# Desafios em Segurança para Redes de Acesso via Rádio Abertas

Igor Monteiro Moraes

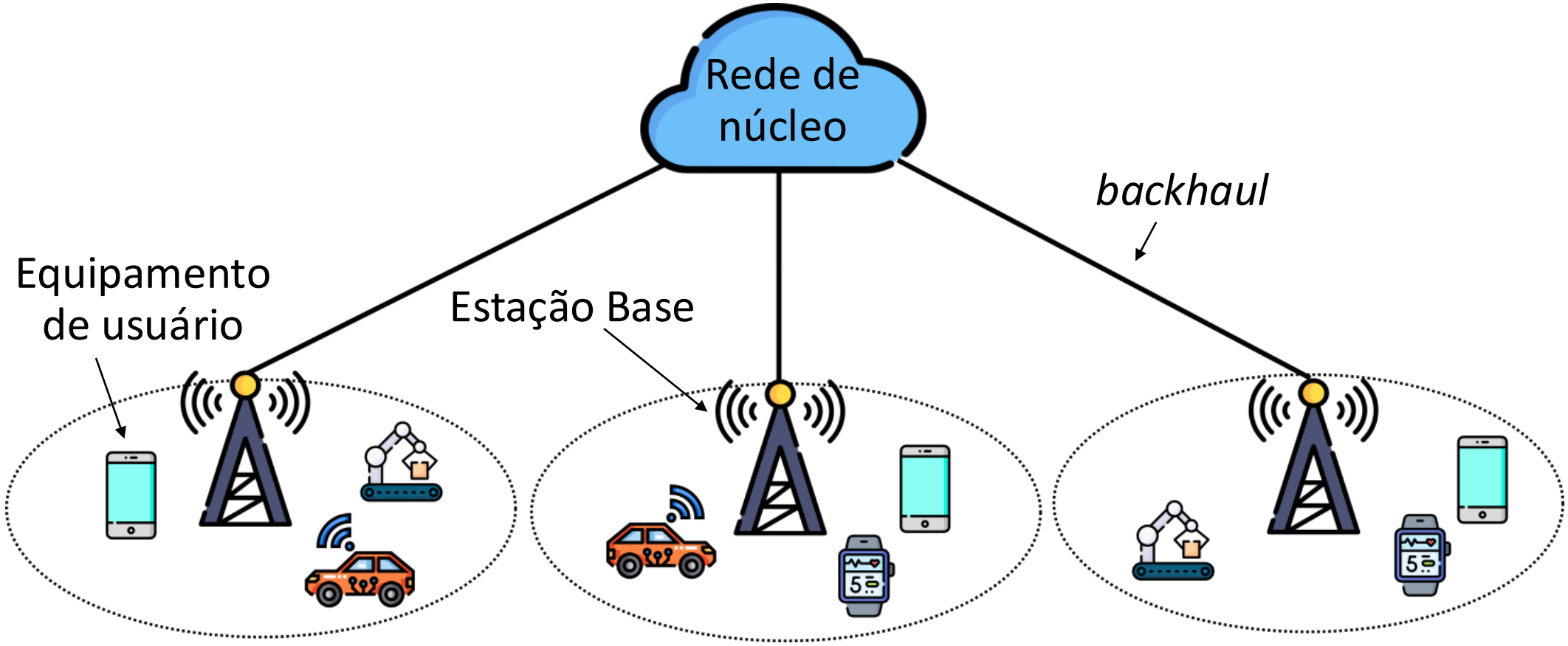
Laboratório Mídiacom
Instituto de Computação
Universidade Federal Fluminense - UFF



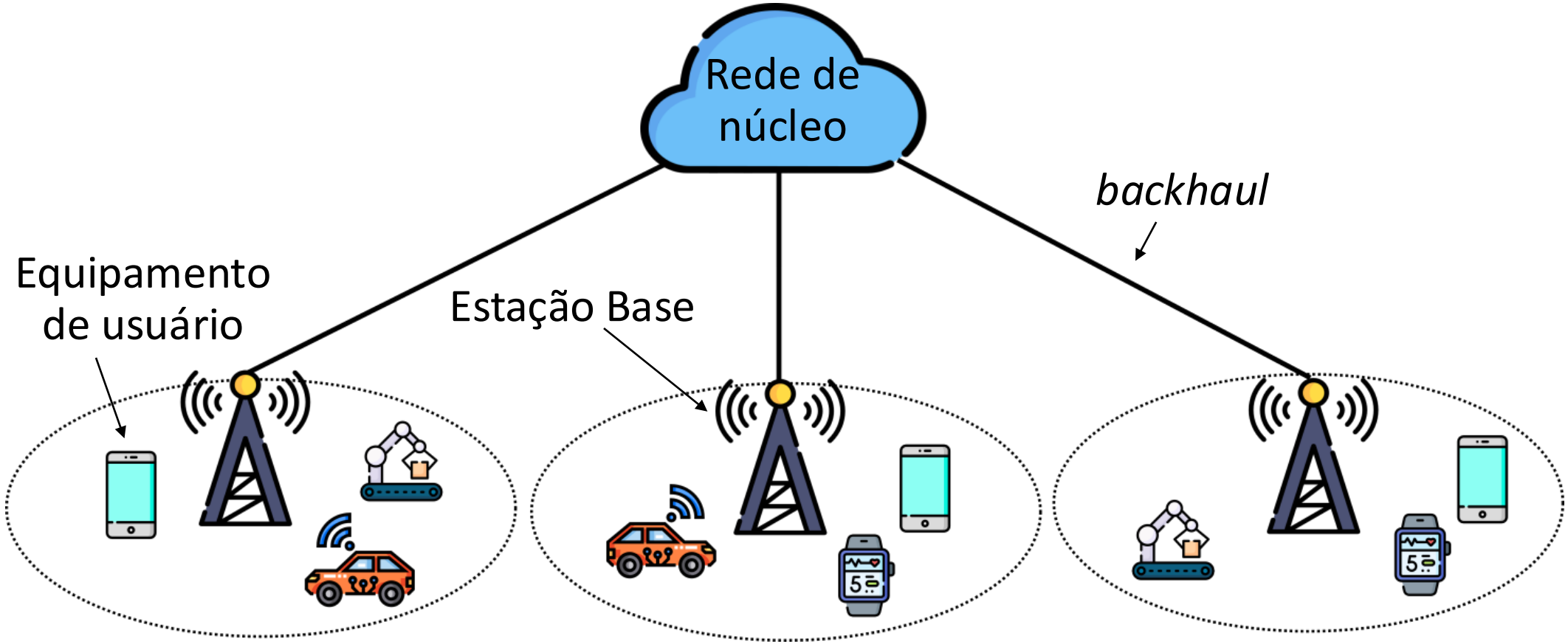
# O que é uma RAN (*Radio Access Network*)?

# O que é uma RAN (*Radio Access Network*)?

# O que é uma RAN (*Radio Access Network*)?



# O que é uma RAN (*Radio Access Network*)?

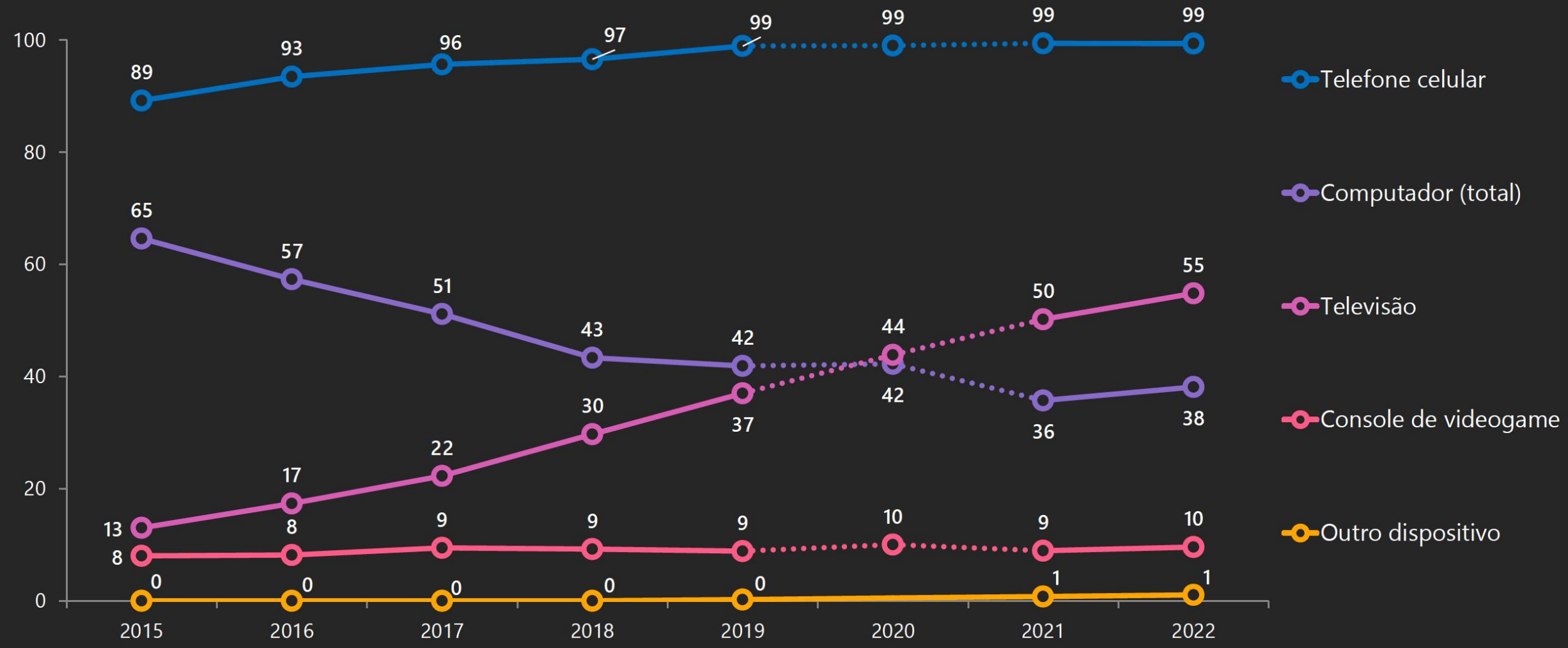



A RAN interconecta os equipamentos de usuários à rede de núcleo através de um enlace de rádio

C16

# USUÁRIOS DE INTERNET, POR DISPOSITIVO UTILIZADO (2015-2022)

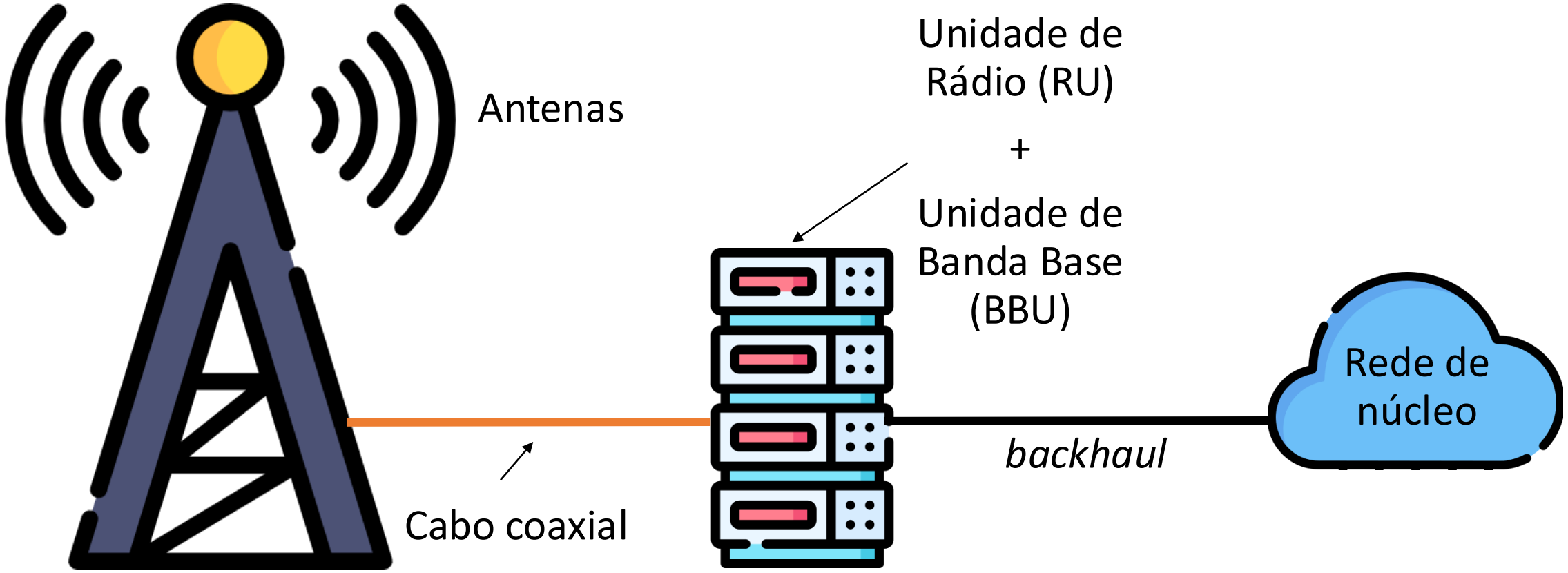
Total de usuários de Internet (%)




Fonte: CGI.br. (2023). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2022.

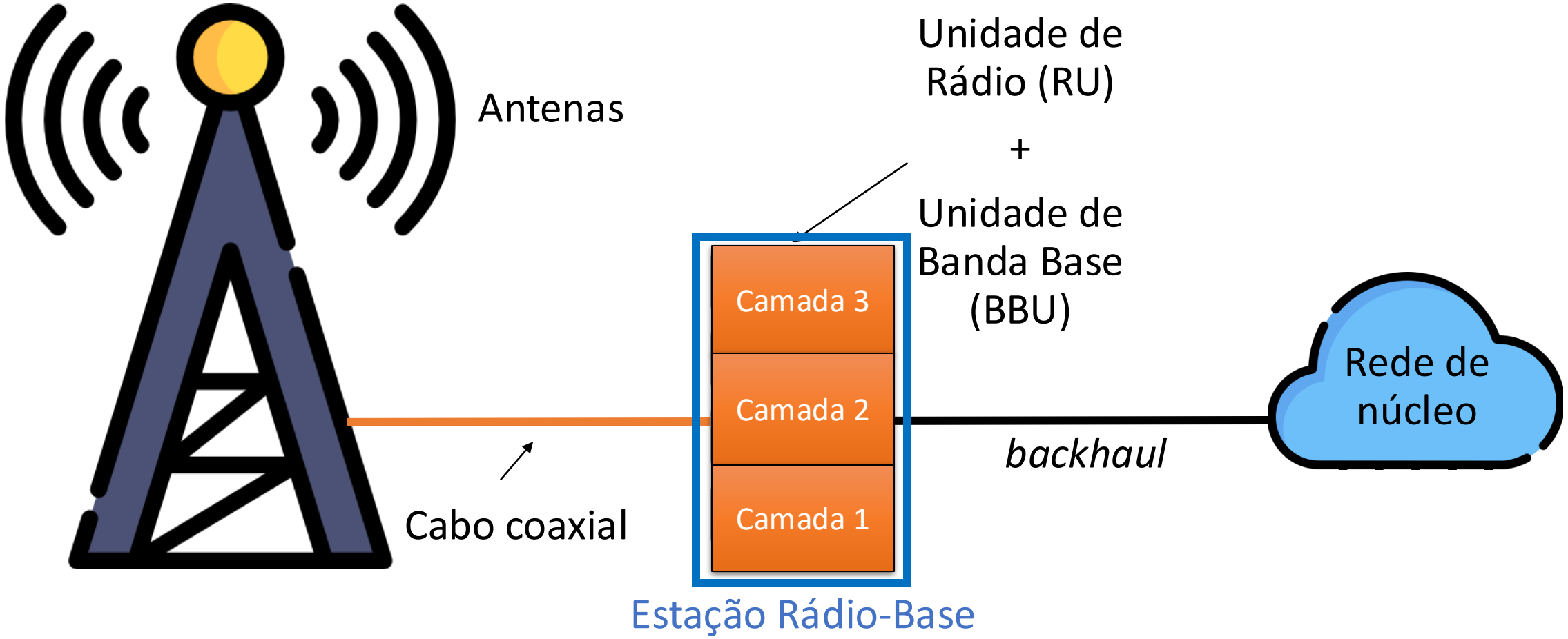
cetic.br nic.br cgi.br

# RAN Tradicional – 1G e 2G

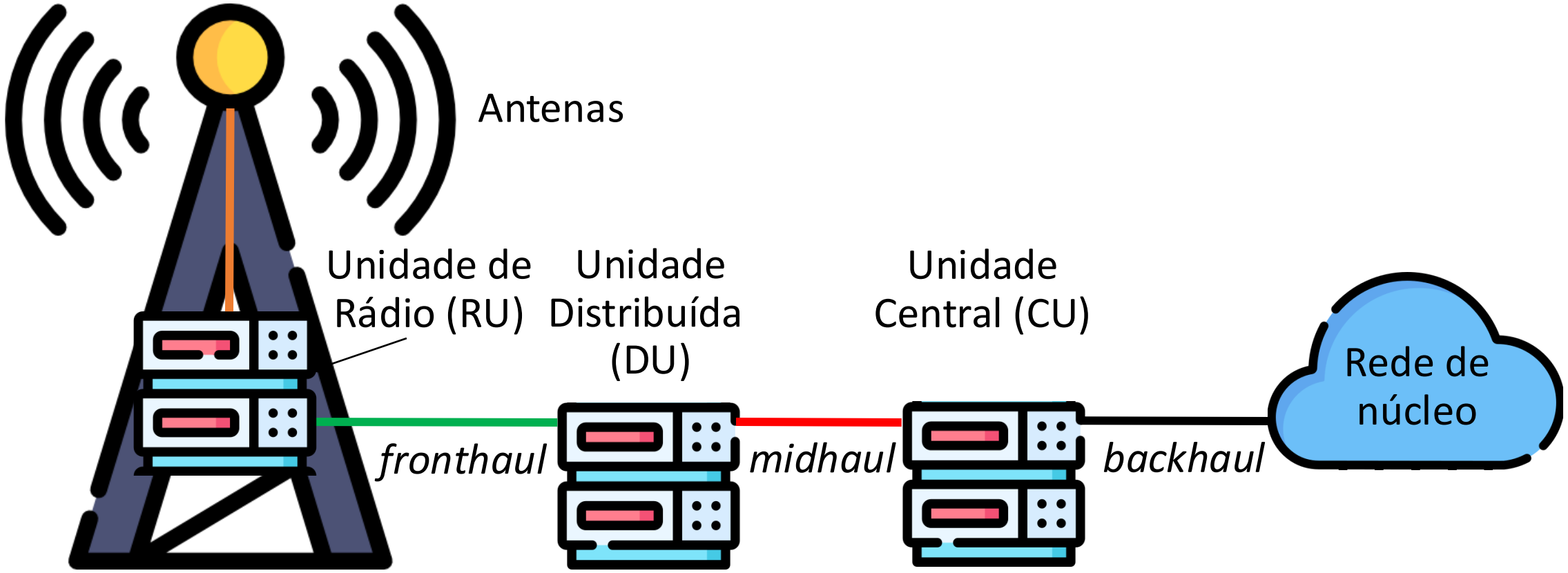



Estação Rádio-Base

# RAN Tradicional – 1G e 2G

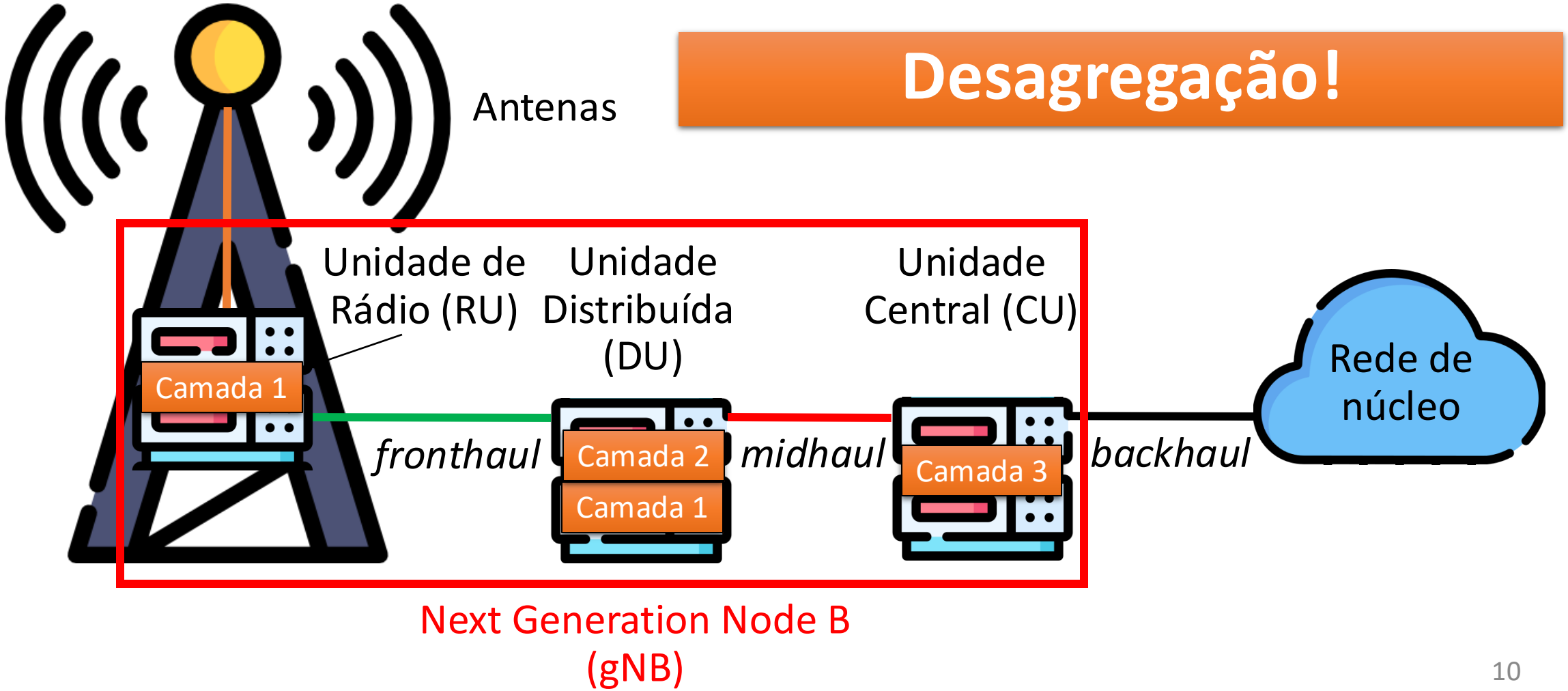


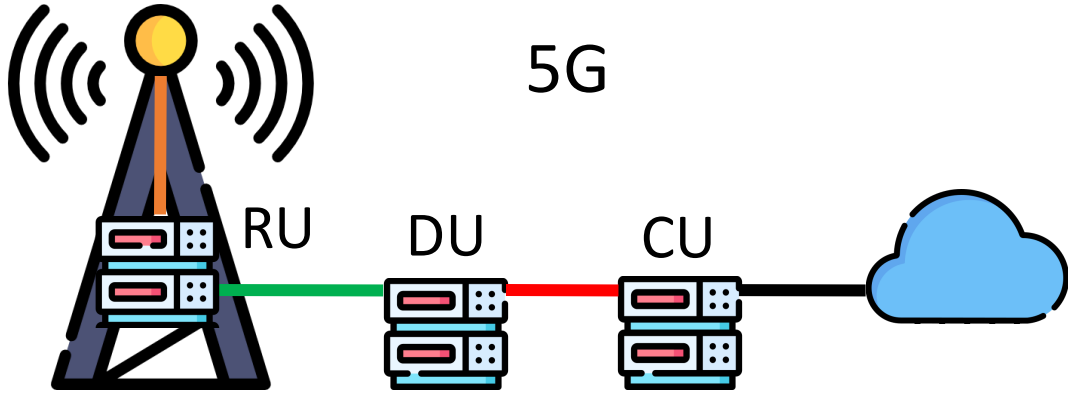
# RAN Contemporânea – 5G



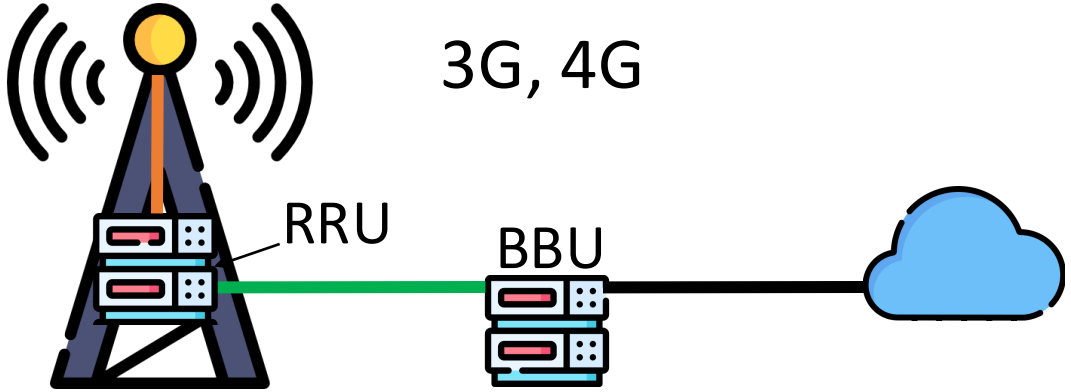

Next Generation Node B (gNB)

# RAN Contemporânea – 5G

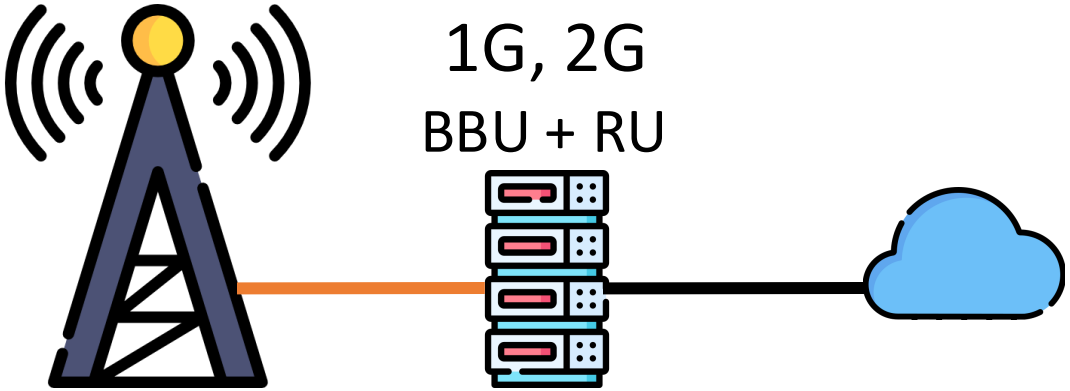





- Sistema proprietário e fechado
- Sem interfaces abertas
- Sem interoperabilidade
- Desagregação ainda maior




- Sistema proprietário e fechado
- Sem interfaces abertas
- Sem interoperabilidade
- Desagregação

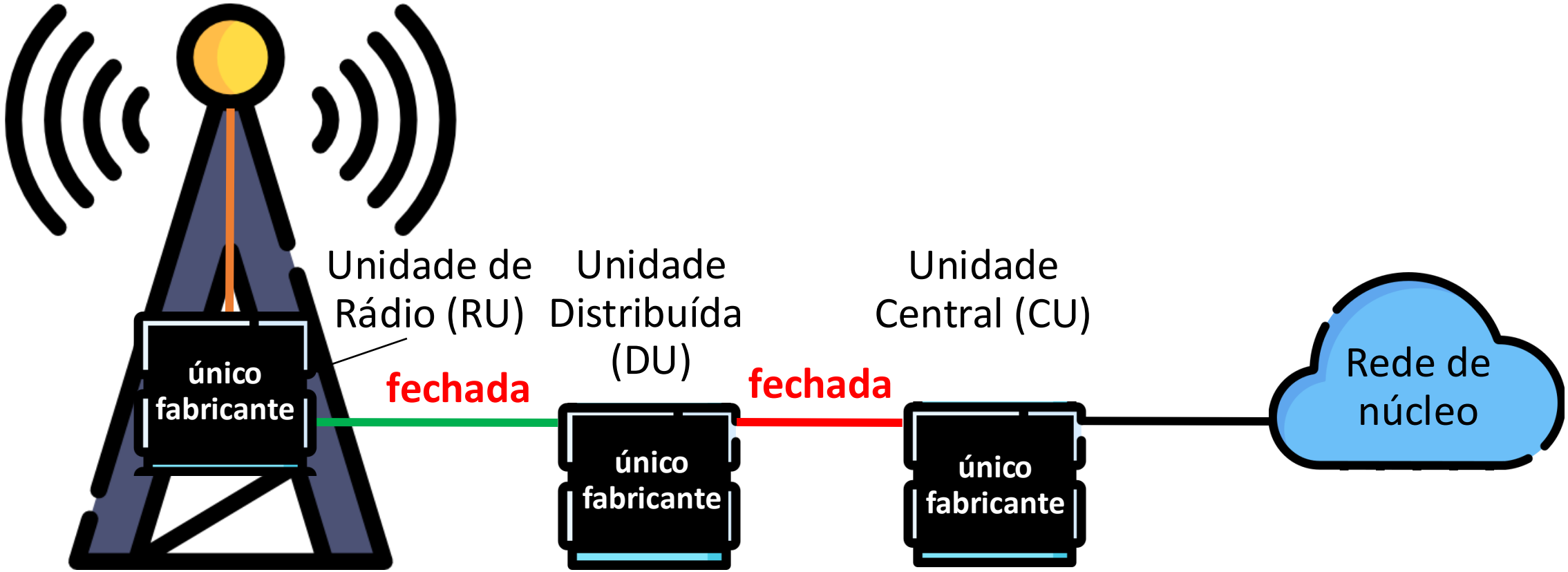



- Sistema proprietário e fechado
- Sem interfaces abertas
- Sem interoperabilidade

desagregação

# As interfaces continuam fechadas e proprietárias!

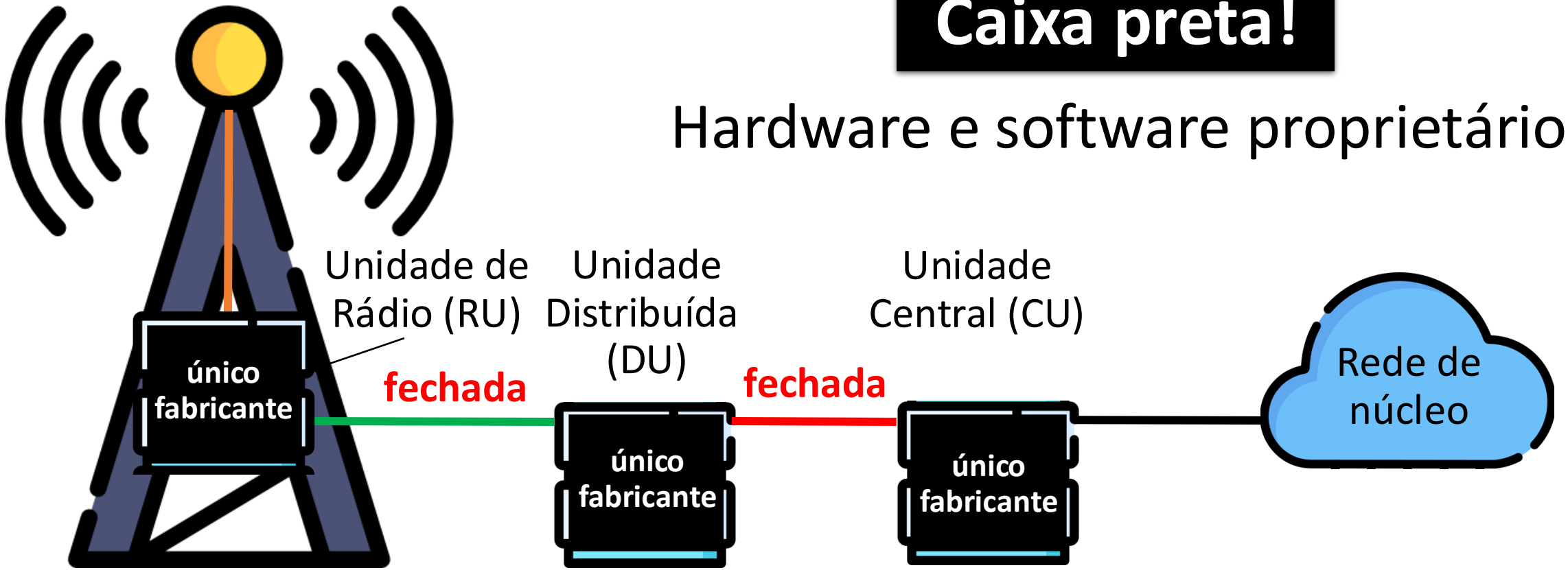
# RAN Contemporânea – 5G



# RAN Contemporânea – 5G

**Caixa preta!**

Hardware e software proprietários

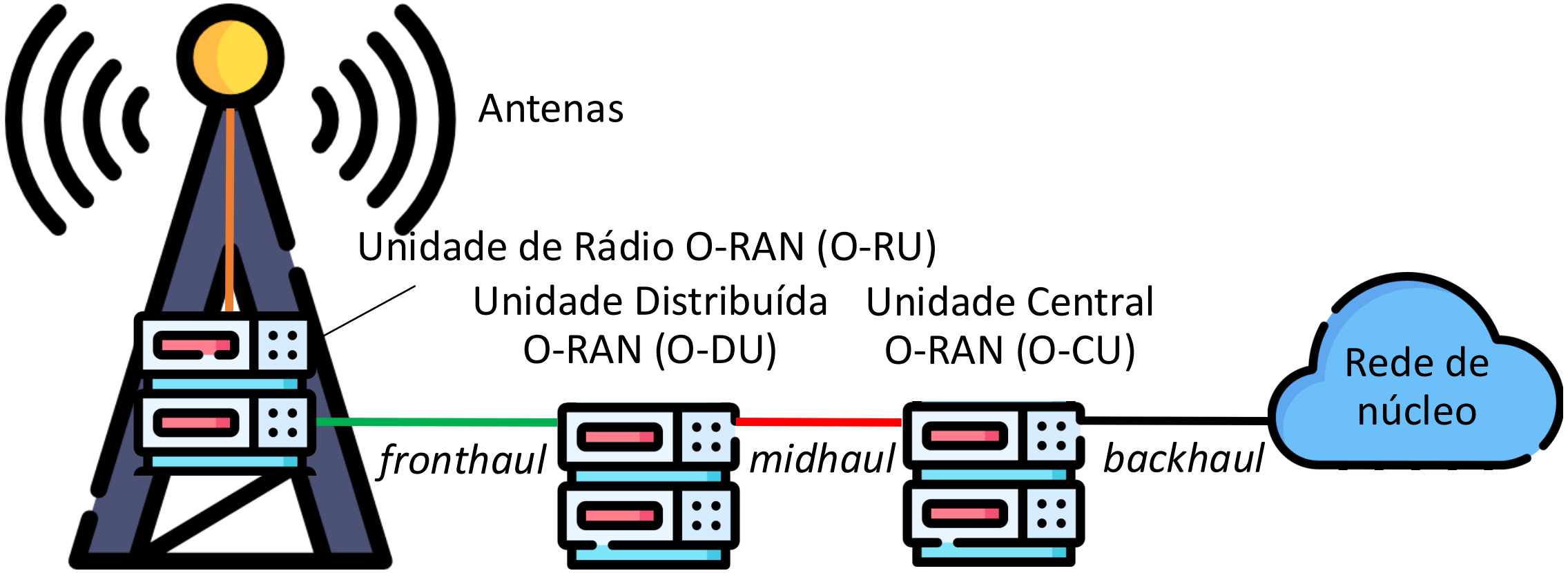


# Problemas

- Limitação da capacidade de reconfiguração e refinamento da operação
  - Diversidade de implementações e diferentes perfis de tráfego
- Dificuldade de otimização e controle dos componentes da RAN de forma conjunta
- Dificuldade de operação de múltiplas gerações da rede
  - Resulta em bloqueio de fornecedor
  - Operadoras limitadas a soluções verticais de um único fornecedor

# O próximo passo é...

# RAN Aberta – O-RAN




Next Generation Node B
(gNB)

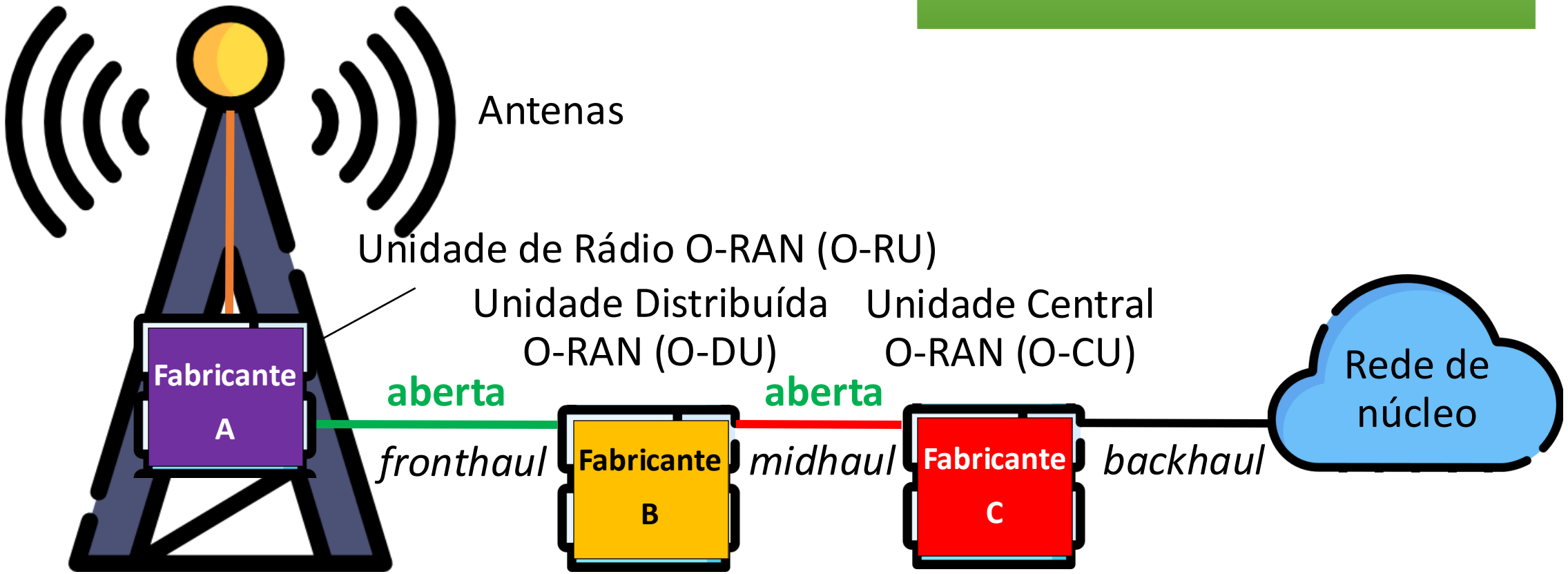
# RAN Aberta – O-RAN

**Interfaces abertas!**


Next Generation Node B (gNB)

# RAN Aberta – O-RAN

**Interfaces abertas!**




Next Generation Node B (gNB)

# RAN Aberta – O-RAN

**Interfaces abertas!**

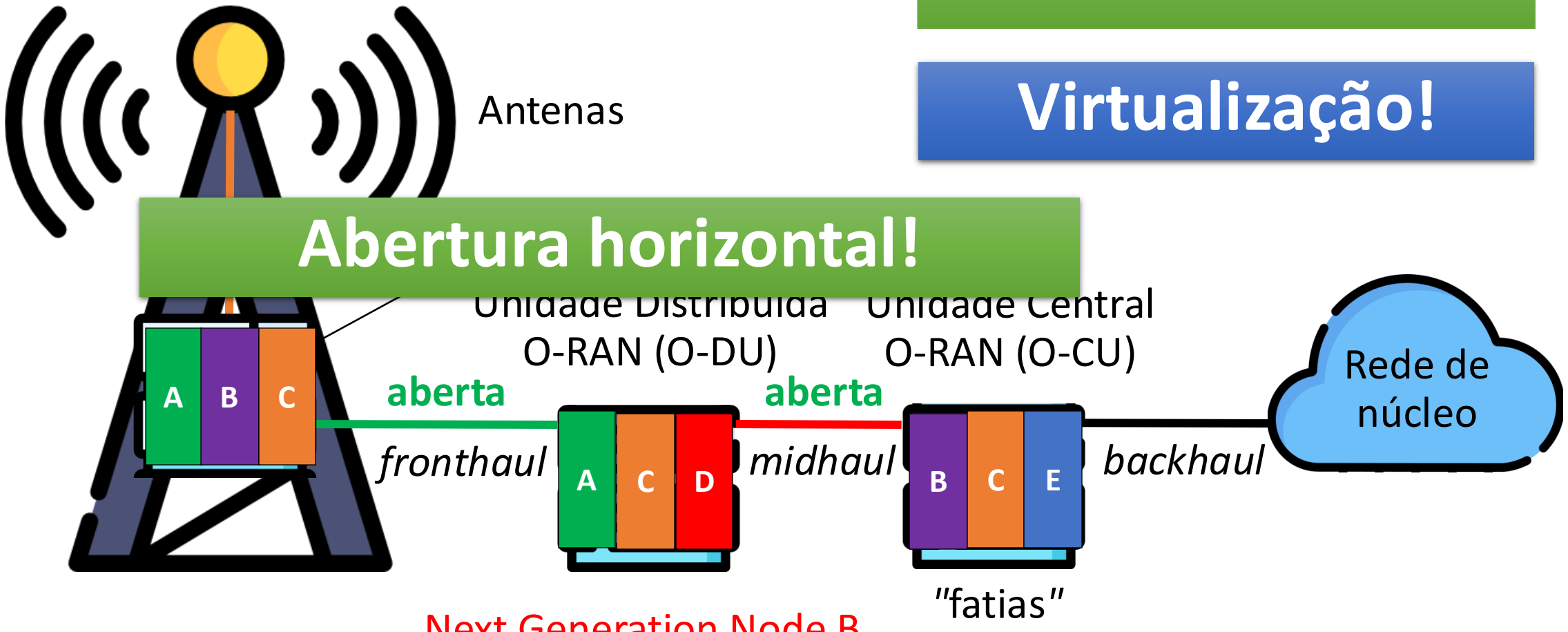

Next Generation Node B
(gNB)

# RAN Aberta – O-RAN

**Interfaces abertas!**

**Virtualização!**

**Abertura horizontal!**

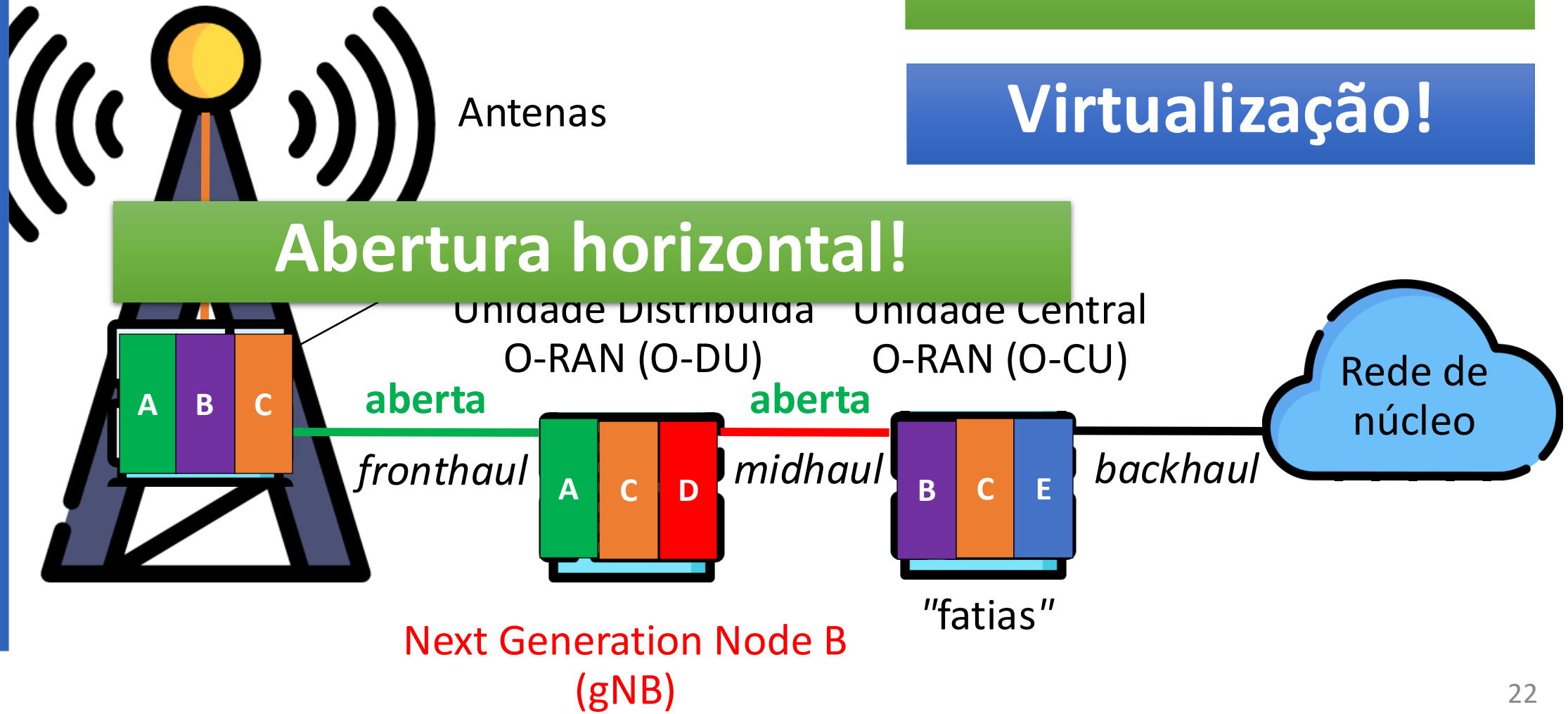


# RAN Aberta – O-RAN

Abertura vertical!

Interfaces abertas!

Virtualização!



# Vantagens da O-RAN

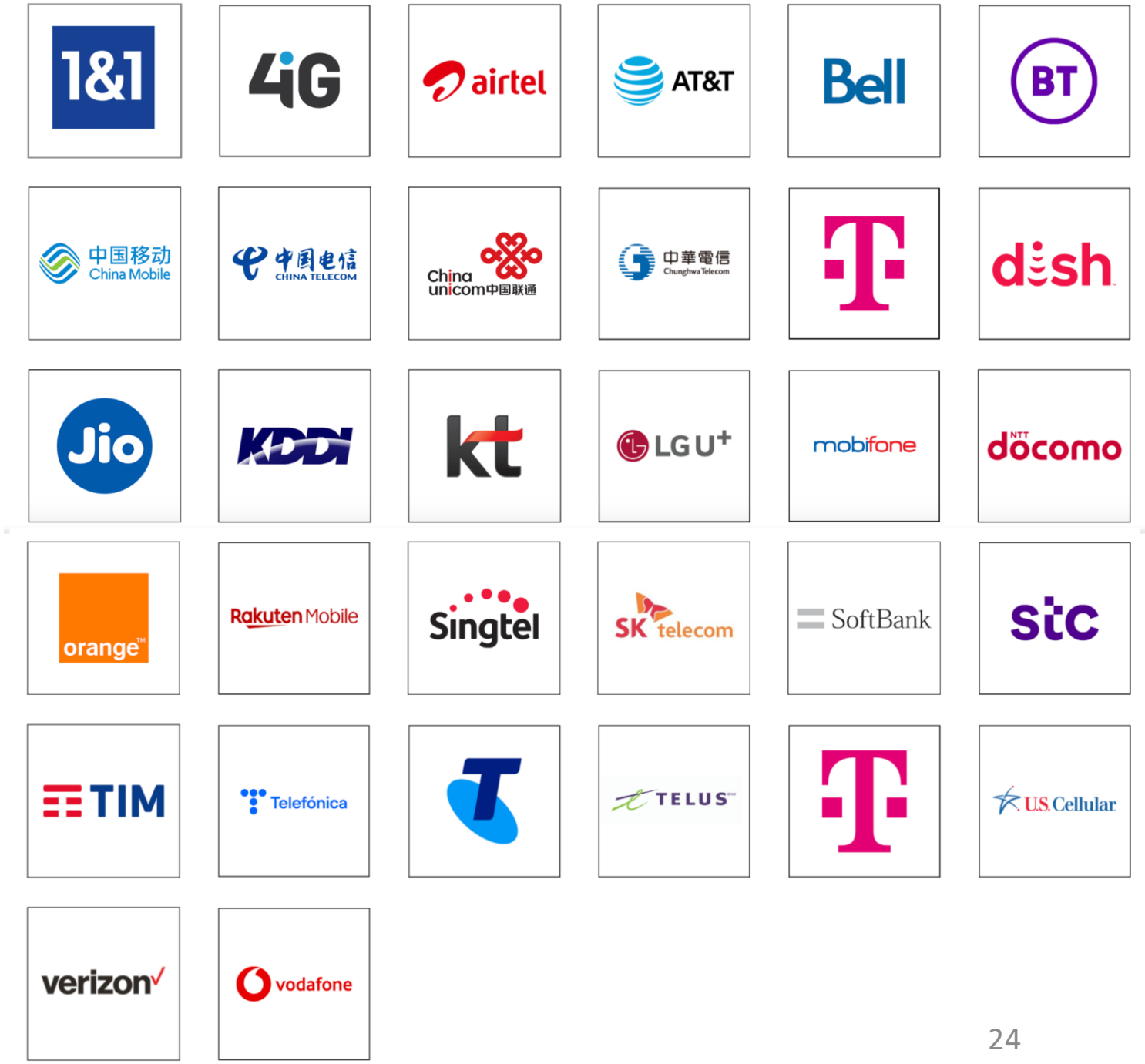
- Desagregação dos componentes + virtualização
  - Implantação da RAN com base em princípios de soluções nativas em nuvem
- Interfaces abertas e padronizadas
  - Empresas menores podem propor soluções
- Divisão das funções de rede em componentes de *software* e *hardware* agnósticos a fornecedores
  - Capacidade de fornecer fatias de rede virtual sob demanda
- Orquestração e gerenciamento de componentes
- **Controle inteligente**

# Membros da O-RAN Alliance

## 32 operadoras

## +

288 instituições contribuidoras (academia e indústria)



gov.br

Órgãos do Governo | Acesso à Informação | Legislação | Acessibilidade | Olá, **Igor**

Ministério da Ciência, Tecnologia e Inovação

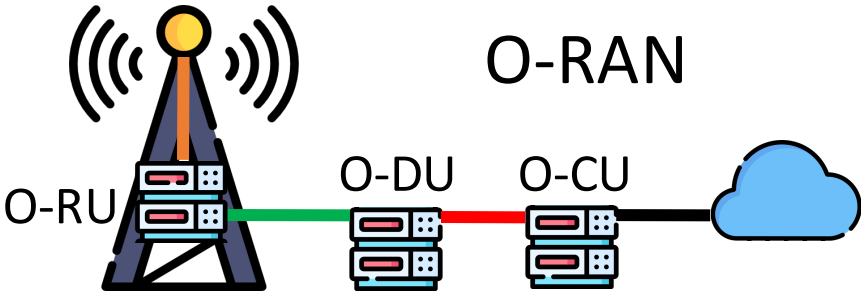
*O que você procura?*

> Assuntos > Notícias > 2021 > 12 > RNP/MCTI e CPQD firmam Acordo de Cooperação Técnica para o Programa OpenRAN @Brasil

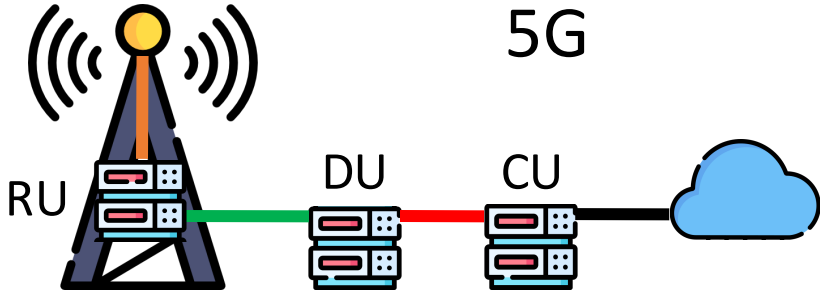
# RNP/MCTI e CPQD firmam Acordo de Cooperação Técnica para o Programa OpenRAN @Brasil

Lançado em agosto de 2021, o Programa OpenRAN Brasil está dividido em três fases. A primeira será focada no controle e orquestração tanto dos recursos ópticos, IP e de rádio quanto dos recursos de nuvem necessários ao funcionamento fim-a-fim de uma rede 5G. Com 36 meses de vigência (até novembro de 2023), o projeto receberá recursos da Lei de Informática e prevê a aplicação de um total de R$ 32,4 milhões em recursos orçamentários.

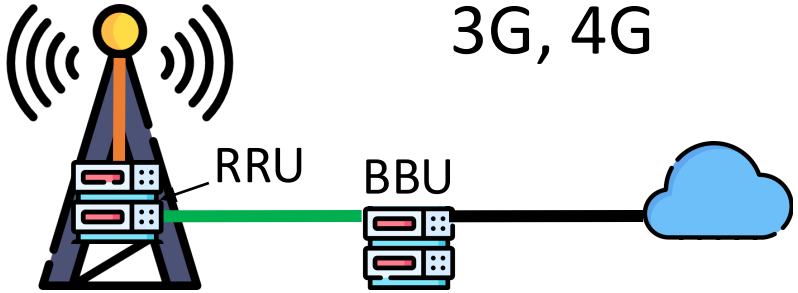
Fonte: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2021/12/rnp-mcti-e-cpqd-firmam-acordo-de-cooperacao-tecnica-para-o-programa-openran-brasil



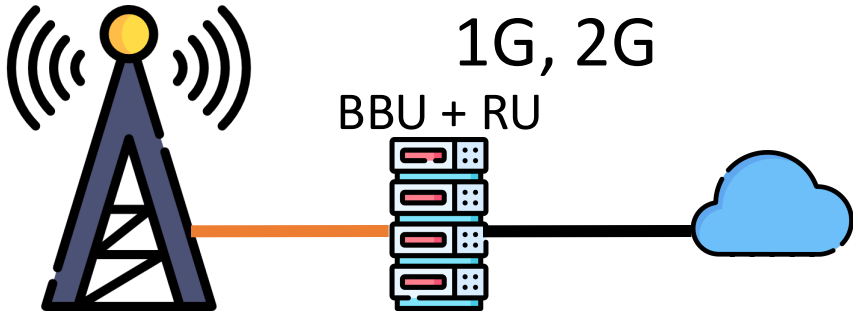

- **HW e SW agnósticos**
- **Interfaces abertas**
- **Multi-fabricante**
- **Virtualização**




- Sistema proprietário e fechado
- Sem interfaces abertas
- Sem interoperabilidade
- Desagregação ainda maior




- Sistema proprietário e fechado
- Sem interfaces abertas
- Sem interoperabilidade
- Desagregação

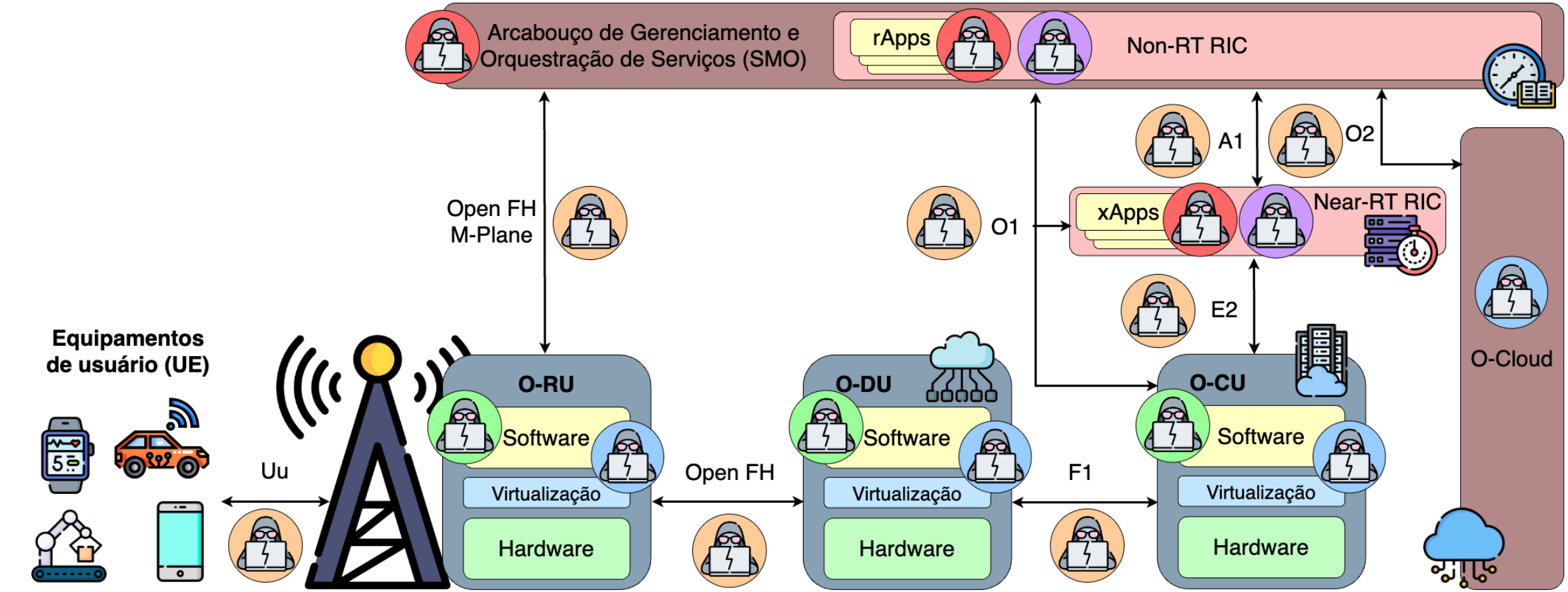



- Sistema proprietário e fechado
- Sem interfaces abertas
- Sem interoperabilidade

# E a segurança?

**E a segurança?**
**Aumento da superfície de ataque!**

# Superfície de Ataque na RAN Aberta




Ameaças aos componentes O-RAN

Ameaças às interfaces abertas

Ameaças ao software de código-fonte aberto

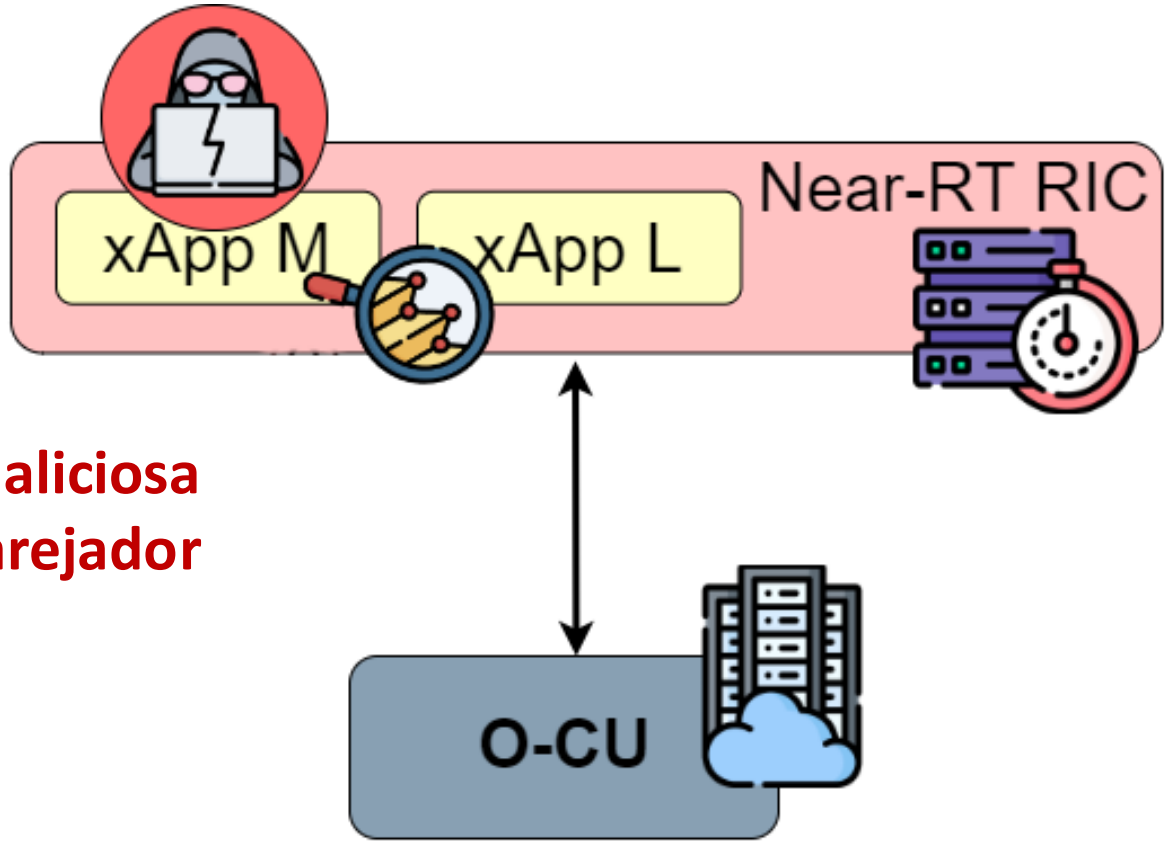
Ameaças à virtualização

Ameaças à inteligência artificial

# Aplicações Maliciosas

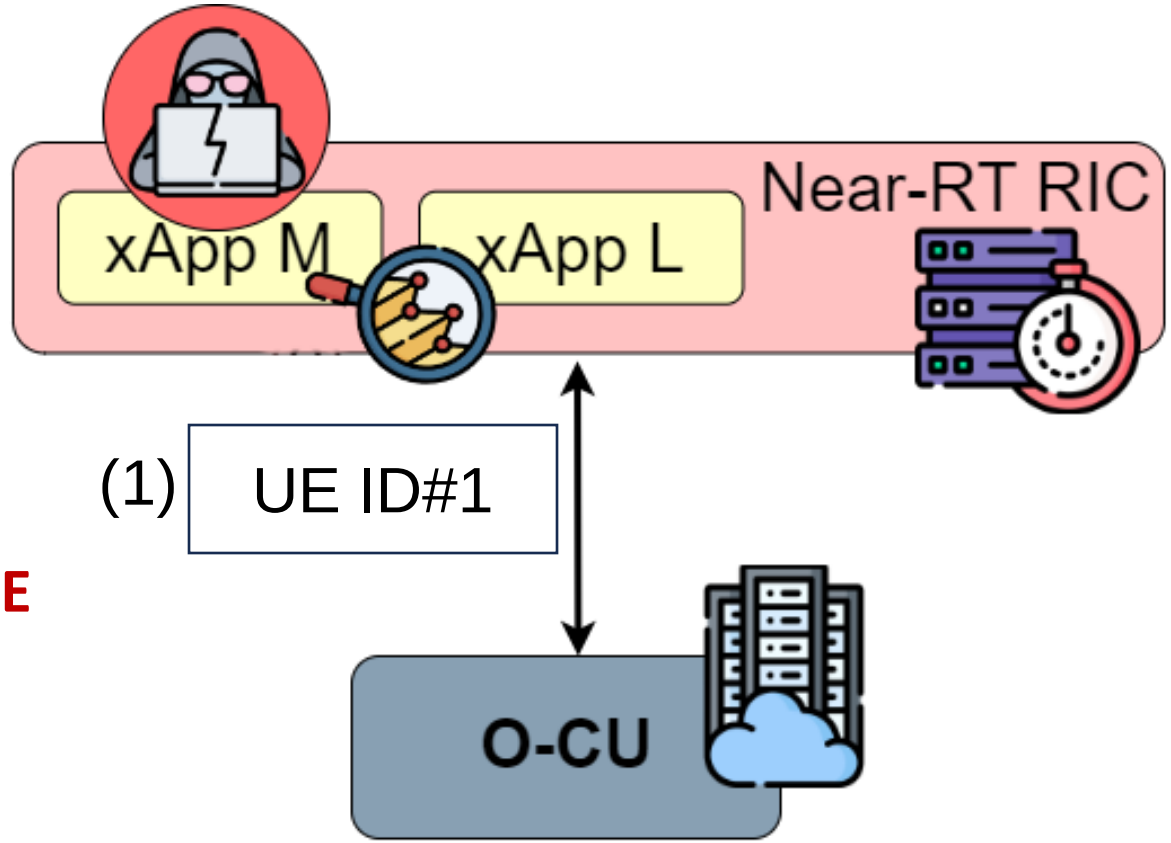
- Qualquer xApp ou rApp pode possuir vulnerabilidades
- Chances de vulnerabilidades aumentam
  - Se a xApp ou rApp for desenvolvida por uma fonte não confiável ou por uma fonte que não a mantenha de forma adequada
  - Se atacantes identificam uma xApp ou rApp que pode ser explorada
    - Podem interromper o serviço oferecido pela rede e assumir o controle de outra xApp ou de todo Near-RT RIC ou Non-RT RIC
  - Um atacante pode ganhar a habilidade de
    - Alterar dados transmitidos através das interfaces A1 e E2
    - Extrair informação sensível e impactar as funções do Near-RT RIC ou do Non-RT RIC para degradar o seu desempenho

# xApp Maliciosa



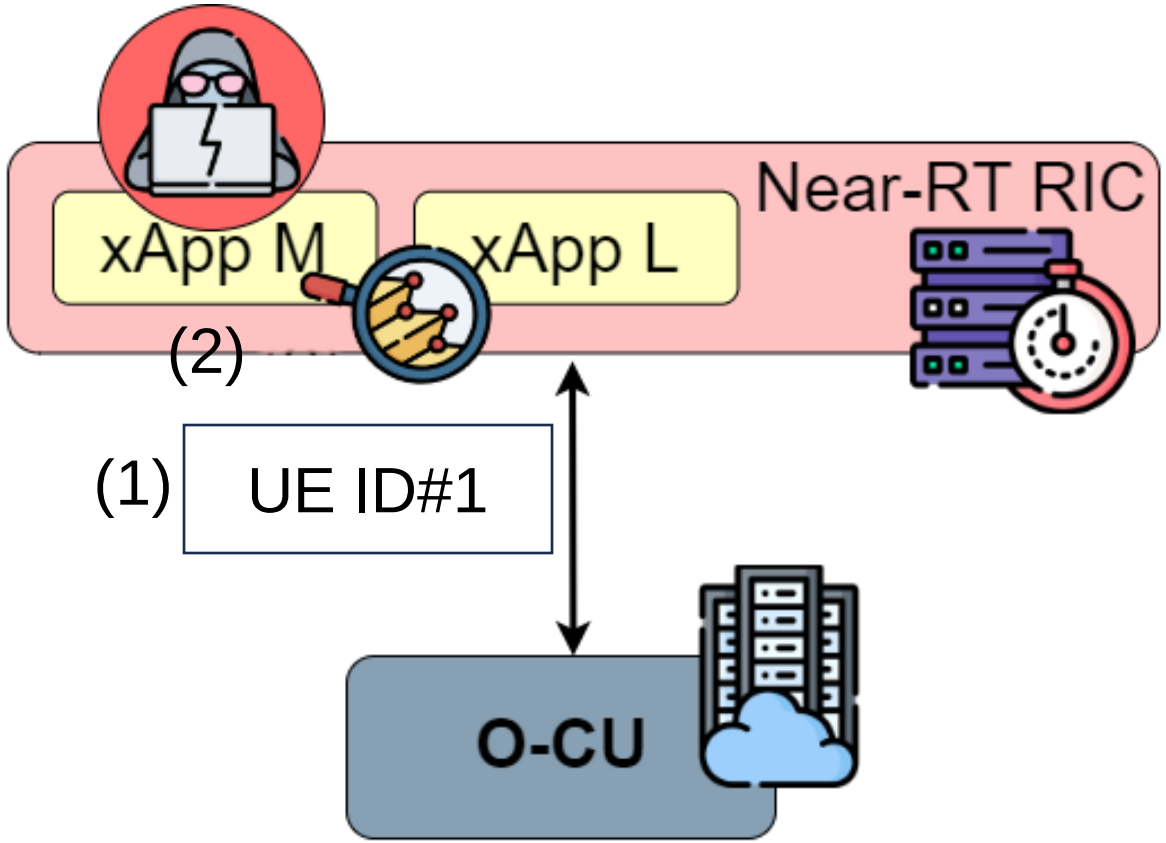

**Uma xApp maliciosa atua como farejador**

# xApp Maliciosa



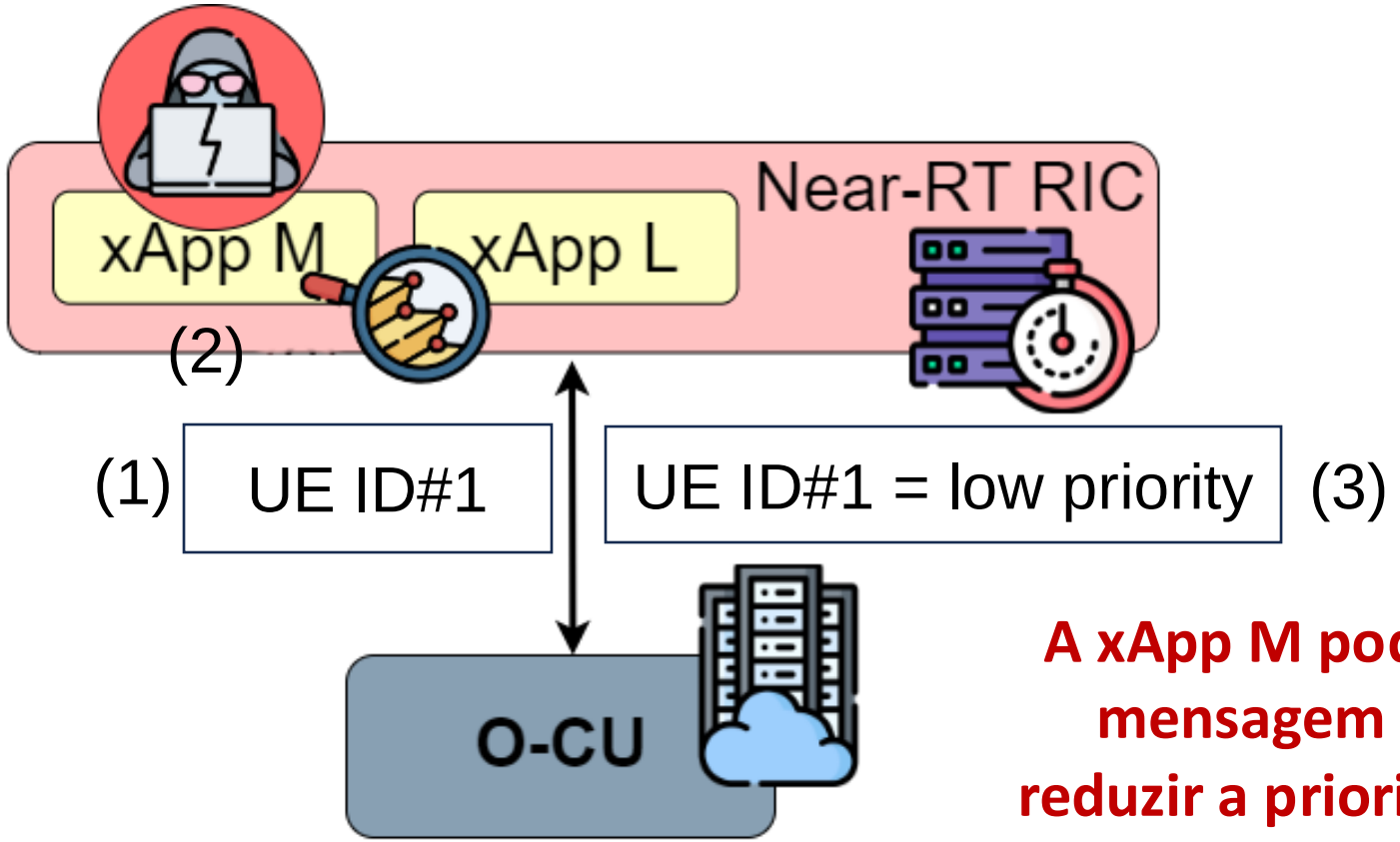

**A xApp legítima L recebe a identificaçãode um UE via interface E2**

# xApp Maliciosa




**A xApp maliciosa M também recebe o identificador do UE**

# xApp Maliciosa




**A xApp M pode enviar uma mensagem à O CU para reduzir a prioridade do UE #1**

# Requisitos de Segurança

- Funções de rede e aplicações – Protocolos recomendados

| Requisito | Near-RT RIC | Non-RT RIC | SMO | O-Cloud | O-DU | O-RU | rApps | xApps |
|---|---|---|---|---|---|---|---|---|
| **Autenticação** | TLS, mTLS, X.509v3, IPsec, IKEv2 | | mTLS, X.509v3, TLS, PSK | TLS, mTLS, X.509v3, MFA | 802.1X | 802.1X | | TLS, mTLS, X.509v3, IPsec, IKEv2 |
| **Confidencialidade** | TLS, IPsec | | TLS | TLS, criptografia | | | | |
| **Integridade** | TLS, IPsec | | TLS | TLS, X.509v3 | | | | |
| **Autorização** | OAuth 2.0 | OAuth 2.0 | OAuth 2.0 | OAuth 2.0 | | | OAuth 2.0 | OAuth 2.0 |
| **Proteção contra reprodução** | | | | TLS, Resumo criptográfico | | | | |
| **Exportação de registros segura** | | | FTPES, TLS, SSH, mTLS, X.509v3 | | | | | |

# Requisitos de Segurança

- Interfaces abertas – Protocolos recomendados

| Requisito | A1 | O1 | O2 | E2 | R1 | Open FH | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | U-Plane | M-Plane | C-Plane | S-Plane |
| **Autenticidade** | | TLS | | | | | | | |
| **Autenticação** | TLS, mTLS | | TLS, mTLS, X.509v3 | IPsec | TLS, mTLS | 802.1X, TLS, SSH | TLS, SSH, mTLS, X.509v3 | 802.1X | |
| **Confidencialidade** | TLS | TLS | TLS | IPsec | | PDCP | TLS, SSH | | |
| **Integridade** | TLS | TLS | TLS | IPsec | | PDCP | TLS, SSH | | |
| **Autorização** | OAuth 2.0 | NACM | OAuth 2.0 | | OAuth 2.0 | 802.1X | | 802.1X | 802.1X |
| **Proteção contra reprodução** | TLS | TLS | TLS | IPsec | | PDCP | TLS, SSH | | |

# Considerações Finais

- Open RAN tem mais funcionalidades que RAN
  - Superfície de ataque aumentada
- *Hardware* programável em ambiente vulnerável
  - Oportunidade de ataque
- Open RAN coleta dados
  - Recompensa maior por ataques

# Minicurso do SBSeg 2023

**Ameaças e Vulnerabilidades em Open RAN: Desafios e Soluções**

Diogo Menezes Ferrazani Mattos, Dianne Scherly Varela de Medeiros, Rodrigo de Souza Couto, Pedro Henrique Cruz Caminha, Lucas Airam Castro de Souza, Felipe Gomes Táparo, Guilherme Araujo Thomaz, João Vitor Valle, Franciele Batista de Oliveira, Miguel Elias Mitre Campista, Luís Henrique Maciel Kosmalski Costa, Igor Monteiro Moraes

DOI: https://doi.org/10.5753/sbc.13567.7.4

# Desafios em Segurança para Redes de Acesso via Rádio Abertas

Igor Monteiro Moraes

Laboratório Mídiacom
Instituto de Computação
Universidade Federal Fluminense - UFF