What is RedCLARA?

RedCLARA is the result of cooperation between Latin American countries to create a high-capacity network dedicated to research and education.
What is RedCLARA?

We strengthen the development of science, education, culture and innovation in Latin America, through the innovative use of networks, infrastructure and advanced information technologies.
What is RedCLARA?

Today this cooperation has 9 countries totaling 15,759,828 km² of territory. This vast territory must be covered by national networks, making it possible to reach the most diverse regions.
Cooperación Latino Americana de Redes Avanzadas
Network characteristics

- High capacity: all backbone links are +100Gbps
- Predictability: traffic flows through a coherent path
- Security: MANRS participant with all 4 actions implemented + 100% score
- Robust monitoring
NEG Systems

- Grafana: Network traffic monitoring
- chronograf: Virtual machines monitoring
- graylog: Management of log messages
- ElastiFlow: Collects and analyzes network flows
- Oxidized: Configuration backup and management

- ZABBIX: Monitoring and alerting system
- Pushover: Push notifications system
- TACACSGUI: User authentication, and command authorization and accounting
- ROUTINATOR: RPKI validation system

TechEX2023
Integrated Monitoring Portal

- One of the most requested features from RedCLARA members was network visibility.
- Network monitoring was present, but information was internal.
Graphical Interface and Authentication

- Graphical interface built with Drupal
- Drupal is an open source Content Management System (CMS)
- Authentication uses Shibboleth for federated login
- Created by SEG (System Engineering Group)
Traffic and BGP Monitoring

- SNMP metrics collected with Telegraf using a polling time of 30 seconds
- Latency measured with IP SLA
- Data is stored in InfluxDB
- Availability and Alerts provided by Zabbix
- Dashboards built with Grafana
Netflow v9 is configured on the routers
• Only 0.01% of the packets are sampled
• Flows are exported to Logstash
• Data is enriched and sent to Elasticsearch
• Dashboards are made for Kibana and are part of ElastiFlow
RNP: Flows

Overview | Top-N | Threats | Flows | Geo IP | AS Traffic

Services (bits/s)

Top Clients
- 147.150.117.68: 99.74MB, 70,070 packets, 1,978 flow records
- 147.150.117.41: 88.27MB, 60,635 packets, 1,821 flow records
- 2001:638:700:0:0:0:1a:1b: 14.56GB, 13,575 packets, 299 flow records
- 192.205.153.244: 14.56GB, 9,757 packets, 228 flow records
- 2001:638:700:0:0:0:1a:1d: 13.26GB, 9,278 packets, 295 flow records
- 141.34.192.140: 12.82GB, 9,000 packets, 256 flow records
- 2001:638:700:0:0:0:1a:1e: 12.82GB, 8,973 packets, 283 flow records
- 141.34.192.138: 12.80GB, 8,984 packets, 283 flow records
- 141.34.192.142: 12.80GB, 9,004 packets, 247 flow records
- 2001:638:700:0:0:0:1a:1f: 12.63GB, 8,830 packets, 207 flow records

Total: 567,715 packets, 40,328 flow records

Top Servers
- 200.17.30.65: 373.99GB, 262,572 packets, 7,099 flow records
- 2001:1270:8120:65: 328.13GB, 228,774 packets, 5,621 flow records
- 200.236.31.10: 11.06GB, 7,372 packets, 110 flow records
- 200.236.31.13: 1.28GB, 1,007 packets, 123 flow records
- 200.144.255.251: 1.52GB, 1,323 packets, 747 flow records
- 129.247.239.1: 1.09GB, 768 packets, 220 flow records
- 2001:67a::f00d:200-89: 78.51GB, 10,351 packets, 5,555 flow records
- 200.236.31.8: 70.319GB, 480 packets, 59 flow records
- 129.247.239.11: 513.066GB, 586 packets, 494 flow records
- 200.17.30.43: 470.084GB, 388 packets, 310 flow records

Total: 567,715 packets, 40,328 flow records

Export: Raw | Formatted
WeatherMap

- The WeatherMap shows current backbone traffic and latency
- It has been built with Zabbix
- General view for backbone circuit outages
WebSSH

• Built with WebSSH (https://github.com/huashengdun/webssh)

• User authentication, command authorization and accounting done by TACACSGUI

• Only ping, traceroute and a set of show commands are allowed
WebSSH

Hu0/1/0/1.959 up up REUNA Copernicus (backup)
Hu0/1/0/1.2008 up up AMPATH Academic (backup)
Hu0/1/0/1.2375 up up RNP SuperComputing 2022
Hu0/1/0/1.2376 up up RNP DPDI Server PoP-SP
Hu0/1/0/1.2377 up up Redbeep SuperComputing 2023
Hu0/1/0/2 down down TO NNF NoviFlow WB5132-P SAO-SP4-SMO3 P26

RP/0/RSP0/CPU0:rir-core-sao# show bgp summary
Mon Sep 18 07:45:27.501 UTC
BGP router identifier 200.0.205.1, local AS number 27750
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000000 RD version: 4666047
BGP main routing table version 4666047
BGP NSR Initial initsync version 48946 (Reached)
BGP NSR/ISSU Sync-Group version 4666047/0
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Spk</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>St/FxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.32.252.205</td>
<td>0</td>
<td>20080</td>
<td>378053</td>
<td>383966</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>1w5d</td>
<td>1592</td>
</tr>
<tr>
<td>198.71.45.210</td>
<td>0</td>
<td>11527</td>
<td>2228562</td>
<td>220434</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>1d12h</td>
<td>17019</td>
</tr>
<tr>
<td>200.0.204.157</td>
<td>0</td>
<td>11340</td>
<td>158336</td>
<td>956779</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>2d27h</td>
<td>147</td>
</tr>
<tr>
<td>200.0.204.178</td>
<td>0</td>
<td>1797</td>
<td>1465288</td>
<td>716818</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>3wod</td>
<td>3</td>
</tr>
<tr>
<td>200.0.204.214</td>
<td>0</td>
<td>1916</td>
<td>371948</td>
<td>930739</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>687</td>
</tr>
<tr>
<td>200.0.205.2</td>
<td>0</td>
<td>27750</td>
<td>493856</td>
<td>1077149</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>4321</td>
</tr>
<tr>
<td>200.0.205.3</td>
<td>0</td>
<td>27750</td>
<td>81229916</td>
<td>1078545</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>8d2d</td>
<td>20649</td>
</tr>
<tr>
<td>200.0.205.4</td>
<td>0</td>
<td>27750</td>
<td>156609</td>
<td>1077838</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>0</td>
</tr>
<tr>
<td>200.0.205.5</td>
<td>0</td>
<td>27750</td>
<td>1739204</td>
<td>1077838</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>338</td>
</tr>
<tr>
<td>200.0.205.7</td>
<td>0</td>
<td>27750</td>
<td>156256</td>
<td>1080550</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>10w3d</td>
<td>0</td>
</tr>
<tr>
<td>200.0.205.8</td>
<td>0</td>
<td>27750</td>
<td>163157</td>
<td>1077838</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>73</td>
</tr>
<tr>
<td>200.0.205.9</td>
<td>0</td>
<td>27750</td>
<td>165342</td>
<td>1077709</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>3d21h</td>
<td>93</td>
</tr>
</tbody>
</table>
• eduroam information is collected from logs
• Logs are ingested to ELK Stak
• Custom dashboards have been created to output the information
Brazil users authentications: 1,094,568 Authentications

Foreign authentications in Brazil: 426,724 Authentications

Countries visited by Brazil users:
- Argentina (0.6%)
- Brazil
- Chile
- Colombia
- Costa Rica
- Ecuador
- Mexico
- Uruguay
- Outside LATAM (98.75%)

Foreign users authenticated in Brazil (by Country):
- Portugal (25.41%)
- Germany (11.13%)
- France (10.13%)
- United Kingdom (8.86%)
- Italy (4.06%)
- Chile (3.05%)
- Switzerland (2.04%)
- Netherlands (3.67%)
- Missing (4.01%)
- Spain (5.36%)
- Austria
DEMO
QUESTIONS?