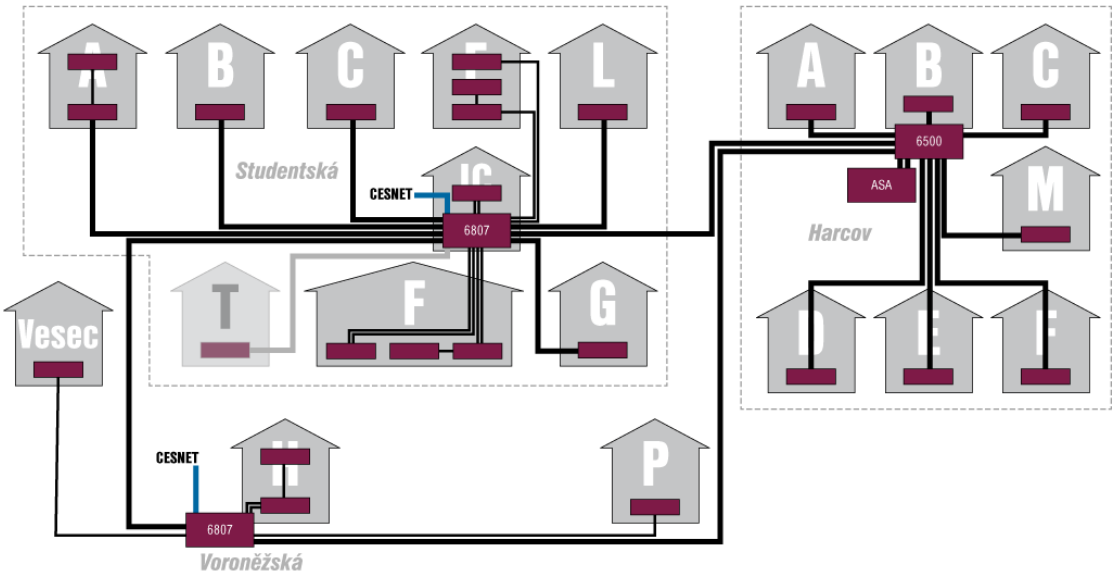
SÍŤ LIANE TUL

Popis prostředí počítačové sítě LIANE na TUL.

Počítačová síť TUL pokrývá až na naprosté výjimky veškeré pracovny a kanceláře ve všech budovách univerzity. Je postavena především na kombinaci sto/čtyřiceti/desetigigabitového (páteř) a gigabitového (koncové stanice) Ethernetu a bezdrátové sítě Wi-Fi, jiné technologie jsou dnes v síti TUL nasazeny jen výjimečně. Prakticky všechny počítače na univerzitě jsou zapojeny do sítě, rychlost jejich připojení je nejčastěji 1 Gb/s nebo 100 Mb/s v závislosti na schopnostech koncového zařízení. Průběžně je rozšiřována bezdrátová infrastruktura standardu IEEE 802.11a/b/g/n/ac/ax napojená na autentizační infrastrukturu *eduroam*, jež umožňuje roaming našich uživatelů v sítích ostatních připojených institucí. Pokrytí bezdrátové sítě v současné době zahrnuje přibližně 700 přístupových bodů (AP).

Síť TUL je zapojena do Internetu rychlostí 100 Gb/s prostřednictvím národní akademické sítě CESNET2, jejíž páteřní uzel se nachází přímo v prostorách TUL. K jádru sítě je připojen zálohovaně, stogigabitovým a čtyřicetigigovým kanálem vedenými DWDM trasami do Prahy, Hradce Králové a Ústí nad Labem. Klíčové páteřní trasy univerzitní sítě pracují rychlostí 100/40 Gb/s a jsou vedeny redundantně, aby případný výpadek některé z nich neodřízl významnou část univerzity od Internetu.

Síť pokrývá i areál studentských kolejí Harcov, který je k páteři připojen dvěma nezávislými spoji o rychlosti 100 Gb/s. Tato hlavní ubytovací kapacita TUL je kompletně pokryta gigabitovým Ethernetem, k němuž je zde celkem připojeno více než 3000 studentských počítačů. Interní rozvody jsou realizovány gigabitovým Ethernetem, autentizace uživatelů probíhá protokolem IEEE 802.1x. Síť je zavedena i do menších kolejí a ubytoven TUL (Vesec, Hanychov), které jsou připojeny optickými trasami s kapacitou 10Gb/s.



Síťové prvky

Páteř sítě tvoří tři L3 přepínače Cisco Catalyst 9500. Tyto přepínače jsou osazeny 100GE, 40 GE, 25GE a 10GE SFP kartami. V každé budově je nejméně jeden agregační přepínač Cisco Catalyst 9300, 9300X, 3750, 3560 nebo 3560X. K agregačnímu přepínači jsou připojeny 48portové přepínače Catalyst 2960G, 2960S, 2960X nebo 9200L. Přepínače 2960S, 2960X a 9200L jsou až na výjimky vzájemně propojeny pomocí stohovacího modulu. Jako firewall jsou použity Cisco ASA 5585X, Cisco ASA 5550, Cisco ASA 5516-X
a iptables/nftables na GNU/Linux. Pro vzdálený přístup pomocí VPN je použit koncentrátor Cisco FPR-1140.

Wifi síť je tvořena dvěma kontrolery Cisco Catalyst 9800 a přístupovými body, přímo řízenými těmito kontrolery.

Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě LIANE na TUL.

V akademické síti LIANE na TUL jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování síření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Ochrana spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).
- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4/MP-BGP, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.
- Podpora IGMPv2, IGMPv3, MLDv2, MLDv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).
- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).

- 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).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).
- Podpora 802.1x včetně používaného módu multi-auth (autentizace více hostů na jednom portu)
- Pro vzdálený přístup je využíváno programové vybavení AnyConnect Secure Mobility Client

Nástroje používané pro správu sítě TUL.

Pro správu sítě TUL jsou používány následující nástroje síťového managementu, s nimiž musí být poptávaná zařízení kompatibilní.

Správa konfigurací

Zálohování konfigurací všech aktivních komunikačních prvků je prováděno centrálně automaticky pomocí programu Cisco Prime Infrastructure v aktuální verzi 3.10[4]. Navíc jsou konfigurace paralelně zálohovány (včetně přehledu sumárních změn) pomocí systému RANCID[1] s webovou nadstavbou ViewVC[2]. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Inventarizace síťových zařízení

Pro inventarizaci veškerých síťových zařízení (typicky aktivních komunikačních prvků a koncových zařízení jako jsou uživatelská PC, notebooky, servery a síťové tiskárny) se využívají dva druhy nástrojů:

- registrační systém genboot[1] pro registraci DNS/DHCP
- on-line Netdisco[2] které na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP, LLDP poskytují informace o zařízeních připojených do sítě (např. počty, typy a verze OS aktivních prvků, informace o topologii sítě, VLAN, IP podsítích, bezdrátových SSID, mapování MAC adres na IP adresy, připojení MAC/IP adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd. s možností pokročilého vyhledávání (např. nalezení fyzického připojení zařízení s danou IP/MAC adresou, nalezení duplicitních MAC/IP adres apod.), včetně uchovávání stavové historie.

[1] Vlastní systém vyvinutý na TUL
[2] https://metacpan.org/pod/App::Netdisco

Pro autorizaci, autentizaci a accounting uživatelů v ubytovacích zařízeních a ve WiFi sítích používáme protokol radius a software Radiator[3].
Pro konfiguraci/správu/monitoring a inventarizaci aktivních prvků včetně WiFi využíváme software Cisco Prime Infrastructure v aktuální verzi 3.10[4]

Monitorování provozu.

Provozní trendy

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Icinga[5], který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozorňování případně eskalace e-mailem/SMS při detekci problémové/chybové situace.
Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků používáme systém G3[6] který je sleduje pomocí protokolu SNMP (typicky zatížení CPU, obsazení operační paměti, stav napájecích zdrojů, teplota, počet BGP prefixů a stavové informace jednotlivých portů/rozhraní jako počet přenesených bytů/rámců/paketů, chybovost portů/rozhraní atd.)
Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, přepínačů a firewallů (s rozšířením Network Security Event Logs /NSEL/) se zpracovávají nevzorkované/vzorkované pomocí software FTAS[7].
Pro monitorování historie latence/jitteru/ztrátovosti se používá aktivní nástroj Smokeping[8].
Pro monitorování problémových provozních stavů se používá standardní mechanismus zpracování nevyžádaných deníkových zpráv generovaných aktivními prvky na bázi protokolu Syslog a SNMP trap.

Bezpečnostní monitorování

Pro monitorování síťové bezpečnosti jsou využívány standardní nástroje Syslog a SNMP trapy.
Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsítí/IP adres. Management rozhraní L2 přepínačů je umístěno ve vyhrazené IP podsíti chráněné firewallem. Pro L3 přepínače/směrovače je konfigurována ochrana Control Plane Policing/CoPP, pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serveru.

[3] https://www.open.com.au/radiator/
[4] https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html
[5] https://www.icinga.org/
[6] https://www.cesnet.cz/sluzby/sledovani-provozu-site/sledovani-infrastruktury/
[7] https://www.cesnet.cz/sluzby/sledovani-provozu-site/sledovani-ip-provozu/
[8] https://oss.oetiker.ch/smokeping/