PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

C. Síť

Dokument obsahuje:	Specifikaci dodávaného síťového řešení.
Verze:	6.1
Schválil za Dodavatele:	RNDr. Vladimír Příbramský
Datum:	10/10/2014

Registrační číslo projektu CZ.1.06/3.4.00/11.07071

Obsah

1 Cíle dokumentu

Cílem tohoto dokumentu je:

- popsat fyzická připojení lokalit, do kterých jsou dodávány technologie projektu NIS IZS.
- definovat způsoby komunikace mezi jednotlivými systémovými prvky s odkazem na využití VPN pro složky IZS a jejich přístup ke službám v datových centrech NIS IZS.
- popsat adresní plán k připojení všech potřebných systémových prvků NIS IZS a specifikovat požadavky na souběžný projekt ITS NGN, který má za cíl povýšit z hlediska přenosové kapacity a dostupnosti síťovou infrastrukturu propojující lokality složek IZS.

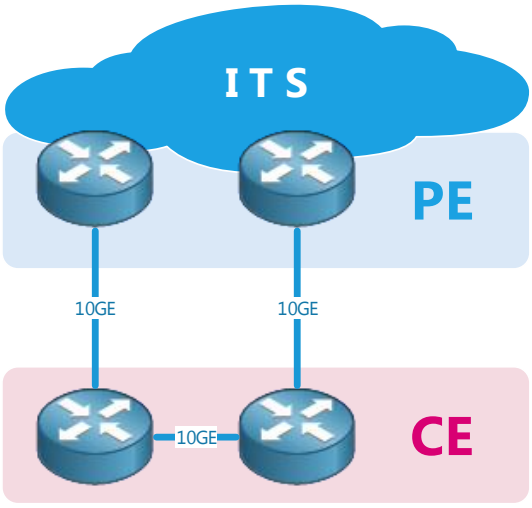
2 Požadavky na připojení k síti ITS (ITS NGN)

Síť ITS a její následovník ITS NGN je definována jako propojovací síť Ministerstva vnitra ČR. Pro projekt NIS IZS zajišťuje propojení jednotlivých složek IZS a jejich konektivitu k datovým centrům NIS IZS. Tento dokument neobsahuje informace o síti ITS NGN, jejíž dostavba je řešena samostatným projektem MV ČR, ale pouze definuje požadavky projektu NIS IZS na tuto přenosovou infrastrukturu.

Připojení k síti ITS NGN bude vždy realizováno na vazbě PE a CE vrstvy, kde bude pomocí dynamického směrovacího protokolu zajištěna rychlá konvergence sítě, automatická změna topologie sítě a volba optimální cesty mezi lokalitami NIS IZS. Propojení bude realizováno pomocí ethernetových rozhraní, na kterých bude možné předávat jednotlivé VPN složek IZS.

2.1 Fyzické připojení lokalit SKDC a KDC

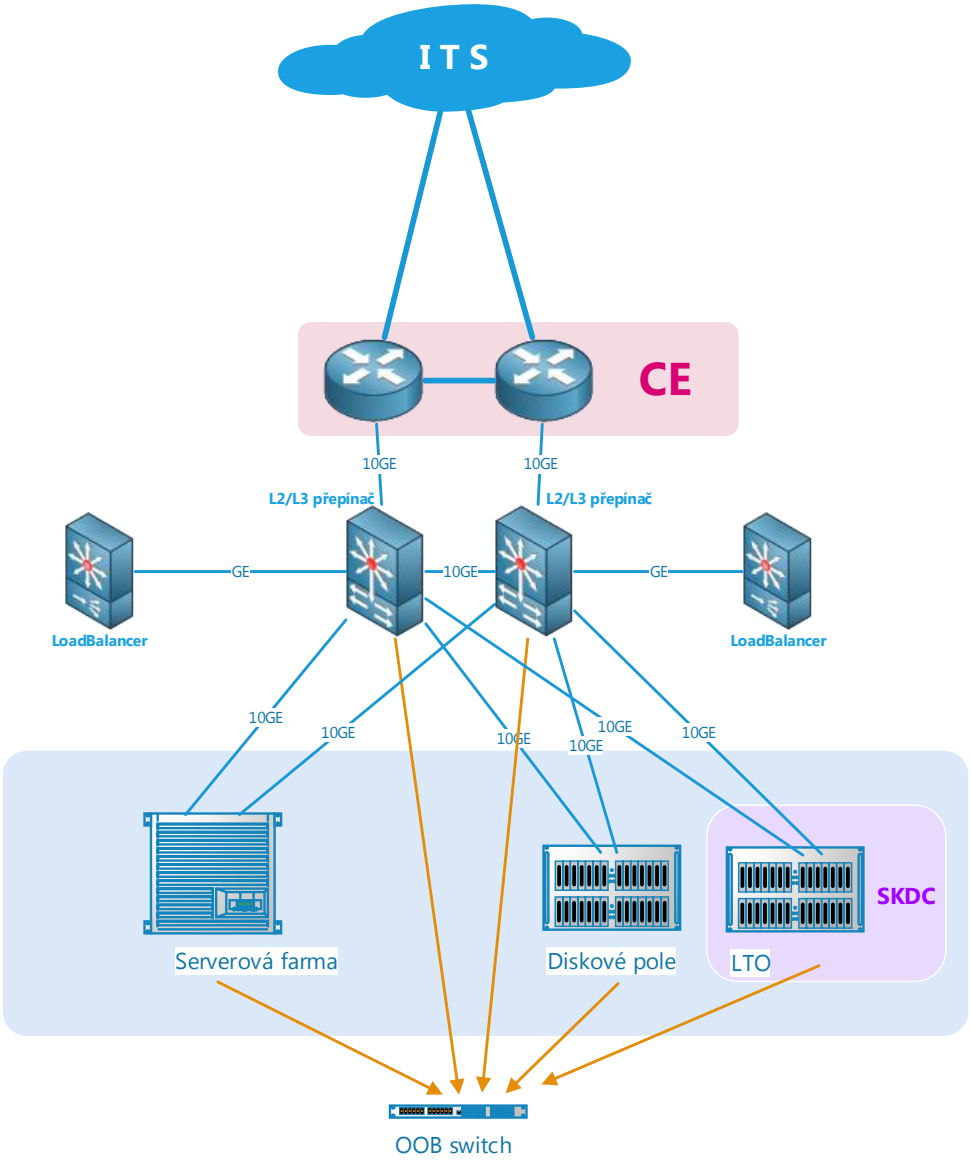
Každé SKDC a KDC bude připojeno 10GE v redundanci v rámci propojení PE a CE vrstvy, jak je vidět na obrázku níže. Na této vrstvě bude 802.1q (VLAN), na kterých budou distribuovány veškerá požadovaná propojení v rámci ITS NGN pomocí dynamických směrovacích protokolů.



Obrázek 1 - Připojení SKDC a KDC k ITS (ITS NGN), fyzická vrstva

3 Zapojení technologií SKDC a KDC

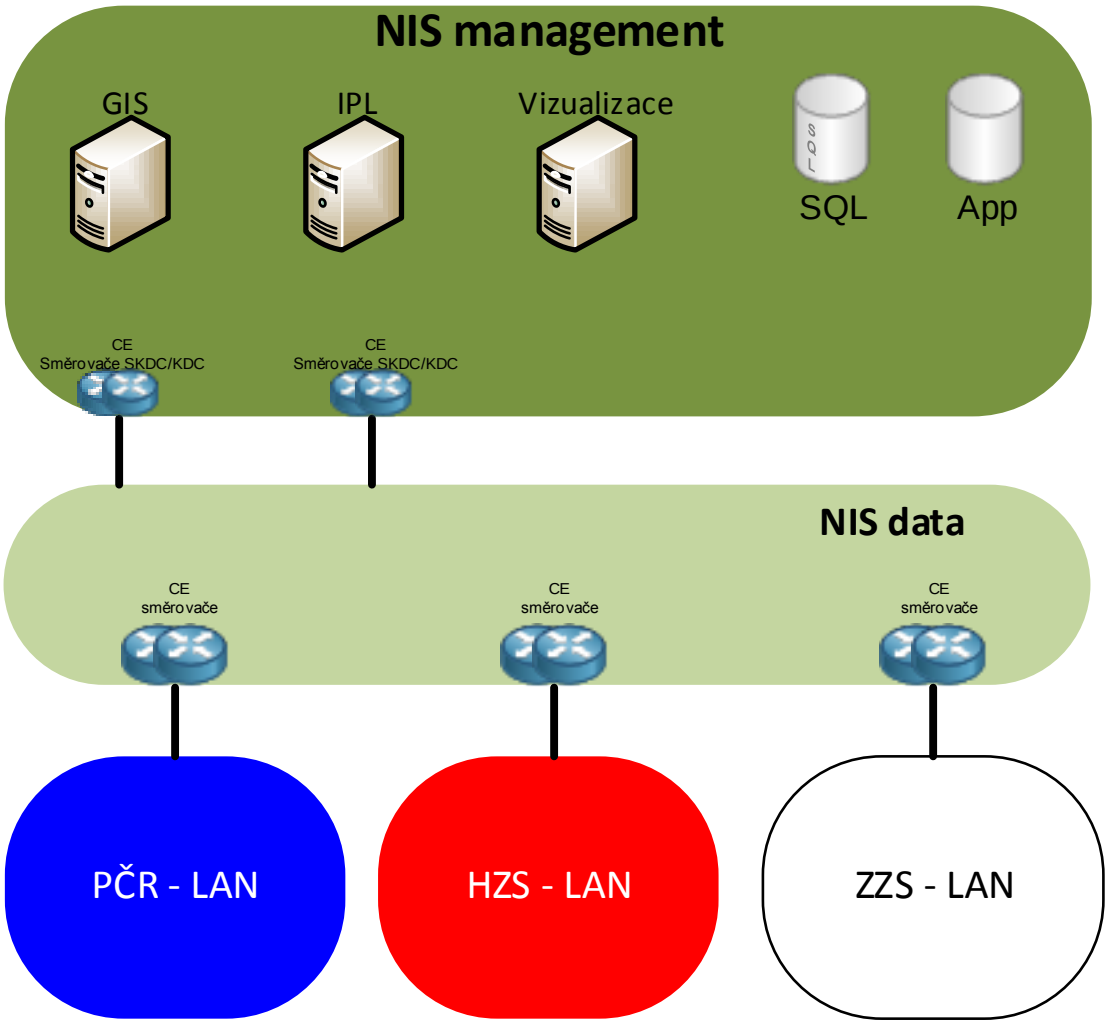
Technologie SKDC a KDC budou připojeny k síti ITS (resp. ITS NGN) dvojicí CE směrovačů, zajišťující dynamické směrování do všech sítí NIS IZS a přístup k externím systémům (systémům OŘ a externím službám realizovaným přes CMS, resp. CMS 2.0). Centrální redundantní L2/L3 přepínače budou obstarávat směrování uvnitř datového centra. Součástí SKDC/KDC bude i dvojice load balancerů, které budou mít na starosti řízení a přístup jednotlivých datových toků ke službám poskytovaným z datových center. Centrální L2/L3 přepínače budou zároveň obsluhovat komunikaci serverové farmy a diskového pole, SKDC bude oproti KDC navíc obsahovat LTO jednotku pro archivaci.



Obrázek 2 Schéma zapojení SKDC/KDC

4 Použití VPN

Dle požadavků jednotlivých složek IZS musí být služby GIS/IPL/Vizualizace dostupné z jejich LAN sítí. Z tohoto důvodu bude zřízena VPN_NIS_data, do které budou vystaveny všechny potřebné služby systému. Do této VPN bude umožněn přístup z jednotlivých LAN složek IZS. Přístup z LAN složek IZS bude řízen tak, aby jednotlivé složky neměly umožněny prostupy do LAN jiných složek. Pro potřeby datových center SKDC a KDC bude zřízena VPN_NIS_management (VPN_NIS_mgmt), která bude sloužit pro vnitřní systémovou komunikaci NIS IZS a nebude do ní umožněn přímý přístup z LAN složek IZS. Pro všechny prostupy mezi VPN platí, že se jedná o řízené prostupy minimálně na úrovni ACL.



Obrázek 3 VPN projektu NIS IZS

Distribuci VPN pro jednotlivé složky bude zajišťovat infrastruktura sítě ITS NGN, kde jednotlivé VPN budou plně odděleny a prostup mezi jednotlivými VPN bude řízen CE směrovači NIS IZS. Z prostředí NIS bude možné přistupovat ke všem GIS serverům a ke všem serverům IPL poskytujícím služby NIS IZS jak v SKDC tak KDC.

Toto vše znamená, že každá LAN složky IZS bude mít síťový přístup ke všem IPL a GIS serverům, ale nebude moci komunikovat s žádnou VPN jiné složky IZS. Veškerá potřebná datová komunikace mezi složkami IZS tak bude zajištěna prostřednictvím služeb IPL.

5 Propojení s externími systémy

Přístup jakýchkoliv systémů OŘ do všech datových VPN NIS IZS bude umožněn pouze přes CE směrovače v jednotlivých SKDC a KDC na základě předem stanovených pravidel přístupu. Přístup ostatních systémů bude umožněn výhradně prostřednictvím služeb vystavených ze strany NIS IZS v CMS (resp. CMS 2.0), kde se o bezpečné propojení stará bezpečnostní politika systému CMS (resp. CMS 2.0).

5.1 Připojení SKDC/KDC k CMS (CMS 2.0)

Systém NIS IZS bude komunikovat s externími systémy jako je JSDI, RÚIAN, ČHMÚ. Tato komunikace bude realizována prostřednictvím VPN NPSTV_CMS, která bude terminována na InterConnect CMS (CMS 2.0), případně budou vytvořeny další propojovací VPN v závislosti na bezpečnostní politice CMS 2.0 (jelikož je projekt v přípravě, tyto politiky není možné předjímat), které budou šířeny k jednotlivým datovým centrům NIS IZS. Na těchto propojeních budou přijímána nejen data z externích systémů, ale zároveň budou sloužit k vystavování služeb NIS IZS do CMS (CMS 2.0).

6 Adresace

Přidělení IP adres jednotlivým regionům (krajům) a VPN podle místa a cíle určení vychází ze zvyklostí IP adresace používané v datových sítích MV a PČR (DSMV). DSMV (datová síť ministerstva vnitra, někdy označovaná jako MPLS síť) je podmnožina ITS MV (Integrovaná telekomunikační síť MV). Rozumí se tím zejména celorepublikově rozprostřená WAN síť určená pro potřeby MV, PČR, HZS a dalších útvarů podřízených Ministerstvu vnitra. Kromě toho DSMV poskytuje zejména transportní služby i pro jiné útvary státní správy a samosprávy.

Pro potřeby adresace projektu NIS IZS byl přidělen blok adres 10.30.0.0/15. IP adresní rozsah pro NIS IZS je zvolen tak, aby byl pro datové sítě MV, PČR, HZS a ZZS nekolizní, takže v případě vzájemného propojení není potřeba provádět překlady adres.

Doporučuje se, aby byly segmenty serverů oddělené na úrovni LAN od segmentů uživatelů. Evidenci IP adres v jednotlivých uživatelských a serverových LAN segmentech vede příslušný lokální administrátor LAN. Evidence LAN a adresních skupin bude vedena centrálně u provozovatele NIS IZS.

Pro datová centra projektu NIS IZS bude využit první blok IP adres 10.30.0.0/16 zbytek zůstává jako rezerva pro další možnosti rozšíření projektu NIS IZS. Rozřazení do jednotlivých C class sítí bude na základě níže uvedené tabulky.

Region	Číslo bloku (B)	Maska
Praha	64	20
Středočeský	128	20
Jihočeský	144	20
Zlínský	152	20
Plzeňský	160	20
Karlovarský	168	20
Ústecký	176	20
Liberecký	184	20
Královéhradecký	192	20
Pardubický	200	20
Jihomoravský	208	20
Vysočina	216	20
Moravskoslezský	224	20
Olomoucký	232	20
CMS	240	20

Tabulka 1 Adresace rozdělení po krajích

Příklad: Pro Ústecký kraj bude přidělen blok 10.30.176.0/20.

Požadavky na adresaci pro SKDC/KDC jsou /24 pro management datové sítě, /23 pro management prvků datového centra a /24 pro publikování služeb do sítí složek IZS. Detailní rozpracování adresního plánu bude součástí implementačního projektu NIS IZS.

7 Specifikace dodávky síťové infrastruktury

7.1 Specifikace síťových komponent

7.1.1 CE směrovač

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (11xKDC, 3x SKDC): 14

7.1.1.1 Závazné parametry

č.	Hardware
1	Formát zařízení - modulární
2	Maximální velikost 2RU
3	Minimálně 2x 10GE s volitelným fyzickým rozhraním
4	Minimálně 2 volné sloty pro rozšíření
5	Neblokující architektura přepínacího/směrovacího subsystému (wire speed)
6	Neblokující architektura přechodu interface - přepínací/směrovací subsystém min. pro všechny poptávané interface současně (platí zejména pro modulární zařízení)
7	Redundantní napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje).
8	Možnost výměny napájecích zdrojů za provozu (hot-swap) bez ovlivnění funkce zařízení jako celku
9	Duální podpora IPv4 a IPv6 (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, tzv. dual stack)
10	Hardwarová podpora L3 přepínání/směrování protokolů IPv4 a IPv6
11	Filtrování TCP a UDP bez negativního vlivu na řádnou funkčnost zařízení
12	Neblokující (wire speed) replikace multicastu v HW
13	Kontrola přípustnosti zdrojové IPv4 a IPv6 adresy na všech (fyzických i logických) L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci RPF check, reverse path forwarding check dle RFC 3704)
14	Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN)
15	Hardwarová podpora dlouhých ethernetových rámců (tzv. jumbo frames) datový obsah rámce (payload) alespoň 9000 B
16	Hardwarová podpora omezení (procentuálního poměru) broadcastového provozu na rozhraní (broadcast storm control)
17	Statické směrování pro IPv4 a IPv6 unicast i multicast
18	Rozkládání zatížení na L3 paralelních cestách (ECMP)
19	OSPF v2 dle RFC 2328
20	OSPF v3 dle RFC 5340
21	Kontrolovaná redistribuce směrovacích informací mezi protokoly
22	Podpora L2 paralelních cest dle IEEE 802.3ad
23	Podpora IEEE 802.3ad přes více karet
24	Podpora detekce jednosměrné komunikace na lince (např. BFD)
25	Možnost omezení počtu naučených MAC adres na rozhraní (obrana proti útokům typu zahlcení vnitřní tabulky MAC adres přepínače/mostu).
26	Podpora výměných DWDM rozhraní (dosah až 80km)
27	Fyzická specifikace
28	Redundatní FAN a PSU
29	Modularní chassis
30	Výkon
31	Non-blocking architektura
32	Distribuovaný „control“ a „forwarding“ plane
33	L2 funkcionality
34	Minimálně 500k MAC na systém
35	Minimálně 128k ARP záznamů na systém
36	Jumbo frames 9000B
37	Podpora IEEE 802.1Q

38	Plný rozsah VLAN (4k)
39	Podpora IEEE 802.1QinQ
40	Inner / Outer VLAN rozsáhlá manipulace
41	podpora LACP
42	Multi Chassis LAG
43	Detekce protilehlého zařízení LLDP (IEEE 802.1AB)
44	Interface spec. funkce
45	per subinterface encapsulation
46	per subinterface Vlan tag type (kombinace single VLAN, QinQ, non-tag (native VLAN))
47	Routed L3 interface, tjkaždý subinterface má subnet
48	Routed VLAN (Bridge) interface
49	L3 capability
50	Minimálně IPv4 3Mil. route v RIB
51	IPv4 HW support
52	RIP, OSPF, ISIS, BGPv4
53	Podpora GRE (Generic Routing Encapsulation)
54	Static routing
55	VRF lite (IPv4/6)
56	Minimálně IPv6 2Mil. route v RIB
57	IPv6 HW support
58	RIPng, OSPFv3, MBGP, ISIS pro IPv6
59	BFD pro BGP, OSFPv2, OSPFv3, ISIS
60	Policy based routing / filter based routing
61	Multicast
62	IGMP snooping v1/2/3
63	IGMP v1/2/3
64	PIM SM/SSM/DM
65	MSDP
66	Podpora IPv6 Multicast (MLDv1 & v2)
67	Podpora IPv6 Multicast (PIM SM)
68	Podpora IPv6 Multicast (PIM SSM)
69	MPLS
70	Hardwarová podpora MPLS
71	LDP / RSVP signalizace
72	RSVP ptmp path
73	RSVP-TE (FRR, Link/node protection)
74	L2VPN
75	VPLS LDP based
76	VPLS BGP based
77	L3VPN (RFC 4364)
78	Mcast in L3VPN – draft Rossen
79	Podpora Label Imposition a Label Disposition (MPLS Provider Edge)
80	Podpora Label Swapping (MPLS Provider Core)
81	Podpora LDP (Label Distribution Protocol)
82	Podpora MPLS TE
83	Podpora P2MP TE
84	Podpora mLDP
85	Podpora IPv6 over MPLS (6PE)
86	Podpora IPv6 VPN over MPLS (6VPE)
87	Bezpečnost
88	Policing / rate limit pro provoz směrem k CPU
89	ACLka na provoz směrem k CPU
90	Podpora IPv6 ACL
91	Podpora reverse path check (uRPF) v hardwaru
92	ACL pro IP

93	Bezstavová Kontrola / řízení provozu L2-L7 (tzv. ACLka)
94	ACLka v HW (TCAM / CAM)
95	Port ACLka (vstup / výstup)
96	VLAN (Bridge) ACLka (vstup / výstup)
97	Routed ACLka (vstup / výstup)
98	Policing pod interface
99	CoS
100	Klasifikace provozu
101	802.1p
102	DSCP
103	IP precedence
104	MPLS exp.
105	Založeno na bezstavovém vyhodnocení paketů v L2-L4
106	Port shaping / Queue shaping
107	Policing
108	Minimálně 8x Queues na port
109	Minimálně 8x forwarding class
110	Minimálně 4 priority per Scheduler
111	Strict priority implementace
112	WRED
113	Rewrite rules – přepsání CoS bitů
114	Podpora IPv6 QoS
115	Vysoká dostupnost
116	Forwarding známých paketů bez asistence „control plane“
117	Management
118	Modularní oprační systém
119	Command-line interface (CLI)
120	Minimálně 10 konfiguračních záloh přímo na zařízení s možností jejich návratu příkazem z CLI
121	Aktivní a „batch“ konfigurace = změny se promítnou do funkce až po potvrzení = časované změny, masivní změny naráz atd
122	Archivace konfigurací do souborů přímo na boxu
123	Archivace konfiguraci na vzdáleném FTP / SCP – i automatická
124	Local přístup do CLI přes konsole port
125	Management zařízení Telnet / SSH
126	FTP, TFTP client a server
127	Podpora NETCONF
128	Syslog
129	Centralizovaná authentikace pro přístup na zařízení Radius/Tacacs+
130	Omezení práv přístupu dle uživatelských rolí
131	Možnost omezení přístupu k managementu (SSH, SNMP)
132	Konfigurační soubory v čitelném formátu (například ASCII, TXT, XML)
133	Možnost nahrání/zálohování konfigurace zařízení po síti pomocí alespoň jednoho z protokolů TFTP, FTP, HTTP, SCP nebo SFTP
134	Možnost povýšení operačního systému zařízení po síti pomocí alespoň jednoho z protokolů TFTP, FTP, HTTP, SCP nebo SFTP
135	Secure Shell (SSHv2)
136	Podpora centrální autorizace příkazů prostřednictvím protokolu TACACS+ nebo RADIUS
137	Out-of-Band Management
138	Tx a Rx optical power monitoring (DOM)
139	Podpora synchronizace času protokolem NTP, minimálně verze 3.
140	Podpora protokolů SNMPv2, SNMPv3 (včetně schopnosti generovat trapy při detekci významných událostí) a syslog.
141	Podpora SNMPv2/v3 MIBs a traps
142	Možnost omezit oprávněné zdrojové IP adresy manažerských stanic pro vzdálený konfigurační přístup
143	Možnost omezit oprávněné zdrojové IP adresy SNMP manažerských stanic
144	Network Management a monitoring
145	Port miroring
146	Real-time-performance monitoring
147	NetFlow v9 IPFIX RFC 3917, 3955 nebo obdobné

148	Ping / traceroute
149	Debug na úrovni protokolů interface a procesů
150	NTP klient
151	DNS klient
152	Podpora interních nástrojů pro debugging procházejícího provozu
153	Podpora interních nástrojů pro on-line měření kvality síťové infrastruktury
154	Výkon
155	Minimální propustnost jednoho šasi 80Gbps
156	Rozšiřující rozhraní
157	Minimálně 2x 10GE s volitelným fyzickým rozhraním
158	Minimálně 20x 1GE SFP s volitelným fyzickým rozhraním
159	Interface moduly (přesnou vlnovou délku a přesný počet modulů zadavatel stanoví v objednávce)
160	Minimálně 1x 10GE Multimode SR optický modul (originál od výrobce)
161	Minimálně 1x 10GE SingleMode LR optický modul (originál od výrobce)
162	Minimálně 1x 10GE SingleMode ER optický modul (originál od výrobce)
163	Minimálně 1x 10GE DWDM SingleMode optický modul C Band Tunable (100-GHz ITU grid)
164	Minimálně 1x 10GBASE-DWDM 15XX.XX nm (100-GHz ITU grid)
165	Minimálně 1x 1GE Multimode SX optický modul (originál od výrobce)
166	Minimálně 1x 1GE Singlemode LX/LH optický modul (originál od výrobce)
167	Minimálně 1x 1GE Metalický modul s koncovkou RJ45(originál od výrobce)
168	Servisní a doplňkové požadavky
169	Záruka a produktová podpora min. 5 let
170	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zahoření
171	Veškeré licence SW potřebné ke specifikovanému řešení
172	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

Tabulka 2 Specifikace CE směrovač pro SKDC/KDC

7.1.2 L2/L3 přepínač

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (11xKDC, 3xSKDC): 14

Tento vysokorychlostní přepínač bude využíván jako centrální komunikační prvek v lokalitách SKDC/KDC a bude zajišťovat datové propojení komponent v rámci datacenter. Do každého SKDC/KDC bude dodávána ve dvou instancích pro zajištění požadované redundance řešení.

7.1.2.1 Závazné parametry

č.	Hardware
1	Neblokující architektura přepínacího subsystému (wire speed)
2	Velikost 1RU
3	Latence pod 2mikro sekundy
4	Propustnost minimálně 1,28 Tbps
5	Přepínací systém minimálně 960 Mpps
6	FCoE na všech portech
7	Minimálně 48 portů 1/10GE/FCoE s volitelným fyzickým rozhraním
8	Minimálně 4 porty 40GE/FCoE s volitelným fyzickým rozhraním
9	Možnost konverze 40GE rozhraní na 4x 10GE rozhraní s podporou FCoE
10	Podpora standardu TRILL nebo ekvivalentní technologie
11	Možnost výměny napájecích zdrojů za provozu (*hot-swap*) bez ovlivnění funkce zařízení jako celku
12	Bezvýpadkový upgrade přepínače (ISSU)

13	Redundantní napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje).
14	Možnost výměny ventilátorů za provozu (*hot-swap*) bez ovlivnění funkce zařízení jako celku (N+1)
15	L2 Funkce
16	Podpora IEEE 802.1Q minimálně 4K VLAN
17	Port Based VLAN
18	Podpora filtrování MAC adres
19	Možnost definování statické MAC adresy na port
20	Podpora statické Link Agregace
21	Podpora protokolu LACP (IEEE 802.3ad)
22	Podpora protokolu LLDP (IEEE 802.1AB)
23	Podpora Jumbo Frame minimálně 9K bytes
24	Podpora protokolu Spanning Tree (IEEE 802.1D)
25	Podpora protokolu Rapid Spanning Tree (IEEE 802.1w)
26	Podpora protokolu Multiple Spanning Tree (IEEE 802.1s)
27	Podpora Spanning Tree BPDU Protect, BPDU Filtering, Loop Protect, Root Protect
28	Uplink Failure Detection
29	Podpora MC-LAG
30	IEEE 802.1
31	IEEE 802.1p
32	IEEE 802.1Qau
33	RFC 951, 1542 BootP
34	L3 Funkce
35	RVI (Routed VLAN Interface)
36	Layer 3 features (IPv4)
37	Static Routing
38	Route mapy
39	Dynamické směrovací protokoly (OSPF, BGP, ISIS)
40	Podpora BFD
41	Podpora VRRP/HSRP nebo podobné
42	VRF-lite (multicast, unicast)
43	DHCP Relay (RFC 3046)
44	Podpora IPv6 v HW - bez impactu
45	RFC 768 UDP
46	RFC 791 IP
47	RFC 792 ICMP
48	RFC 793 TCP
49	RFC 826 ARP
50	RFC 894 IP over Ethernet
51	RFC 1122 Host requirements
52	RFC 1256 IPv4 ICMP Router Discovery (IRDP)
53	RFC 1519 Classless Interdomain Routing (CIDR)
54	RFC 1812 Requirements for IP Version 4 routers
55	ECMP
56	Multicast features

57	IGMP v2/v3 (RFC 3376)
58	Anycast RP
59	PIM-SM
60	Static RP
61	Security and ACL
62	Secure interface login and password
63	Ingress and Egress ACLs: allow and deny, Port ACLs, VLAN ACLs, Routed ACLs
64	Local proxy Address Resolution Protocol (ARP)
65	Static ARP support
66	Storm Control, Port error disable and auto-recovery
67	Control Plane denial-of-service (DoS) protection
68	Port Security
69	Traffic Storm Control
70	Unicast RPF
71	Control Plane Policing
72	Rate Limits
73	Quality of service (QoS)
74	Layer 2 QoS: classification, rewrite, queuing
75	Layer 3 QoS
76	Rate Limiting
77	Ingress policing:1rate2color - Egresspolicer,policermarkdownaction
78	8 hardware queues per port
79	Strict priority queuing (LLQ), DWRR
80	802.1p remarking
81	Layer 2 classification criteria: Interface, MAC address, Ethertype, 802.1p, VLAN,
82	Trust IEEE 802.1p/DSCP (ingress)
83	Remarking of bridged packets
84	Traffic Mirroring
85	Port-based
86	Možnost definovat směr zrcadleného provozu (vstupní/ výstupní)
87	Možnost zrcadlení celého LAG portu
88	VLAN-based
89	SPAN and RSPAN are supported
90	Minimálně 2 instance
91	Data center bridging (DCB)
92	PFC (Priority Flow Control) – IEEE 802.1Qbb
93	ETS (Enhanced Transmission Selection) – IEEE 802.1Qaz
94	DCBX (Data Center Bridging Exchange Protocol
95	IEEE 802.3x - Link-level flow control
96	FC-BB-5
97	Podpora technologie N-Port Identifier Virtualization (NPIV)
98	Management
99	Seriová konzole (RJ45)
100	USB port

101	Podpora správy přepínače přes NETCONF
102	Out-Of-band management
103	Podpora SSHv2
104	Podpora SNMPv2, SNMPv3
105	Podpora odesílání logů na syslog server
106	sFlow nebo NetFlow/IPFIX
107	Omezení práv přístupu dle uživatelských rolí
108	RFC 854 Telnet client and server
109	Podpora synchronizace času z centrálního časového serveru, NTP protokol
110	Možnost správy přepínače přes HTTP/HTTPS (GUI)
111	RFC 1492 TACACS+
112	RFC 2138 RADIUS Authentication
113	RFC 2139 RADIUS Accounting
131	Servisní a doplňkové požadavky
132	Záruka a produktová podpora min. 5 let
133	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zahoření
134	Veškeré licence SW potřebné ke specifikovanému řešení
135	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

Tabulka 3 Specifikace SKDC/KDC - L2/L3 přepínač

7.1.3 LoadBalancer

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (11xKDC, 3xSKDC): 14

LoadBalancer bude zajišťovat potřebné aplikační funkce a požadované rozložení zátěže na zařízení a služby vystavené v rámci datových center. Do každého SKDC/KDC bude dodáván zdvojeně.

7.1.3.1 Závazné parametry

č.	Základní vlastnosti
1	LoadBalancer - HW Appliance
2	Dedikovaný management port
3	Konzolový port pro správu
4	Rozměry maximálně 2RU
5	Redundantní AC napájení
6	Možnost výměny zdroje za chodu (hot swap)
7	Minimálně 4x 1GE rozhraní
8	Možnost nasazení více zařízení (aktivní / záložní)
9	Výkon
10	Propustnost minimálně 1Gbps
11	Počet současných spojení na L4 minimálně 1M
12	Počet nových spojení za vteřinu (CPS) na L7 minimálně 100K
13	Počet nových spojení za vteřinu (CPS) na L4 minimálně 50K
14	SSL offloading propustnost minimálně 500Mbps
15	SSL transakcí za vteřinu (TPS) minimálně 300
16	Síťová podpora
17	IPv6
18	VLAN (802.1Q) minimálně 900

19	Směrovací protokoly - RIP, OSPF, BGP
20	LACP/802.3ad
21	Monitorování stavu serverů (Health monitoring)
22	Monitorování stavu serverů - ICMP
23	Monitorování stavu serverů - TCP
24	Monitorování stavu serverů - UDP
25	Monitorování stavu serverů - SSL Hello
26	Monitorování stavu serverů - HTTP obsah
27	Monitorování stavu serverů - POP3
28	Monitorování stavu serverů - IMAP4
29	Monitorování stavu serverů - SMTP
30	Monitorování stavu serverů - SIP
31	Monitorování stavu serverů - Možnost kombinace metod
32	Monitorování stavu serverů - Možnost definovat interval ověřování
33	Monitorování stavu serverů - Možnost definovat timeout
34	Monitorování stavu serverů - Možnost definovat počet opakování před prohlášením služby za dostupnou
35	Loadbalancing - Na základě L3 - L7 parametrů
36	Loadbalancing - IP hash
37	Loadbalancing - HTTP cookies
38	Loadbalancing - SSL session ID
39	Loadbalancing - Hodnoty obsažené v HTTP hlavičce
40	Loadbalancing - Možnost vkládání cookies pro perzistenci spojení
41	Loadbalancing - Možnost modifikace URL
42	Loadbalancing - Aplikačního provozu na základě vrstev L3 – L7
43	Loadbalancing - Možnost balancingu na základě provozu (v příchozím i odchozím směru)
44	Management
45	Centrální management
46	Možnost definovat uživatele s různým oprávněním
47	Management přes protokol SSH
48	Management přes protokol HTTPS (GUI)
49	Podpora protokolu SNMP
50	Ukládání konfigurace v texovém formátu
51	Podpora Syslog
52	Podpora protokolu NTP pro synchronizaci času
53	Servisní a doplňkové požadavky
54	Záruka a produktová podpora min. 5 let
55	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zahoření
56	Veškeré licence SW potřebné ke specifikovanámu řešení
57	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

Tabulka 4 Specifikace Load Balancer

7.1.4 OOBM přepínač

Počet instancí v rámci 1 lokality: 2

Počet lokalit celkem (11xKDC, 3xSKDC): 14

Tento přepínač bude sloužit k vytvoření oddělené Out-Of-Band management sítě pro správu infrastruktury umístěné v rámci datových center.

7.1.4.1 Závazné parametry

č.	Základní vlastnosti
1	Třída zařízení přepínač
2	Formát zařízení pro instalaci do Racku maximální velikost 1RU

3	Možnost rozšíření o redundantní zdroj
4	Možnost stohování
5	Minimální počet zařízení ve stohu 8
6	Minimální kapacita sběrnice stohu 80Gbps
7	Dostupná provedení – minimálně následující varianty
8	24 portů 10/100/1000, 4 porty GE (SFP)
9	Výkonnostní parametry
10	Propustnost přepínacího subsystému minimálně 56Gbps
11	Protokoly fyzické vrstvy
12	Podpora standardu IEEE 802.3ad
13	Minimálně 24 konfigurovatelných portchannel skupin
14	Podpora IEEE 802.3ad přes více přepínačů ve stohu
15	Podpora "jumbo rámců"
16	Protokoly 2. vrstvy
17	IEEE 802.1D
18	IEEE 802.1Q
19	Podpora Private VLAN nebo ekvivalentní
20	Minimální 1000 aktivních VLAN
21	IEEE 802.1x
22	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)
23	Podpora integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)
24	IEEE 802.1s - multiple spanning trees
25	IEEE 802.1w - Rapid Tree Spanning Protocol
26	Detekce protilehlého zařízení (např. CDP nebo LLDP)
27	Protokol pro definici šířených VLAN (např. GVRP nebo ekvivalentní)
28	Detekce jednosměrnosti optické linky (např. OAM link fault management nebo ekvivalentní)
29	STP root guard nebo ekvivalentní
30	STP loop guard nebo ekvivalentní
31	Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)
32	Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech
33	Protokol IP
34	Podpora IGMP snooping
35	Podpora IPv6 MLD snooping
36	Podpora IPv6 port ACL
37	Podpora IPv6 QoS
38	Podpora IPv6 RA guard
39	Podpora IPv6 source guard
40	Popdora DHCPv6 snooping
41	Podpora IPv6 ND inspection
42	QoS
43	Podpora QoS classification – ACL, DSCP, CoS based
44	Podpora QoS marking - DSCP, CoS
45	Podpora QoS Policing
46	Podpora QoS - Strict Priority Queue pro ukládání paketů IP telefonního provozu
47	Podpora rate limiting
48	Bezpečnost
49	ACL na rozhraní IN/OUT (včetně virtuálních - VLAN)
50	Možnost definovat povolené MAC adresy na portu
51	Možnost definovat maximální počet MAC adres na portu
52	Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)
53	Podpora bezpečnostních fun kcí umožňujících ochranu proti podvržení zdrojové IP adresy – IP source guard nebo ekvivalentní
54	Podpora bezpečnostních funkcí umožňujících ochranu proti připojení neautorizovaného DHCP serveru – DHCP snooping nebo ekvivalentní
55	Podpora bezpečnostních funkcí umožňujících inspekci provozu protokolu ARP – ARP inspection enbo ekvivalentní
56	Podpora koncových zařízení

57	Podpora IEEE 802.3az
58	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a automatické nastavení vhodných QoS parametrů daného portu
59	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a jeho automatické přiřazení do dedikované voice VLAN
60	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
61	Management
62	CLI rozhraní
63	SSHv2
64	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
65	SNMPv2
66	SNMPv3
67	DNS klient
68	NTP klient s MD5 autentizací
69	RADIUS klient pro AAA (autentizace, autorizace, accounting)
70	TACACS+ klient
71	Port mirroring (SPAN)
72	Vzdálený port mirroring (RSPAN)
73	Syslog
74	Podpora interních nástrojů pro debugging procházejícího provozu
75	Monitorování aplikačních toků
76	Podpora monitorování aplikačních toků s využitím Sampled NetFlow nebo sFlow
77	Podpora monitorování aplikačních toků na fyzických i VLAN rozhraních
78	Možnost nastavení vzorkovací rychlosti
83	Servisní a doplňkové požadavky
84	Záruka a produktová podpora min. 5 let
85	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zahoření
86	Veškeré licence SW potřebné ke specifikovanámu řešení
87	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

Tabulka 5 Specifikace OOBM přepínač

8 Seznam obrázků

9 Seznam tabulek