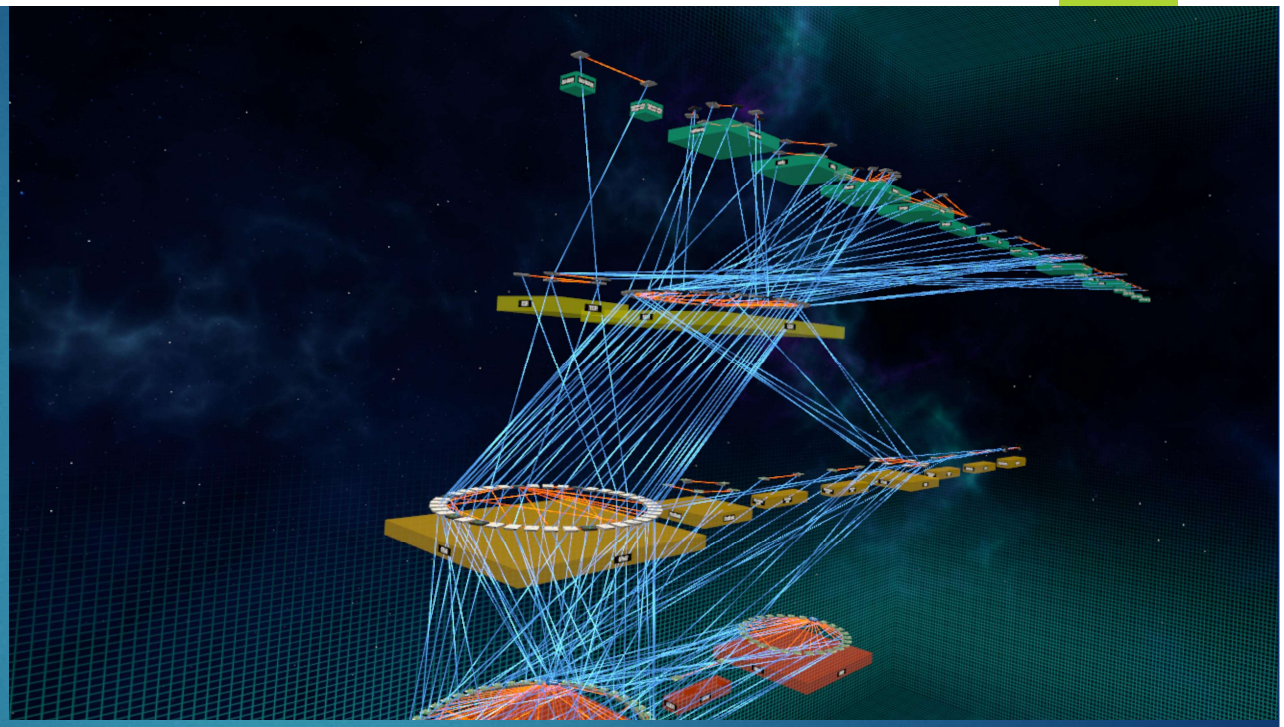
Photon

DEMONSTRATION



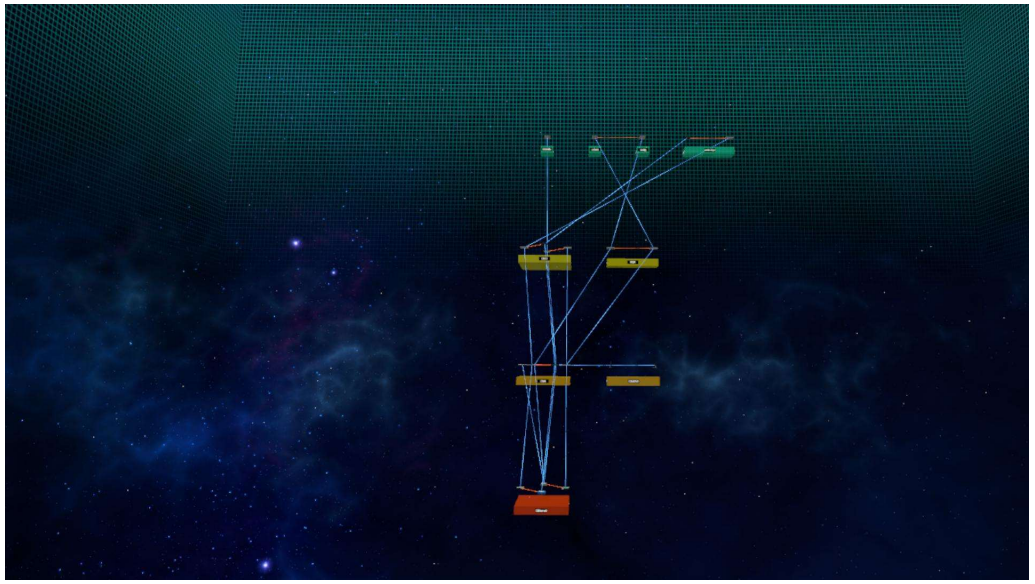
Photon Summary

Photon is a PC VR application for viewing 3D visualizations of network traffic.

Import PCAP Files

Includes multiplayer support.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.7	52.24.87.6	TCP	66	52929 → 443 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=526692320 TSecr=3064983827
2	2.076214	192.168.1.7	192.168.1.1	DNS	80	Standard query 0x2956 A ios.nccp.netflix.com
3	2.076789	192.168.1.7	192.168.1.1	DNS	80	Standard query 0x9a61 AAAA ios.nccp.netflix.com
4	2.089734	192.168.1.1	192.168.1.7	DNS	275	Standard query response 0x2956 A ios.nccp.netflix.com CNAME ios.nccp.geo.netflix.com CNAME ios.nccp.us-west-2
5	2.093364	192.168.1.7	192.168.1.1	DNS	96	Standard query 0xd088 A ichnaea.us-west-2.prodaa.netflix.com
6	2.094467	192.168.1.1	192.168.1.7	DNS	371	Standard query response 0x9a61 AAAA ios.nccp.netflix.com CNAME ios.nccp.geo.netflix.com CNAME ios.nccp.us-wes
7	2.094915	192.168.1.1	192.168.1.7	DNS	224	Standard query response 0xd088 A ichnaea.us-west-2.prodaa.netflix.com A 54.69.204.241 A 52.42.153.22 A 54.68.
8	2.099322	192.168.1.7	54.69.204.241	TCP	78	53105 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=526694443 TSecr=0 SACK_PERM
9	2.107174	192.168.1.7	54.191.17.51	TCP	78	53114 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=526694450 TSecr=0 SACK_PERM
10	2.145347	54.69.204.241	192.168.1.7	TCP	74	443 → 53105 [SYN, ACK] Seq=0 Ack=1 Win=17898 Len=0 MSS=1460 SACK_PERM TSval=2242334683 TSecr=526694443 WS=256
11	2.147897	192.168.1.7	54.69.204.241	TCP	66	53105 → 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=526694489 TSecr=2242334683
12	2.148494	192.168.1.7	54.69.204.241	TLSv1.2	274	Client Hello (SNI=ichnaea.netflix.com)
13	2.153975	54.191.17.51	192.168.1.7	TCP	74	443 → 53114 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=2911517093 TSecr=526694450 WS=256
14	2.155408	192.168.1.7	54.191.17.51	TCP	66	53114 → 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=526694496 TSecr=2911517093
15	2.170268	192.168.1.7	54.191.17.51	TLSv1.2	583	Client Hello (SNI=ios.nccp.netflix.com)

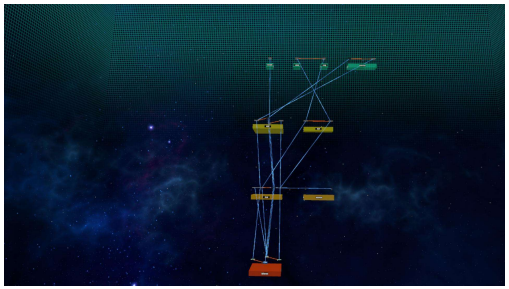


Workflow

Select Network File

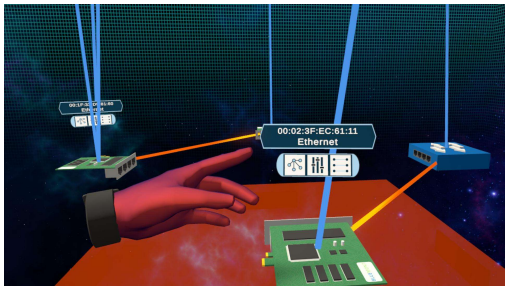
Use the file selector to browse & import a PCAP file

Load Visualization



View the big picture summary of network activity

Filter & Examine



Inspect individual network devices at multiple protocol levels

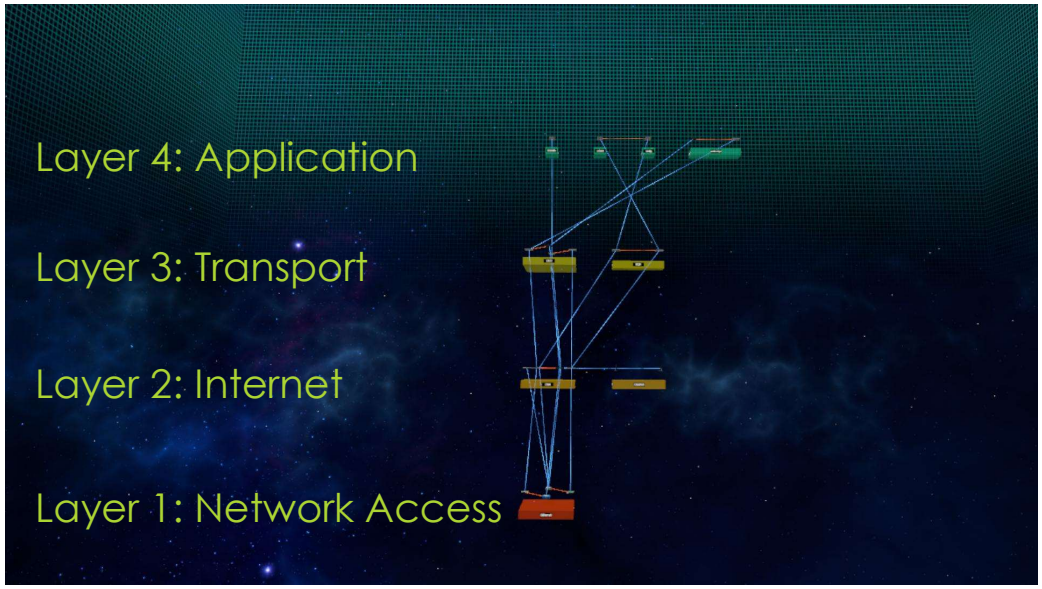
Visualization Explained

HOW TO INTERPRET THE 3D VISUALIZATION

Protocol View

Detected Devices are grouped by protocol.

Protocols are stacked into the 4-layer TCP/IP model.

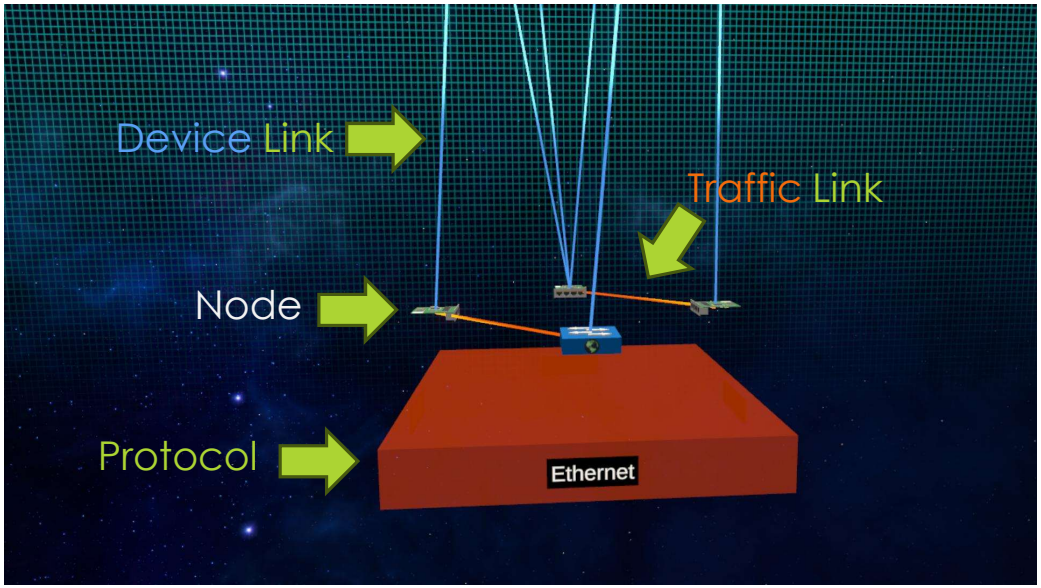


Elements

Nodes represent a network device at a particular protocol level.

Blue Device links connect a single device across protocol levels.

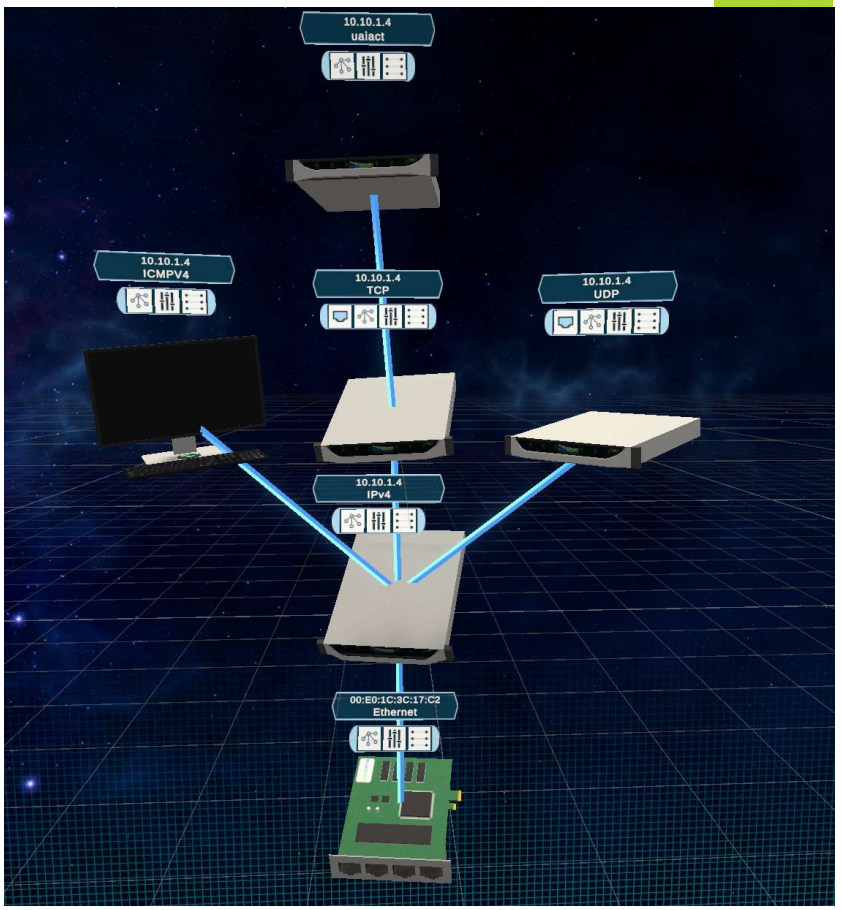
Orange Traffic links represent traffic flow between network devices.



Device View

Here we see a single network device identified by MAC and IP address.

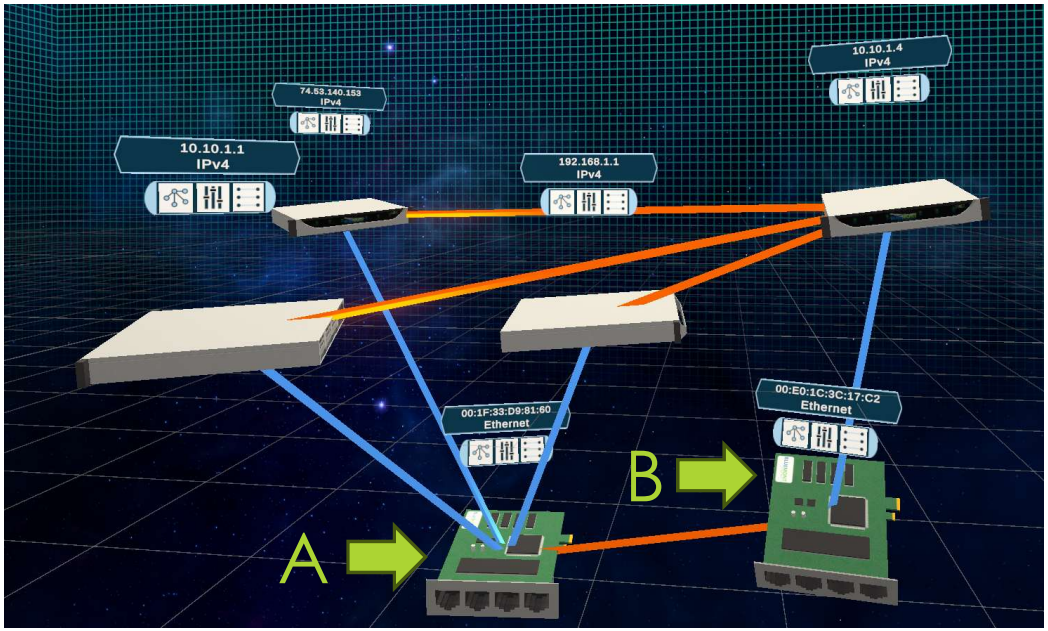
Each node represents a specific protocol the entity used during the capture.



Interpreting The Network Diagram

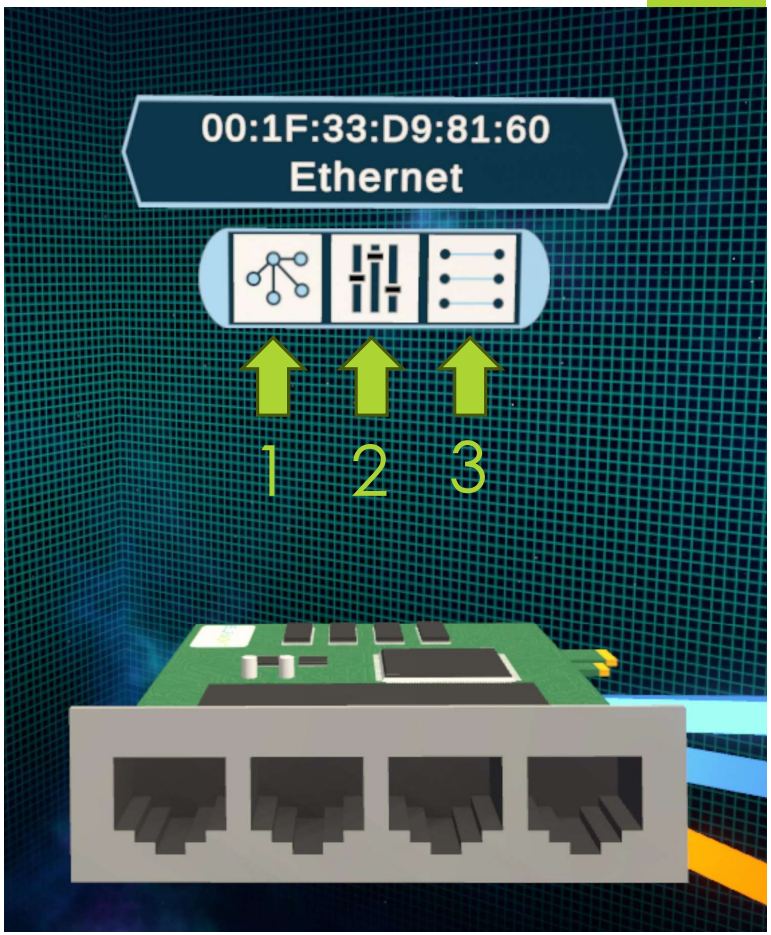
The orange links indicate traffic between devices A and B.

Device A used 3 different IPv4 addresses during the capture.



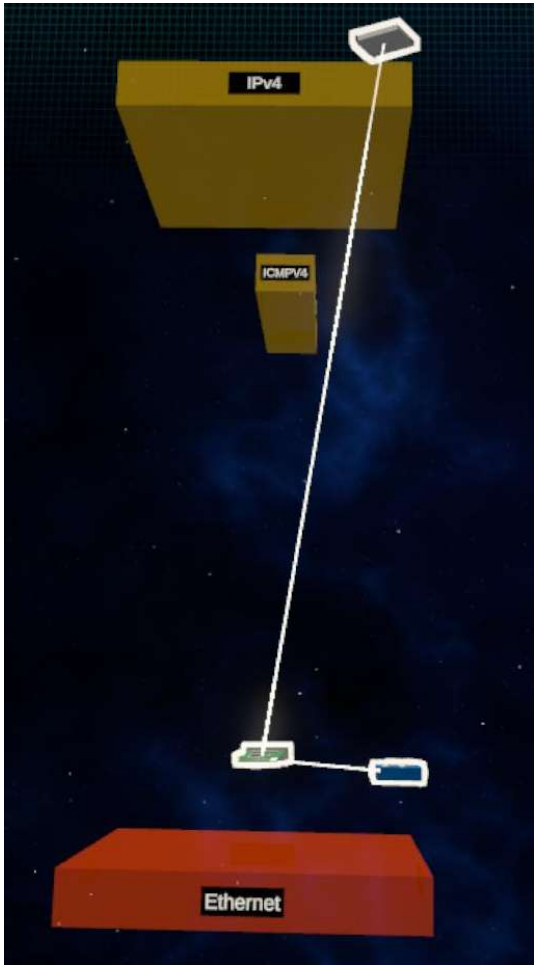
Node Buttons

1. Nearest Neighbor Filter
2. Node Packet Transfer Stats
3. Links List



Nearest Neighbor

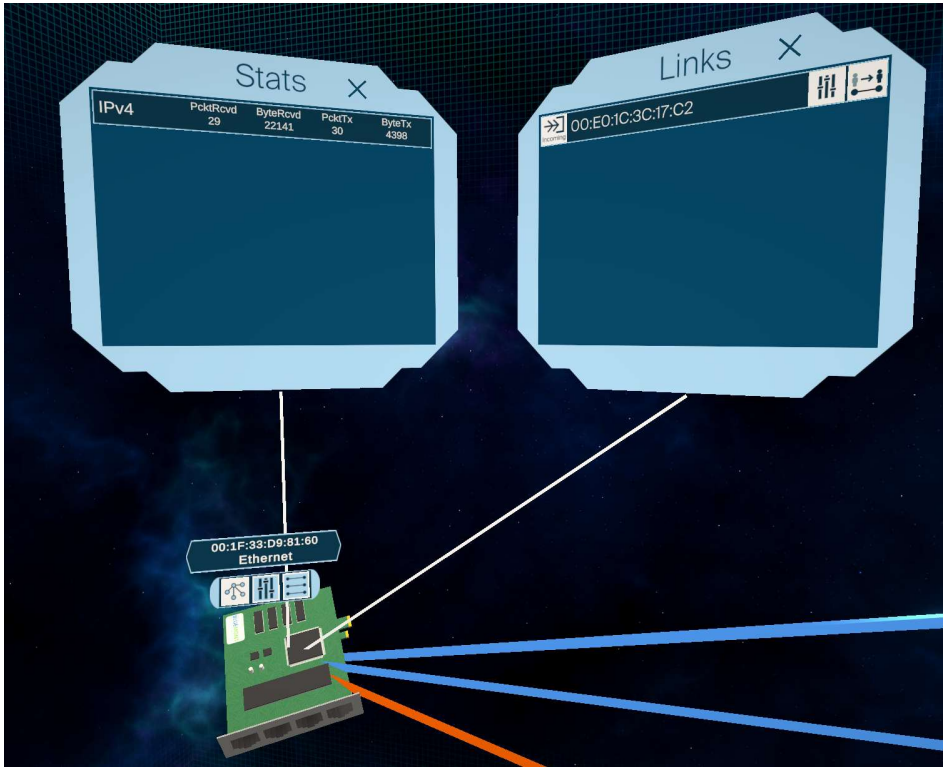
Nearest neighbor filter hides all nodes in the network except the target node's nearest traffic and device links.



Node Stats & Links List

Node stats show info about packet transfer.

Links list shows all detected traffic links.



Version 1.0 - Additional Features

- Peer to Peer Multiplayer Support With Voice Chat
- 3D Annotations (Draw Mode)
- Network Model Filters (by Protocol & Link Type)

Version 1.5 – Planned Features

- More Detailed Application Layer Deep Packet Analysis Using nDPI
- In App Network Capture Support
- Improved Network Layout Options

Contact Us

- Bernadette Gagnon
- eMail: bg@BluemontTechnology.com

- Eric F. Downward
- eMail: eric@BluemontTechnology.com

- Phone: 540-955-6072