IPv6 - Desafios para implantação em uma Rede de Campus

Universidade Estadual de Campinas - Unicamp
AS 53187

Outubro 2022

Agenda:

1. Sobre a Unicamp
2. Visão geral da rede
3. Cronologia da implantação de IPv6
4. Segurança em IPv6
5. Conclusão: Pendências e desafios futuros

1. Sobre a Unicamp

Universidade Pública em Campinas, SP, fundada em 1966 - Terceira maior Universidade da América Latina

6 *Campi*: Campinas, Limeira, Paulínia e Piracicaba - cerca de 7.2 Milhões de m2 de área total

24 Faculdades e Institutos, 4 Hospitais, 2 Colégios Técnicos, 21 Centros e Núcleos Interdisciplinares

21360 Alunos de Graduação em 65 cursos

17750 Alunos de Pós-Graduação em 158 cursos

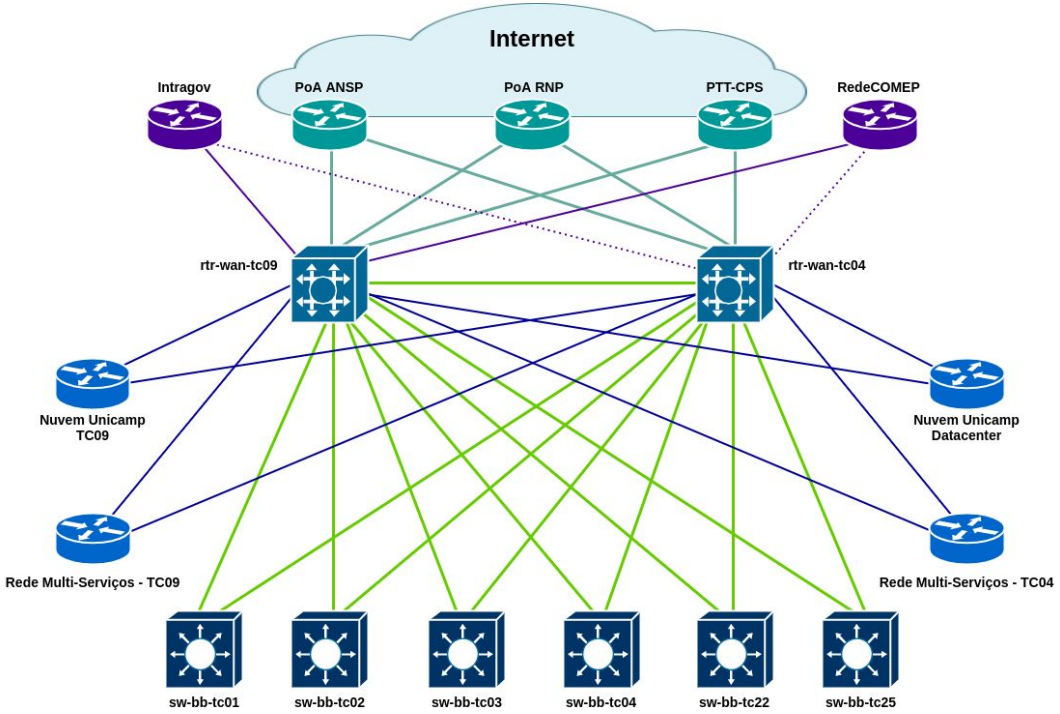
3300 Alunos de Ensino Técnico em 36 cursos

Cerca de 1930 docentes e 6830 servidores

Cerca de 800 mil consultas/ano na área da Saúde

Fonte: Anuário Estatístico Unicamp 2022

2. Visão geral da Rede



AS 53187

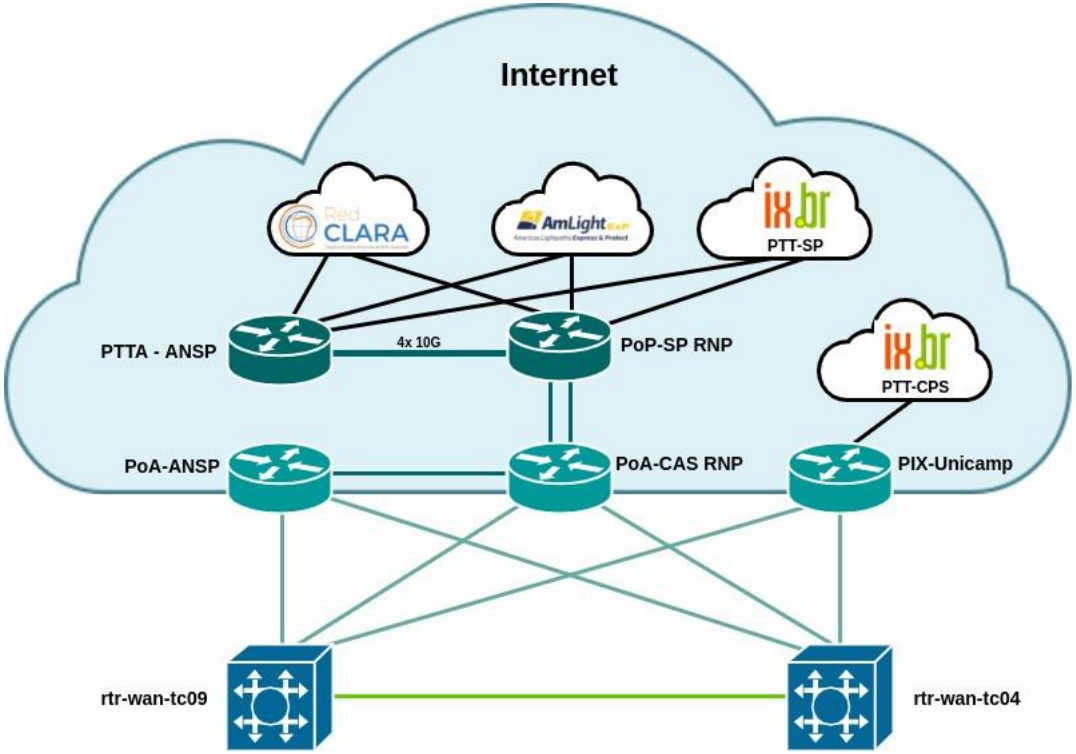
Rede da Unicamp:

- Atende mais de 60 mil usuários diários, entre alunos, docentes, funcionários e visitantes.
- Cerca de 20.000 dispositivos na rede cabeada local.
- Mais de 30.000 dispositivos móveis.
- Rede sem-fio composta por mais de 900 APs - indoor e outdoor
- Cerca de 90 Unidades, conectadas ao backbone, entre Faculdades, Institutos, Centros de Pesquisa e Órgãos Administrativos

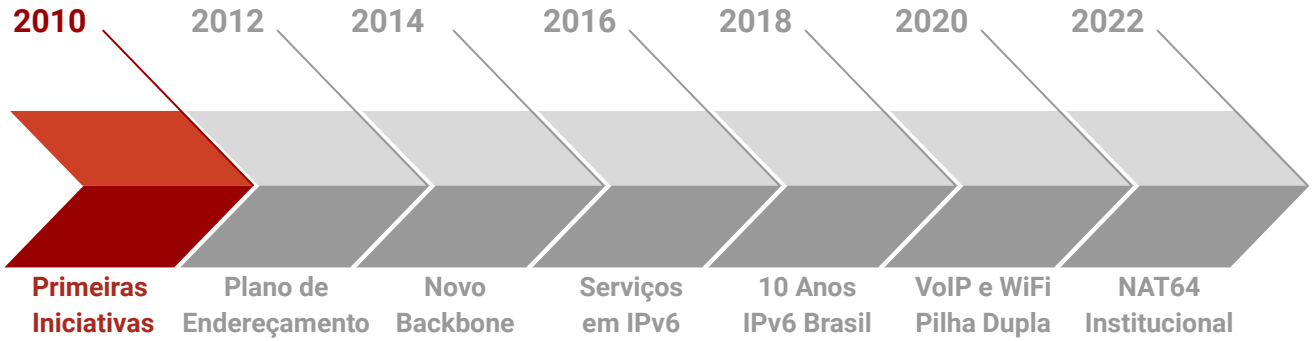
2. Visão geral da Rede

Conexões externas:

- **Conexão principal pela RNP**
  - **Unicamp hospeda o PoA da RNP em Campinas**
  - **Conectividade física para São Paulo (PoP-SP) através da Br.Digital.**
- **Conexões lógicas com a rede da Rednesp (ANSP) e com o IX.br em SP.**
- **Peering com Google, Amazon, Facebook e Router Servers do IX.br**
- **Unicamp hospeda um dos PIX do IX.br em Campinas**



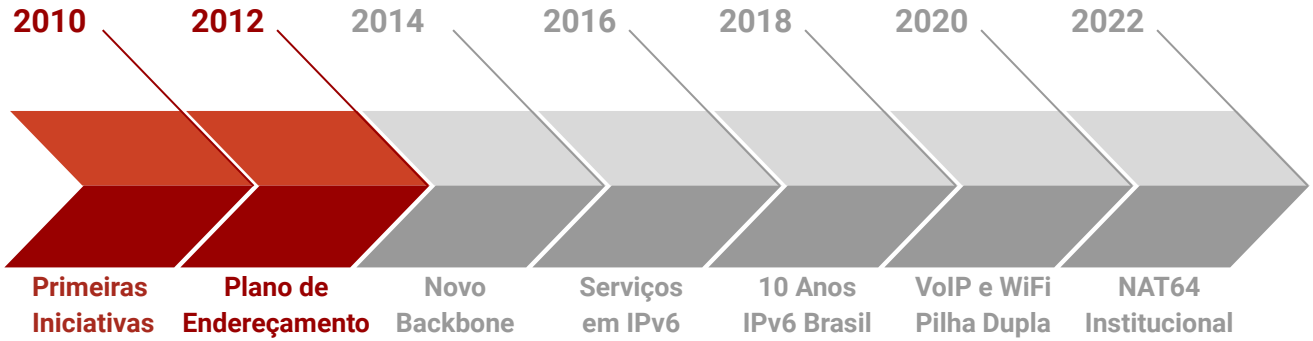
3. Cronologia da implantação do IPv6



2010-2011 - Primeiras iniciativas:

- Criação de um Grupo de Trabalho para estudo da implantação do IPv6
- Capacitação da equipe do GT em parceria com o NIC.br
- Alocação do prefixo IPv6 para o AS 53187 - 2801:8a::/32

3. Cronologia da implantação do IPv6



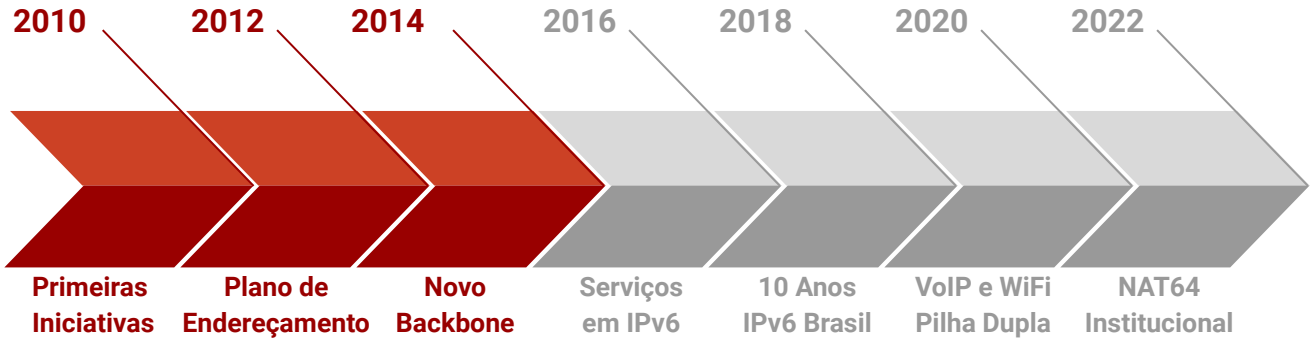
2012 - Início da Implantação:

- Definição do Plano de Endereçamento
- Participação de redes da Unicamp no World IPv6 Launch - Fevereiro/2012
- Equipamentos do backbone ainda não suportam plenamente IPv6

3. Cronologia da implantação do IPv6

Plano de Endereçamento - Unicamp

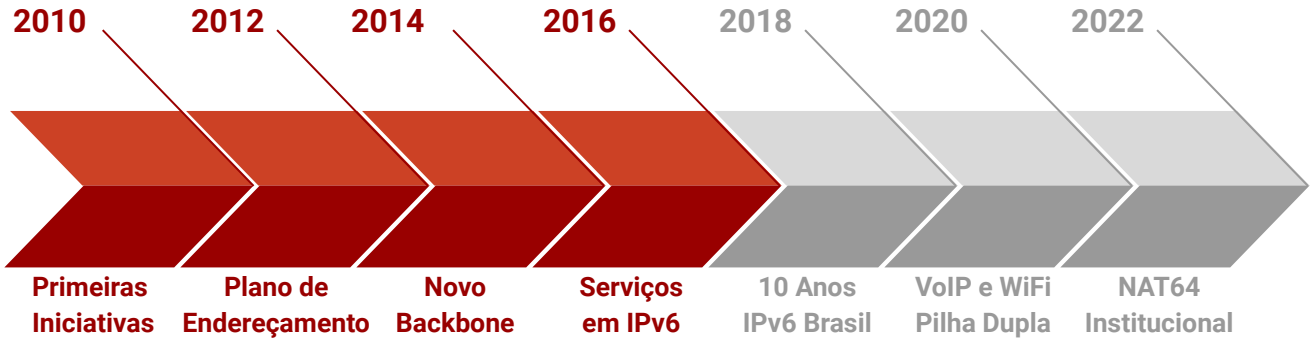
3. Cronologia da implantação do IPv6



2013-2014 - Novo backbone:

- Atualização do backbone com suporte completo a IPv6
- Roteamento externo (sessões BGP) em IPv6
- Disponibilidade de entrega de IPv6 para todas redes internas
- Treinamento on-site pelo NIC.br para os profissionais de redes - 1a. Turma - 50 integrantes

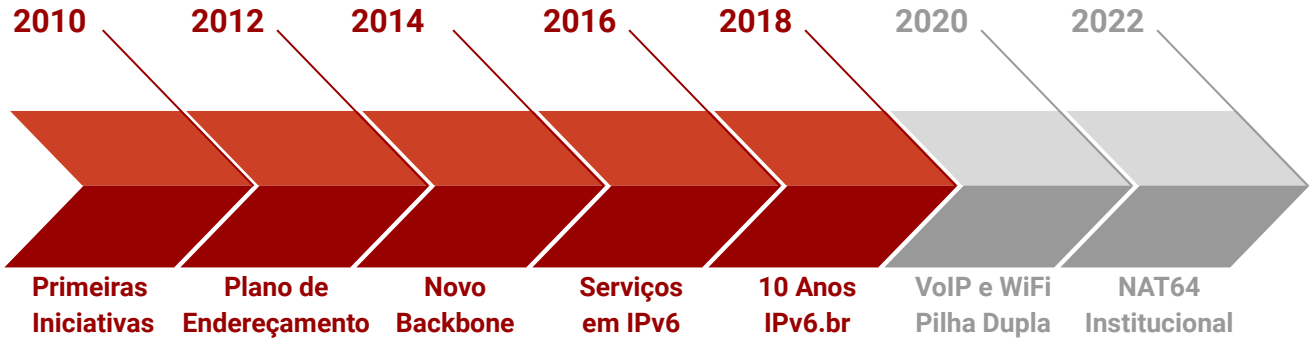
3. Cronologia da implantação do IPv6



2015-2016 - Serviços básicos em IPv6:

- **Servidores DNS:**
  - **Autoritativos para unicamp.br - BIND com pilha dupla, registros AAAA para nomes unicamp.br**
  - **Recursivos Unicamp - Unbound com pilha dupla, respostas para clientes locais via IPv6**
- **Servidores NTP**

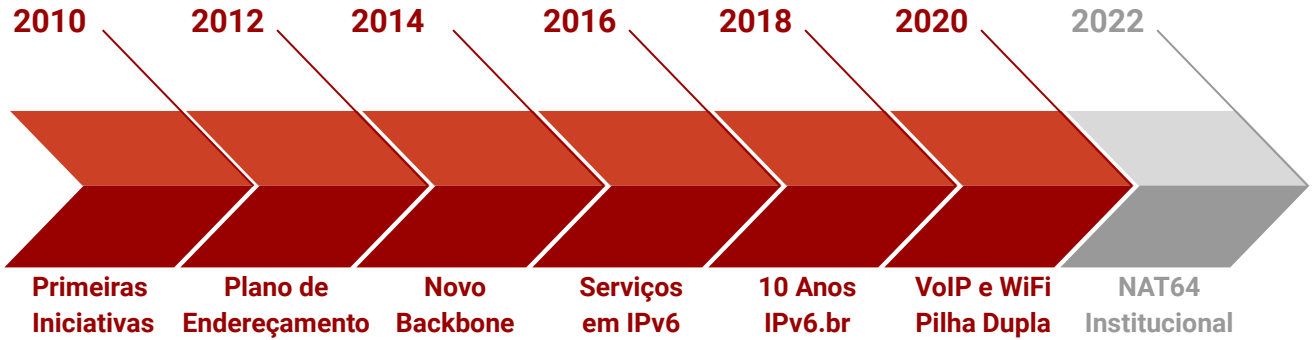
3. Cronologia da implantação do IPv6



2017-2018 - 10 anos da iniciativa IPv6.br:

- Participação na edição de 10 anos do Fórum Brasileiro de IPv6 - 10anos.ipv6.br
- Segunda edição do treinamento on-site pelo NIC.br - 55 participantes

3. Cronologia da implantação do IPv6

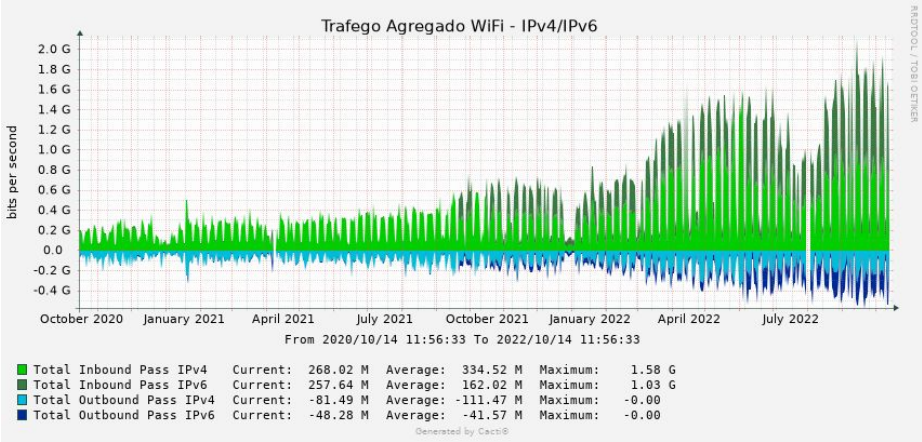


2019-2020 - VoIP e WiFi em pilha dupla:

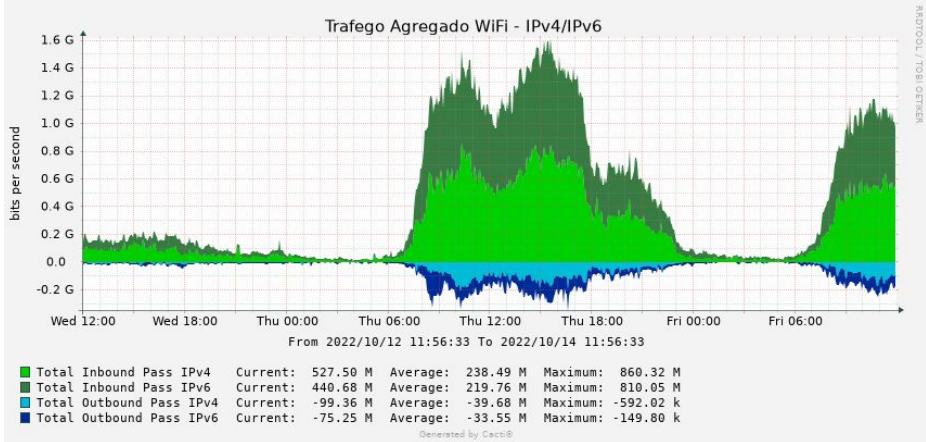
- **Início da implantação de VoIP na rede do campus - puramente IPv6 em algumas unidades**
- **WiFi em pilha dupla:**
  - **Entrega de endereços IPv6 por SLAAC - Stateless Address Auto-Configuration**
  - **Entrega de IPv4 por DHCP - range da classe 100.64.0.0/10 (RFC 6598) roteada dentro da Universidade, com NAT44 para tráfego externo**

3. Cronologia da implantação do IPv6

Tráfego na rede WiFi institucional (pilha dupla)

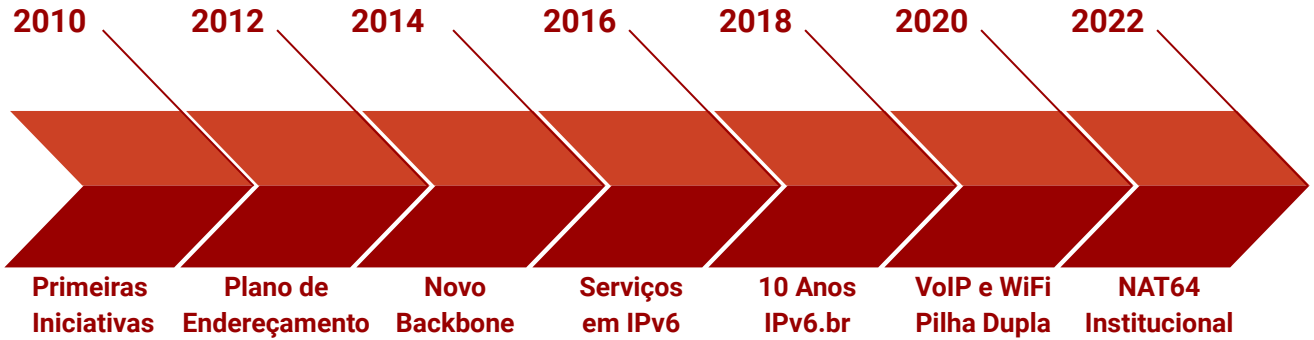


Tráfego IPv4/IPv6 - Último ano



Exemplo de Tráfego diário IPv4/IPv6

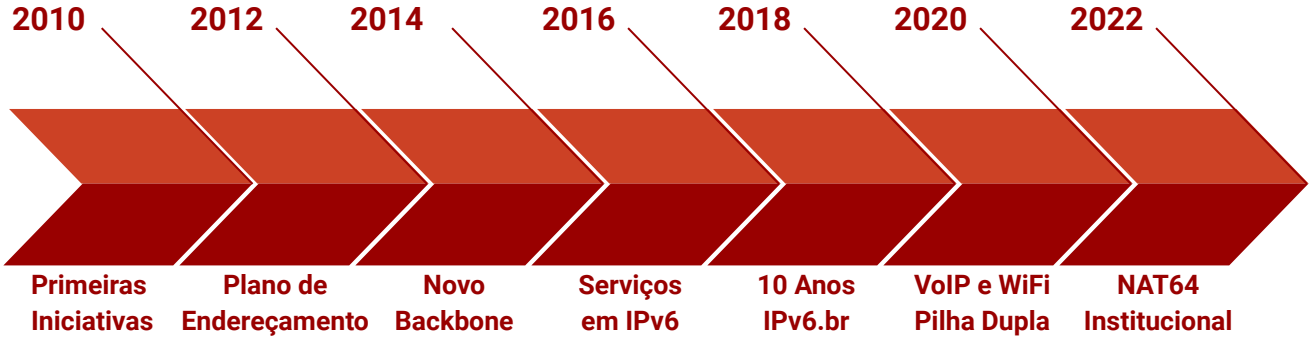
3. Cronologia da implantação do IPv6



2021-2022 - Crescimento no uso de IPv6:

- Aumento do tráfego IPv6 - resultado das iniciativas anteriores, efeito da Pandemia
- Limitações dos roteadores em lidar com o aumento das tabelas de rotas - Instabilidade
- Retrocesso: necessidade de limitar serviços em IPv6 - desativação da pilha dupla em WiFi
- Substituição emergencial dos roteadores de borda (2021) - reativação da pilha dupla
- Trabalho apresentado pela equipe da Unicamp vence o 9o. Desafio IPv6 do LACNIC

3. Cronologia da implantação do IPv6

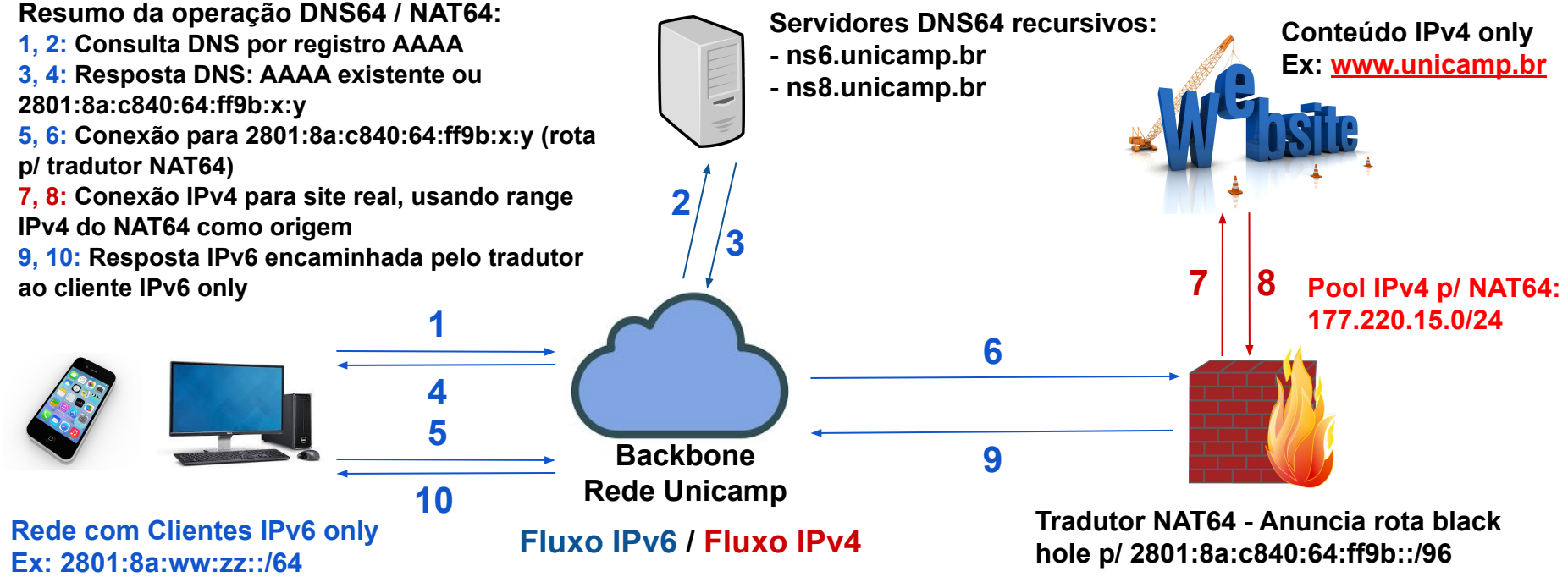


2022 - Implementação de uma solução NAT64 institucional:

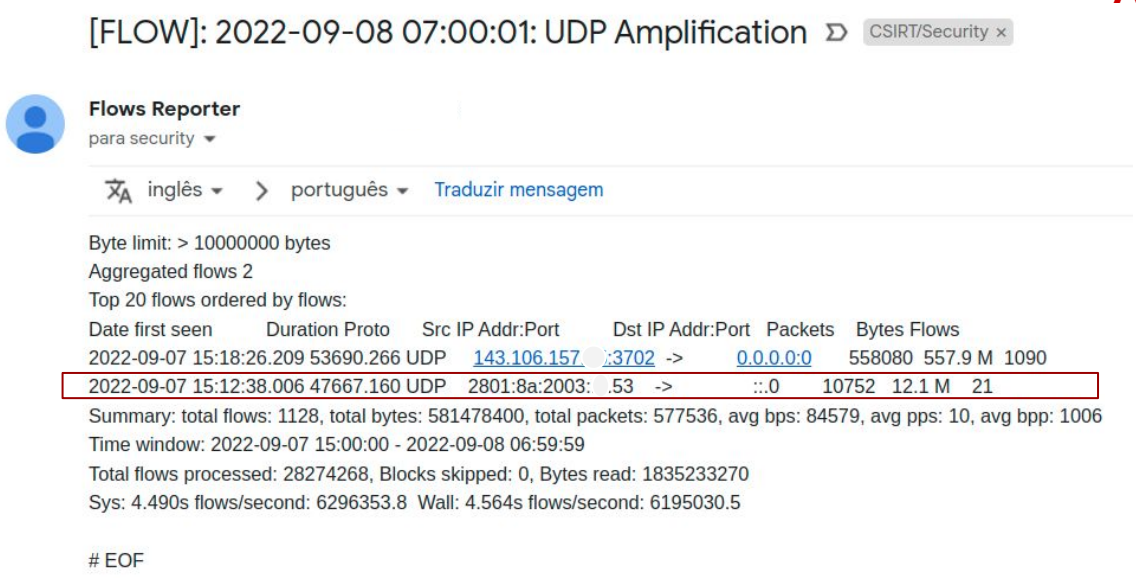
- Resolução DNS64 combinada com tradução NAT64
- Permite a construção de redes locais internas puramente IPv6

3. Cronologia da implantação do IPv6

Resumo da operação DNS64 / NAT64:
1, 2: Consulta DNS por registro AAAA
3, 4: Resposta DNS: AAAA existente ou 2801:8a:c840:64:ff9b:x:y
5, 6: Conexão para 2801:8a:c840:64:ff9b:x:y (rota p/ tradutor NAT64)
7, 8: Conexão IPv4 para site real, usando range IPv4 do NAT64 como origem
9, 10: Resposta IPv6 encaminhada pelo tradutor ao cliente IPv6 only



4. Segurança em IPv6:



[FLOW]: 2022-09-08 07:00:01: UDP Amplification CSIRT/Security ×

Flows Reporter
para security

inglês > português Traduzir mensagem

Byte limit: > 10000000 bytes
Aggregated flows 2
Top 20 flows ordered by flows:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port		Packets	Bytes	Flows
2022-09-07 15:18:26.209	53690.266	UDP	143.106.157.	:3702	->	0.0.0.0:0	558080	557.9 M	1090
2022-09-07 15:12:38.006	47667.160	UDP	2801:8a:2003:	.53	->	::.0	10752	12.1 M	21

Summary: total flows: 1128, total bytes: 581478400, total packets: 577536, avg bps: 84579, avg pps: 10, avg bpp: 1006
Time window: 2022-09-07 15:00:00 - 2022-09-08 06:59:59
Total flows processed: 28274268, Blocks skipped: 0, Bytes read: 1835233270
Sys: 4.490s flows/second: 6296353.8 Wall: 4.564s flows/second: 6195030.5

EOF

Análise de tráfego através de Flows:

- Captura de tráfego via sFlow nos roteadores de backbone.
- Análise das amostras pelo coletor e geração de relatórios personalizados utilizando scripts desenvolvidos pelo CSIRT/Unicamp
- Relatórios enviados por e-mail para avaliação pela equipe do CSIRT.

4. Segurança em IPv6:

Exemplos de relatórios de Flows:

- Top talkers - maiores tráfegos
- Maiores tráfegos em SMTP
- Amplificação de UDP
- Participação em Botnets
- Suspeita de mineração de criptomoedas

[FLOW]: 2022-09-11 07:00:01: Top Talkers CSIRT/Security ×

Flows Reporter
para security

inglês > português Traduzir mensagem

Byte limit: > 20000000000 bytes
Top 20 Src IP Addr ordered by bytes:

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2022-09-10 15:00:01.097	57598.571	any	143.106.7..	524526(13.6)	268.6 M(12.1)	241.6 G(22.9)	4662	33.6 M	899
2022-09-10 21:53:29.588	30918.145	any	177.220.97.	10949(0.3)	89.7 M(4.0)	131.3 G(12.5)	2900	34.0 M	1464
2022-09-10 15:00:32.788	57388.126	any	2801:8a:2040:4000:	87407(2.3)	44.8 M(2.0)	67.4 G(6.4)	779	9.4 M	1505
2022-09-10 15:02:20.970	57436.807	any	143.106.6..	17986(0.5)	34.8 M(1.6)	51.6 G(4.9)	606	7.2 M	1480

Summary: total flows: 3859100, total bytes: 1053060682240, total packets: 2226695680, avg bps: 146258542, avg pps: 38657, avg bpp: 472
Time window: 2022-09-10 15:00:00 - 2022-09-11 06:59:59
Total flows processed: 26157438, Blocks skipped: 0, Bytes read: 1699759677
Sys: 5.050s flows/second: 5179373.8 Wall: 5.513s flows/second: 4744258.0

EOF

Maiores detalhes sobre o processo de captura e análise:

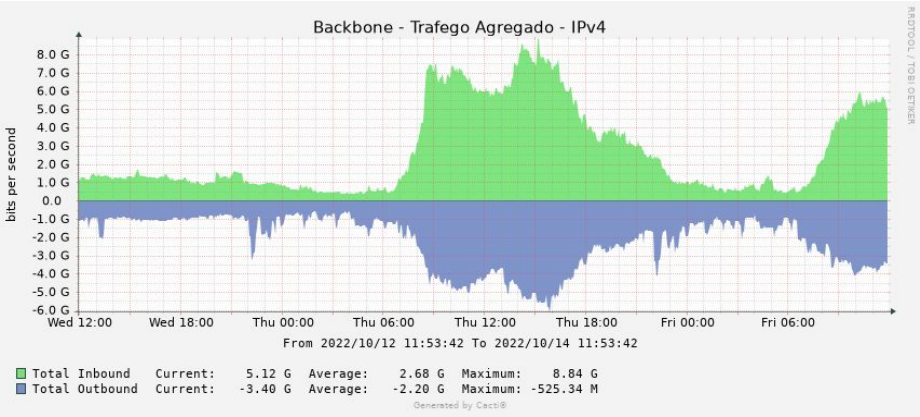
- PDF - Apresentação do CSIRT/Unicamp no 4o. Fórum de CSIRTs - CERT.br - 2015
- Vídeo - Uso de Flows no Tratamento de Incidentes de Segurança - GTS 26 (2015)

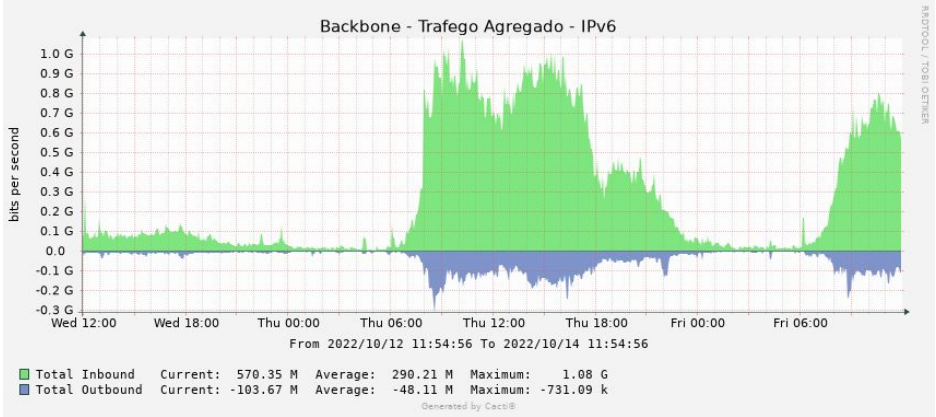
5. Conclusão: Pendências e desafios futuros:

- **Nuvem Unicamp sem suporte a IPv6:**
  - **Impacto: sites corporativos sem acesso via IPv6 - tráfego IPv6 inbound menor**
  - **Limitação do orquestrador Cloudstack - migração prevista para VMWare vCloud**
- **Sistemas Legados:**
  - **Software com código que referencia diretamente endereços IPv4**
  - **Aplicações com controle de acesso que não suportam IPv6**
- **Migração da rede WiFi para um ambiente puramente IPv6:**
  - **Motivação: evitar o uso de endereçamento IPv4 privado na rede sem-fio**
  - **Desafios impostos por dispositivos legados:**
    - **Android anterior a 4.0) não suporta IPv6**
    - **Android sem suporte a DHCPv6**
- **Maior adoção de IPv6 pelas unidades:**
  - **Necessidade de investimento em RH e/ou (re)capacitação**
  - **Ativação de IPv6 nativo na rede MPLS Intragov que atende algumas unidades remotas**

5. Conclusão: Pendências e desafios futuros:

Utilização diária de IPv4 e IPv6 no backbone





Tráfego IPv6 representa em torno de 10% do total de tráfego interno

Agradecimentos:

- NIC.br
- Equipe da DRSI/CCUEC/Unicamp
- Grupo de Trabalho em IPv6
- Comunidade de TIC da Unicamp

Questões?

Contatos:

- Equipe de Redes Unicamp - noc@unicamp.br
- CSIRT/Unicamp - security@unicamp.br
- Grupo de Trabalho IPv6 - ipv6@unicamp.br