Petrozavodsk State University
Institute of Mathematics and Information Technology

An Algorithm for Building an Enterprise Network Topology Using Widespread Data Sources

Anton Andreev, Iurii A. Bogoiavlenskii

cs.karelia.ru

FRUCT21 November 6-10 , 2017, Helsinki, Finland

Network topology graph

The field of automated network topology discovery has taken on greater importance as networks become more dynamic and complex in nature.

A lot of network management tasks depend on the network description, which is very convenient to be represented as graph containing connections between network elements and their groups:

- network devices, their ports;
- various logical groups of devices and ports:
  - broadcast domains (VLAN),
  - IP-subnets,
  - virtual devices and VPN.

Topology graph applications:

- network documentation;
- root cause analysis;
- network modeling and design;
- load study and visualization.

cs.karelia.ru

The problem of network topology graph building

Main troubles of link layer topology discovery:

- IEEE 802.1 standards originally don't provide the ability of network elements discovery;
- recently standardized tools of network topology discovery (LLDP) are still not common enough and can not provide all necessary information (VLAN, connections blocked by STP);
- data heterogeneity and incompleteness;
- network topology volatility;
- complexity of modern networks (VLAN, VPN, virtualization).

Related works

Limitations of existing methods:

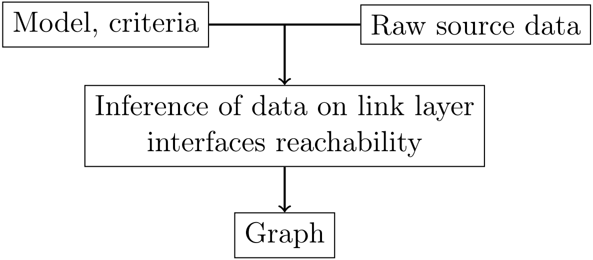
- only link layer topology is considered;
- some methods are incapable of working in networks that include IEEE 802.1Q VLAN, others does not consider important aspects of VLAN structure (eg. commutation, default VLAN);
- use particular single data source;
- most algorithms require AFT completeness close to 100% and a small number of inaccessible devices.

Widespread data sources:

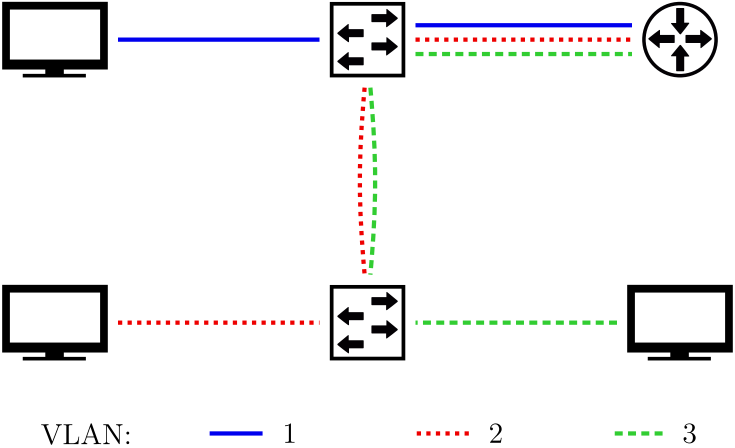
- LLDP, CDP — physical connections with direct neighbors only that have an IP address;
- STP — link layer connections with neighbor switches;
- ARP — reachability of layer 3 interfaces in the same subnet;
- AFT — reachability of layer 2 interfaces in the same broadcast domain;

Our method

- subject of the study are midsize enterprises (containing up to a 1000 of devices and up to 10000 of network computers) that provide services to their own employees and to a limited number of smaller enterprises;
- physical, link and network layers are considered together;
- all widespread data sources are used;
- an algorithm based on the formal model;
- incomplete data inference and structure element detection basing on formal criteria.

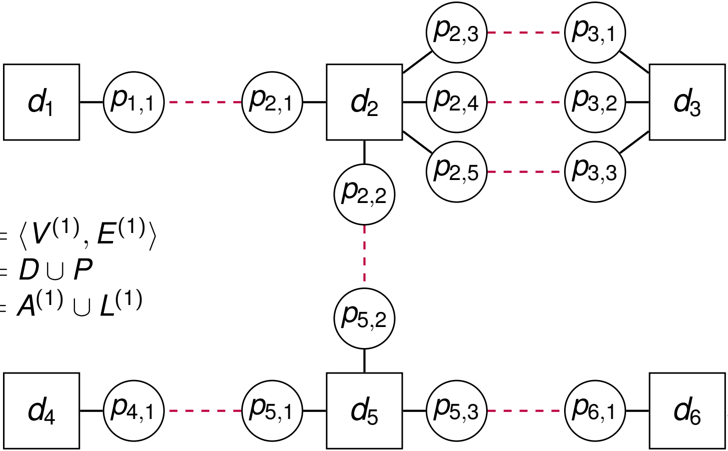


The layout of the sample network



Model of the physical layer

D — set of devices; P — set of network ports;
$A^{(1)}$ — set of edges of association of ports with devices;
$L^{(1)}$ — set of physical layer connection edges;

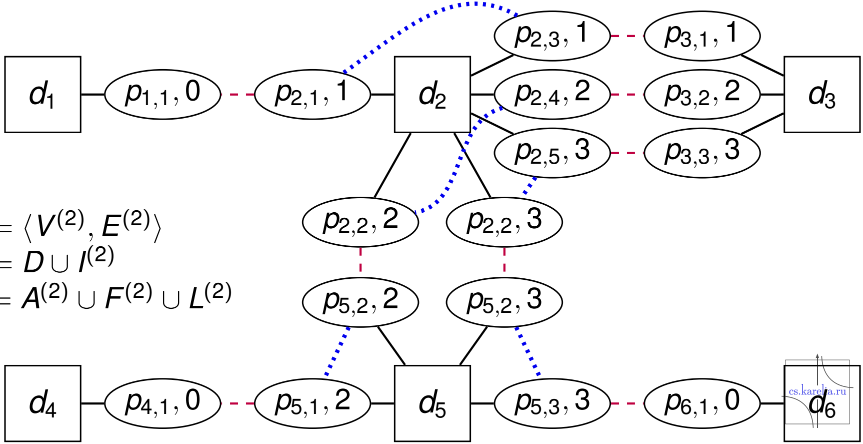


$$G^{(1)} = \langle V^{(1)}, E^{(1)} \rangle$$
$$V^{(1)} = D \cup P$$
$$E^{(1)} = A^{(1)} \cup L^{(1)}$$

Model of the link layer

$I^{(2)}$ — set of link layer interfaces;

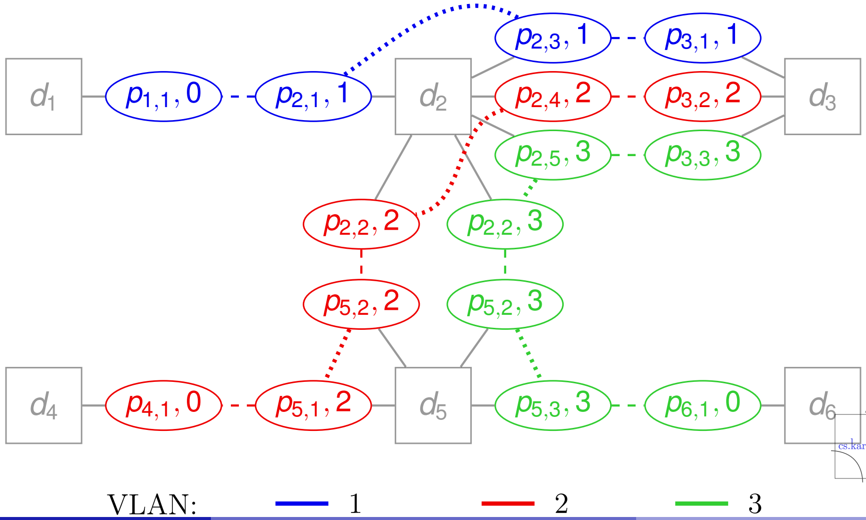
$A^{(2)}$, $F^{(2)}$, $L^{(2)}$ — edges of link layer association, commutation and connection;



$G^{(2)} = \langle V^{(2)}, E^{(2)} \rangle$
$V^{(2)} = D \cup I^{(2)}$
$E^{(2)} = A^{(2)} \cup F^{(2)} \cup L^{(2)}$

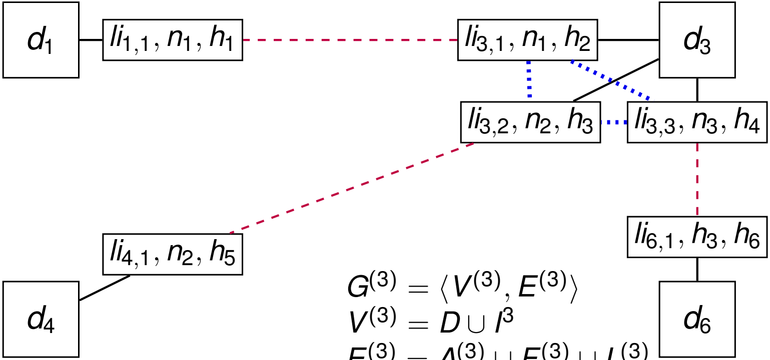
Model of the broadcast domains

Connected components of the graph $\widehat{G}^{(2)} = \langle I^{(2)}, L^{(2)} \cup F^{(2)} \rangle$



Model of the network layer

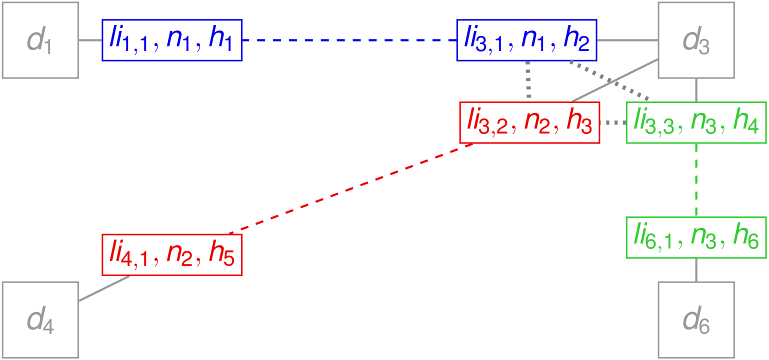
$I^{(3)}$ — set of network layer interfaces;
$A^{(3)}$, $F^{(3)}$, $L^{(3)}$ — edges of network layer association, routing and connection;



$$G^{(3)} = \langle V^{(3)}, E^{(3)} \rangle$$
$$V^{(3)} = D \cup I^3$$
$$E^{(3)} = A^{(3)} \cup F^{(3)} \cup L^{(3)}$$

Model of the IP-subnets

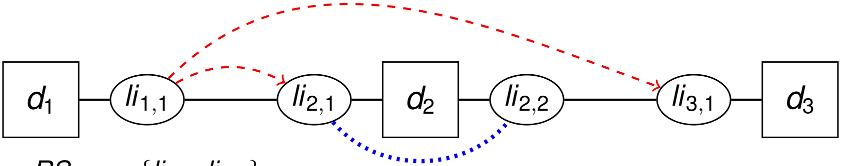
Connected components of the graph $\widehat{G}^{(3)} = \langle I^{(3)}, L^{(3)} \rangle$



Reachability sets of link layer interfaces

Definition of reachability sets for a link layer interface:

- Link layer interface li_2 is reachable from interface li_1, if there is a link layer path between them for which the first and the last edges are not commutation edges.
- $RS_{li_1} \subseteq I^{(2)}$, all the interfaces which are reachable from li_1.

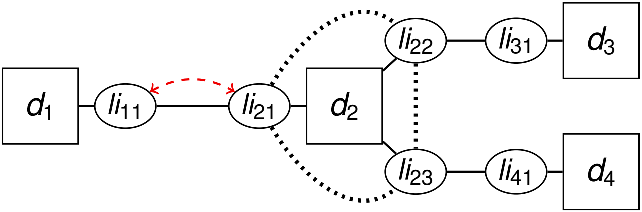


$RS_{li_{1,1}} = \{li_{2,1}, li_{3,1}\}$

Are necessary for generalized processing of heterogeneous data sources.

Properties of the reachability sets

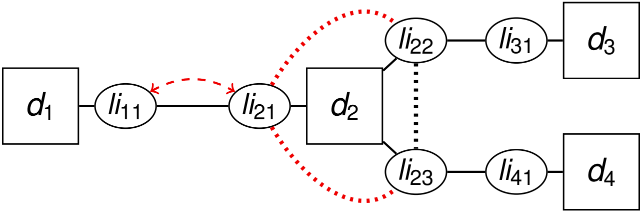
1. If an interface li_2 is reachable from li_1, then li_1 is reachable from li_2
2. If an interface li_2 is reachable from li_1, then from li_1 are reachable all interfaces, which are reachable from interfaces in commutation with li_2



Data inference is based on these properties of reachability sets proven by us within theorems.

Properties of the reachability sets

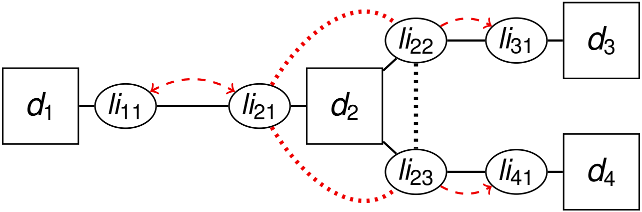
1. If an interface li_2 is reachable from li_1, then li_1 is reachable from li_2
2. If an interface li_2 is reachable from li_1, then from li_1 are reachable all interfaces, which are reachable from interfaces in commutation with li_2



Data inference is based on these properties of reachability sets proven by us within theorems.

Properties of the reachability sets

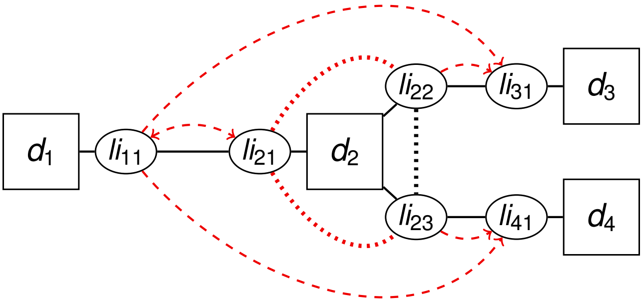
1. If an interface li_2 is reachable from li_1, then li_1 is reachable from li_2
2. If an interface li_2 is reachable from li_1, then from li_1 are reachable all interfaces, which are reachable from interfaces in commutation with li_2



Data inference is based on these properties of reachability sets proven by us within theorems.

Properties of the reachability sets

1. If an interface li_2 is reachable from li_1, then li_1 is reachable from li_2
2. If an interface li_2 is reachable from li_1, then from li_1 are reachable all interfaces, which are reachable from interfaces in commutation with li_2



Data inference is based on these properties of reachability sets proven by us within theorems.

The source data used by algorithm

Data are obtained with SNMP (Simple Network Management Protocol)

- Data on devices, their interfaces and addresses: IF-MIB, IP-MIB
- Data on VLAN: Q-BRIDGE-MIB, VTP-MIB, CISCO-VLAN-MEMBERSHIP-MIB, etc.
- Data on device environment: spanning tree (BRIDGE-MIB), neighbor data (CISCO-CDP-MIB, LLDP-MIB)
- Data on interface reachability: address forwarding tables – AFT (BRIDGE-MIB), routing tables (IP-MIB, RIPv2-MIB, BGP4-MIB, etc.), ARP cache (RFC1213-MIB, IP-MIB)

cs.karelia.ru

The algorithm of the network topology graph building

1. Polling of network devices and obtaining from them data on the structure of the network using SNMP;
2. Building graph fragments that describe the devices (with their ports and interfaces), existence of which follows directly from the results of the input data analysis;
3. Building reachability sets for existing link interfaces using the input dataset and inferring missing records in them using reachability set properties;
4. Graph edge building using formal criteria
   - link layer connection and commutation edges based on the analysis of the reachability sets;
   - physical and network layer connection edges based on the definitions of the model;
   - inference of the devices, data about which are missing from the network input data.

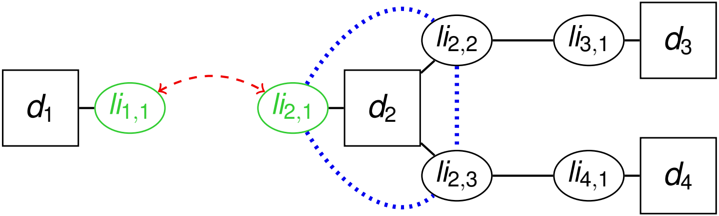
Link layer connections discovery

Definition

$CRS_{li} \subset I^{(2)}$ — set of link layer interfaces that are reachable from interfaces in commutation with li

Criterion

Interfaces li_1 и li_2 are connected on link layer if and only if $RS_{li_1} = CRS_{li_2} \cup \{li_2\}$ and $RS_{li_2} = CRS_{li_1} \cup \{li_1\}$.



cs.karelia.ru

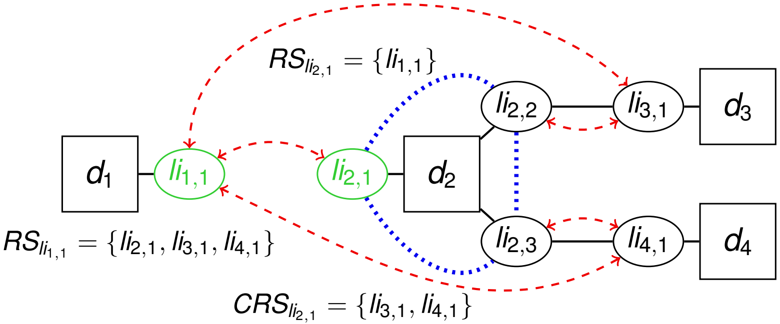
Link layer connections discovery

Definition

$CRS_{li} \subset I^{(2)}$ — set of link layer interfaces that are reachable from interfaces in commutation with li

Criterion

Interfaces li_1 и li_2 are connected on link layer if and only if $RS_{li_1} = CRS_{li_2} \cup \{li_2\}$ and $RS_{li_2} = CRS_{li_1} \cup \{li_1\}$.



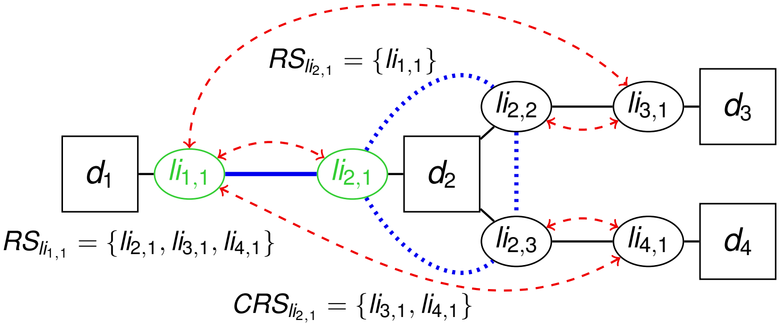
Link layer connections discovery

Definition

$CRS_{li} \subset I^{(2)}$ — set of link layer interfaces that are reachable from interfaces in commutation with li

Criterion

Interfaces li_1 и li_2 are connected on link layer if and only if $RS_{li_1} = CRS_{li_2} \cup \{li_2\}$ and $RS_{li_2} = CRS_{li_1} \cup \{li_1\}$.



Mathematically proven criteria

The criteria for detection of edges and vertices of the graph indirectly presented in the source data.

- Three criteria for the detection of link layer connection edges ($L^{(2)}$)
- Criterion for the detection of physical layer connection edges ($L^{(1)}$)
- Criterion for the detection of network layer connection edges ($L^{(3)}$)
- Criterion for the detection of link layer commutation edges ($F^{(2)}$)
- Two criteria for the detection of ambiguous situations with border devices
- Two criteria for the detection of edges within VPN
- Three criteria for the detection of ambiguous situations with internal devices

cs.karelia.ru

Algorithm structure and procedures

- Procedure *COLLECT* to collect data and put result to *CData*
- Procedure *BUILD_VERTICES* to build graph vertices using *CData*
- Procedure *INIT_RS* to initialize reachability sets using *CData*
- REPEAT
  - Procedure *INFER_RS* for data inference
  - Procedure *BUILD_LINK_LINKS* for link layer edge building
  - Procedure *BUILD_PHYS_LINKS* for physical layer edge building
- WHILE some edge is found
- Procedure *BUILD_NET_LINKS* for network layer edge building

Time complexity

Worst-case asymptotic complexity $O(|P| * |I^{(2)}|^8)$

Best-case asymptotic complexity $\Omega(|I^{(2)}|^4)$

Sample execution time (data collection time excluded)

Number of communication devices	Number of hosts	Number of VLANs	Execution time, sec.
6	87	2	7
20	400	10	125
49	896	101	814

System: Windows 10, 8-thread Intel Core i7, Oracle JDK 8-144

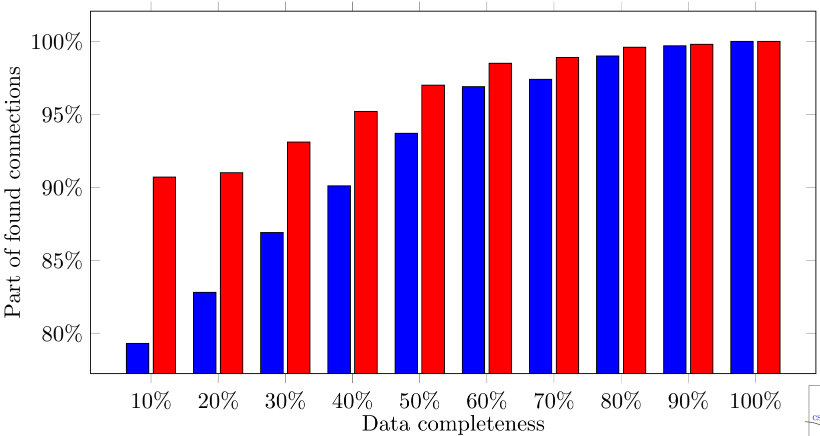
Testing in the network of PetrSU

Number of discovered elements, without and with use of data inference

	CDP		STP		AFT		All	
Devices	907	907	907	907	907	915	907	945
Ports	1151	1151	1151	1151	1151	1814	1151	1923
L1 links	63	63	15	15	1	796	63	832
L2 interfaces	3452	3452	3452	3452	3452	4337	3512	4483
L2 links	612	612	560	560	101	1399	672	1570
Comm-s	8229	8229	8229	8229	8229	14071	8229	14738
L3 interfaces	962							
L3 links	767	767	103	103	1	9061	672	9679
Routings	3717							

Data presence influence

Blue — part of found connections between communication devices.
Red — part of found connections between all devices.



cs.karelia.ru

Conclusion

- a formal method of discovering physical, link and network layers topology of an enterprise network is proposed;
- developed and proved 14 criteria for network elements discovery;
- developed, evaluated and tested the algorithm for automated network topology graph building.

Future work:

- parallel version of the algorithm;
- better testing and evaluation of the actual time complexity and performance when building the topology of real life networks;
- the experimental study of algorithm behavior on various networks.

Thank you for your attention!

ybgv@cs.petrsu.ru
andreev@cs.petrsu.ru

cs.karelia.ru