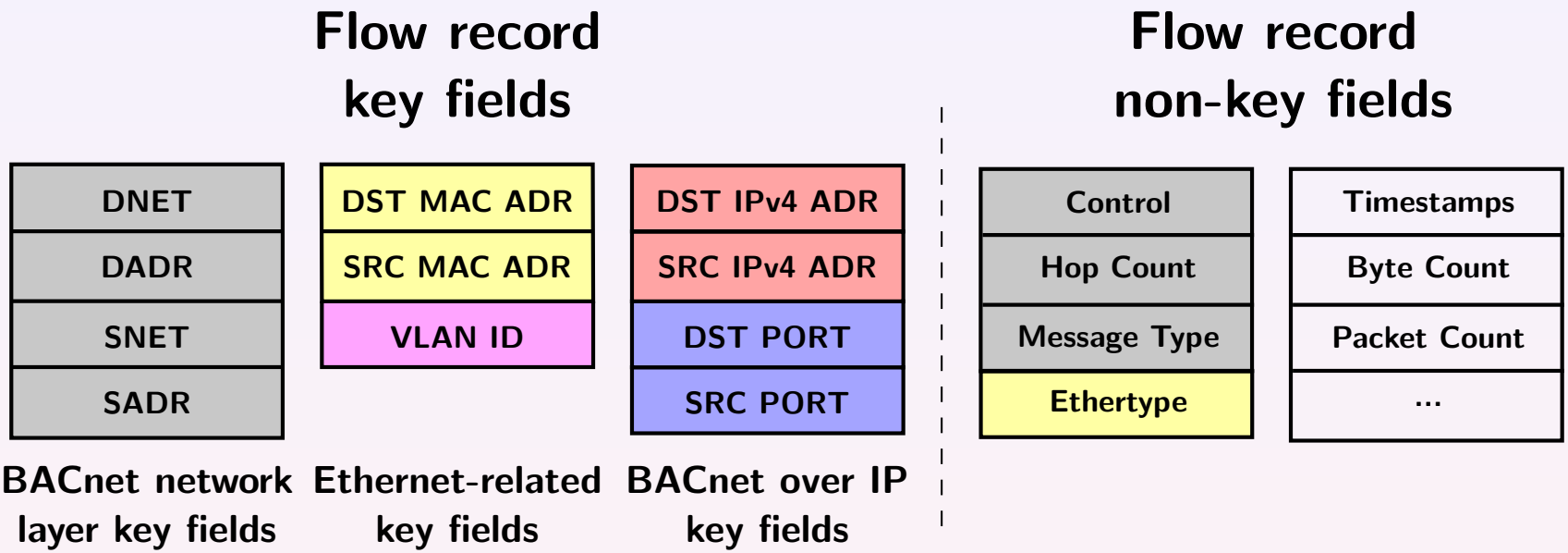
BACnetFlow


Flow record key fields
DNET
DADR
SNET
SADR
DST MAC ADR
SRC MAC ADR
VLAN ID
BACnet network layer key fields
Ethernet-related key fields

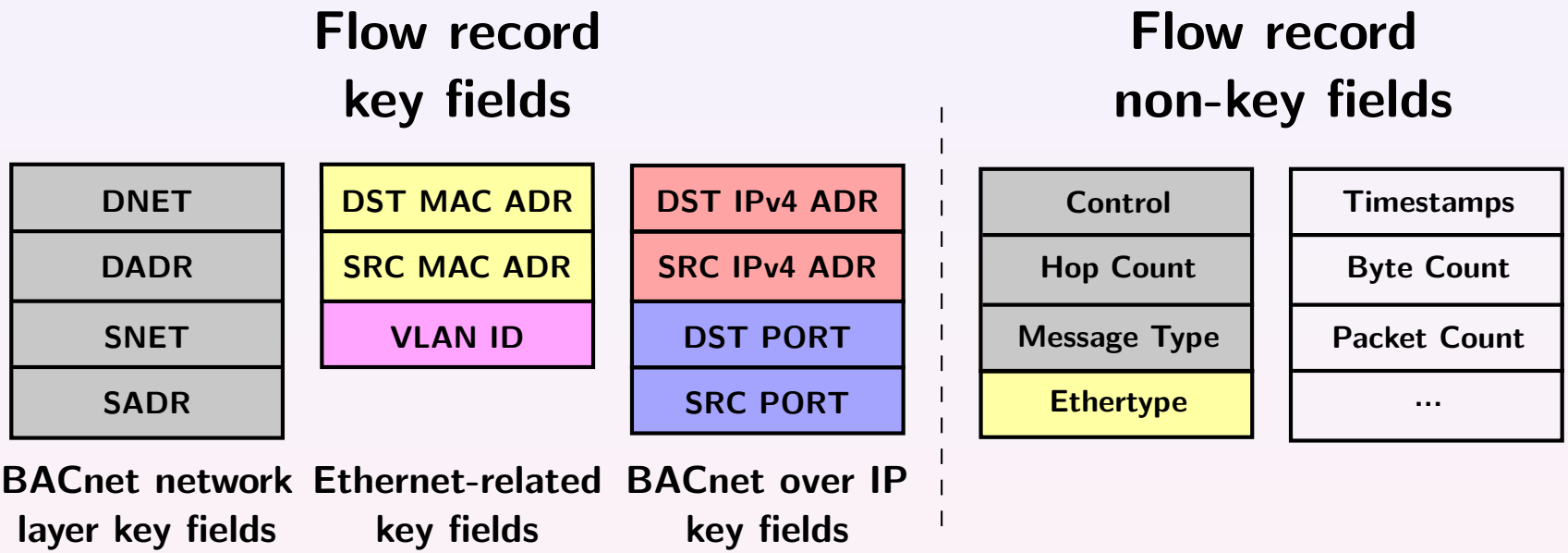
BACnetFlow


Flow record key fields
DNET
DADR
SNET
SADR
DST MAC ADR
SRC MAC ADR
VLAN ID
DST IPv4 ADR
SRC IPv4 ADR
DST PORT
SRC PORT
BACnet network layer key fields
Ethernet-related key fields
BACnet over IP key fields

BACnetFlow

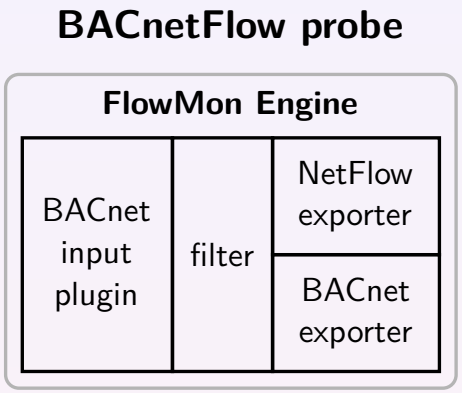

Flow record key fields
Flow record non-key fields
DNET
DADR
SNET
SADR
DST MAC ADR
SRC MAC ADR
VLAN ID
DST IPv4 ADR
SRC IPv4 ADR
DST PORT
SRC PORT
Control
Hop Count
Message Type
Ethertype
Timestamps
Byte Count
Packet Count
...
BACnet network layer key fields
Ethernet-related key fields
BACnet over IP key fields

BACnetFlow



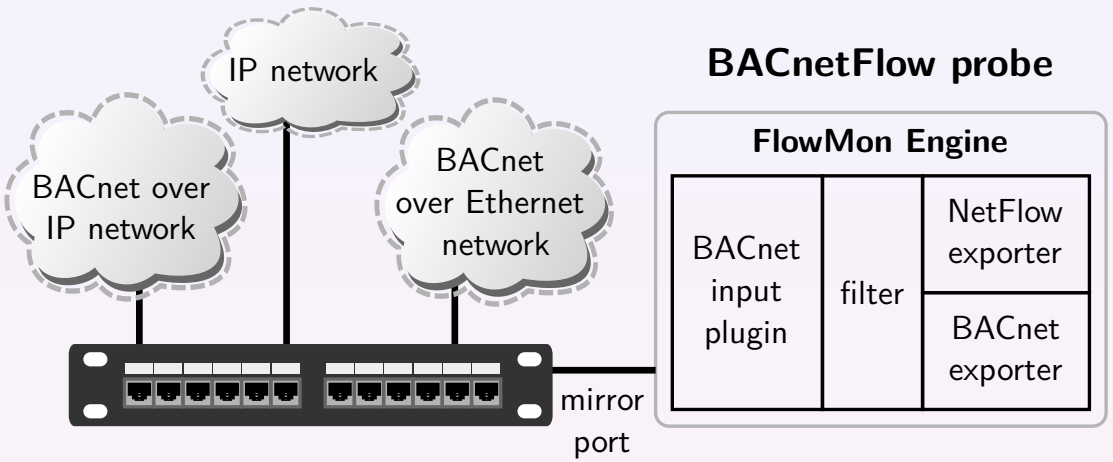
Need of flexible flow information protocol (IPFIX).

BACnetFlow Monitoring System Architecture



BACnetFlow Probe based on FlowMon exporter engine with BACnet plugins.

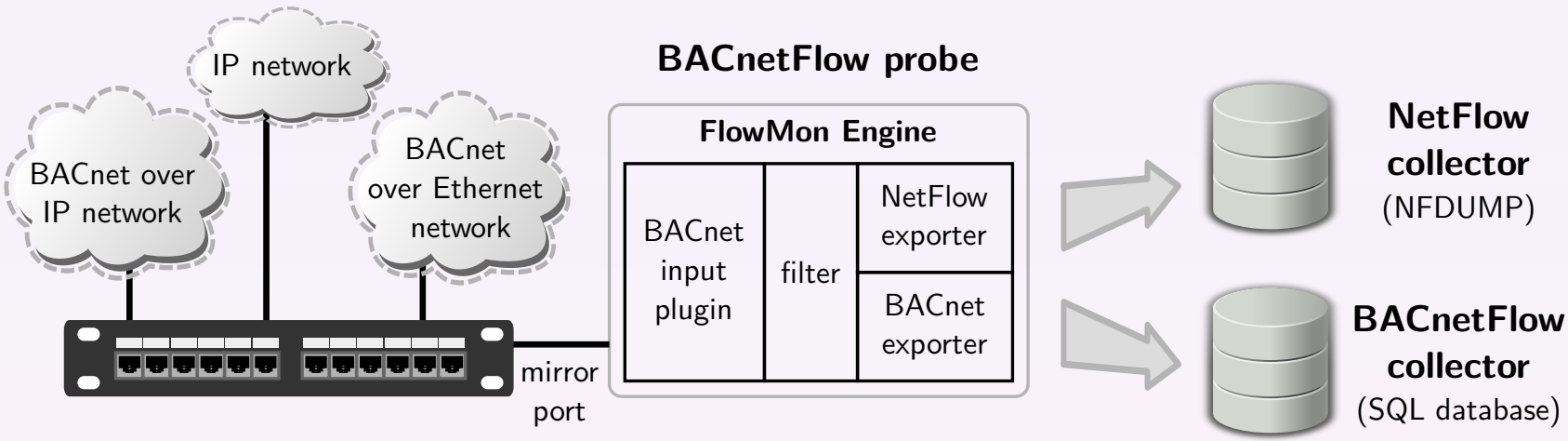
BACnetFlow Monitoring System Architecture



BACnet Network is an Ethernet network at rate of 10-1000 Mbps.

BACnetFlow Probe based on FlowMon exporter engine with BACnet plugins.

BACnetFlow Monitoring System Architecture



BACnet Network is an Ethernet network at rate of 10-1000 Mbps.

BACnetFlow Probe based on FlowMon exporter engine with BACnet plugins.

BACnetFlow Collectors stores flow information for further analysis.

Part III

Measurement and Analysis

Monitored Network

- Masaryk University Campus
- more than 24 teaching pavilions
- BACnet over Ethernet and BACnet over IP BMS networks
- monitoring of the 1 Gbps mirror port of the core switch
- week long measurement (Jan 16, 2012 – Jan 23, 2012)

Overall Traffic Statistics

Protocol	Bytes	Packets	Flows	bps	pps
TCP	3.6 T	3.6 G	533628	47.4 M	6013
BACnet/IP	7.2 G	79.5 M	5.3 M	95.2 K	131.4
BACnet/Eth	5.4 G	59.8 M	6.2 M	71.4 K	98.9
UDP	814.0 M	6.6 M	2.5 M	10757	10
ICMP	722.4 M	7.0 M	1.1 M	9550	11
ARP	680 M	10.5 M	1.8 M	8995	17.4
Other	63.7 M	0.6 M	0.6 M	105	1
OSPF	25.6 M	191079	1990	338	0
PIM	4.6 M	61131	6435	60	0
IGMP	2.0 M	31509	14012	26	0
ICMP6	1.7 M	18362	1261	22	0
Total	3.7 T	3.8 G	4.3 M	47.6 M	6282

Overall Traffic Statistics

Protocol	Bytes	Packets	Flows	bps	pps
TCP	3.6 T	3.6 G	533628	47.4 M	6013
BACnet/IP	7.2 G	79.5 M	5.3 M	95.2 K	131.4
BACnet/Eth	5.4 G	59.8 M	6.2 M	71.4 K	98.9
UDP	814.0 M	6.6 M	2.5 M	10757	10
ICMP	722.4 M	7.0 M	1.1 M	9550	11
ARP	680 M	10.5 M	1.8 M	8995	17.4
Other	63.7 M	0.6 M	0.6 M	105	1
OSPF	25.6 M	191079	1990	338	0
PIM	4.6 M	61131	6435	60	0
IGMP	2.0 M	31509	14012	26	0
ICMP6	1.7 M	18362	1261	22	0
Total	3.7 T	3.8 G	4.3 M	47.6 M	6282

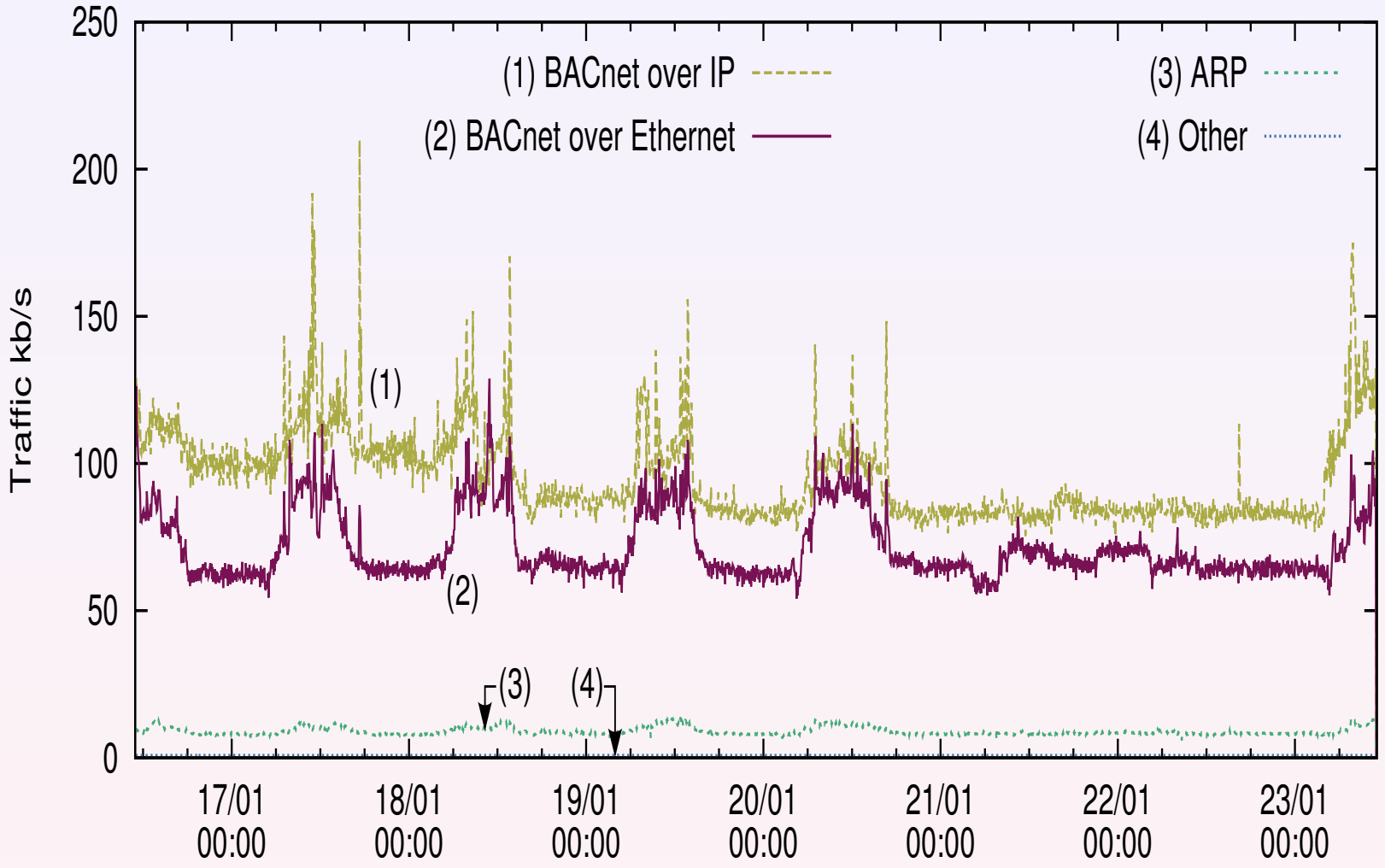
Overall Traffic Statistics

Protocol	Bytes	Packets	Flows	bps	pps
TCP	3.6 T	3.6 G	533628	47.4 M	6013
BACnet/IP	7.2 G	79.5 M	5.3 M	95.2 K	131.4
BACnet/Eth	5.4 G	59.8 M	6.2 M	71.4 K	98.9
UDP	814.0 M	6.6 M	2.5 M	10757	10
ICMP	722.4 M	7.0 M	1.1 M	9550	11
ARP	680 M	10.5 M	1.8 M	8995	17.4
Other	63.7 M	0.6 M	0.6 M	105	1
OSPF	25.6 M	191079	1990	338	0
PIM	4.6 M	61131	6435	60	0
IGMP	2.0 M	31509	14012	26	0
ICMP6	1.7 M	18362	1261	22	0
Total	3.7 T	3.8 G	4.3 M	47.6 M	6282

Overall Traffic Statistics

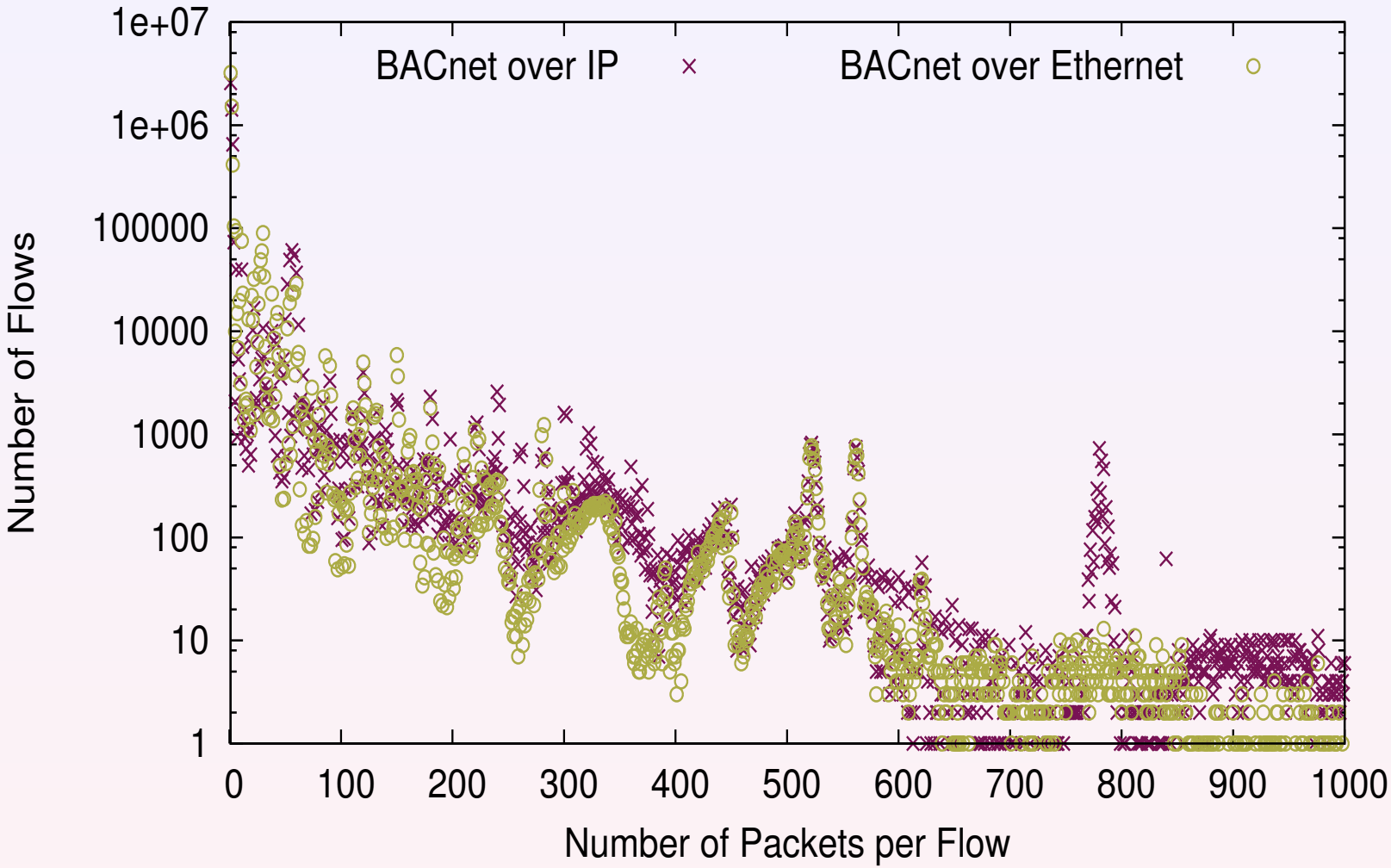
Protocol	Bytes	Packets	Flows	bps	pps
TCP	3.6 T	3.6 G	533628	47.4 M	6013
BACnet/IP	7.2 G	79.5 M	5.3 M	95.2 K	131.4
BACnet/Eth	5.4 G	59.8 M	6.2 M	71.4 K	98.9
UDP	814.0 M	6.6 M	2.5 M	10757	10
ICMP	722.4 M	7.0 M	1.1 M	9550	11
ARP	680 M	10.5 M	1.8 M	8995	17.4
Other	63.7 M	0.6 M	0.6 M	105	1
OSPF	25.6 M	191079	1990	338	0
PIM	4.6 M	61131	6435	60	0
IGMP	2.0 M	31509	14012	26	0
ICMP6	1.7 M	18362	1261	22	0
Total	3.7 T	3.8 G	4.3 M	47.6 M	6282

Diurnal Patterns in BMS Network Traffic



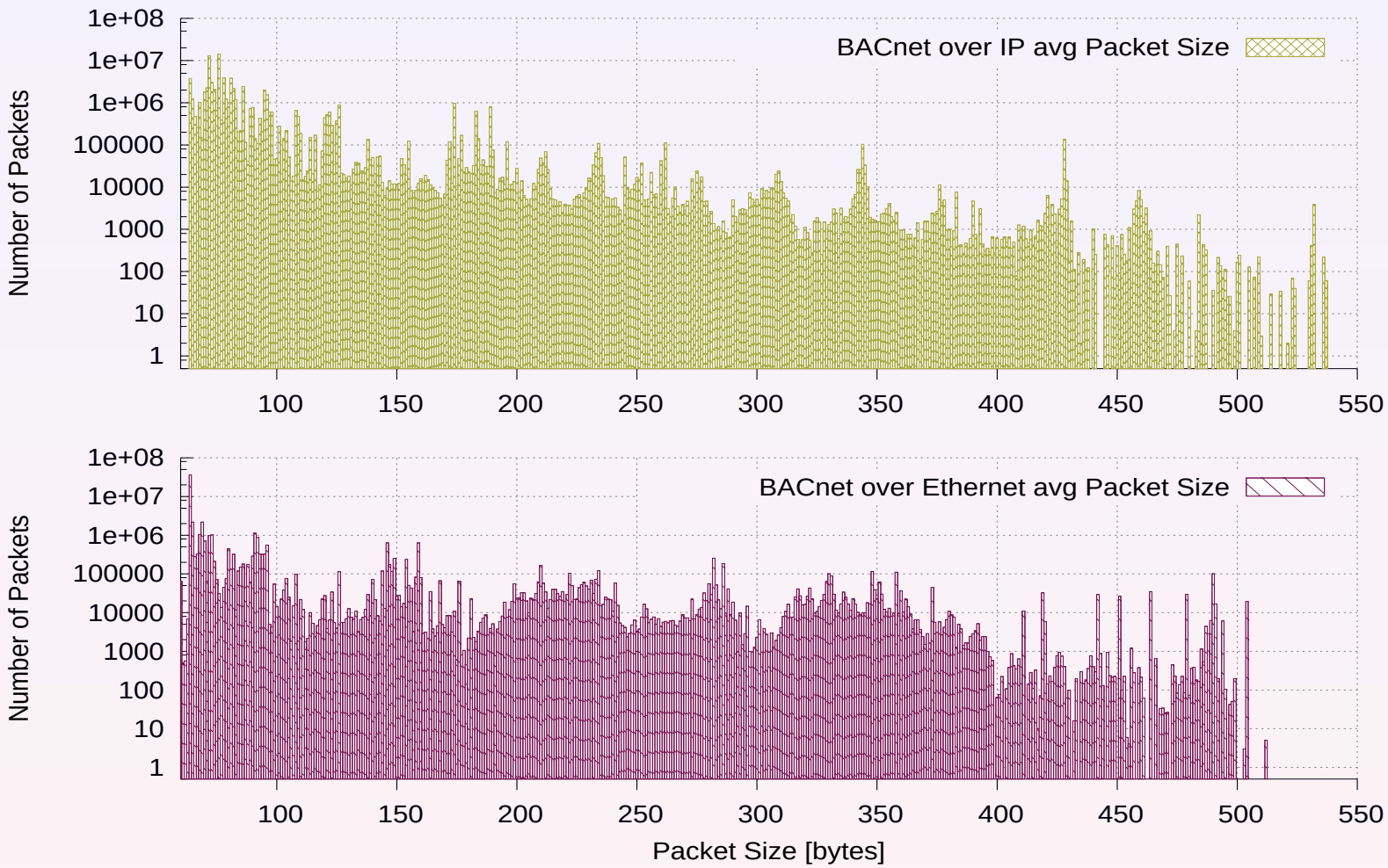
: Traffic load in kilobits per second

Packets Distribution per Flow



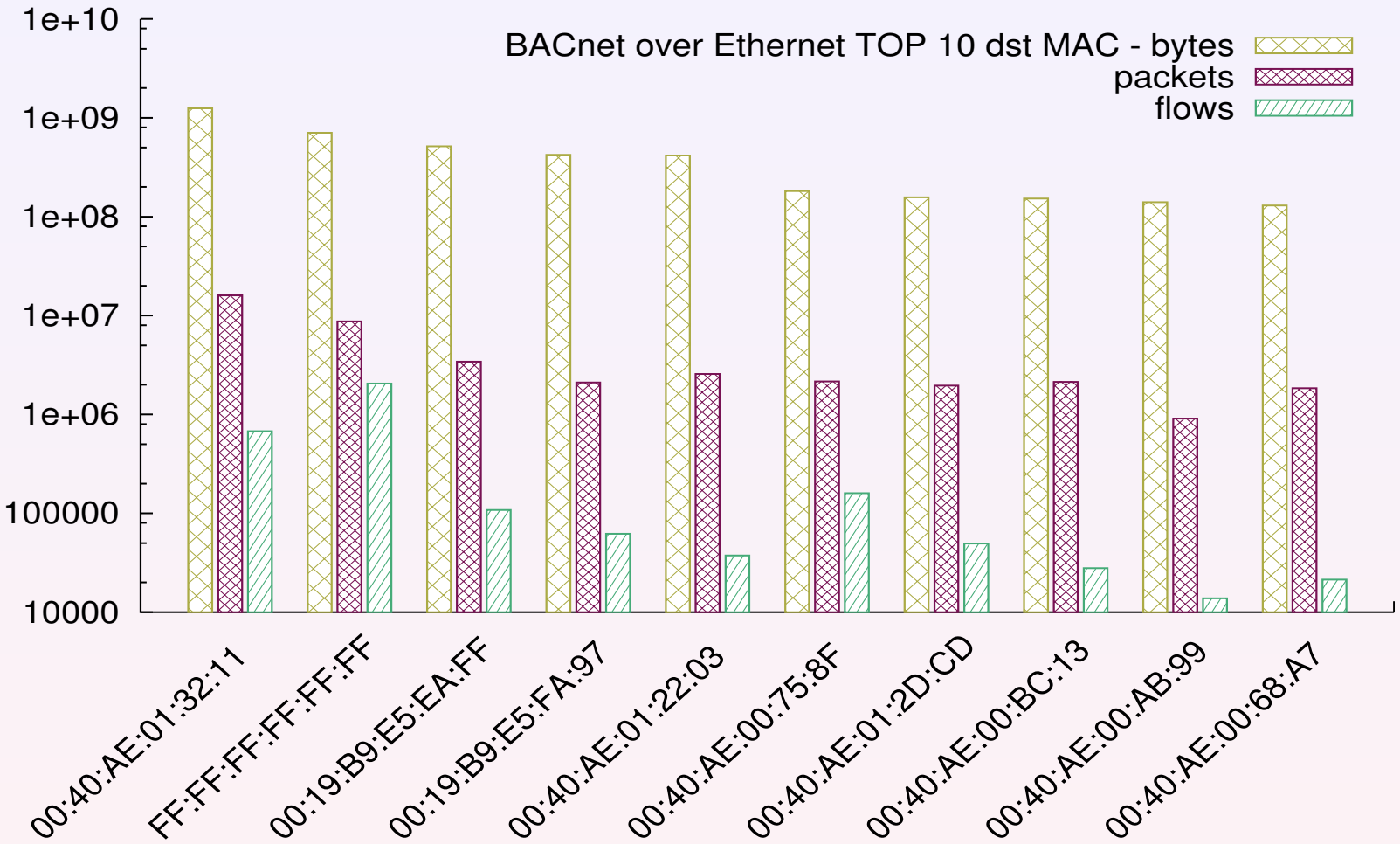
: Traffic load in packets per second

Packets Distribution per Flow



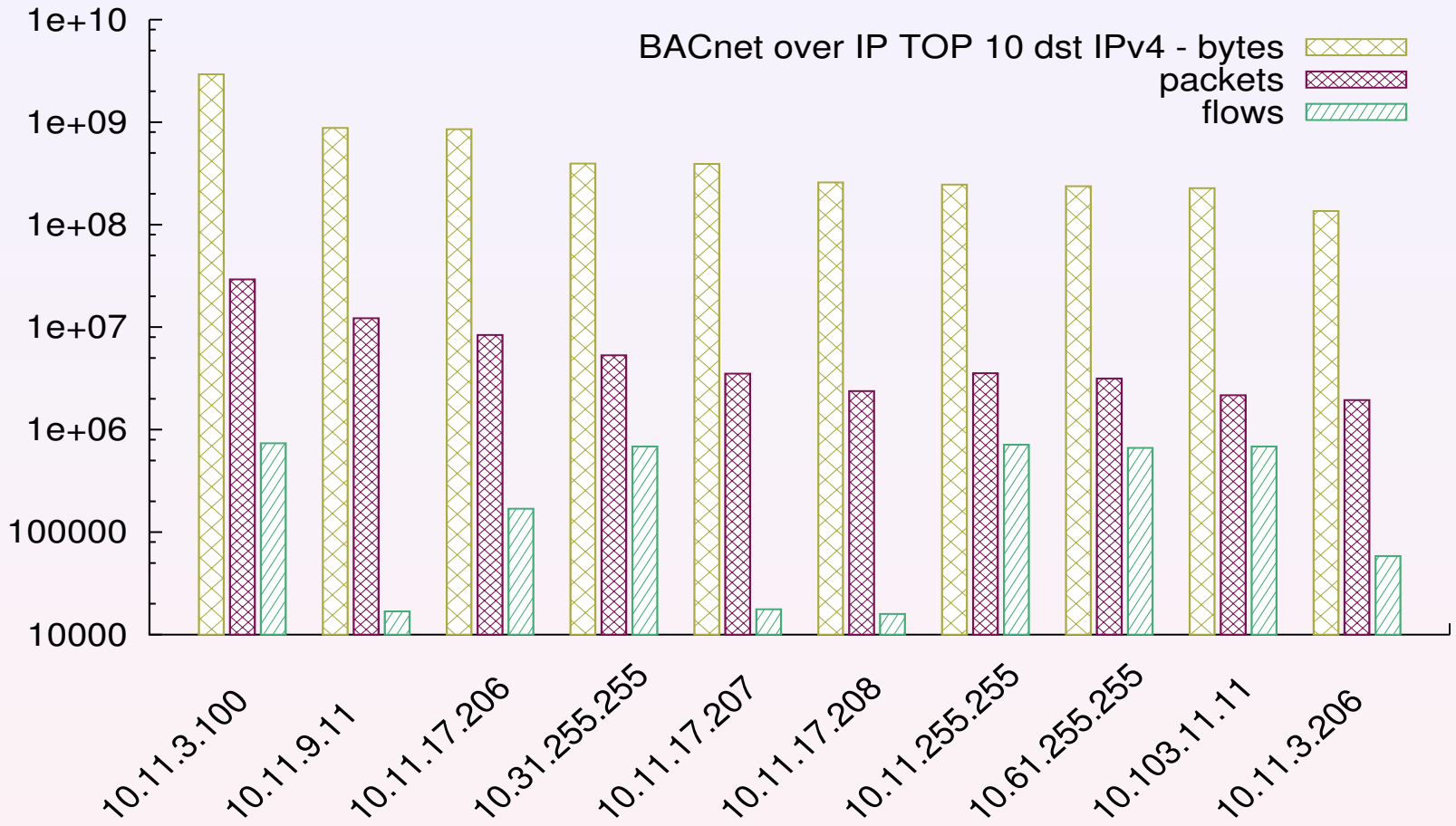
- BACnet average packet size

Top Talkers – BACnet over Ethernet



- BACnet TOP 10 destination addresses / bytes

Top Talkers – BACnet over IP



- BACnet TOP 10 destination addresses / bytes

Part IV

Conclusion

Conclusion

- We deployed the prove of concept system for the flow monitoring in BMS networks.
- We presented the first flow measurement from the BMS network.
- BMS and SCADA networks **CAN** contain diurnal patterns.

Future Work

- IPFIX protocol for the flow information export.
- Explore usability of flow-based monitoring in BMS networks for security issue detection.

Thank You For Your Attention!

Traffic Measurement and Analysis of Building Automation and Control Networks

Radek Krejčí et al.
rkrejci@cesnet.cz

This material is based upon work supported by Masaryk University and also supported by the "CESNET Large Infrastructure" project LM2010005 funded by the Ministry of Education, Youth and Sports of the Czech Republic.