# CSNOG 2019


# Report of Contributions

https://indico.csnog.eu/e/c2019

Contribution ID : **10** Type : **not specified**

# VoIP podvody

*Tuesday, 28 May 2019 16:25 (25)*

Obsahem přednášky budou poznatky o charakteru VoIP útoků využívajících protokol SIP a o různých způsobech ochrany proti nim, obojí plynoucí z osobních zkušeností za posledních 10 let.

**Primary author(s) :** Mr FIŠER, Ivo

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **11** Type : **not specified**

# Co se děje v DNS Protokolu? Aneb jak moc je DNS velbloud unavený?

*Tuesday, 28 May 2019 11:35 (25)*

V přednášce bych se rád zaměřil na novinky v DNS protokolu a v DNS soukromí, které byly buď v nedávné době standardizovány nebo se připravuje jejich standardizace.

- Soukromí v DNS
- Refresh algoritmů v DNS
- DNS over TLS/QUIC/HTTP

a další...

**Primary author(s) :** SURÝ, Ondřej (Internet Systems Consortium)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **12** Type : **not specified**

# F-Tester - platforma pro měření parametrů TCP/IP sítí

*Wednesday, 29 May 2019 14:30 (30)*

Prezentace je zaměřena na představení platformy F-Tester určené pro měření parametrů TCP/IP sítí. Platforma F-Tester vznikla na půdě Katedry telekomunikační techniky, fakulty elektrotechnické ČVUT v Praze jako část výstupů nkolika projektů zaměřených na testování a diagnostiku TCP/IP komunikačních sítí v průmyslu a běžných přístupových sítích. V rámci prezentace budou uvedeny výstupy z měření průmyslových širokopásmových modemů komunikujících po silovém vedení (BPL). V prezentaci bude rovněž demonstrováno nasazení měřicí platformy F-Tester pro měření NGA přípojek, které je realizováno v souladu s metodickými pokyny ČTÚ.

**Primary author(s) :** Mr KOCUR, Zbyněk (Katedra telekomunikační techniky); Mr VONDROUŠ, Ondřej (Katedra telekomunikační techniky)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **13** Type : **not specified**

# DNS flag day … nějak bylo, nějak bude?

*Tuesday, 28 May 2019 14:00 (30)*

V únoru 2019 proběhla akce DNS flag day, během které byla celosvětově ukončena podpora některých nestandardních autoritativních DNS serverů.

V této přednášce krátce shrneme průběh akce v roce 2019 a podíváme se, co by nás mohlo čekat v letech následujících.

**Primary author(s) :** ŠPAČEK, Petr (CZ.NIC)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **15** Type : **not specified**

# Introduction to NOGs, especially CSNOG

*Tuesday, 28 May 2019 17:15 (20)*

In this talk, we will introduce the concepts of NOG meetups across the world and describe differences between a regular conference and a NOG meetup. We will also introduce the program committee and open nominations for four seat that will be vacated after CSNOG 2019.

**Primary author(s) :** CALETKA, Ondřej (CESNET, z. s. p. o.)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **17** Type : **not specified**

# Using streaming telemetry for network automation and monitoring

*Tuesday, 28 May 2019 12:00 (30)*

We are fast approaching the point where event-driven automation becomes reality and one of its key parts is streaming telemetry. The last few years have shown that SNMP can't provide the scale or level of metrics that are essential for event-driven automation or monitoring to operate / evolve?. Emerging technologies like SDN and Kubernetes brings even more challenges when monitoring network devices. In this session we will be discussing gRPC, OpenConfig, IOS-XR, Kafka or Grafana.

**Primary author(s) :** Mr PROKOP, Matyas (Principle Architect)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **18** Type : **not specified**

# Automated network OS testing

*Wednesday, 29 May 2019 12:00 (30)*

NAPALM is open source Python library that implements a set of functions to interact with different vendor network devices and provides unified API for them.
There is support mainly for configuring devices and retrieving operational state from them.

In Orange Business Services we decided to use this library to automate recurring testing of new versions of Juniper JunOS and CISCO IOS software that we deploy in our networks. We wanted to have these automated tests reliable as manual tests with user-friendly fronted and faster execution, so engineers can focus on more complex manual tests and simple and mid-simple tests are executed during nights/weekends.
As a result of several months work we have now environment with web fronted for scheduling and reviewing tests. We also needed to extend NAPALM with several functions for
parsing operational data. These functions are covering different SP areas as IS-IS, LDP, BFD, MP-BGP, PIM, MPLS TE, … and help us to properly check overall status of the box.
As a next step we consider also using RobotFramework with CI/CD principles for fully automatic test execution.

**Primary author(s) :** KUBINA, Tomáš

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **20** Type : **not specified**

# Secure routing in the Internet

*Tuesday, 28 May 2019 11:10 (25)*

The routing security in the Internet is a long-standing problem and several attempts to address the main concerns have been made in last few years: Filters generated from IRR, RPKI and BPGSec. We examine current situation from different perspectives: Threats and attacks that can be observed in the DFZ, deployment of the security mechanisms, issues holding the deployment back and the projections of efficacy of the mechanisms now and predicted impact in foreseeable future.

**Primary author(s) :** HLAVACEK, Tomas (CZ.NIC)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **22** Type : **not specified**

# Vliv kvalitativních datových parametrů a maximální rychlosti na TCP propustnost: Doporučení pro stanovení vztahu mezi rychlostmi dle Nařízení EU 2015/2120

*Tuesday, 28 May 2019 16:50 (25)*

V listopadu roku 2018 byl vytvořen v rámci ČTÚ MSEK Polygon v podobě modelu procesu měření VIS MSEK. Mezi primární cíle MSEK Polygonu patří intenzivní odborné školení pracovníků ČTÚ a provádění výzkumných studií dopadu datových parametrů a metod řízení na kvalitu služby přístupu k internetu v pevném místě a jiných specifických služeb. V rámci studie vlivu kvalitativních datových parametrů na TCP propustnost měřenou dle doporučení IETF RFC 6349 se podařilo identifikovat vliv maximální rychlosti a její souvislost s limity kvalitativních datových parametrů dle technické specifikace MEF 23.1. Na základě těchto výsledků vzniklo doporučení pro stanovení vztahu mezi rychlostmi dle Nařízení EU 2015/2120 tak, aby co nejvíce odpovídalo fyzikálnímu chování metody měření a navíc umožňovalo poskytovatelům služeb přístupu k síti internet provádět prostřednictvím hodnoty maximální rychlosti optimalizaci své přístupové sítě, s ohledem na dodržení kvality služby z pohledu práv koncového uživatele.

**Primary author(s) :** Dr KOUDELKA, Petr; TOMALA, Karel

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **23** Type : **not specified**

# Integrace DDoS Protectoru v prostředí propojovacího uzlu NIX.CZ

*Wednesday, 29 May 2019 15:00 (30)*

Přednáška popisuje způsob mitigace DDoS útoků v prostředí neutralního propojovacího uzlu NIX.CZ pomocí zařízení DDoS Protector vyvinutým sdružením CESNET. Rozebírá jakým způsobem si může připojený člen řídit provoz procházející DDoS Protectorem a jak může ovlivnit proces DDoS mitigace. Diskutovány budou rovněž možnosti rozložení DDoS útoků přesahující hodnoty 100Gb/s na více DDoS Protectorů.

**Primary author(s) :** PODERMAŃSKI, Tomáš (CESNET z.s.p.o.)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **24** Type : **not specified**

# Intro: Global NOG Alliance

*Tuesday, 28 May 2019 17:35 (15)*

What is the Global NOG Alliance and the Story behind

**Primary author(s) :** Mr FICHTMUELLER, Rene (Board Member)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **25** Type : **not specified**

# DNS-přes-???

*Tuesday, 28 May 2019 15:00 (30)*

Svět DNS se rychle mění a zdá se, že časy centralizovaných DNS resolverů v síti operátor jsou ty tam.

V roce 2019 nejspíš Mozilla ze svého prohlížeče Firefox začne ve výchozím nastavení posílat DNS-přes-HTTPS (DoH) na resolvery mimo síť operátora. Zároveň je na vzestupu DNS-přes-TLS (DoT) protokol, které také ovlivňuje, co vypadá provoz v síti operátorů.

V této přednášce shrneme poslední vývoj okolo DNS transportů a prodiskutujeme, jaké změny to sebou přináší. Také se pokusíme nastínit možné další scénáře vývoje a jak se na ně připravit.

**Primary author(s) :** ŠPAČEK, Petr (CZ.NIC)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **26** Type : **not specified**

# Handling Abuse and Misuse in the DNS

*Wednesday, 29 May 2019 10:00 (30)*

This presentation discusses the abuses and misuse in the Domain Name System (DNS) and the best practices in analyzing and handling those abuses.

**Primary author(s) :** Mr WIJAYATUNGA, Champika (ICANN)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **27** Type : **not specified**

# Jak šlape CZ DNS Anycast

*Tuesday, 28 May 2019 14:30 (30)*

Za poslední rok jsme náš DNS anycast opět pořádně "promazali" a jeho výkon a odolnost se tak dále znatelně zvýšily. Jak a jak moc jsou jednotlivé jeho části využívány a kam se vyplatí vrhnout naše síly v budoucnu? Na tyto a další otázky se pokusím odpovědět zejména pomocí dat získaných díky projektu ADAM (Advanced DNS Analysys and Monitoring).

**Primary author(s) :** BRŮNA, Zdeněk

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **28** Type : **not specified**

# Technické zajímavosti z implementace MPLS VPN a multicast VPN

*Wednesday, 29 May 2019 09:00 (30)*

Při realizaci MPLS VPN sítě pro ŘSD bylo potřeba vyřešit řadu zajímavých situací. Připomenu posluchačům základní principy MPLS VPN řešení, multicastu a multicast VPN řešení. Projdeme si v obecné rovině technické požadavky a jak vypadá jejich realizace. Vysvětlím, jak jsme ošetřili routing na zařízeních, kde se v jedné VRF potkávají routy z různých protokolů. Jak zabránit smyčkám v routingu a zajistit dostatečnou spolehlivost. Na vhodných místech bude výklad doplněn ukázkou konfigurace.

**Primary author(s) :** ROŠKA, Radim

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **29** Type : **not specified**

# War games: Live security DDoS drills

*Tuesday, 28 May 2019 16:00 (25)*

Companies operating in the critical path of internet traffic are constantly exposed to DDoS attacks of all types and scales. Ideally, the smaller and more mundane attacks are mitigated automatically. But because scale can vary and attacks can progress dynamically as attackers get creative, operations teams need to be ready to respond.

In this talk, we will share what we have learned by running war game-style DDoS preparedness training at NS1 and how the drills can be used as a means of strengthening team, tools, and technology around DDoS mitigation.

**Primary author(s) :** VČELÁK, Jan (NS1); WEYRICK, Shannon (NS1)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **32** Type : **not specified**

# Adaptive mitigation of DDoS attacks using BGP Flowspec

*Wednesday, 29 May 2019 09:30 (30)*

Prupose of the presentation is to demonstrate capabilities of BGP Flowspec implemented on routers to mitigate volumetric DDoS attacks while adapting on continuously changing attack pattern. Attack detection is based on flow (NetFlow/IPFIX) technology that enable to identify attack pattern that is automatically converted into set of BGP Flowspec rules and pushed to routers for attack mitigation. Continuous monitoring of attack characteristics enables to update mitigation rules automatically when deviation from current attack pattern is detected. As part of the presentation we would like to explain flow data and show what value it brings for network operators in broader context than just DDoS protection.

**Primary author(s) :** MINAŘÍK, Pavel (Flowmon Networks a.s.); Mr KNAPEK, Jiří (Flowmon Networks a.s.)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **33** Type : **not specified**

# Measuring Internet stability: Czech Republic, Slovakia and beyond

*Wednesday, 29 May 2019 11:30 (30)*

For four years now, Qrator Labs were releasing annual reports on national Internet segments' reliability. The source of the data is the state and the history of ISP relations, as seen via mutual BGP announcements. The 2019 report is going to see light in August.

When we want to understand a current situation in some region in telecom world, first of all we need to gather some information about it. We need to understand who are the biggest players on market, how diverse is this market at all, who are the critical points of failure. The are several approaches to this.

In our report we want to play around one of possible approaches: a view in terms of autonomous systems' relations. We'll look at the current resource distribution between ASNs and how good the current security practices are applied by them. Also we'll try to highlight the top of ISPs and check the stability of a region in a whole.

**Primary author(s) :** Mr BOGOMAZOV, Eugene (Qrator Labs CZ)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **34** Type : **not specified**

# Tutorial: Running BGP in 2019

*Tuesday, 28 May 2019 09:00 (90)*

Simple solutions usually have complicated consequences. For decades, Border Gateway Protocol was a simple tool; as a result, today it is quite complicated for network operations teams.

The tutorial aims at giving an overview of today's BGP best current practices, the now built-in cryptography and security of BGP, and free tools an autonomous system's operator could use to manage their network and troubleshoot issues.

Finally, a ROA signing party (which resembles PGP signing parties but is a little bit different) would be held.

**Primary author(s) :** Mr BOGOMAZOV, Eugene (Qrator Labs CZ)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **36** Type : **not specified**

# Observing your MANRS

*Wednesday, 29 May 2019 14:00 (30)*

There are over 60,000 networks comprising the Internet that exchange reachability information using the Border Gateway Protocol (BGP), but the problem is that BGP is almost entirely based on trust with no built-in validation of the legitimacy of routing updates. This causes many problems such as IP prefix hijacking, route leaks, and IP address spoofing, and there have been a growing number of major incidents in the past few years. There are solutions to address these issues, but securing one's own network does not necessarily make it more secure as it remains reliant on other operators also implementing these solutions too.

The Mutually Assured Norms for Routing Security (MANRS) initiative https://www.manrs.org) therefore tries to address these problems by encouraging network operators, content providers and IXPs to subscribe to four actions including filtering, anti-spoofing, coordination and address prefix validation, and has developed resources to help them implement these. This includes the MANRS Best Current Operational Practice (https://www.manrs.org/bcop/) which is a technical document providing step-by-step instructions, along with a set of online training modules, whilst the forthcoming MANRS Observatory will allow network operators to view the routing incidents that affect their networks.

By implementing these actions, operators are promoting a culture of collaborative responsibility, and are improving the security of the global routing system. MANRS is an opportunity to demonstrate they are committed to a secure Internet and by setting an example to other operators.

**Primary author(s) :** MEYNELL, Kevin (Internet Society)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **37** Type : **not specified**

# Potlačení nežádoucího provozu pomocí BGP Flowspec

*Wednesday, 29 May 2019 11:00 (30)*

Představíme open source nástroj ExaFS, který vyvíjí sdružení CESNET. Jedná se o webovou aplikaci, která prostřednictvím BGP Flowspec distribuuje pravidla na směrovače páteřní sítě. Je tak možné nežádoucí provoz už na vstupu do páteřní sítě zahodit, objemově omezit, nebo i přesměrovat na zařízení pro detailní analýzu. Aplikace nabízí také API s možností automatizace blokování na základě analýzy provozu v reálném čase.

**Primary author(s) :** Mr VERICH, Josef (CESNET z. s. p. o.)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **38** Type : **not specified**

# Highlights of RIPE NCC Tools: RIPE Atlas, RIPEstat and the Website Dashboard

*Wednesday, 29 May 2019 16:00 (30)*

This presentation aims to show how the publicly available RIPE NCC analytical tools and data sets can be used for active network measurements or to get country-specific information about networks. The presentation will highlight the following tools and services:

**RIPE Atlas**
RIPE Atlas employs a global network of probes that measure Internet connectivity and reachability, providing an understanding of the state of the Internet in real time. In this presentation, we will show some of the latest developments such as various APIs, VM anchors and the new probe version that can help carry out active network measurements.

**RIPEstat**
RIPEstat is a web-based interface that provides everything you ever wanted to know about IP address space, Autonomous System Numbers (ASNs), and related information for hostnames and countries in one place. We'll show you how you can get the most out of it.

**RIPE.net My Dashboard**
We'll show a new feature you can use on the www.ripe.net website - the My Dashboard view. It allows you to customise the website with information that you would like to see. You can for instance choose from widgets showing the latest RIPE Policy documents, your RIPE Atlas credits or upcoming RIPE NCC webinars.

**Primary author(s) :** HOLOP, Frantisek

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **40** Type : **not specified**

# SpaceLab

*Wednesday, 29 May 2019 16:30 (20)*

Věděli jste, že i v ČR se pracuje na projektu, který má v konečné fázi umožnit poskytování internetu z vesmíru? Nově vzniklý český projekt SpaceLab EU se zaměřil na rozvinutí myšlenky vývoje a využití air-breathing ion propulsion technologie pro malé satelity na velmi nízkých oběžných drahách (VLEO) a vytvoření satelitní sítě (SaaS - Satellite as a Service) ve výškách mezi 220 - 280km, kde by se latence snížila na třetinu oproti v současnosti plánovaným projektům a plánům poskytování internetu z vesmíru.
Proč vám o tom vykládáme na konferenci poskytovatelů internetu a síťových operátorů?
Protože více než polovina problémů k vyřešení leží v síťové části. Protože my věříme, že Evropa a Česká republika by měli vést open-source aktivity v oblasti connectivity from space a pojistit tak sebe a celý svět proti případným problémům s kontrolou internetu ala Čína, ala USA, ala Blízký Východ. A v neposlední řadě, protože chceme s partou nadšených expertů posunout náš projekt zase o krok dál.
Co se dozvíte: jak nápad na satelitní motor bez paliva vznikl, kdo se ho ujal, jaké jsou problémy, kde nyní jsme a proč si myslíme, že SaaS a open source jdou dohromady.

**Primary author(s) :** PALÁN, Petr

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **42** Type : **not specified**

# New Top Level Domains and the Issue of Universal Acceptance

*Wednesday, 29 May 2019 16:50 (10)*

This short presentation will explain how the expansion of the Domain Name System (DNS) has influenced the digital environment for Internet users.

With the introduction of new top-level domains (TLDs), such as .top, .guru or .online, competition increased and gave Internet users a greater choice to get their desired domain name. Moreover, the introduction of Top Level Domains in non-ASCII scripts (known as Internationalised Domain Names/IDNs), such as .□□□□ (google) or .□□ (trademark) gives the majority of the world's population, using non-ASCII scripts, equal opportunities of accessing the Internet.

However, to fully embrace the advantages of the expanded DNS, there is a need to comply with some technical requirements – with the so-called Universal Acceptance issue.

This presentation will highlight what ICANN and the community are doing to address this topic and how others can contribute to improving the user experience.

**Primary author(s) :** Ms VINOPALOVÁ, Žaneta (ICANN, GSE Intern); Ms SCHITTEK, Gabriella (ICANN, GSE Senior Manager – Nordic & Central Europe)

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019

Contribution ID : **43** Type : **not specified**

# Don’t let your IPv6 deployment break

When deploying IPv6, the currently most often deployment model is to dual-stack the end-user’s LAN. Combined with the Happy Eyeballs (RFC 8305/6555), this often masks broken IPv6 deployments.

Still, there are tools that do not perform Happy Eyeballs – and for those tools, a broken IPv6 networking configuration results *de facto* in a broken service, even in dual-stack environment where the IPv4 counterpart is available. In IPv6-only network, broken IPv6 connectivity and/or DNS configuration results in IPv6 hosts being completely inaccessible.

This talk will focus on real-life brokenness experience and how to avoid it.

**Primary author(s) :** ZAJÍC, Radek

**Session Classification :** CSNOG2

**Track Classification :** CSNOG 2019