



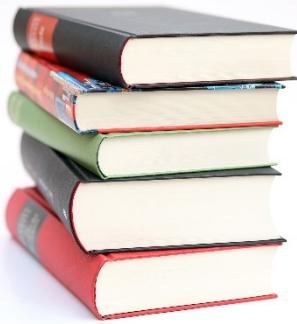
UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 12

Technológie, ktoré vieme z PS1 ...a ich implementácia na KIS a FRI

Počítačové siete 1

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU



Osnova dnešnej prednášky

- Aký je plán tento a budúci týždeň
- Informácie ku skúške
- Technológie a protokoly vyučované v PS1 a ich využitie na KIS a FRI
- Aké ďalšie sietové predmety možno absolvovať na FRI

Plán semestra PS1 2022

Prednášky		Kapitoly na Netacad-e	Cvičenia	Ostrý test (Moodle)	Cvičný test (Netacad)
1.	Princípy smerovania, statické smerovanie	SRWE_14 Routing Concepts SRWE_15 IP Static Routing SRWE_16 Troubleshoot Static and Default Routes	Opakovanie PIKSu		
2.	Úvod do dynamického smerovania (protokoly RIPv2, RIPng)	(nie je aktuálne pokrytý v Netacad curricule v7.0)	Static routing	T01_static	SRWE 14-16: Routing Concepts and Configuration ExamExternal tool
3.	Úvod do prepínaných sietí, LAN dizajn a konfigurácia prepínačov	SRWE_1 Basic Device Configuration SRWE_2 Switching Concepts ENSA_11 Network Design	RIPv2, RIPng	T02_RIP	Modul quizzes
4.	Virtuálne LAN siete, smerovanie medzi nimi a ich škálovanie	SRWE_3 VLANs SRWE_4 Inter-VLAN Routing	Port security	T03_prepinac	SRWE 1-4: VLANs, and InterVLAN Routing ExamExternal tool
5.	Riešenie redundancie a slučiek v prepínanej sieti (STP)	SRWE_5 STP Concepts	VLANs	T04_VLANs	Modul quiz
6.	Redundancia default brány. Agregácia portov.	SRWE_6 EtherChannel SRWE_9 FHRP Concepts	STP	T05_STP	Modul quizzes
7.	Sieťová bezpečnosť, ACL zoznamy na kontrolu prístupu	ENSA_03 Network Security Concepts ENSA_04 ACL Concepts ENSA_05 ACLs for IPv4 Configuration	Etherchannel, HSRP	T06_EthCh+FHRP	SRWE 5-6: Redundant Networks
8.	Dynamické pridelenie adries (DHCPv4 a DHCPv6)	SRWE_7 DHCPv4 SRWE_8 SLAAC and DHCPv6	ACL	T07_ACL	Modul quizzes
9.	Preklad adries (NAT pre IPv4)	ENSA_06 NAT for IPv4	DHCPv4, v6	T08_DHCP	SRWE 7-9: Available and Reliable Networks
10.	Bezpečnosť v LAN	SRWE_10 LAN Security Concepts SRWE_11 Switch Security Configuration	NAT	T09_NAT	Modul quizzes
11.	Bezdrôtová LAN	SRWE_12 WLAN Concepts SRWE_13 WLAN Configuration	Útoky na DHCP	T10_security	Modul quizzes
12.	Praktické ukážky nasadenia technológií	Informácie ku skúške, praktické ukážky, informácie k nadvážujúcim predmetom	WLAN	T11_WLAN	SRWE 10-13: L2 Security and WLANs

Aký je plán tento týždeň

Prednáška 12: Opakovanie a praktické ukážky implementácie technológií a protokolov vyučovaných v PS1 v sieti KIS a FRI

Tento týždeň sa nepreberá žiadna nová téma, poskytnú sa informácie:

- ku skúške
- k technológiám a protokolom vyučovaným v PS1 a ako sú implementované
- k nadväzujúcim sieťovým predmetom (aj inžiniersky odbor ASI - aplikácia)
- Slajdy z prednášky

- Nahláste si tu, ktoré testy chcete opravovať v 13. týždni:



DOTAZNÍK

Záujem o opravu testov 2022/23

Cvičenie 12: WLAN

- Tento týždeň sa **cvičí téma WLAN** a píše sa posledný priebežný test z prednášky 11
- Vyplniť je nutné po cvičení: Netacad> Assignments> Course Feedback (vyplniť do termínu písania FINAL exam z domu)
 - nájdete ho tu: www.Netacad.com > Názov_vášej_Cisco_triedy > Assignments > Course Feedback
 - je to Cisco dotazník, pre zistovanie vašej spokojnosti s kurzom a inštruktormi, na základe ktorého sme hodnotení ako inštruktori, ako aj celá Cisco akadémia. Bez jeho vyplnenia vás nevieme v tomto kurze uzavrieť a vyžiať pre Vás certifikát, a nespustíme ani FINAL exam test.
- Odovzdáva sa DÚ (PT aktivita), bonus 1 bod do nedele 23:59 (pribudne na Moodle do stredy 07:00)

Tu si nahláste, ktoré testy, **max. 3**, chcete opraviť (**najneskôr do 11.11.2022**)

Aký je plán budúci týždeň

Cvičenie 13: FINAL exam (povinné), a opravné testy (nepovinné)

- Tento týždeň sa rieši (pokiaľ sa nedohodnete s vyučujúcim inak, ak napríklad máte sklz, a niektoré cvičenie vám odpadlo a pod.):
 1. Netacad> Assignments> **FINAL exam** (povinné)
 - uzavreté otázky na Netacade, v angličtine, cca 50 otázok, max. 1,45 hod.
 2. **Opravné testy** (voliteľné, deadline pre výber testov na opravu je uvedený v Moodle v cvičení predošlého týždňa, aj priestor na nahlásenie, ktoré testy chcete záväzne opraviť)
 - Opraviť možno ktorýkoľvek test 1-11, ktorý ste nepísali, alebo z ktorého ste získali pre vás neuspokojivý počet bodov.
 - Max. možno opraviť tri testy
 - Berie sa posledný pokus, nie vyššie skóre

Pokiaľ nemáte aktivované, požiadajte vyučujúceho o aktiváciu na cvičení tento týždeň

Vyplňte Course feedback do najbližšieho cvičenia

Home / I'm Teaching / 2022_cna2_JU



Course
Home



Grades



Viewing as student. Switch back

2022_cna2_JU

Course Feedback



Course Feedback

Final Exam

Restricted Not available unless: The activity **Course Feedback** is marked complete

Prepare For Your Future



Certification Preparation and Discount Vouchers



Career Resources and Employment Opportunities



Skúška

Podmienky ku skúške

priebežné otvorené otázky

[váha 25% z celkového skóre]

- píšu sa na 2. až 12. cvičení
- každý za 5 bodov, spolu $11 \times 5 = 55$ bodov
- započítavajú sa ku skúške
- min. treba 60% bodov, t.j. min. 33 bodov z 55.

priebežné testy z kapitol

[váha 0% z celkového skóre]

- príprava na veľký test FINAL exam na skúške
- doma, voliteľné ale odporúčané

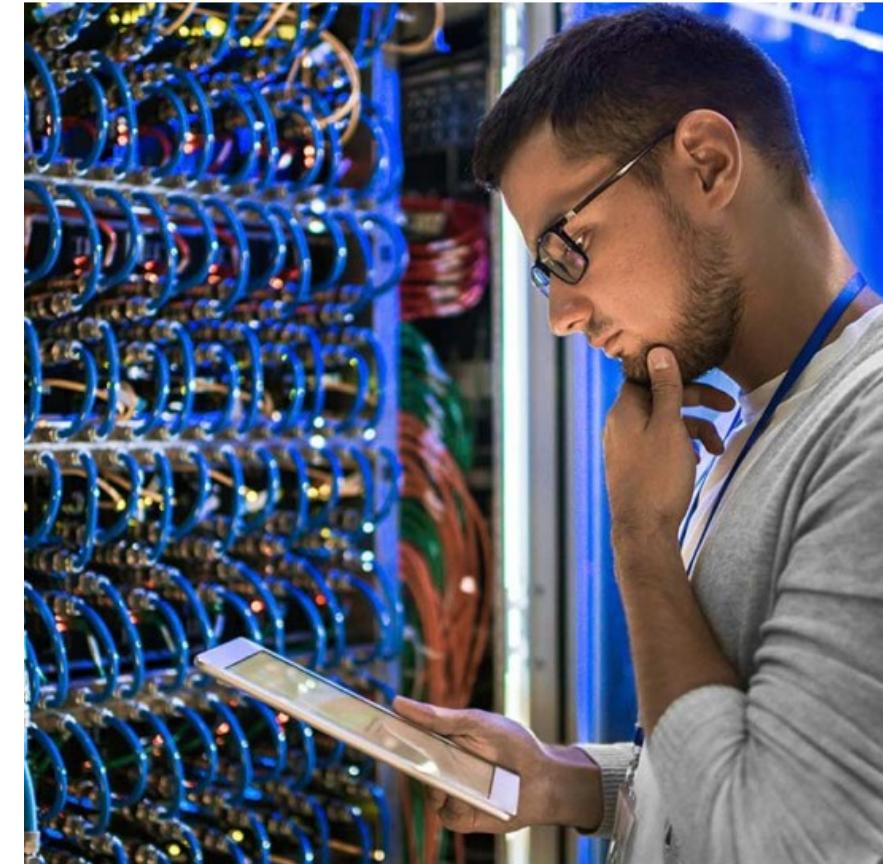
domáce úlohy v PT a aktivita

[bonusové body]

- DÚ v PT: max. 1 bod za každú
 - Dobrovoľné (povinnosť určuje cvičiaci)
 - Aktivita na cvičeniach, prednáškach, vo fórách a diskusiách

Skúška

- **CCNA 2 Final Exam** test
[váha 15% z celkového skóre]
 - teoreticko-praktické otázky na portáli Netacad (s výberom odpovede)
 - min. 60% z FINAL testu.
- **písomno/ústna skúška** s otvorenými otázkami
[váha 25% z celkového skóre]
 - 4 otázky
 - max. 5 bodov za jednu otázku, spolu $4 \times 5 = 20$ bodov.
 - min. 60% bodov, t.j. min. 12 z 20 bodov.
- praktická skúška **Skill Exam**
[váha 35% z celkového skóre]
 - Konfigurácia zariadení podľa zadania – veľká topológia
 - Min. 60% bodov



Hodnotenie

- Stupnica:
 - <92,100> bodov A
 - <84, 92) bodov B
 - <76, 84) bodov C
 - <68, 76) bodov D
 - <60, 68) bodov E
- Celkové skóre =

Priebežné testy s otvorenými otázkami [25%] +
FINAL exam [15%] +

Finálny test s otvorenými otázkami/Ústne skúšanie [25%] +
SKILL exam [35%]

 - pričom pre každú časť je potrebné dosiahnuť minimálne 60% úspešnosť



Hodnotenie

- Stupnica:
 - <92,100> bodov A
 - <84, 92) bodov B
 - <76, 84) bodov C
 - <68, 76) bodov D
 - <60, 68) bodov E
- Celkové skóre =

Priebežné testy s otvorenými otázkami [25%] + FINAL exam [15%] +
Finálny test s otvorenými otázkami [25%] + SKILL exam [35%]

 - pričom pre každú časť je potrebné dosiahnuť minimálne 60% úspešnosť

Spoločné termíny 2022/2023

Vypísané termíny skúšky – vzdelávanie.uniza.sk

Zoznam termínov na predmet: počítačové siete 1						
Dátum/čas	Miestnosť	Skúšajúci	Kapacita	Počet prihlásených	Typ	Poznámka
12.01.2023 / 08:00	RA012	Mgr. Jana Uramová PhD.	70	0	riadny termín	Skúška PS1, test (cca 30min) a SKILL exam (cca 2 hod), spolu cca 2-3 hod.
20.01.2023 / 08:00	RA013	Mgr. Jana Uramová PhD.	70	0	riadny termín	Skúška PS1, test (cca 30min) a SKILL exam (cca 2 hod), spolu cca 2-3 hod.
27.01.2023 / 08:00	RA013	Mgr. Jana Uramová PhD.	70	0	riadny termín	Skúška PS1, test (cca 30min) a SKILL exam (cca 2 hod), spolu cca 2-3 hod.
03.02.2023 / 08:00	RA013	Mgr. Jana Uramová PhD.	70	0	riadny termín	Skúška PS1, test (cca 30min) a SKILL exam (cca 2 hod), spolu cca 2-3 hod.
10.02.2023 / 08:00	RA013	Mgr. Jana Uramová PhD.	70	0	riadny termín	Skúška PS1, test (cca 30min) a SKILL exam (cca 2 hod), spolu cca 2-3 hod.
16.02.2023 / 08:00	RA013	Mgr. Jana Uramová PhD.	70	0	riadny termín	Skúška PS1, test (cca 30min) a SKILL exam (cca 2 hod), spolu cca 2-3 hod.

Skúška



▼ Skúška - materiály a príprava

Skúška 2022/23

- na prihlásenie na skúšku je potrebné mať:
 - min. **33** bodov z 55 z priebežných testov z cvičení (60%)
 - min. 60% z FINAL examu CCNA2 (SRWE, Switching, Routing and Wireless Essentials kurz na Netacad-e)
 - vyriešené a skontrolované všetky DÚ, ktoré zadal vyučujúci pre konkrétnego študenta (globálne sú DÚ dobrovoľné a hodnotené bonusovými bodmi)
 - vyplnený **Course Feedback**
 - nájdete ho tu: www.Netacad.com > Názov_vášej_Cisco_triedy > Assignments > Course Feedback
 - je to Cisco dotazník, pre zistovanie vašej spokojnosti s kurzom a inštruktormi, na základe ktorého sme hodnotení ako inštruktori, ako aj celá Cisco akadémia. Bez jeho vyplnenia vás nevieme v tomto kurze uzavrieť a vyžiadáť pre Vás certifikát.

Skúška

uzavrieť a vyžiať pre Vás certifikát.

- Teoretická časť: **písomný test** z tém celého semestra - **4 otázky / max. 20**

bodov - potrebné je získať **min. 12 b.** / váha 25% z celkového skóre

- Táto časť skúšky je dobrovoľná, študent na túto časť nemusí ísť, ak získa dostatok bodov z iných častí
- Ak sa však na túto časť skúšky prihlási a prejaví záujem, musí získať minimálne 60% celkových bodov, t.j. min 12 bodov. Pri menšom počte získaných bodov sa mu výsledok tejto časti zaokrúhli na nulu.
- Teoretické preskúšanie môže byť realizované aj ústnym skúšaním (je to v rézii skúšajúceho na danom termíne skúšky)

- Praktická časť: **SKILL exam** - komplexné zadanie / **max. 100%** - potrebné je získať min. **60%** / váha 35% z celkového skóre

- na reálnom HW v labe (počas pandémie získate prístup na konzolu zariadení remote, topológiu vám pripraví skúšajúci)
- alebo zadanie v PT z obsahu celého semestra (počas pandémie budete pracovať na PC v laboch KIS, so vzdialeným prístupom)
- alebo topológia v GNS3 (nie je nutné dopredu nič vedieť o GNS3, inštrukcie dostanete na skúške, je to len forma prístupu a virtuálnej-emulovanej topológie)
- Pre všetky varianty SKILL examu platí:

- Táto časť skúšky je dobrovoľná, študent na túto časť nemusí ísť, ak získa dostatok bodov z iných častí
- Ak sa však na túto časť skúšky prihlási a prejaví záujem, musí získať minimálne 60% bodov. Pri menšom počte získaných bodov sa mu výsledok tejto časti zaokrúhli na nulu.

Podmienky pre hodnotenie platia tie, ktoré sme si uviedli na začiatku semestra,

Skúška

Podmienky pre hodnotenie platia tie, ktoré sme si uviedli na začiatku semestra,
pričom počas skúšky je nutné **dodržiavať tieto zásady**:

- študent je povinný pracovať **samostatne** bez cudzej pomoci
- okrem pera a kalkulačky (obyčajnej, nie tej na mobile) je dovolené používať **vlastné poznámky** s konfiguračnými príkazmi pre Cisco IOS (iba papierovú formu, nie elektronickú), alebo vytlačenú konfiguračnú príručku, ale iba počas praktickej časti skúšky. Používanie materiálov v elektronickej podobe je počas skúšky zakázané. Upozorňujeme, že spoliehať sa výhradne na pomoc konfiguračnej príručky, bez dostatočnej prípravy na skúšku, dopadá takmer vždy neúspechom na skúške, listovanie v papieroch bez porozumenia vám zaberie celý čas a topológiu nebude mať funkčnú. Pomocný papier na poznámky rozdá skúšajúci, a študent je povinný ho bezodkladne podpísat a pri odchode odovzdať vyučujúcemu.
- študent je povinný mať pri sebe počas skúšky **index** a preukázať sa ním na požiadanie skúšajúcemu
- ak študent skúšku chce **predčasne ukončiť**, musí bezodkladne svoje rozhodnutie označiť vyučujúcemu, ešte pred vypnutím počítača
- **porušenie** uvedených zásad znamená výsledok skúšky nedostatočne

Skúška

Termíny skúšky budú uvedené na [vzdelávaní](#):

- termíny sú spoločné pre všetkých študentov. Aj keď pri vypísaní bude svietiť meno 1 vyučujúceho, ktorý všetky termíny vypísal, skúšajúci sa budú na termínoch meniť podľa ich dostupnosti
- zmeny v prihlásovaní sú dovolené najneskôr 1 deň pred skúškou do 12:00 na obed (ak sa študent nedostaví na skúšku, je mu zapísaná známka FX)
- časovo by skúška mala trvať podľa plánu cca 3 hodiny (teoretická aj praktická časť spolu)
 - teoretický test 35 min
 - praktická časť cca 2 hod
- skúšať sa bude v týchto termínoch:
 - piatky 08:00 (termíny sú už vypísané, 6 termínov so začiatkom v týždni od 9.1.2023), skúška v PT
 - pravdepodobne streda 9:00 (termíny vypíše Prof. Segeč, 4-5 termínov so začiatkom v týždni od 9.1.2023), skúška na reálnom HW alebo v GNS3

Certifikáty

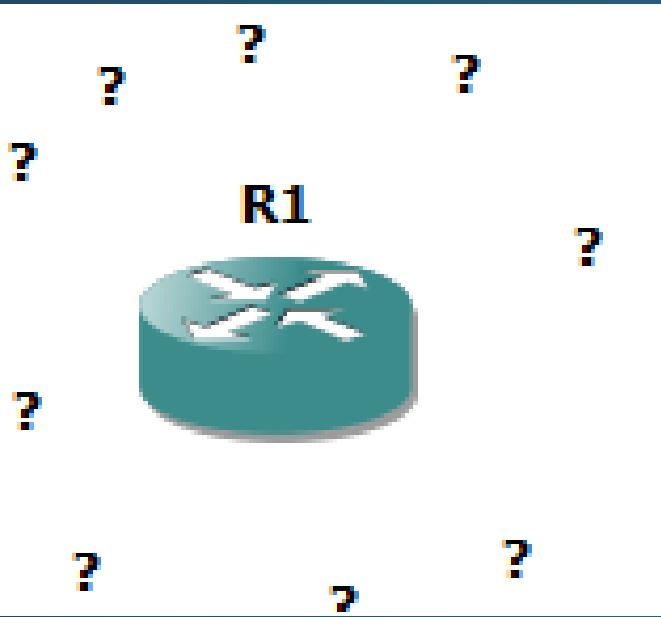
Žiadost o certifikáty:

- Ak ste úspešne absolvovali štúdium predmetu PS1 (kurz CCNA2 a časť kurzu CCNA3), môžete získať certifikát o absolvovaní kurzu CCNA2 Routing&Switching Essentials na našej akadémii v Žiline.
 - Pozn.: po úspešnom absolvovaní predmetu PS2 (kurz CCNA4 a zvyšná časť kurzu CCNA3), môžete potom v nasledujúcom semestri získať certifikát o absolvovaní kurzu CCNA3 a CCNA4.
- Na vyžiadanie certifikátov treba vyplniť [formulár](#) (za každý kurz jeden). Certifikáty si môžete následne v cene **10€/ks** vyzdvihnúť na sekretariáte KIS (p. Liskayová) v **utorok a štvrtok** od **7,00 do 10,00** hod, najneskôr **do 2 týždňov** od ich vyžiadania.



Technológie, ktoré vieme z PS1 ...a ich implementácia na KIS a FRI

Postupne... prejdeme po všetkých témach z PS1



Prednáška 1+2:

Úvod do bežných smerovačov (1800 - 4000)

Smerovanie v IP sietiach

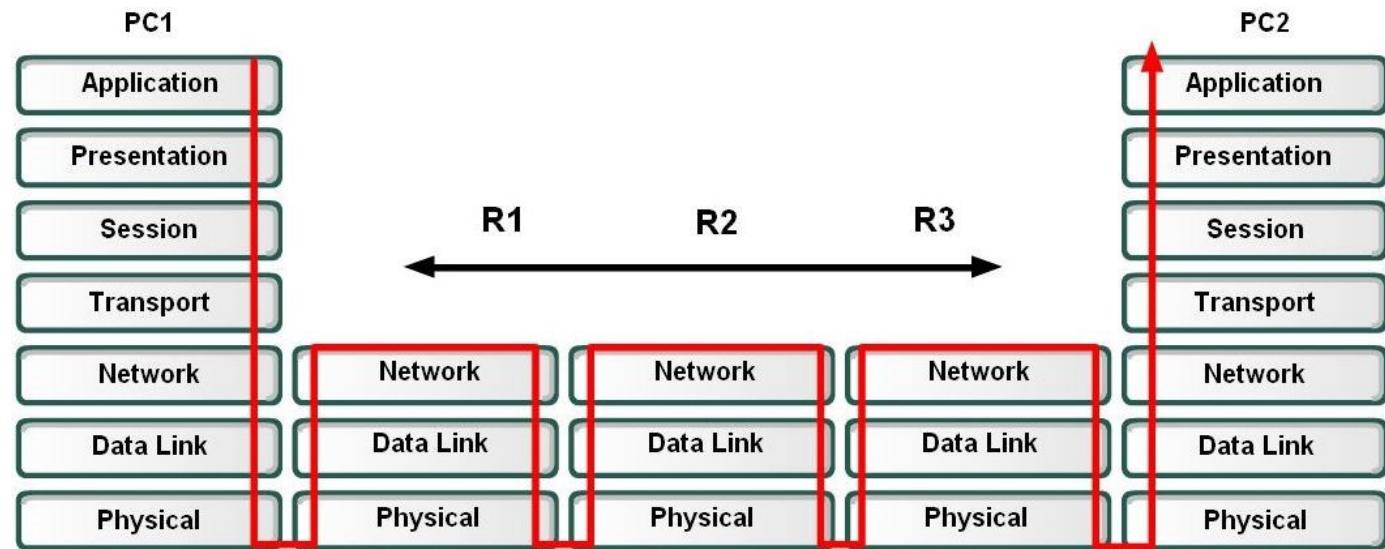
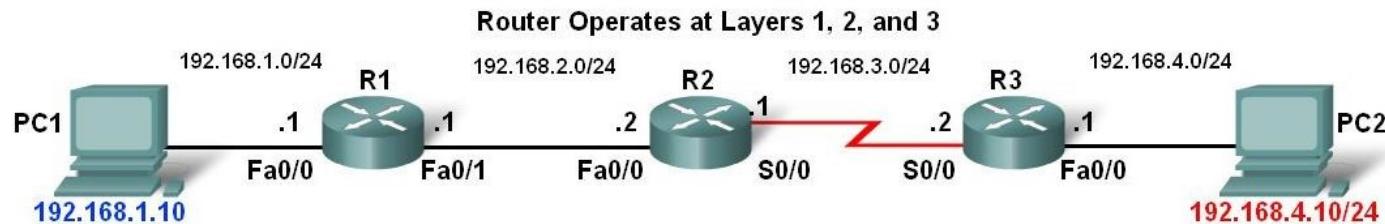
Konfigurácia IPv4 a IPv6 static routes

RIPv2, RIPng

**Na KISe – smerovanie a filtrovanie robí Cisco ASA a Fortinet Fortigate
NA FRI – L3 prepínače
... dynamic: OSPF**

Smerovanie IPv4, IPv6

- RIPE 25.11.2019 došiel posledný /22 rozsah IPv4 >> UKÁŽKA
- KIS – jediná katedra na FRI ktorá využíva aj IPv6:
 - Interná siet' KIS (VPN) >> UKÁŽKA
 - Rozsah SANET, CiKT
 - Labáky KIS
 - IPv6 cez IP4 tunel
 - Jeden cez Budapešť
 - Druhý cez Prahu
 - Viacero poskytovateľov pre IPv6 tunel a získanie IPv6 rozsahu
 - Napr: tunnelbroker.net
 - Podmienka – mať verejnú IPv4
 - myIP.com



Tunnelbroker Login

Username:
Password:
Login **Register** [Forgot Password?](#)

Hurricane Electric Free IPv6 Tunnel Broker

IPv6 Tunnel Broker

Check out our new [usage stats!](#)
And then hit up our new [Forums!](#)

Welcome to the Hurricane Electric IPv6 Tunnel Broker! Our free tunnel broker service enables you to reach the IPv6 Internet by tunneling over existing IPv4 connections from your IPv6 enabled host or router to one of our IPv6 routers. To use this service you need to have an IPv6 capable host (IPv6 support is available for most platforms) or router which also has IPv4 (existing Internet) connectivity. Our tunnel service is oriented towards developers and experimenters that want a stable tunnel platform.

tunnelbroker.net

- Tunnelbroker

- Podmienka: privátna IPv4 adresa, inak neobmedzené použitie
- Vytvorit si ucet
- Create general tunnel
- EU – Budapešť alebo Praha
- V labe – vyžiadaný /48 rozsah
- Example config – pre rozne zariadenia - parada
- Ak mam dynamicku IP, tak cez dynamic DNS by sa to dalo, ale iba na Mikrotikoch a Cisco, ostatne obmedzene...

Tunnelbroker Login

Username:

Password:

[Forgot Password?](#)

Hurricane Electric Free IPv6 Tunnel Broker

IPv6 Tunnel Broker

Check out our new [usage stats!](#)

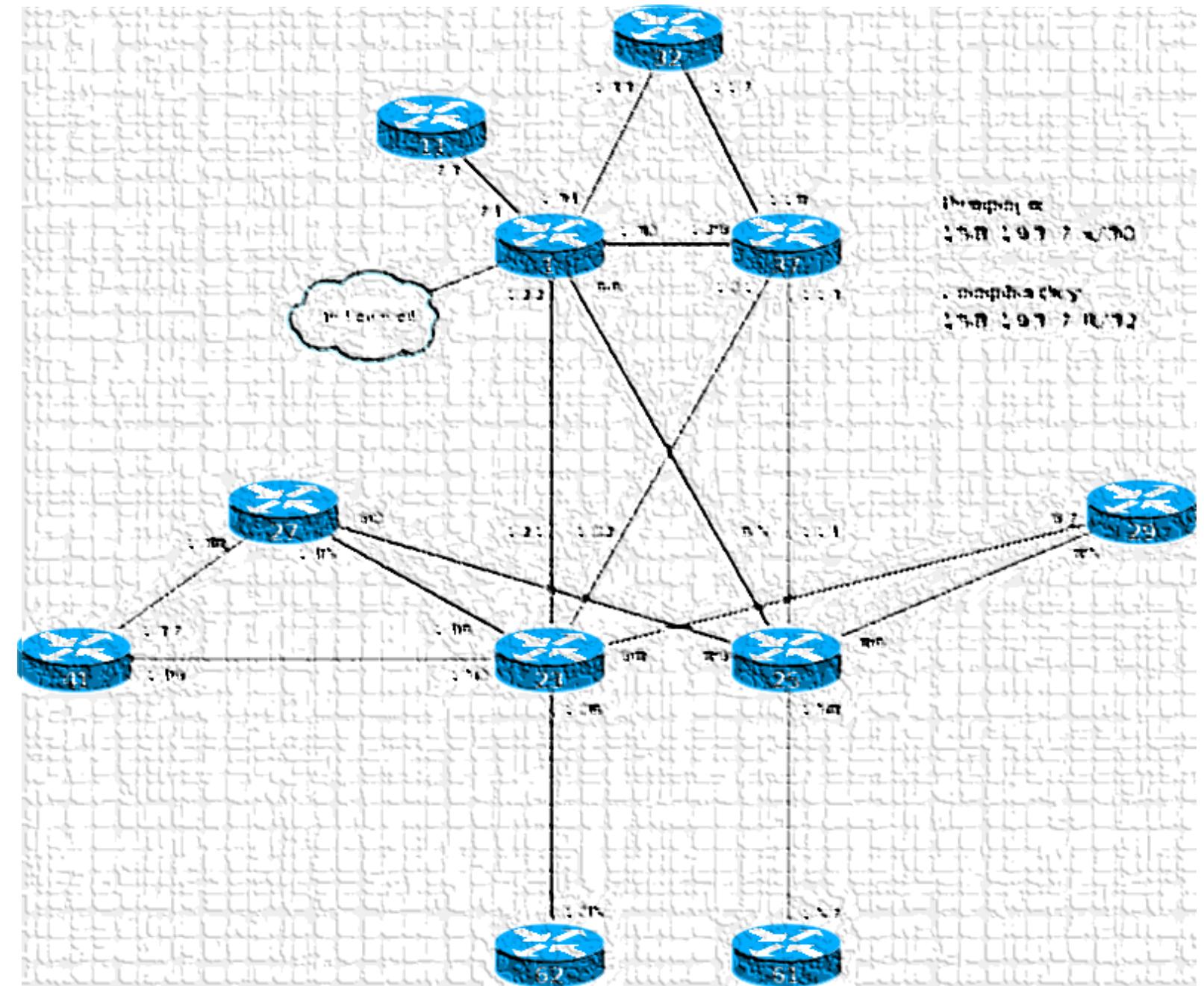
And then hit up our new [Forums!](#)

Welcome to the Hurricane Electric IPv6 Tunnel Broker! Our free tunnel broker service enables you to reach the IPv6 Internet by tunneling over existing IPv4 connections from your IPv6 enabled host or router to one of our IPv6 routers. To use this service you need to have an IPv6 capable host (IPv6 support is available for most platforms) or router which also has IPv4 (existing Internet) connectivity. Our tunnel service is oriented towards developers and experimenters that want a stable tunnel platform.

Routing na FRI

- OSPFv2, v3
 - Spodné dva FRI

>> UKÁŽKA

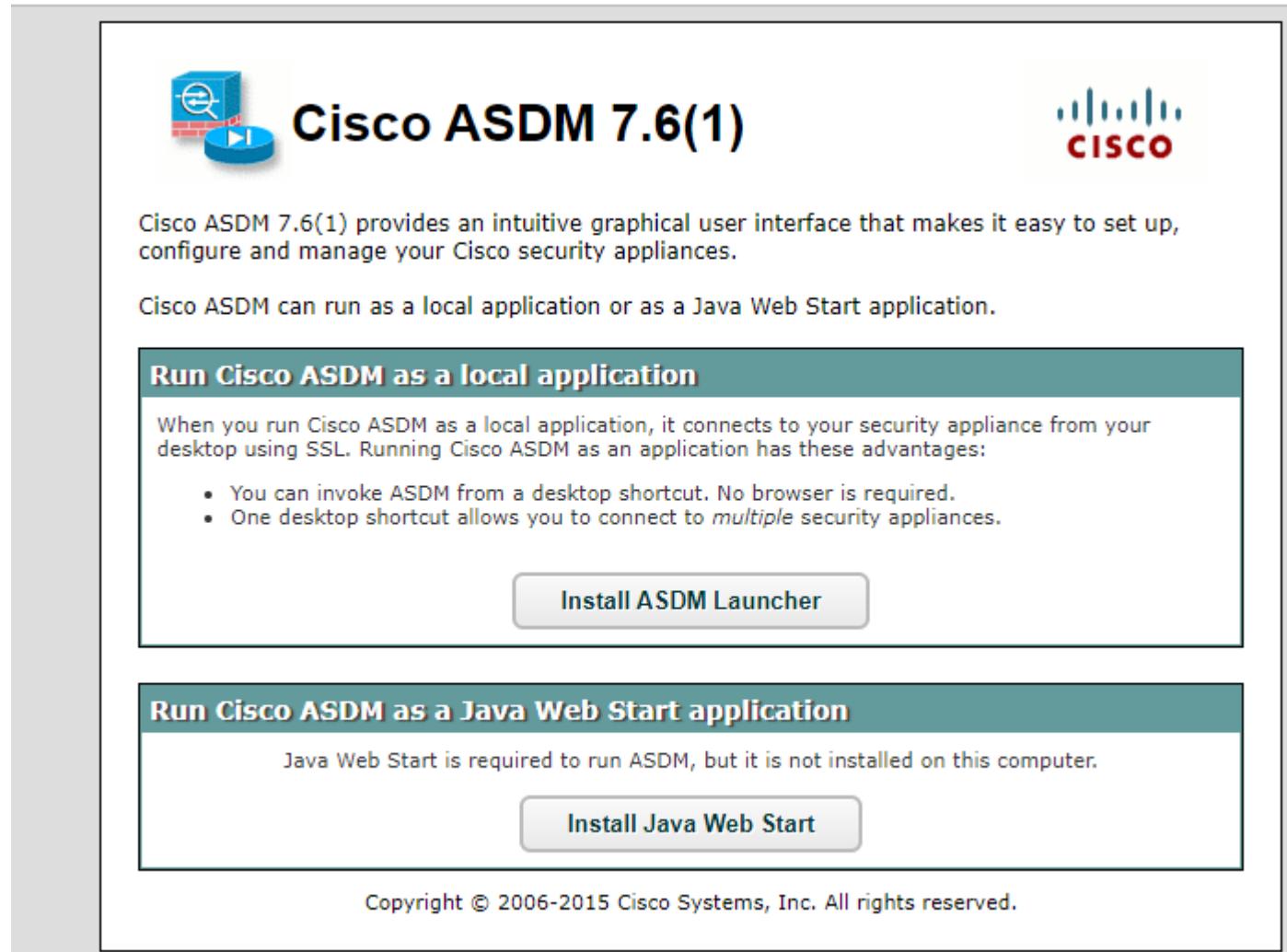


Cisco ASA firewall

Routing na KIS

- Dynamicky: OSPFv2, v3

>> UKÁŽKA



The image shows the Cisco ASDM 7.6(1) landing page. At the top left is a blue icon of a cube with a search and play button. To its right is the text "Cisco ASDM 7.6(1)". In the top right corner is the Cisco logo. Below the title, a text block states: "Cisco ASDM 7.6(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances." Another text block below it says: "Cisco ASDM can run as a local application or as a Java Web Start application." Two main sections are highlighted with teal headers: "Run Cisco ASDM as a local application" and "Run Cisco ASDM as a Java Web Start application". Each section contains descriptive text and a "Install [application name]" button. At the bottom of the page is the copyright notice: "Copyright © 2006-2015 Cisco Systems, Inc. All rights reserved."

Smerovanie – Fortigate – Status window - Dashboard

KIS - Jumpln server - Remote Desktop

FortiGate - FortiGate-200E-KIS +

Not secure | https://192.168.255.1/ng/system/dashboard/1

☰ Search + Add Widget

FortiGate-200E-KIS Favorites Dashboard

Status System Information Licenses (173.243.140.6) Security Fabric Administrators CPU

Hostname: FortiGate-200E-KIS
Serial Number: FG200E4Q17900915
Firmware: v7.2.3 build1262 (Feature)
Mode: NAT
System Time: 2022/12/05 19:11:09
Uptime: 05:03:01:42
WAN IP: 158.193.138.31

Licenses: FortiCare Support, Firmware & General Updates, AntiVirus, Web Filtering, Security Rating

FortiToken: 0/2

Security Fabric: FortiGate-200E-KIS, Security Fabric Connection is disabled.

Administrators: 1 HTTPS, 0 FortiExplorer, palo super_admin

CPU: Current usage 0%

Memory Sessions Routing

Memory: 1 minute, Current usage 18% (19:10:10 to 19:11:00)

Sessions: IPv4 + IPv6, 1 minute, Current sessions 683 (19:10:10 to 19:11:00), SPU 21.7%

Routing: 62 Routes (Type: OSPF 26, Connected 18, Static 10, OSPF (router::ospf_nssa...) 7, OSPF (Inter area) 1)

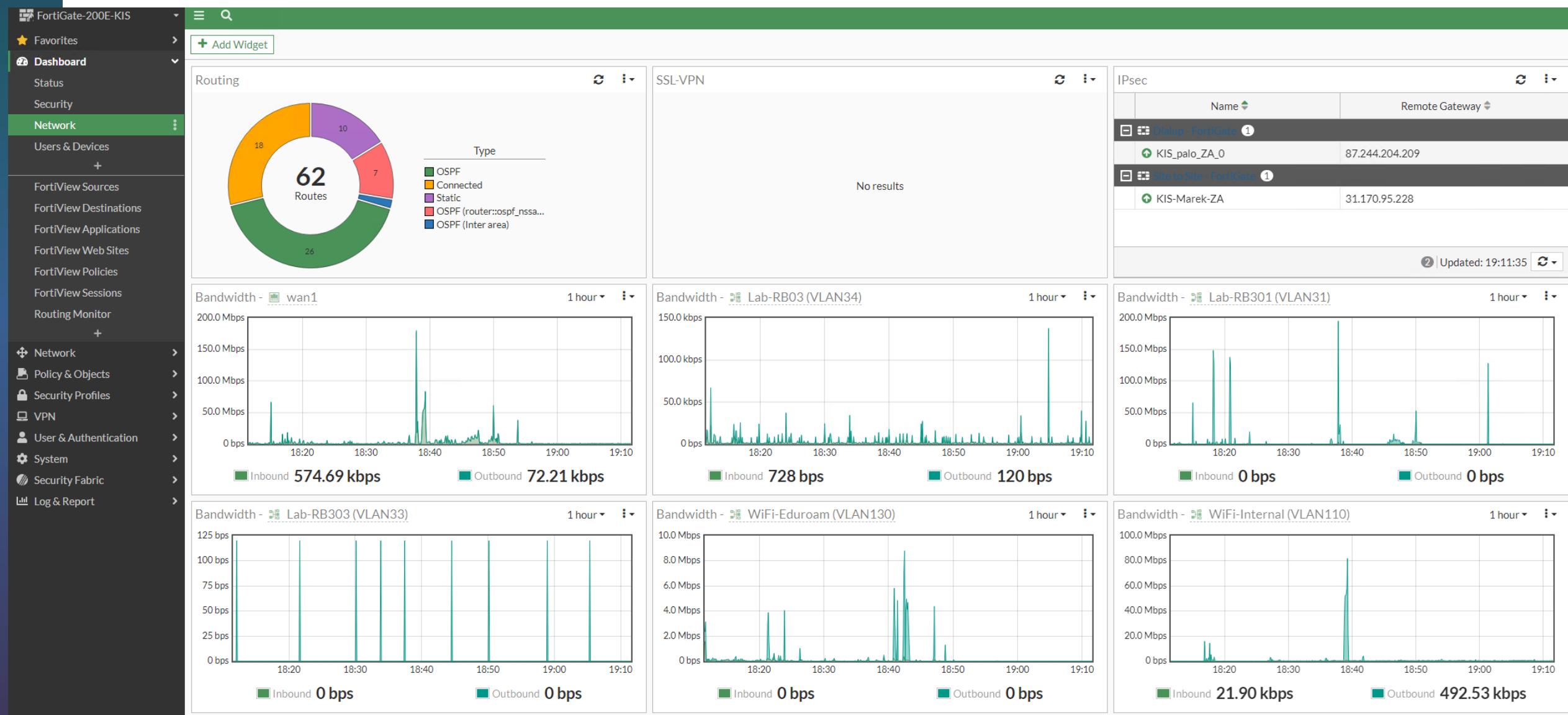
FortiView VPN by Connections IPsec

FortiView VPN by Connections: 1 hour, User, Connections (Dialup - FortiGate 1)

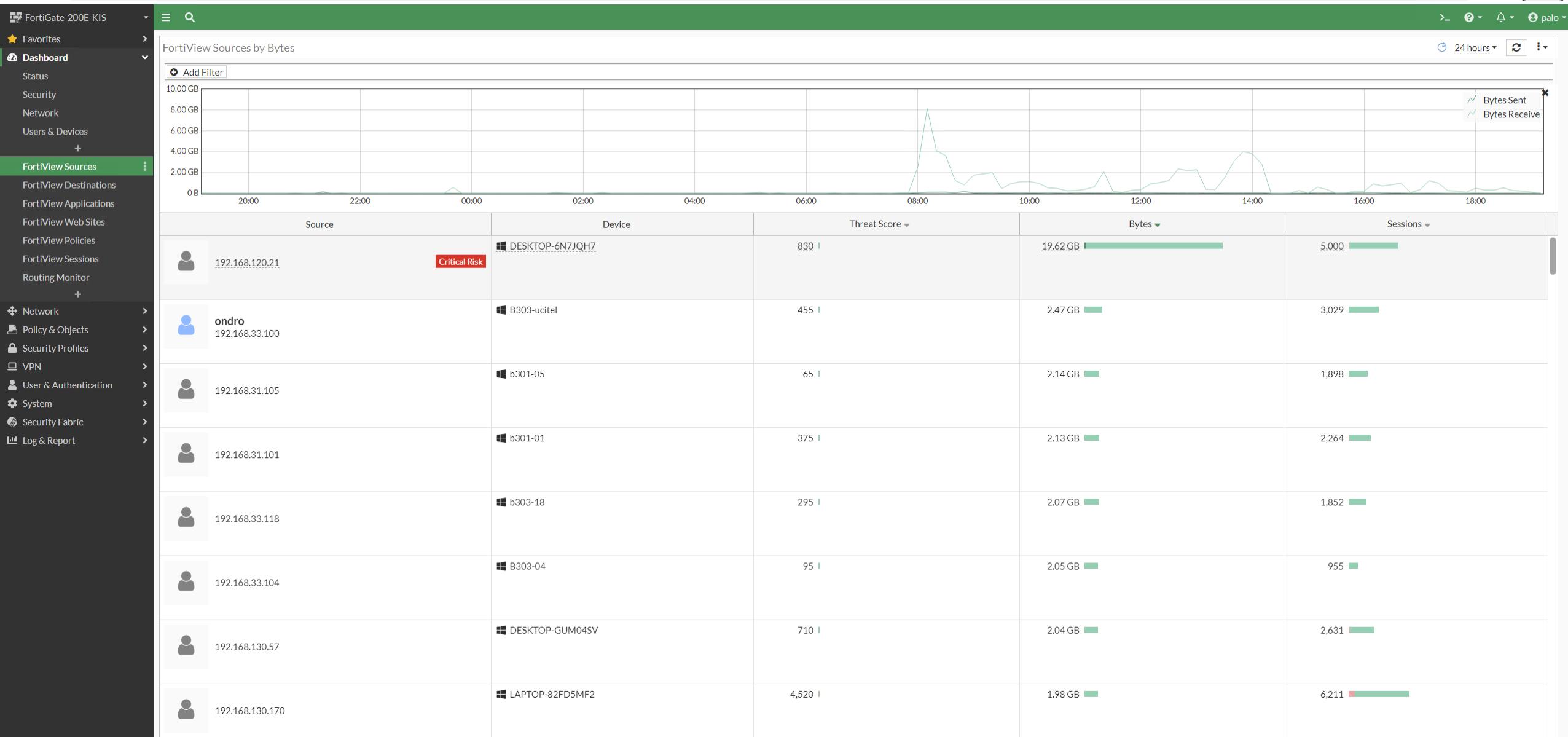
IPsec: Name, Remote Gateway

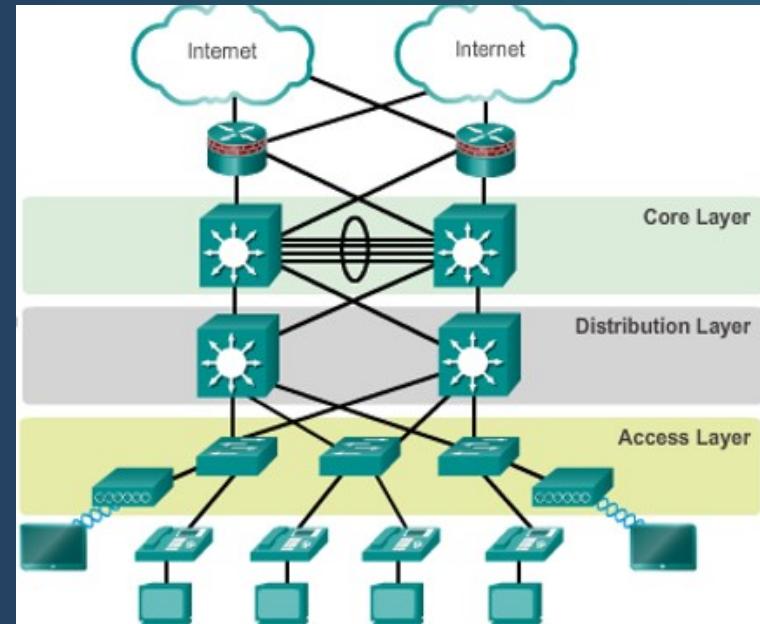
Log & Report

Fortigate – prehľad rozhraní



Fortigate – prehľad kol'ko dát ktorá IP preniesla





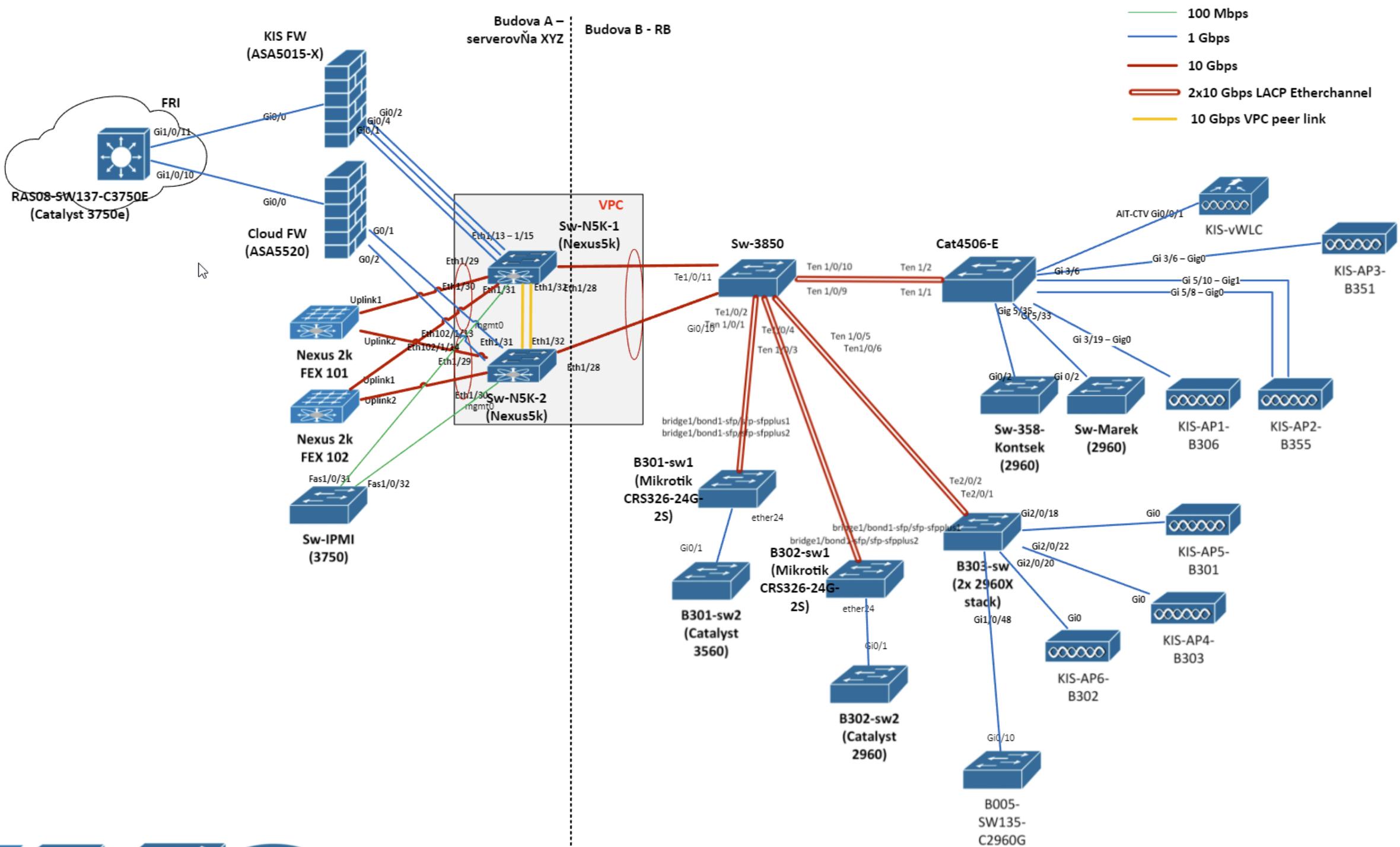
Prednáška 3

Prepínané siete a hierarchický dizajn škálovateľných LAN

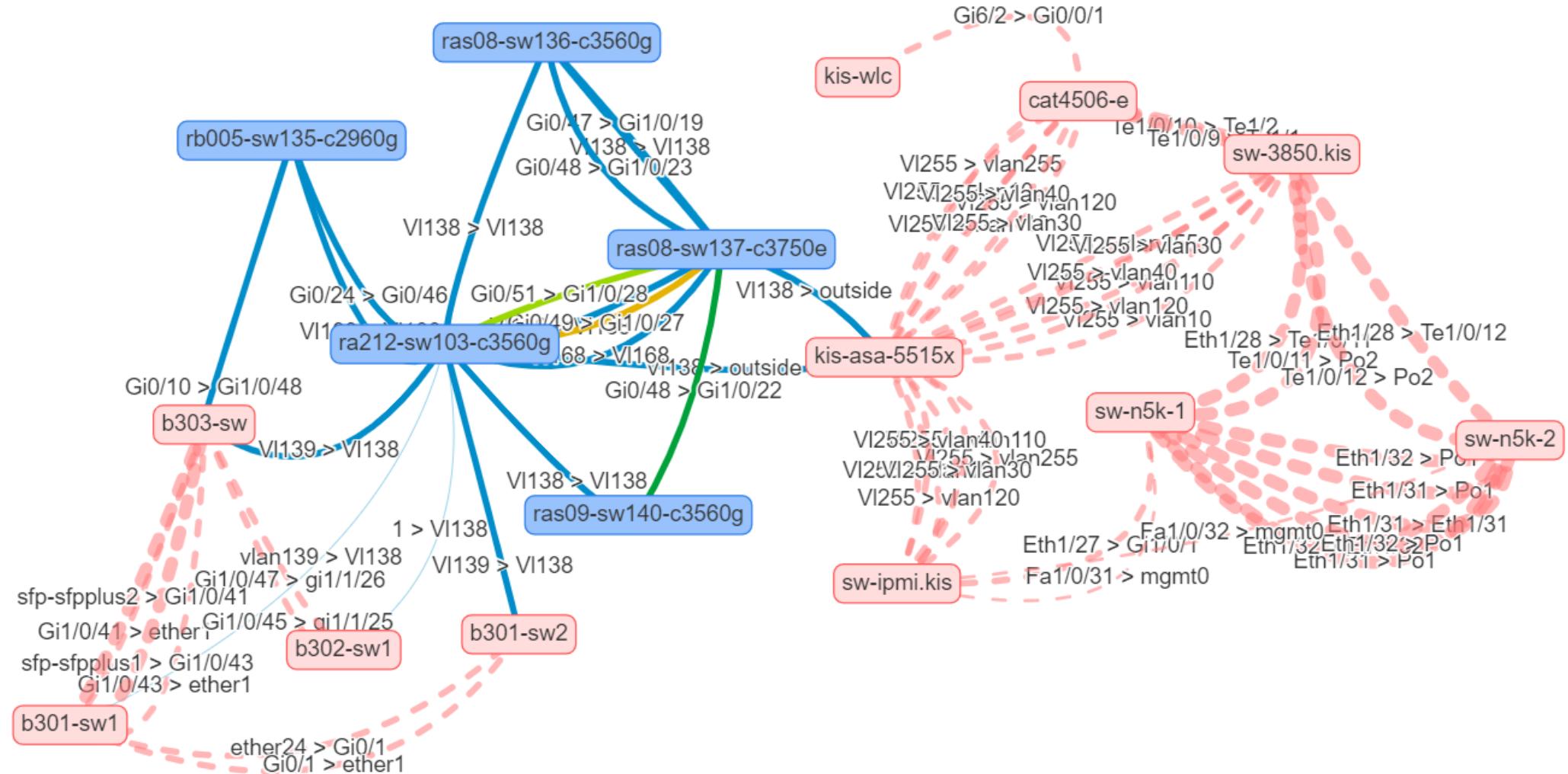
Konfigurácia prepínačov, port security, ssh

FRI infraštruktúra



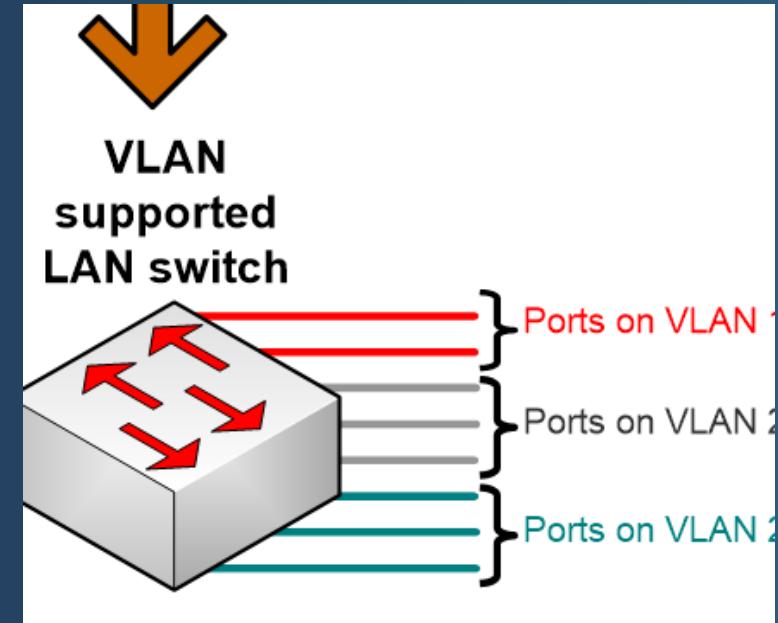


KIS infra – automatický sken a topo mapa



Prednáška 4

VLANs, interVLAN routing, VTP, DTP



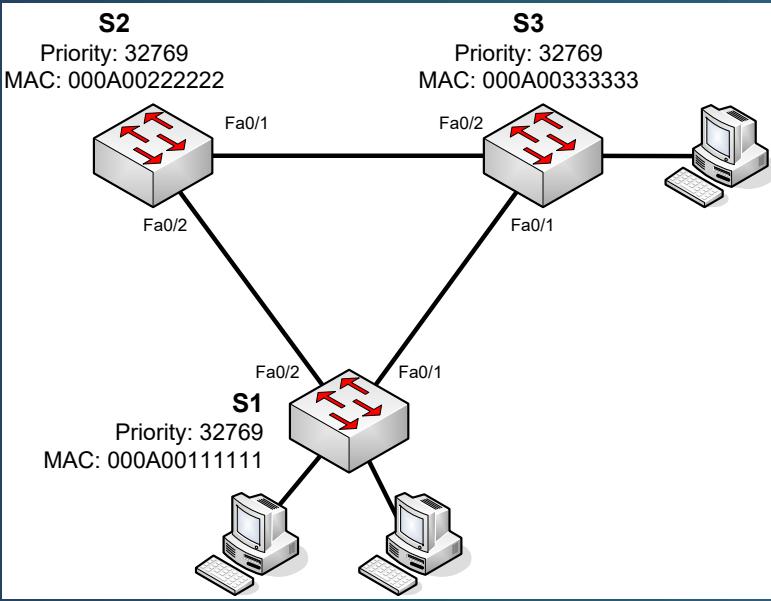
VLANy na KISe

- show vlan
 - KIS, FRI

>> UKÁŽKA 1

>> UKÁŽKA 2





Prednáška 5

STP

Na KISe – multiple PVST

Na FRI – RSTP

>> UKÁŽKA 1

>> UKÁŽKA 2

show span

With or without STP...

- „Hackerský“ útok v parlamente 2022
 - Ako prehodenie jedného kábla znefunkční celú siet'
 - <https://zive.aktuality.sk/clanok/8j9rWnz/ziadny-hackersky-utok-na-parlament-nebol-vypadok-mal-sposobit-kabel-a-zle-nastavenie-it-detaily/>





Prednáška 6

HSRP, Etherchannel

HSRP – ani na KIS, ani na FRI

Etherchannel – na KIS aj FRI

sh eth sum

>> UKÁŽKA (KIS)



Prednáška 7

IPv4 a IPv6 ACL (standard, extended)

Na KISe – filtrovanie robí Cisco ASA a Fortinet Fortigate

Na FRI – ACLs na L3 prepínačoch

Definovanie ACL na Cisco ASA (KIS siet')

```
access-list vlan10_multicast standard permit host 233.10.47.10
access-list VLAN10-IN extended permit ip object-group WIFI-APS object
KIS-WLC-Int
access-list VLAN10-IN extended deny ip object KIS-VLAN-10-IPv4 object
KIS-VLAN-255-IPv4
access-list VLAN10-IN extended permit ip object KIS-VLAN-10-IPv4 any
access-list VLAN255-IN extended permit ip any any
access-list VPN-DISABLED-NAT extended permit ip object KIS-VLAN-10-IPv4
object KIS-VPN-NET
access-list VPN-DISABLED-NAT extended permit ip object KIS-VLAN-255-IPv4
object KIS-VPN-NET
access-list VPN-ALLOWED-NETWORKS standard permit 192.168.10.0
255.255.255.0
access-list VPN-ALLOWED-NETWORKS standard permit 192.168.255.0
255.255.255.0
```

Web GUI na Cisco ASA (KIS siet')

Cisco ASDM 7.6(1) for ASA - 192.168.10.1

File View Tools Wizards Window Help Type topic to search

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Access Rules

Add Edit Delete Find Diagram Export Clear Hits Show Log

Configuration > Firewall > Access Rules

#	Enabled	Source Criteria:	Destination Criteria:	Service	Action	Hits	Logging
1	<input checked="" type="checkbox"/>	any	Any less secure ne...	IP ip	Permit		
		mgmt (0 implicit incoming rules)					
		outside (36 incoming rules)					
1	<input checked="" type="checkbox"/>	block_address	any	IP ip	Deny	7701	<input checked="" type="checkbox"/> disa...
2	<input checked="" type="checkbox"/>	any	SSH-PRISTUP-64	TCP SSH	Permit	TOP 10 29...	
3	<input checked="" type="checkbox"/>	any	WEB-PRISTUP-64	TCP WEB	Permit	TOP 10 11...	
4	<input checked="" type="checkbox"/>	any	158.193.138.32	SERV ASA	Permit	0	
5	<input type="checkbox"/>	any	CLOUD-PUBLIC-NET	IP ip	Permit	0	
6	<input checked="" type="checkbox"/>	any	CASTOR-64	SERV_CASTOR	Permit	TOP 10 36...	
7	<input type="checkbox"/>	any	NLAB-64	SERV_NLAB	Permit	0	
8	<input checked="" type="checkbox"/>	KIS-LWAPs-Ext	KIS-WLC-Ext	UDP CAPWAP	Permit	0	
9	<input checked="" type="checkbox"/>	KIS-LWAPs-Ext	KIS-WLC-Int	UDP CAPWAP	Permit	19	
10	<input checked="" type="checkbox"/>	158.193.139.100	192.168.255.9	IP ip	Permit	0	
11	<input checked="" type="checkbox"/>	158.193.139.100	158.193.152.9	IP ip	Permit	0	
12	<input checked="" type="checkbox"/>	KIS-AP5	158.193.152.9	IP ip	Permit	0	
13	<input checked="" type="checkbox"/>	KIS-AP5	192.168.255.9	UDP 12222-12223	Permit	0	
14	<input checked="" type="checkbox"/>	Laboratoria-4	158.193.152.2	UDP 12222-12223	Permit	0	
15	<input checked="" type="checkbox"/>	Laboratoria-4	158.193.152.2	UDP 445	Permit	0	
16	<input checked="" type="checkbox"/>	Uniza	SI ICH-SFR VFR	TCP 445	Permit	11	

Addresses

Add Edit Delete Filter:

Name

Network Objects

- any
- any4
- any6
- Cloud-firewall-IPv4
- cloud-network/25
- cloud-network4
- cloud-network6/64
- cloud-private-web
- CLOUD-PUBLIC-NET
- cloud-public-web
- DC_IP4
- DC_IP6
- DC_public_IP4
- dmz-network/25
- dmz-network6/64
- Eagle
- Eagle-pollux
- ECPI_email

Zoznam a mená rozhraní

Fortigate FW

The screenshot shows the FortiGate 200E-KIS interface configuration page. The left sidebar lists navigation options: Favorites, Dashboard, Network (selected), Interfaces (selected), DNS, IPAM, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Diagnostics, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, and Log & Report.

The main area displays a summary of interfaces at the top, followed by a table listing individual interfaces. The table columns are: Name, Type, Members, and IP/Netmask.

Name	Type	Members	IP/Netmask
802.3ad Aggregate 15	802.3ad Aggregate	port1 port2	0.0.0/0.0.0
Loopback Interface 1	Loopback Interface		172.31.255.255/255.255.255.255
Physical Interface 19	Physical Interface		0.0.0/0.0.0
ha	Physical Interface		0.0.0/0.0.0
mgmt	Physical Interface		192.168.10.203/255.255.255.0
port3	Physical Interface		0.0.0/0.0.0
port4	Physical Interface		0.0.0/0.0.0
port5	Physical Interface		0.0.0/0.0.0
port6	Physical Interface		0.0.0/0.0.0
port7	Physical Interface		0.0.0/0.0.0
port8	Physical Interface		0.0.0/0.0.0
port9	Physical Interface		0.0.0/0.0.0
port10	Physical Interface		0.0.0/0.0.0
port15	Physical Interface		0.0.0/0.0.0
port16	Physical Interface		0.0.0/0.0.0
port17	Physical Interface		0.0.0/0.0.0
port18	Physical Interface		0.0.0/0.0.0
wan1	Physical Interface		158.193.138.31/255.255.255.0
wan2	Physical Interface		0.0.0/0.0.0
Software Switch 1	Software Switch	port11 port12 port13 port14	0.0.0/0.0.0
Tunnel Interface 2	Tunnel Interface		0.0.0/0.0.0
I2t.root	Tunnel Interface		0.0.0/0.0.0

Fortigate FW - Traffic monitoring – accept/deny policies and results

Traffic Monitoring Results								
	Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	
FortiGate-200E-KIS	2022/12/05 19:15:16	212.70.149.10		158.193.154.84	tcp/31005	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
	2022/12/05 19:15:16	173.214.175.178		158.193.154.215	tcp/7121	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
	2022/12/05 19:15:16	163.172.111.147		158.193.154.161	tcp/11094	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
User & Authentication	2022/12/05 19:15:16	185.81.68.21		158.193.152.176 (b03-176.netlab.kis.fri.uniza.sk)	tcp/2443	✗ Deny	Implicit Deny	
System	2022/12/05 19:15:16	192.241.200.59		158.193.154.3	udp/5353	✓ Accept (74 B / 0 B)	TEST Novy CC FW 100F	
Security Fabric	2022/12/05 19:15:16	192.241.200.59		158.193.154.110	udp/5353	✓ Accept (74 B / 0 B)	TEST Novy CC FW 100F	
Log & Report	2022/12/05 19:15:16	192.168.10.11	Cisco ASA 5515-X	192.168.211.1	tcp/49152	✓ Accept (420 B / 0 B)	KIS->Internal_networks	
Forward Traffic	2022/12/05 19:15:15	71.6.147.254		158.193.154.246	tcp/8833	✓ Accept (44 B / 0 B)	TEST Novy CC FW 100F	
Local Traffic	2022/12/05 19:15:15	165.227.25.154		158.193.152.200	tcp/26592	✗ Deny	Implicit Deny	
Multicast Traffic	2022/12/05 19:15:15	209.159.158.114		158.193.154.156	HTTPS	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
Sniffer Traffic	2022/12/05 19:15:15	192.168.10.11	Cisco ASA 5515-X	192.168.211.1	tcp/49152	✓ Accept (420 B / 0 B)	KIS->Internal_networks	
ZTNA Traffic	2022/12/05 19:15:15	212.70.149.10		158.193.154.253	tcp/32868	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
System Events	2022/12/05 19:15:15	209.159.158.114		158.193.154.79	HTTPS	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
Security Events	2022/12/05 19:15:15	193.163.125.20		158.193.152.166	tcp/14001	✗ Deny	Implicit Deny	
Log Settings	2022/12/05 19:15:15	162.142.125.141		158.193.152.187	tcp/2222	✗ Deny	Implicit Deny	
Threat Weight	2022/12/05 19:15:15	43.192.44.118		158.193.154.109	PING	✓ Accept (40 B / 0 B)	ICMP	
FortiAnalyzer Reports	2022/12/05 19:15:15	43.192.44.118		158.193.154.109	icmp/0/8	✓ Accept (ip-conn)	ICMP	
	2022/12/05 19:15:15	101.68.211.3		158.193.154.198	tcp/8081	✓ Accept (44 B / 0 B)	TEST Novy CC FW 100F	
	2022/12/05 19:15:15	92.63.197.154		158.193.152.208	tcp/5877	✗ Deny	Implicit Deny	
	2022/12/05 19:15:15	193.163.125.30		158.193.152.222	tcp/61336	✗ Deny	Implicit Deny	
	2022/12/05 19:15:15	198.235.24.162		158.193.152.175 (b03-175.netlab.kis.fri.uniza.sk)	tcp/8333	✗ Deny	Implicit Deny	
	2022/12/05 19:15:15	192.241.199.180		158.193.154.236	tcp/49152	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	
	2022/12/05 19:15:15	208.100.26.228		158.193.152.131	tcp/50075	✗ Deny	Implicit Deny	
	2022/12/05 19:15:15	192.168.34.124	B03-24	158.193.139.15	HTTP	✓ Accept (260 B / 0 B)	Labaky->Internet	
	2022/12/05 19:15:14	100.241.100.100		150.100.154.101	tcp/10150	✓ Accept (40 B / 0 B)	TEST Novy CC FW 100F	

FW policy

FortiGate-200E-KIS

Edit Policy

ID: 7

Name: NTP

Incoming Interface: any

Outgoing Interface: any

Source: all, all

Negate Source:

IP/MAC Based Access Control: +

Destination: all, all

Negate Destination:

Schedule: always

Service: NTP

Action: ACCEPT DENY

Inspection Mode: Flow-based

Firewall/Network Options:

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

NAT46 / NAT64:

Protocol Options: PROT default

Security Profiles:

- AntiVirus:
- Web Filter:
- DNS Filter:
- Application Control:
- File Filter:
- VoIP:

SSL Inspection: SSL no-inspection

Logging Options:

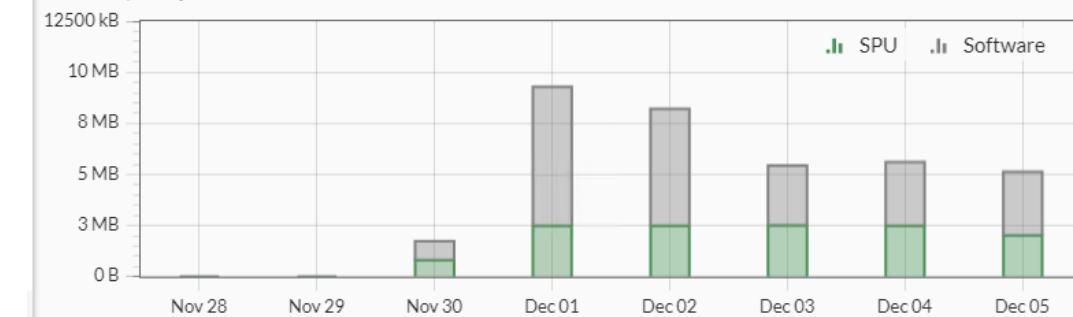
Log Allowed Traffic: Security Events: All Sessions

Statistics (since last reset)

ID	7
Last used	4 second(s) ago
First used	5 day(s) ago
Active sessions	38
Hit count	417,336
Total bytes	35.40 MB
Current bandwidth	986 bps

Clear Counters

Last 7 Days Bytes IPv4 + IPv6



Additional Information

API Preview

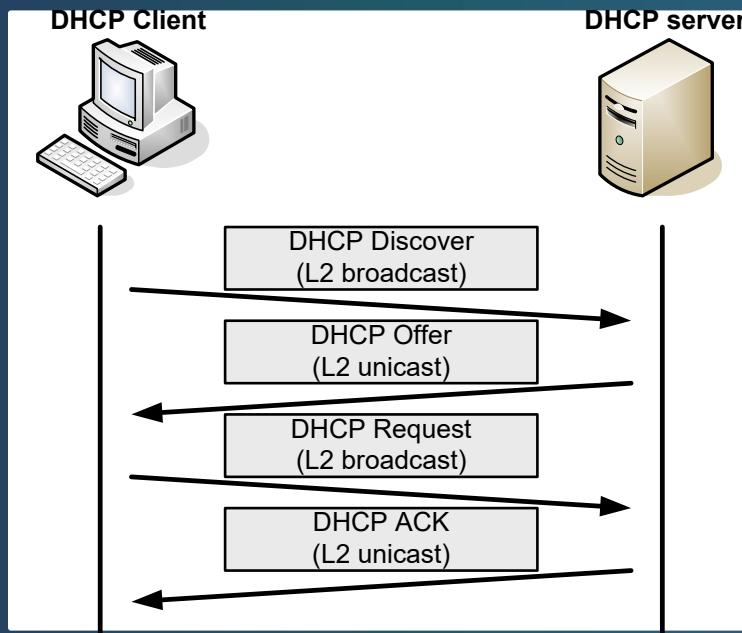
Edit in CLI

Online Guides

- Relevant Documentation [↗](#)
- Video Tutorials [↗](#)
- Consolidated Policy Configuration [↗](#)

FortiAnswers

Join the Discussion [↗](#)



Prednáška 8

DHCPv4

DHCPv6 (SLAAC, Stateless, Statefull)

Na KISe - používame ISC DHCP:

ISC Internet Systems Consortium (isc.org)

(Open Source For an Open Internet)

- DHCP

- BIND

- Kya (má nahradit' DHCP)

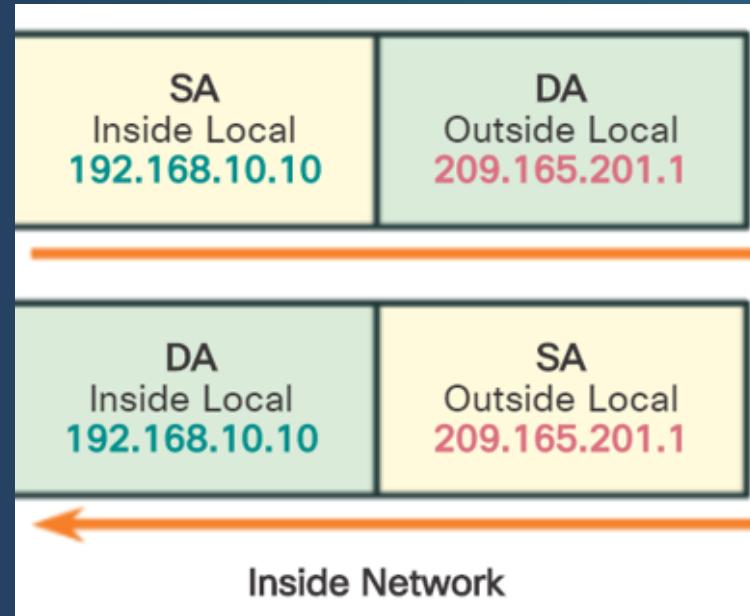
(Open SSH)

>> UKÁŽKA

>> UKÁŽKA: kis-labs.dhcpd

>> UKÁŽKA: kis-labs.dhcpd6





Prednáška 9

NAT

Na FRI – individuálne na katedrách

Na KISe pre internú siet' robí Cisco ASA a Fortinet Fortigate

>> UKÁŽKA: ASA: Configuration/Firewall/NAT rule, Fortigate: Central SNAT (source NAT)

NAT na Fortigate FW

FortiGate-200E-KIS

Favorites >

Dashboard >

Network >

Policy & Objects >

- Firewall Policy ★
- Central SNAT** ★
- Multicast Policy
- IPv6 Multicast Policy
- IPv4 DoS Policy
- IPv6 DoS Policy
- ZTNA
- Authentication Rules
- Addresses
- Internet Service Database
- Services
- Schedules
- DNAT & Virtual IPs
- IP Pools
- Protocol Options
- Security Profiles >
- VPN >
- User & Authentication >
- System >

Search

+ Create New | Edit | Delete | Search | | Q

IPv4 9

ID	From	To	Source Address	Destination Address	Translated Address
1	Lab-RB301 (VLAN31) Lab-RB303 (VLAN33) Lab-RB302 (VLAN32) Lab-ECDL (VLAN30) Lab-RB03 (VLAN34) WiFi-Guest (VLAN120) WiFi-Eduroam (VLAN130) VoIP (VLAN40) WiFi-Internal (VLAN110) Management (VLAN255) KIS-Marek-ZA		Labaky-IPv4 WiFi-Eduroam-IPv4 WiFi-Guest-IPv4 VoIP-IPv4 WiFi-Internal-IPv4 KIS_MGMT-IPv4 Marek-ZA_LAN		
2	DMZ-Private (VLAN201)		DMZ_PRIVATE-IPv4		
3	Lab-RB03 (VLAN34)		B03-IPv4		B03-public-NAT
4	Lab-ECDL (VLAN30)		ECDL-IPv4		ECDL-public-NAT
5	Lab-RB301 (VLAN31)		B301-IPv4		B301-public-NAT
6	Lab-RB302 (VLAN32)		B302-IPv4		B302-public-NAT
7	Lab-RB303 (VLAN33)		B303-IPv4		B303-public-NAT
8	KIS-Internal (VLAN10) WiFi-Internal (VLAN110)		KIS-Internal-IPv4 WiFi-Internal-IPv4		Katedra-public-NAT
9	WiFi-Guest (VLAN120) WiFi-Eduroam (VLAN130)		WiFi-Eduroam-IPv4 WiFi-Guest-IPv4		WiFi-public-NAT



Prednáška 11 WLAN

Na KISe: Cisco WLC a AP

>> UKÁŽKA: Cisco wireless controller

Cisco Wireless Controller



Cisco Wireless Controller

AP or Client Search

Advanced



NETWORK SUMMARY



ACCESS POINTS

BY USAGE



- KIS-AP8-B003
- KIS-AP5-B301
- KIS-AP4-B303
- KIS-AP6-B302
- KIS-AP7-B360
- KIS-AP2-B355
- KIS-AP1-B306
- KIS-AP3-B351



OPERATING SYSTEMS

	Name	Clients
1	Android	2
2	Microsoft-Workstation	1
3	Linux-Workstation	1
4	Epson-Device	1

Zoznam APs riadených pomocou WLC

ACCESS POINTS

2.4GHz 5GHz

AP Name	Clients	Usage	Uptime	Chann...	Channels	Covera...	Interfe...	Rogues	MAC Addr
KIS-AP5-B301	3	24.0 GB	19 Days 5 Hours	42	1	20	42	14	38:90:a5
KIS-AP8-B003	1	31.2 GB	19 Days 4 Hours	30	11	8	30	5	50:0f:80:
KIS-AP6-B302	0	18.2 GB	18 Days 19 Hours	30	11	0	30	6	5c:83:8f:
KIS-AP2-B355	0	3.7 GB	15 Days 44 Minu...	16	11	0	16	8	4c:77:6d
KIS-AP1-B306	1	5.7 GB	15 Days 44 Minu...	22	11	0	21	8	4c:77:6d
KIS-AP7-B360	2	9.5 GB	14 Days 5 Hours	18	1	2	18	3	70:7d:b9
KIS-AP3-B351	0	1.5 GB	15 Days 44 Minu...	8	6	0	8	2	4c:77:6d
KIS-AP4-B303	0	17.3 GB	19 Days 4 Hours	16	6	5	16	96	00:a6:ca

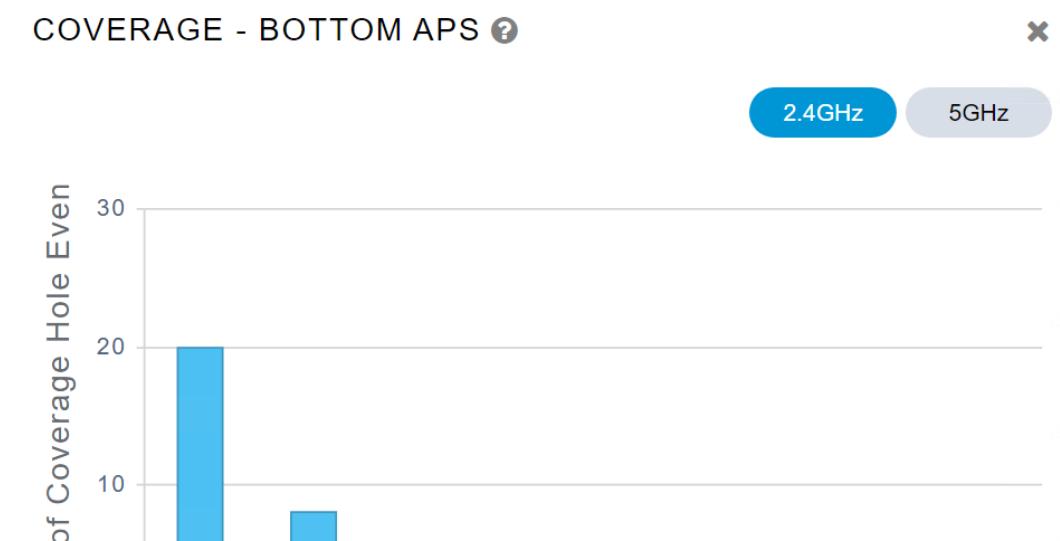
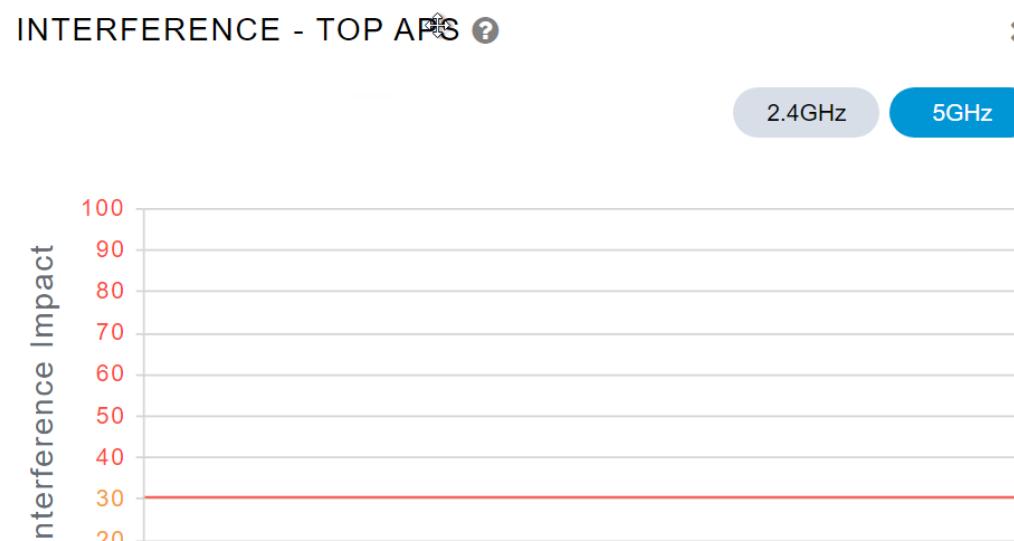
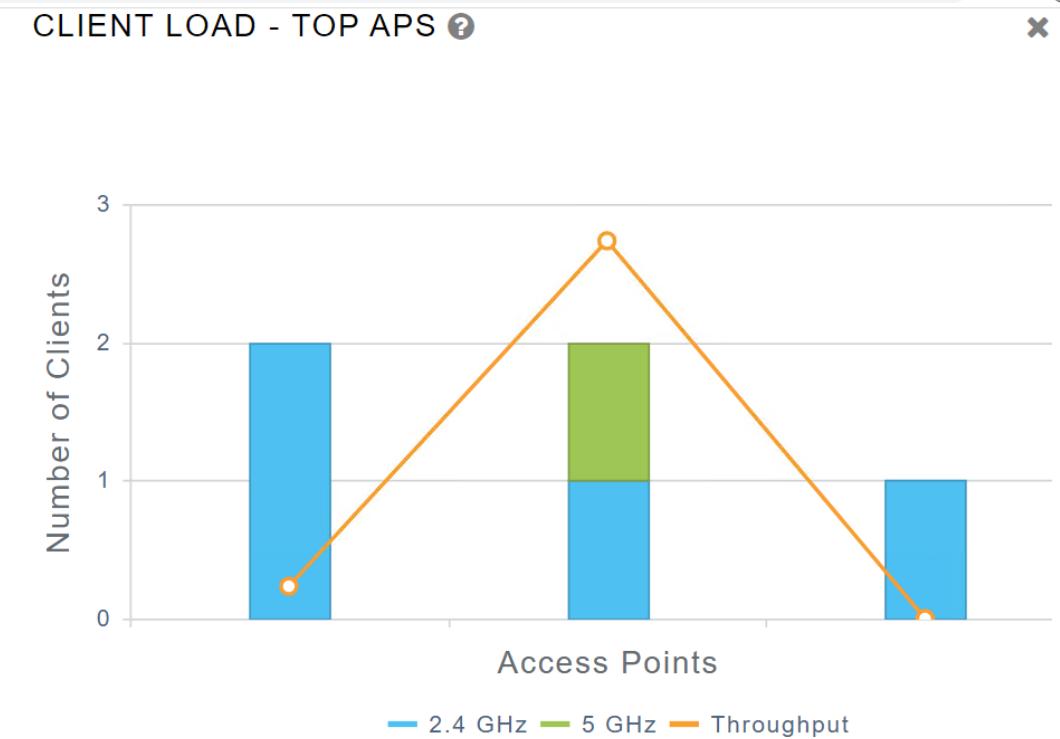
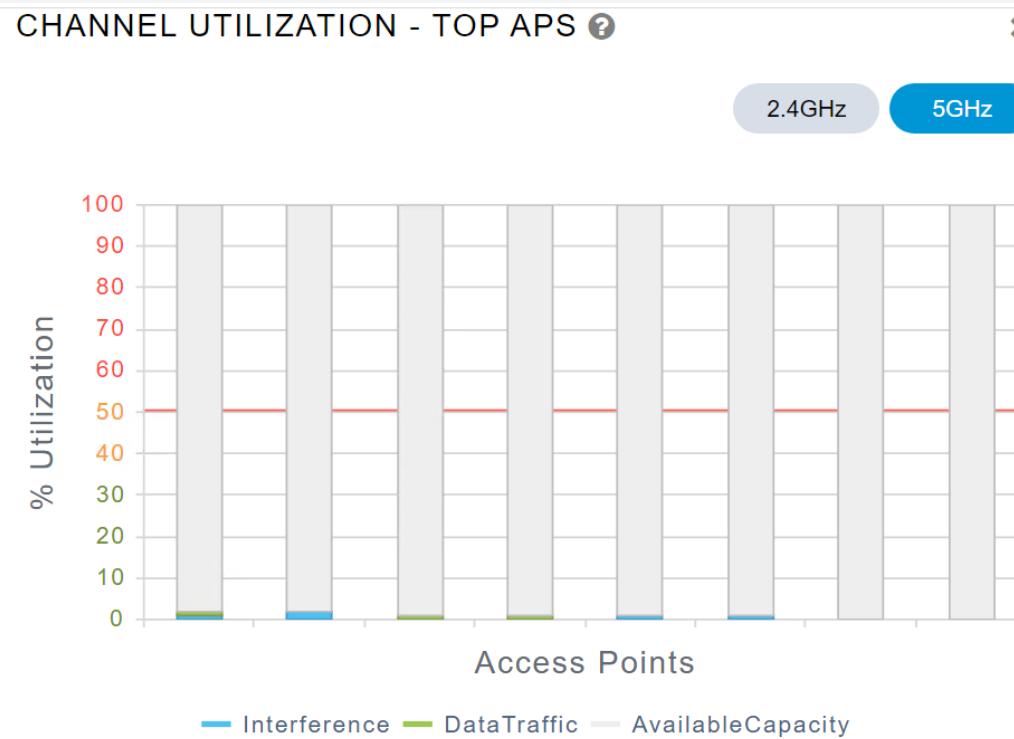
1 25 items per page1 - 8 of 8 items

Pripojení klienti v dashboarde

CLIENTS

Clients	Total	7	Wireless		6	Apple		0
	2.4GHz		5GHz	Fastlane		Analytics		
User Name	AP Name	Protocol	Connection ...	Status	Signal Q...	Signal S...	WLAN	
Unknown	KIS-AP5-B301	802.11n	0	Online	22	-77	eduroa	
Unknown	KIS-AP7-B360	802.11n	72	Online	45	-53	KIS-G	
Unknown	KIS-AP5-B301	802.11n	0	Online	8	-92	eduroa	
kralik	KIS-AP8-B003	802.11ac	200	Online	30	-66	KIS	
kralik	KIS-AP8-B003	802.11n	72	Online	38	-63	KIS	
kis\marek	KIS-AP7-B360	802.11n	43	Online	22	-75	KIS	
1001989@uniza.sk	KIS-AP1-B306	802.11n	58	Online	14	-78	eduroa	
1	25	items per page	1 - 7 of 7 items					

AP performance - vyt'aženie



Summary

100 Access Points Supported

Cisco Virtual Wireless Controller

Controller Summary

Management IP Address	192.168.201.6 , 2001:4118:300:121::32/64
-----------------------	--

Service Port IP Address	0.0.0.0 , ::/128
-------------------------	------------------

Software Version	8.10.171.0
------------------	------------

Emergency Image Version	8.10.142.0
-------------------------	------------

System Name	KIS-vWLC
-------------	----------

Up Time	15 days, 6 hours, 4 minutes
---------	-----------------------------

System Time	Mon Dec 5 19:24:46 2022
-------------	-------------------------

Redundancy Mode	N/A
-----------------	-----

802.11a Network State	Enabled
-----------------------	---------

802.11b/g Network State	Enabled
-------------------------	---------

Local Mobility Group	kis
----------------------	-----

CPU Usage	0%
-----------	----

Memory Usage	75%
--------------	-----

vWLC Config	Small
-------------	-------

Access Point Summary

	Total	Up	Down	
802.11a/n/ac/ax Radios	8	● 8	● 0	Detail
802.11b/g/n/ax Radios	5	● 5	● 0	Detail
Dual-Band Radios	3	● 3	● 0	Detail
Dual-5G Radios	0	● 0	● 0	Detail

GUI kontrolera, home page pre monitoring

Rogue Summary

Active Rogue APs	81	Detail
Active Rogue Clients	5	Detail
Adhoc Rogues	1	Detail
Rogues on Wired Network	0	

Session Timeout

Top WLANs

Profile Name	# of Clients	
KIS	3	Detail
KIS-Guest	1	Detail
eduroam	1	Detail

Most Recent Traps

- Rogue AP: 70:df:2f:8e:63:b1 detected on Base Radio MAC: 38:90:a5:90:6b:a0 Interface
- Rogue AP: e8:48:b8:e9:97:d7 detected on Base Radio MAC: 38:90:a5:90:6b:a0 Interface
- Rogue AP : 86:69:93:89:a4:5a removed from Base Radio MAC : 00:a2:ee:a6:9f:10 Interface
- Rogue AP: 44:d9:e7:2c:81:71 detected on Base Radio MAC: 38:0e:4d:00:aa:50 Interface
- Rogue AP : 84:b2:61:90:d5:5d removed from Base Radio MAC : 38:90:a5:90:6b:a0 Interface
- [View All](#)

Top Flex Applications

WIFI WLAN

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANS

Current Filter: None

[Change Filter] [Clear Filter]

Create New

Go

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	KIS	KIS	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	2	WLAN	KIS-Guest	KIS-Guest	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	3	WLAN	eduroam	eduroam	Enabled	[WPA2][Auth(802.1X)]



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics



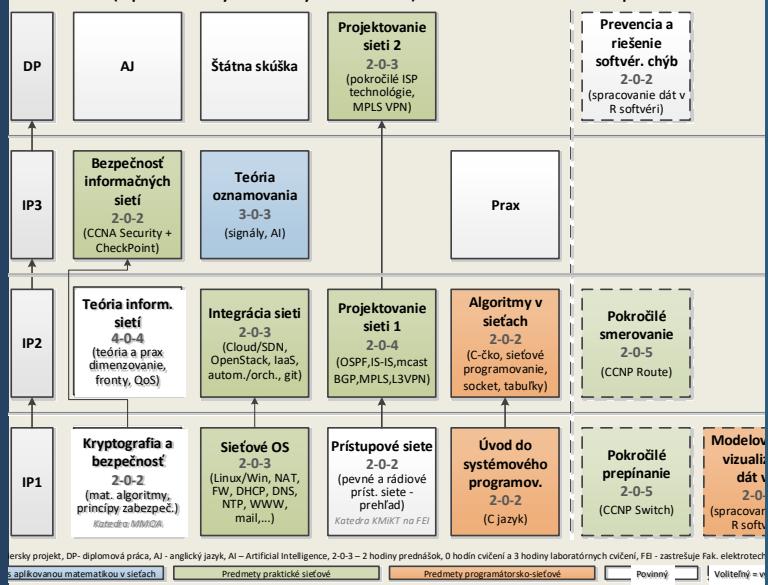
MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

**Ďakujem za pozornosť,
ale... toto nie je posledný slajd.**

Obsahom boli ukážky, ako máme technológie a protokoly preberané v PS1 implementované na KIS/FRI/UNIZA.

Vyjadrite svoj názor na [prednášku](#) tohto týždňa (alebo cvičenie).

ASI (aplikovaný sieťový inžinier) - aktuálna zostava predmetov 2023/2024



Aké ďalšie predmety o siet'ach vás čakajú

PDF dostupné na Moodle...