VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

FYZICKÁ BEZPEČNOST A MANAGEMENT SÍTĚ NA FYZICKÉ VRSTVĚ

PHYSICAL SECURITY AND NETWORK MANAGEMENT ON PHYSICAL LAYER

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Ondřej Rozsypal

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Jan Hajný, Ph.D.

SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Ondřej Rozsypal ***ID:*** 163899

Ročník: 2 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Fyzická bezpečnost a management sítě na fyzické vrstvě

POKYNY PRO VYPRACOVÁNÍ:

Téma je zaměřeno na oblast fyzické bezpečnosti počítačových sítí. Úkolem je prostudovat systémy managementu sítě na fyzické vrstvě a jejich spolehlivost v detekci přepojení síťových zařízení a funkčnost v extrémních podmínkách. Výstupem bude zprovoznění systému monitoringu kabeláže, testování v reálném zapojení IP sítě, ohodnocení slabin systému a určení parametrů sítě (vlastnosti vedení, zásuvek, síťových prvků, atd.), které mohou vést k chybám v systému. Součástí zadání je požadavek na návrh opatření, jak zabránit případnému zneužití slabin předloženého systému monitoringu fyzické vrstvy. Výstupem práce je laboratorní úloha demonstrující slabiny systému a možná nápravná opatření.

DOPORUČENÁ LITERATURA:

[1] DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. 2. aktualiz. vyd. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

[2] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

Termín zadání: 5. 2. 2018 ***Termín odevzdání:*** 21. 5. 2018

Vedoucí práce: doc. Ing. Jan Hajný, Ph.D.
Konzultant: doc. Ing. František Urban, CSc., Network Group

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

Abstrakt

Tato diplomová práce se zabývá problematikou fyzické bezpečnosti, zvláště managementu sítě na fyzické vrstvě referenčního modelu ISO/OSI. První část této práce je zaměřena na motivaci pro zavedení inteligentního řešení. Druhá část vysvětluje základní principy a prvky použité v systémech managementu fyzické vrstvy. Další část se zaměřuje na konkrétní řešení systému pro management fyzické vrstvy od společnosti Molex. V posledních částech této práce jsou popsány zjištěné slabiny systému a provedeno srovnání daného řešení oproti jeho konkurentům. Příloha k této práci zahrnuje vytvořenou laboratorní úlohu.

Klíčová slova

bezpečnost, fyzická vrstva, management, AIM, Molex, MIIM

Abstract

This master's thesis is focused on physical security, mainly the network management of the ISO/OSI physical layer. First part deals with the motivation of introducing inteligent solutions. The second part explains the basic principles used in the physical layer management. The third section is focused on particular solutions available by the Molex company. The last parts of this thesis describe identified weaknesses and a comparison of such solution and other solutions provided by competition. The appendix of this thesis involves a created laboratory exercise.

Keywords

security, physical layer, management, AIM, Molex, MIIM

Bibliografická citace:

ROZSYPAL, O. Fyzická bezpečnost a management sítě na fyzické vrstvě. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 70 s. Vedoucí diplomové práce doc. Ing. Jan Hajný, Ph.D.

Prohlášení

Prohlašuji, že svou závěrečnou práci na téma „Fyzická bezpečnost a management sítě na fyzické vrstvě“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.
Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne 21. května 2018 ……

podpis autora

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technicka 12, CZ-61600 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizovaný v laboratořích podpořených projektem Centrum senzorických, informačních a komunikačních systémů (SIX); registrační číslo CZ.1.05/2.1.00/03.0072, operačního programu Výzkum a vývoj pro inovace.

Poděkování

Děkuji vedoucímu diplomové práce doc. Ing. Janu Hajnému za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce.
Zároveň bych také rád poděkoval panu doc. Ing. Františku Urbanovi, CSc. a společnosti NETWORK GROUP, s.r.o. za poskytnuté zázemí a umožnění tuto práci vypracovat.

V Brně dne 21. května 2018 .....

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

1 ÚVOD

S postupem času význam informačních technologií a jejich využití ve všech oblastech společnosti stále více narůstá. Dnes už pomalu těžko najdeme odvětví podnikání, kterých se tyto technologie při nejmenším nedotkly. Zároveň s touto skutečností však roste nebezpečí možného narušení bezpečnosti či neoprávněného přístupu do infrastruktury podniku, například za cílem získání důležitých informací. Z těchto důvodu se stále více podniků zaměřuje na ochranu a pokročilý management své síťové infrastruktury.

Datové sítě se stávají složitějšími. Jelikož stále více služeb migruje na IP technologie, tak je důležité zajistit neustálou provozuschopnost a dostupnost těchto služeb. Rozmanitost a množství zařízení s podporou protokolu IP mohou velmi komplikovat rozhodování, návrh sítě, realizaci projektu a sledování aktiv.

Základním kamenem každého dnešního podniku je IT síť, která funguje spolehlivě, efektivně a umožňuje poskytovat důležité informace pro rozhodování při řešení případného problému. S dnešními provozními rozpočty musí provozovatelé sítí a IT týmy pracovat s méně zdroji a zároveň zajistit dostupnost síťových služeb a případné problémy řešit daleko rychleji.

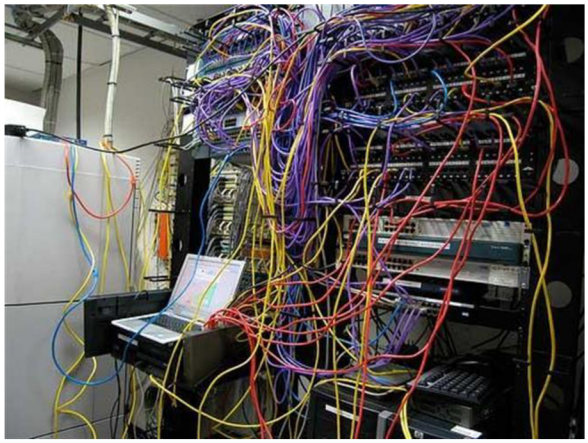
Tím, že převezmeme kontrolu nad nejrozsáhlejším IT aktivem – infrastrukturou fyzické vrstvy – můžeme zjistit více informací o stavu sítě a připojených zařízeních, řešit problémy rychleji a zajistit organizaci robustnější a bezpečnější síť než kdykoliv předtím.

V dnešním zaneprázdněném korporátním prostředí závisí úspěch podnikání na schopností IT oddělení zajistit spolehlivou konektivitu kritických síťových prvků pro své uživatele. Z pohledu financí se každoročně vynakládají obrovské prostředky na nástroje, které IT manažerovi umožňují sledovat stav sítě, spravovat síťové prvky, plánovat a realizovat různé úlohy (work orders) a řešit problémy (trouble-shoot). Jen málo z těchto nástrojů se však ve skutečnosti zabývá problematikou fyzického rozložení – síť, která se rozšiřuje od přepínače v datovém centru nebo telekomunikační místnosti, přes horizontální vedení až do datové zásuvky v pracovní oblasti. Typicky se nástroje zabývají pouze malou části fyzické vrstvy, jako jsou například seznamy záznamů o aktivech nebo seznamy úloh (work orders), ale obecně však jejich integrace s běžně užívanými nástroji pro správu sítě je nedostatečná. Tato situace zanechává v IT oddělení starosti s tím, že musí pracovat se samostatnými systémy, které dohromady však poskytují špatný celkový pohled na stav fyzické topologie.

V této diplomové práci se budeme zabývat i konkrétním řešením, které zmíněné nedostatky snaží minimalizovat a poskytnout nejen lepší centralizaci pro monitoring fyzické vrstvy, ale i lepší prezentaci stavu síťové topologie.

2 MOTIVACE PRO ZAVEDENÍ INTELIGENTNÍHO MANAGEMENTU

Připojení v rozsáhlých firemních sítích nebo datacentrech se stávají s postupným růstem příliš komplikované a počet rozmístěných propojovacích panelů může růst až do stovek, přičemž počet portů může být až několik tisíc. Samozřejmě s tím roste i změť propojovacích kabelů. Na obr. 2.1 a obr. 2.2 můžeme vidět dva přístupy k organizaci kabeláže.

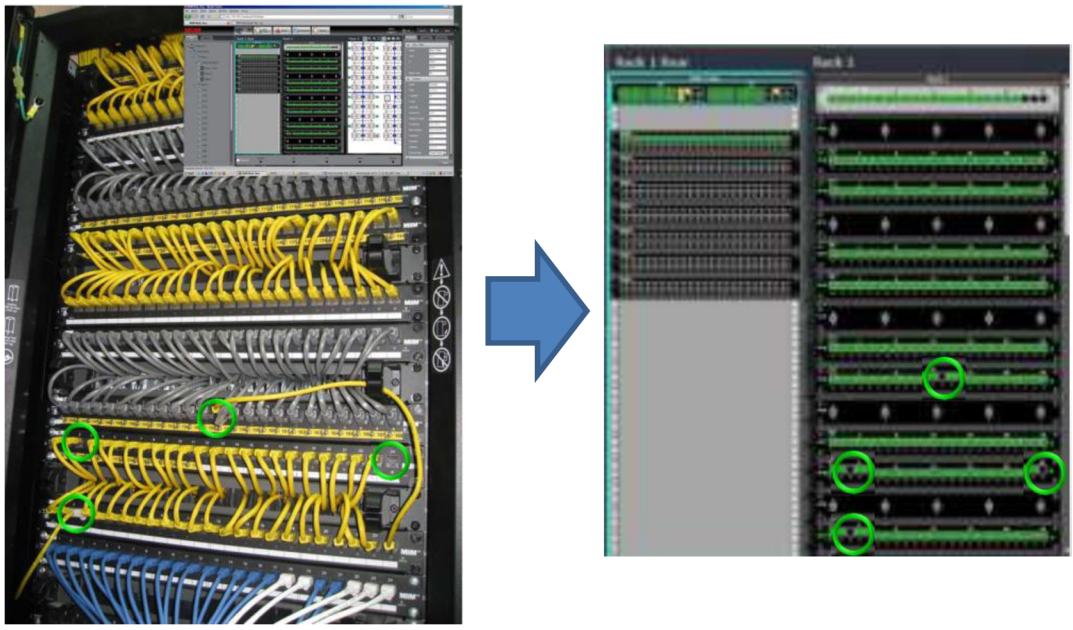


Obr. 2.1 Příklad zanedbané správy kabeláže [1]

Obr. 2.2 Příklad řádně vedené správy kabeláže [1]

Kabeláž na obr. 2.1 je hůře kontrolovatelná, nekonzistentní, neflexibilní a se špatnou viditelností. To vše vede ke ztrátě času, degradaci investic, zvýšení stresu a malé účinnosti. Avšak i v řádně vedené organizaci kabeláže ve druhém vyobrazeném

případě (obr. 2.2) může být také ve vetší síťové infrastruktuře problematické se orientovat nebo vykonávat úlohy (nalezení volných portů, přidání, odebrání propojení nebo změna propojení). Situaci může ulehčit implementace systému managementu fyzické vrstvy, který nám poskytne lepší pohled na volné porty. Na obr. 2.3 můžeme vidět příklad zobrazení volných portů propojovací zóny v systému MIIM určený pro management sítě na fyzické vrstvě od společnosti Molex. Na základě získaných informací ze systému jsme tak schopni vykonat plánovanou změnu v propojovací zóně bez žádných prostojů.



Obr. 2.3 Volné porty při reálnem pohledu a v systému pro management [1]

2.1 Vedení dokumentace

S postupným růstem datové sítě se stává složitější i práce s dokumentací. Například práce s dokumentací všech propojovacích panelů, portů a připojení v Excelu (viz obr. 2.4) je při větší síti administrativně neefektivní a často vede k chybám lidského faktoru:

- Zvolení nesprávné dokumentace,
- zapomenutí aktualizace dokumentace při změně,
- použití nesprávné verze dokumentace,
- informační zpoždění.

Company Logo Here

Standard Port
Special Port
Unused Port

<COMPANY> - CABLE MAPPING

Type (L1/L2)	Source		Patch Panel		Destination		Notes #1	Notes #2
	Device Hostname	Port/NIC	Fabic	Port	Device Hostname	Port/NIC		
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/1			HQ-EDGE-FW-pri	Gi0/2	Internet Edge Firewall	
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/2			HQ-MPLS-RTR	Gi0/1	WAN Router:Po1	in Po12
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/3						
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/4						
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/5			HQ-VOIP-RTR	Gi0/1	Voice Gateway	
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/6						
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/7						
RJ45/Ethernet	HQ-CORE-SW-A	Gi1/8						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/1						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/2			HQ-MPLS-RTR	Gi0/2	WAN Router:Po1	in Po12
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/3						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/4						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/5						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/6						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/7						
RJ45/Ethernet	HQ-CORE-SW-A	Gi2/8						
LC (MM)/Ethernet	HQ-CORE-SW-A	Te3/1			HQ-ACCESS-STACK01	Te1/1/1	Access Switch:Po1	in Po31
LC (MM)/Ethernet	HQ-CORE-SW-A	Te3/2						
LC (MM)/Ethernet	HQ-CORE-SW-A	Te3/3						
LC (MM)/Ethernet	HQ-CORE-SW-A	Te3/4						
LC (MM)/Ethernet	HQ-CORE-SW-A	Te4/1			HQ-ACCESS-STACK01	Te3/1/1	Access Switch:Po1	in Po31
LC (MM)/Ethernet	HQ-CORE-SW-A	Te4/2						
LC (MM)/Ethernet	HQ-CORE-SW-A	Te4/3						
LC (MM)/Ethernet	HQ-CORE-SW-A	Te4/4						
SFP+ (Twinax)/Ethernet	HQ-CORE-SW-A	Te5/1			HQ-CORE-SW-B	Te5/1	B-Side Core Switch:Po1	in Po1
SFP+ (Twinax)/Ethernet	HQ-CORE-SW-A	Te5/2						
SFP+ (Twinax)/Ethernet	HQ-CORE-SW-A	Te6/1			HQ-CORE-SW-B	Te6/1	B-Side Core Switch:Po1	in Po1
SFP+ (Twinax)/Ethernet	HQ-CORE-SW-A	Te6/2						

Obr. 2.4 Příklad dokumentace propojovací zóny v Excelu

Pro IT správce existuje řada možností, jak změnit jednorázově manuální proces, který je náchylný k chybám, do jednoho uceleného a inteligentně spravovaného řešení. U spousty výrobců se setkáme s řešením s různými označeními (DCIM, AIM, IIMS, IPLMS). Ve všech případech se však převážně jedná o tu samou činnost a mají za úkol dosažení stejného cíle: zobrazení sítě v reálnem čase pro rychlé upozornění na incidenty (neautorizované přepojení a přesuny HW), přehled o nevyužívaných zařízeních, fyzická lokace zařízení, automatizaci tvorby dokumentace a rutinních úkolů, zobrazení dostupných portů a dalších informací a statistik.

Při implementaci pokročilého inteligentního řešení získávají správci IT daleko více informací. Pracovní úlohy jsou doručovány v reálnem čase s přesnými informacemi, takže běžné úlohy a problémy jsou řešeny tehdy, kdy je to zapotřebí. Rovněž odpadají potíže s udržováním dokumentace například v tabulkovém procesoru, kde po každém úkolu musí být činnost manuálně aktualizována v dokumentaci. To vše vede ke zvýšení efektivity IT oddělení, časovým úsporám, nižším mzdovým a provozním nákladům [2].

2.2 Užívané akronymy pro správu síťové infrastruktury

Spousta řešení pracuje na stejném principu, avšak výrobci pro tyto systémy používají vlastní označení. Zde jsou uvedené nejčastější akronymy, které různí

výrobci používají pro správu systémů síťové infrastruktury a jejich stručná charakteristika [3]:

- **DCIM** (správa infrastruktury datových center). Řešení DCIM se mohou pohybovat od softwarových řešení až po kompletní řešení hardwaru, softwaru a senzorů.
- **IPLMS** (inteligentní řešení managementu fyzické vrstvy). Tento termín odkazuje na kombinování inteligentních propojovacích panelů se softwarovými funkcemi pro poskytování informací o stavu připojení na portech. Typicky je termín spojen s řešením konkrétního dodavatele datových center.
- **IIMS** (inteligentní řešení správy infrastruktury). Tento termín se týká správy všech složek moderního IT prostředí. Typicky je spojen s řešením konkrétního dodavatele datových center.
- **AIM** (automatizovaná správa infrastruktury). Toto řešení zahrnuje jak hardware, který automaticky detekuje vložení nebo odstranění propojovacích kabelů prostřednictvím například inteligentních propojovací panelů, tak i software, který shromažďuje, ukládá a sděluje tyto informace. Tento termín bude blíže popsán v další kapitole.

2.3 Bezpečnost organizace

Organizace investují každoročně spoustu financí do bezpečnostních technologií, jako jsou biometrika, čipové karty, systémy detekce narušení (IDS), firewally a antivirový software. Při zaměření na zabezpečení k prevenci útoku zvenčí se často přehlíží stejně destruktivní hrozby zevnitř společnosti prostřednictvím fyzické vrstvy. Fyzická vrstva zahrnuje všechny komponenty sítě včetně počítačů, přepínačů, IP telefonů, serverů, kabelů, propojovacích panelů, koncové datové zásuvky, periférie a zařízení pro řízení přístupu. Nedostatek zabezpečení na fyzické vrstvě vystavuje organizace interním útokům, odtajnění citlivých informací a zneužití zařízení.

Častá praxe ukazuje, že mnoho bezpečnostních narušení pochází zevnitř organizace. Například technický pracovník nebo zaměstnanec organizace přistoupí neoprávněně do telekomunikační místnosti, manipuluje s kabely nebo sabotuje síť. Vetřelec nainstaluje bezdrátový hotspot do zranitelného místa budovy a později získává citlivá data. Hrozeb pro organizace na fyzické vrstvě existuje opravdu hodně. V této práci se zaměříme právě na monitoring prvně uvedeného příkladu hrozby [4].

2.4 Procesy MACs

Přesuny, přidávání a změny, známé pod zkratkou MACs, je sada úkolů, které IT týmy pravidelně provádějí, aby udržovaly výpočetní techniku v souladu s požadavky uživatelů, například:

- Změny v sítí (např. přepojení),
- nastavení nového účtu,
- inovace HW a SW,
- výměna zařízení,
- změny uživatelského účtu/přístupu.

Systém MACs může odkazovat na malou změnu, například na upgrade jednoho síťového přepínače nebo na rozsáhlý upgrade, jako jsou například odstavení serverů v jednom místě, a opětovné uvedení do provozu a konfigurace těchto serverů na jiném místě. IT architekti by měli navrhnout systémy pro snadné přizpůsobení MACs procesů. MAC je běžně používaný termín v telefonním managementu, stejně jako ve správě sítí, kde dochází k častým změnám.

Mnoho podniků standardizuje sadu úkolů MACs a poskytuje zaměstnancům pokyny, jak o ně žádat a zdokumentovat je. Dokumentace by měla být dostatečně kompletní, aby jiný technik mohl snadno provést přesun, přidání nebo změnu. V některých organizacích může být MACs součástí větší iniciativy správy IT aktiv. Systémy, kterým se tato diplomová práce věnuje, provádí tuto optimalizaci procesů MACs na fyzické vrstvě. Pokud bychom na fyzické vrstvě prováděli management manuálně bez optimalizovaného MACs, mohou nastat tyto nevýhody:

- Nutnost fyzického potvrzení dostupnosti portu,
- nutnost fyzického potvrzení plnění úlohy,
- nelze sledovat neautorizované procesy MACs,
- vzdáleně nelze vyřešit problémy s připojením,
- vyžaduje práci s náročnou údržbou databáze,
- informace o řízení jsou neúplné nebo nepřesné.

Při správě životního cyklu aktiv IT může být MACs také označováno jako IMACs (instalace, přesunu, přidávání a změny) nebo IMACDs (instalace, přesuny, přidávání, změny a odstranění) [5].

2.5 Automated Infrastructure Management

Systém AIM automatizuje proces zjišťování a dokumentaci infrastruktury síťové kabeláže v datacentrech či podnikových sítí. Nasazením AIM řešení mohou síťový administrátoři zefektivnit poskytování a monitorování síťové konektivity, získat přesný přehled toho, co je v síti připojeno, snížit prostoje včasným oznámením neplánovaných změn a vytvořit aktuální reporty o stavu infrastruktury.

Systémy automatizované správy infrastruktury (AIM) jsou inteligentním přístupem k řízení fyzické vrstvy, které poskytuje síťovým administrátorům bezkonkurenční kontrolu nad jejich sítěmi. Systém AIM může zkrátit dobu potřebnou k nasazení nových aktiv, což zase šetří provozní náklady. Úspory nákladů na životnost infrastruktury mohou převážit počáteční investice do systému AIM.

Systém AIM se skládá z inteligentních hardwarových a softwarových komponent, které jsou navrženy tak, aby detekovaly vložení a odstranění propojovacích kabelů. Software shromažďuje a ukládá výsledné informace o připojení, vztahující se ke konektivitě kabeláže, a o připojení kabeláže z informací z jiných zdrojů (tj. systémy vyšších vrstev) prostřednictvím aplikačních programových rozhraní (API). Systémy AIM mohou také zajistit schopnost objevit síťová zařízení a určit jejich fyzickou polohu.

S využitím AIM systému správce sítě přesně ví, na jakém místě je požadované zařízení připojené. Má v reálném čase přehled o fyzické konektivitě sítě a schopnost generovat výstrahy při neplánovaném připojení nebo odpojení. Systém také poskytuje systém řízení pracovních úloh, za pomocí kterého technik přesně ví, na jakém místě má danou úlohu vykonat. Nakonec systémy AIM generují reporty, které například ukazují, kde vše je co připojeno [6].

2.5.1 Využití systému AIM

Systémy AIM zlepšují několik aspektů správy datových center nebo podnikových sítí, například:

- **Správa změn** – Tím, že zachycuje informace o každém fyzickém připojení a přenáší je prostřednictvím rozhraní API do systémů správy sítě vyšší úrovně, poskytuje systém AIM přesný pohled v reálném čase na fyzickou síťovou konektivitu a může zobrazovat upozornění v případě neplánované nebo neoprávněné změny.
- **Správa aktiv** – Pokud správce sítě nemá přehled o portech, které jsou na přepínači skutečně využity, může se například rozhodnout zbytečně zakoupit nový přepínač. Systémy AIM poskytují přesný přehled o tom, které

přepínací porty se používají (a kam jsou propojeny), takže správci sítě mohou optimalizovat správu majetku a omezit zbytečné výdaje. Systémy AIM mohou také sledovat distribuci, využití a správu PoE zařízení.

- **Odstraňování problémů** – Systémy AIM dokumentují i přesné umístění problému s konektivitou. V některých případech mohou systémy AIM způsobit, že porty LED budou blikat, takže technik vidí přesné místo události v rackové skříni. Tento přístup výrazně zrychluje řešení problémů, protože technik nemusí věnovat čas ověřováním manuální dokumentace nebo hledáním místa, kde se problém vyskytuje.
- **Zabezpečení** – systémy AIM zvyšují zabezpečení sítě, protože mohou hlásit, když je port odpojen nebo připojen na neplánované místo. Bez AIM například může útočník odpojit server a přesunout jej do kanceláře, aby mohl přistupovat k serveru prostřednictvím portu pro správu a obcházet logická bezpečnostní opatření. Správce sítě uvidí, že server na několik minut přešel do offline stavu a poté se vrátil zpět online stavu. Taková anomálie může být často spíše ignorována než identifikována jako problém. Se systémem AIM se správce dozví, že server byl přesunut na jiné místo.
- **Reportování a dodržování předpisů** – organizace fungující na základě předpisů, musí poskytovat přesné dokumenty o řízení změn ve svých sítích (MACs) pro účely auditu a souladu. Systémy AIM vytvářejí aktuální informace (reporty) o stavu sítě, které usnadňují jejich dodržování.
- **Obnova po havárii** – Bez aktuální dokumentace je IT manažer v případě katastrofy (např. výpadek elektrické energie, požár, povodeň nebo zemětřesení) omezen pouze na odhad, když se pokusí o obnovu datového centra nebo ústředny nebo podnikové sítě. Tvorba dokumentace v reálném čase se systémem AIM umožňuje přesně vědět, co bylo nainstalováno, kde a jak bylo vše připojeno, takže datové centrum nebo podnikové sítě mohou rychle a s menšími náklady obnovit svou činnost. Přesná dokumentace také usnadňuje oznamování pojistných událostí.

3 MANAGEMENT FYZICKÉ VRSTVY

Jak bylo naznačeno v úvodu, tak s neustálým vývojem komunikačních technologií roste také rozsah a složitost sítí, zároveň také i nároky na jejich spolehlivost a bezpečnost. Je tedy nutné mít dobře organizovanou strukturu fyzické vrstvy, zavedený systém propojování v propojovací zóně a dále také zdokumentované mapy portů. Do nedávné doby byli k dispozici aplikace, která informovali o stavu všech vrstev sítě. Výjimku však tvořila vrstva, na které celá síť stojí, tedy fyzická vrstva.

Aplikace pro monitoring sítě využívající protokol SNMP vidí pouze logickou strukturu sítě, ale nejsme schopni zjistit pomocí něho například, které porty propojovacího panelu jsou propojeny, nebo kam až dosahuje datový kanál. V poslední době se tak o tuto problematiku začalo zajímat stále více výrobců působících v oblasti strukturované kabeláže, například Molex, RiT, Tyco Electronics, Commscope a další. Ve všech případech se jedná o komerční řešení, kde si jednotliví výrobci drží své know-how pro monitoring, jelikož pro systémy managementu fyzické vrstvy neexistuje žádný ucelený standard, který by společně dodržovali, proto jsou jednotlivé systémy zpravidla mezi sebou nekompatibilní [4].

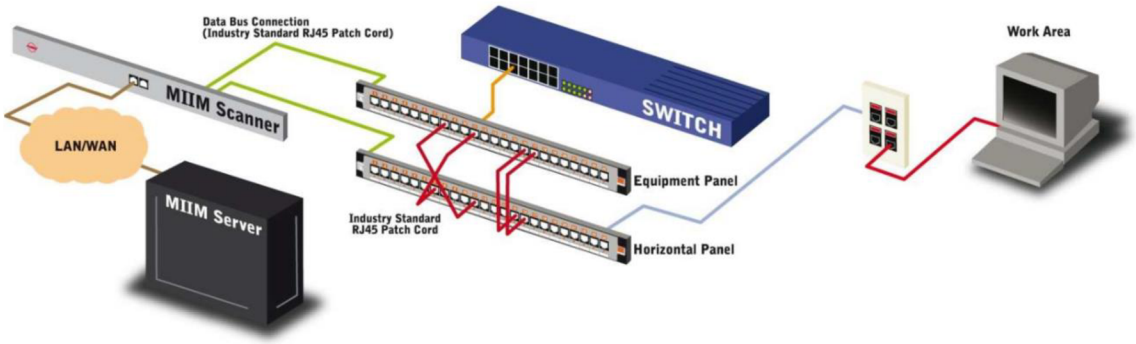
Při získání kontroly nad fyzickou vrstvou pomocí systému managementu fyzické už není nutné provádět následující činnosti:

- Udržovat manuálně záznamy MACs,
- manuálně aktualizovat síťovou mapu nebo tabulku,
- potvrdit fyzicky dostupnost portu,
- manuálně rozdělit pracovní úlohy,
- fyzicky potvrdit, že pracovní úlohy jsou splněny.

3.1 HW a SW pro management fyzické vrstvy

Základním prvkem managementu sítě na fyzické vrstvě je vhodná kombinace hardwaru monitorujícího propojovací zónu a také softwaru udržující databázi o aktuálním stavu. Z hlediska hardwaru je zapotřebí zajistit, aby bylo v reálném čase jasně identifikované propojení mezi konkrétním portem aktivního prvku a portem propojovacího panelu, popřípadě i portem datové zásuvky. Proto je potřeba do síťové infrastruktury přidat několik speciálních komponent, nejčastěji se jedná o propojovací panely přizpůsobené pro monitoring sítě a monitorovací hardware (tzv.

skener). Dále je nutný software, který bude monitorovaná data zpracovávat, uchovávat databázi a zprostředkovávat uživateli informace o aktuálním stavu, nejlépe v grafické podobě. Na obr. 3.1 můžeme vidět příklad základního schématu systému řešení pro managementu fyzické vrstvy. Konkrétně se jedná o schéma systému MIIM od společnosti Molex.



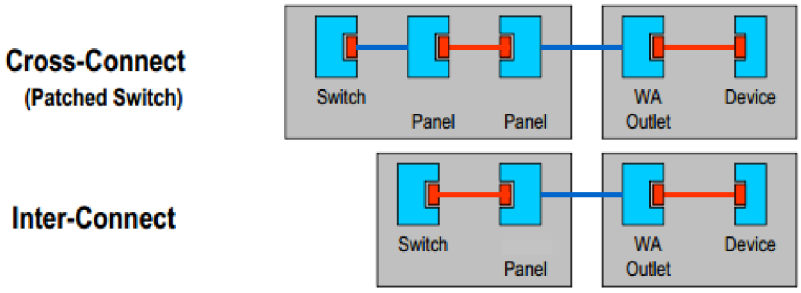
Obr. 3.1 Schéma zapojení systému MIIM pro management fyzické vrstvy [7]

Pro IT správce systém managementu fyzické vrstvy nabízí spoustu zajímavých funkcí. Asistovaná realizace propojení za pomocí LED diod panelu (viz obr. 3.2) a tvorba databáze se všemi prvky v síti spolu s jejím umístěním jsou jedny ze základních funkcí. Dále můžeme v systému definovat vše od místnosti v budově (včetně plánu), racků, aktivních prvků, propojovacích panelů, datových zásuvek až po koncové zařízení a uživatele. Pohyb a aktivita v síti je monitorovaná a aktualizována v databázi v reálnem čase za pomocí skeneru. Pracovníci IT tak mohou sledovat stav sítě svém počítači, aniž by musel být fyzicky přítomen v telekomunikační místnosti [8].

Obr. 3.2 Asistované propojení LED signalizací

3.2 Architektura propojovacích panelů

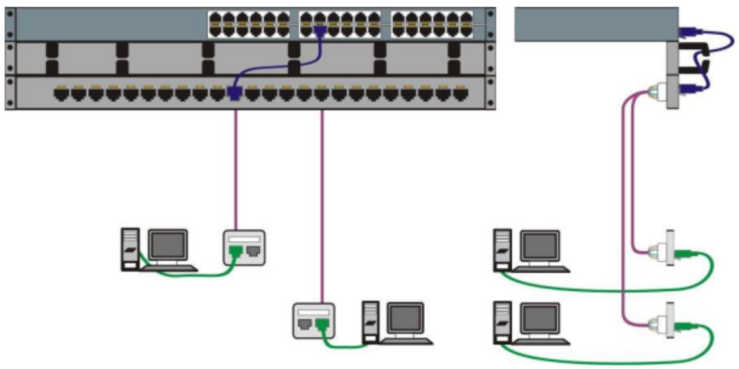
Při samotné instalaci sítě je nutné brát v potaz nasazení inteligentních propojovacích panelů, které budou schopny sledovat stav zapojených propojovacích panelů. Inteligentní panely u jednotlivých portů často mají signalizační LED, díky kterým může být technik naveden, na kterých portech propojovacích panelů má být realizovaná úloha (propojení, odpojení nebo přepojení). Nejčastěji se u výrobců setkáme s jednoduchou nebo dvojitou reprezentací propojovacích panelů.



Obr. 3.3 Schéma jednoduchého (Inter-Connect) a dvojitého (Cross-Conmect) zapojení [9]

3.2.1 Jednoduchá reprezentace (Inter-Connect)

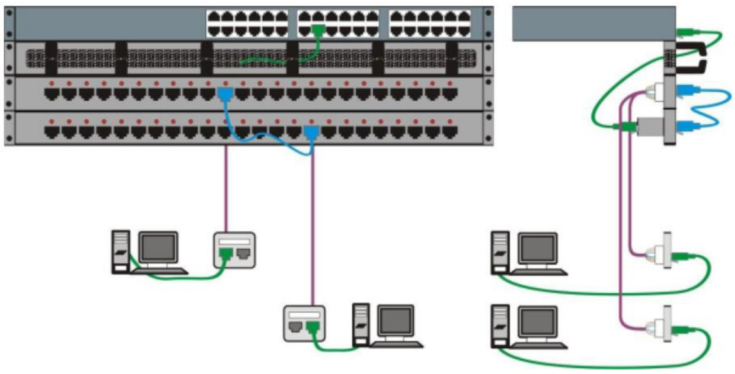
Jednoduchá reprezentace využívá pouze jeden propojovací panel, viz obr. 3.4. K tomuto panelu jsou vedeny koncové datové zásuvky. Panel pak prostřednictvím propojovacích kabelů spojujeme s aktivním prvkem, nejčastěji přepínačem. Využití najde v instalacích s požadavkem na nízkou pořizovací cenu a menšími nároky na prostor v racku. Nevýhodou omezené monitorování propojovací zóny, omezené možnosti plánování úloh v sytému pro management, omezená navigace pomocí LED a identifikace koncového zařízení. Nevýhodou také může být, že v případě častého přepojování můžeme mechanicky opotřebovávat porty přepínače.



Obr. 3.4 Zapojení jednoduché reprezentace [8]

3.2.2 Dvojitá reprezentace (Cross-Connect)

Nejčastěji se však u systémů pro management fyzické vrstvy setkáme s dvojitou reprezentací, kde oproti jednoduché využíváme dvojnásobný počet inteligentních propojovacích panelů. Polovina inteligentních propojovacích panelů reprezentuje porty přepínače a další polovina reprezentuje koncové zásuvky, viz obr. 3.5. Na rozdíl od jednoduché reprezentace jsem schopen monitorovat i propojovací zónu v rackové skříni. Výhodou je tak vznik přepojovacího pole, kdy nám inteligentní propojovací panely poskytují navigaci pomocí LED diod u portů při přepojování.



Obr. 3.5 Zapojení dvojité reprezentace [8]

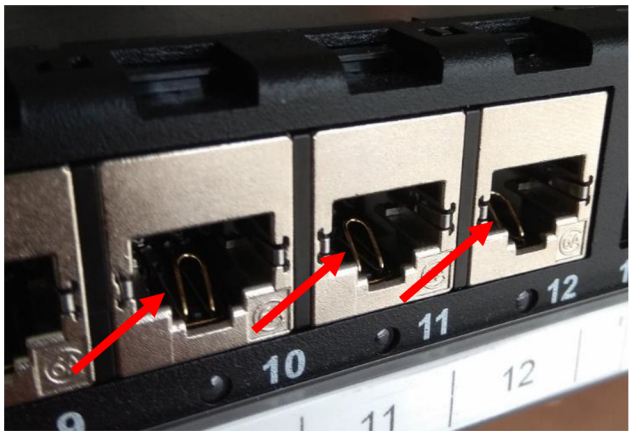
3.3 Monitoring

Monitorování propojovací zóny může být založeno na různých principech. Jelikož pro systém managementu fyzické vrstvy neexistuje jednotný standard, tak se vždy jedná o komerční řešení, kdy jednotliví výrobci využívají různé principy. Zároveň i tak různá řešení nejsou mezi sebou kompatibilní. Často dochází ke kombinaci principu monitoringu fyzické vrstvy s vrstvami vyššími. Dnes se setkáme s následujícími principy monitorování fyzické vrstvy:

- Mikrospínač/senzor v portu propojovacího panelu,
- propojovací kabel s 9-pinem,
- RFID čip,
- impedanční vlastnosti,
- využití vyšších vrstev.

3.3.1 Princip mikrospínače

Využití mikrospínačů uvnitř portů propojovacích panelů se stává pomalu zastaralým principem. Každý port v propojovacím panelu obsahuje spínač, který je při připojeném kabelu v sepnutém stavu. Systém na základě toho je tak schopen monitorovat, ke kterým portům je připojen propojovací kabel. Tyto systémy však mají zásadní nedostatek v tom, že v případě provedení změn v propojovací zóně během odstávky managementu sítě na fyzické vrstvě, systém nedokáže zpět určit relevantní mapu spojů. Dále nedokáže zjistit stav, pokud by v propojovací zóně došlo k přestřižení kabelu, jelikož spínače budou sepnuté, tak systém daný propoj bude brát, že je v pořádku. V současnosti se tento princip pro monitorování využívá v kombinaci s dalším principem. Na obr. 3.6 můžeme vidět příklad mikrospínače uvnitř spodní části portu. Princip podobný mikrospínači využívá například společnost Commscope.

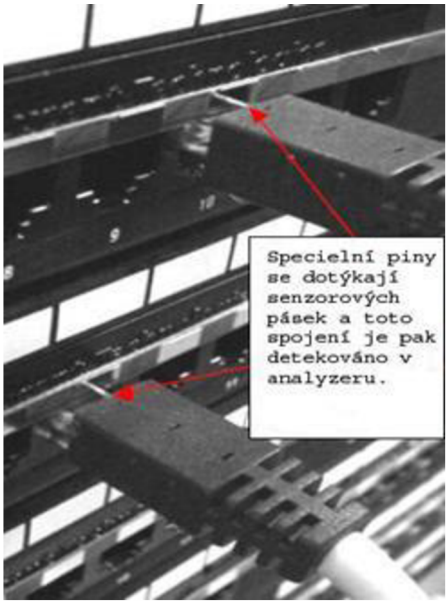


Obr. 3.6 Propojovací panel s mikrospínači

3.3.2 Princip devátého pinu

Pro možnost tzv. devátého pinu využíváme inteligentní propojovací panely, které mají navíc jeden kontakt (reprezentovaný například senzorovou páskou), pomocí kterého se prostřednictvím propojovacích kabelů s devátým pinem vytváří monitorovací okruh (viz obr. 3.7). Tento kontakt tak umožňuje celému systému sledovat zapojení jednotlivých kabelů, protože jeho připojení či přerušení může skener zaznamenat a poslat serveru. Díky tomu, že informace o zapojení kabelu získává dalším pinem, tak monitoring nijak neovlivňuje přenášená data. Jsme tak schopni přesně určit propojení konkrétních portů za jakýchkoliv okolností. Propojovací panely mají senzorové pásky, pomocí níž jsou jednotlivé propojovací

kabely hlídány skenerem. Tyto pásky jsou dostupné pro všechny typy aktivních prvků. Někteří výrobci nabízejí propojovací panely, které jsou připraveny na budoucí upgrade managementu sítě tak, že lze u nich přední kryt vyměnit za kryt obsahující senzorové pásky.



Obr. 3.7 Příklad principu 9-pinu [10]

Jedná se sice o vyspělejší řešení než při použití s mikrospínačem, ale jsme nucení použít speciální propojovací kabely s devátým kontaktem, což činí toto řešení mírně finančně náročnější. Toto řešení využívá mnoho výrobců systému pro management sítě, jako například Panduit, AMP, Rit a další.

3.3.3 Princip RFID čipu

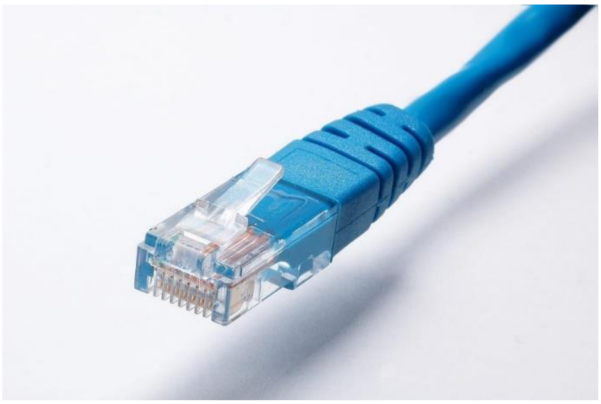
V případě principu postaveném na RFID čipu je každé připojení kabelu jasně alokováno a čteno elektronicky. Každý port panelu je vybaven čtecí anténou, která okamžitě identifikuje a upozorňuje na změnu připojení. RFID čip na obou koncích propojovacího kabelu (viz obr. 3.8) obsahuje identifikační informace (jméno, standard, výrobce atd.). Nevýhodou je právě nutnost využití speciálních kabelů, které jsou tak dražší než klasické propojovací kabely. Typickým výrobcem systému fungujícím na principu RFID je společnost Bolden.

Obr. 3.8 Příklad kabelu s RFID čipem [11]

3.3.4 Princip impedančních vlastností

Poslední novinkou v určení spojení v propojovací zóně je princip založený na měření impedančních vlastností fyzické vrstvy, který bude blíže popsán v další kapitole u řešení MIIM od společnosti Molex. Nejsme nuceni využívat speciální propojovací kabely jako například u principu s devátým pinem. Poměrně zásadní výhodou těchto systémů je schopnost monitorovat za hranicemi propojovací zóny a můžeme tak mapovat celou linku od aktivního prvku až po koncové zařízení.

Výhodou je tak možnost získávání dalších informací jako je odpojení a připojení vypnutého koncového zařízení od koncové datové zásuvky. To přináší vyšší bezpečnost. Při pokusu o odcizení koncového zařízení (počítač, tiskárna) systém zaregistruje její odpojení od datové zásuvky a upozorní na tuto skutečnost pověřeného IT pracovníka. Systém s tímto umožňuje sledovat i stav horizontální kabeláže a jsme schopni rychleji lokalizovat a odstranit problém v případě fyzické poruchy sítě.



Obr. 3.9 Příklad běžného propojovacího kabelu

Tyto systémy jsou často označovány jako systémy druhé nebo nové generace a mají výhodu v tom, že získávají informace o celém kanálu prostřednictvím měření fyzikálních vlastností sítě (impedanci síťové karty). Tím se tak omezuje zátěž sítě v důsledku získávání dalších informací z vyšších vrstev. To je typické pro systémy

první generace. První generace systémů využívá služby vyšších vrstev, konkrétně dotazy SNMP protokolu, pro získání informací o stavu aktivních prvků a koncových zařízení. Využívají funkci „polling“, což je periodické zasílání dotazů na zařízení v předem definovaném rozsahu IP adres. Systémy nové generace využívají tzv. „smart polling“, kde dotazu dochází tehdy, když nastala změna na dané lince – připojení, odpojení, zapnutí a vypnutí zařízení. Snižujeme tedy tak provoz na sítí spojený se systémem pro management.

3.4 Skener

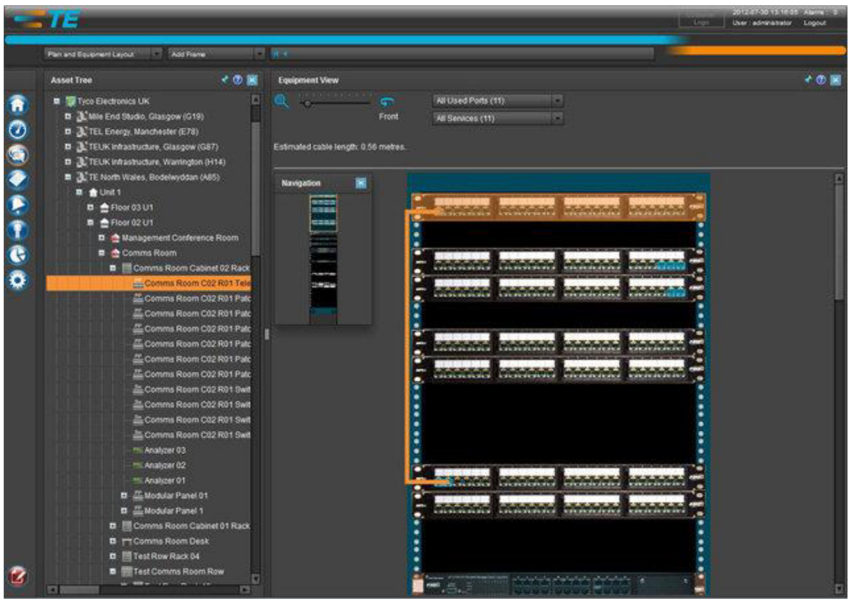
Nezbytnou součástí systému managementu sítě je skener, v různých řešeních označován také jako monitor nebo analyzer (viz obr. 3.10). Jedná se o zařízení, ke kterému je připojeno několik propojovacích panelů. Panely jsou ke skeneru často připojeny prostřednictvím zvláštního konektoru, umístěného na zadní straně panelu. Skener je z pohledu uživatele síťové zařízení, které má vlastní IP adresu. Skener shromažďuje údaje z jednotlivých portů propojovacích panelů, zpracuje je v relevantní informace a předá serveru.

Obr. 3.10 Příklad řešení skeneru PanView IQ od společnosti Panduit [12]

3.5 Software managementu sítě na fyzické vrstvě

Řešení softwaru pro management sítě na fyzické vrstvě se může u jednotlivých výrobců lišit. Systém nejčastěji funguje na principu klient-server. Server disponuje databází, která obsahuje veškeré informace a rozhraní pro funkci s okolím. Jedná se tedy zpravidla o databázový server, který komunikuje prostřednictvím TCP/IP

protokolu se skenery, a ke kterému mohou IT správci přistupovat prostřednictvím klientských aplikací. Ty mohou být samostatné s vlastním GUI (viz obr. 3.11) nebo web-based (přístup k rozhraní prostřednictvím webového prohlížeče).



Obr. 3.11 SW řešení systému Quareo od Tyco Electronics [13]

V databázi se ukládají nejrůznější informace, jako například umístění racků, propojovacích panelů, aktivních síťových prvků, zobrazení jednotlivých spojů v propojovací zóně, údaje o koncových zařízeních a jejich uživatelích. Údaje jsou získávány ze skenerů v reálném čase a vypovídají o aktuálních spojích. Důležitá je také návaznost z vyšších vrstev. Jedná se o informace jako například IP a MAC adresu připojených koncových zařízení, informace stavu portů partů aktivních prvků získané prostřednictvím protokolu SNMP. Způsob získávání informací z vyšších vrstev a jejich využití závisí na konkrétním výrobci a možnostech daného systému.

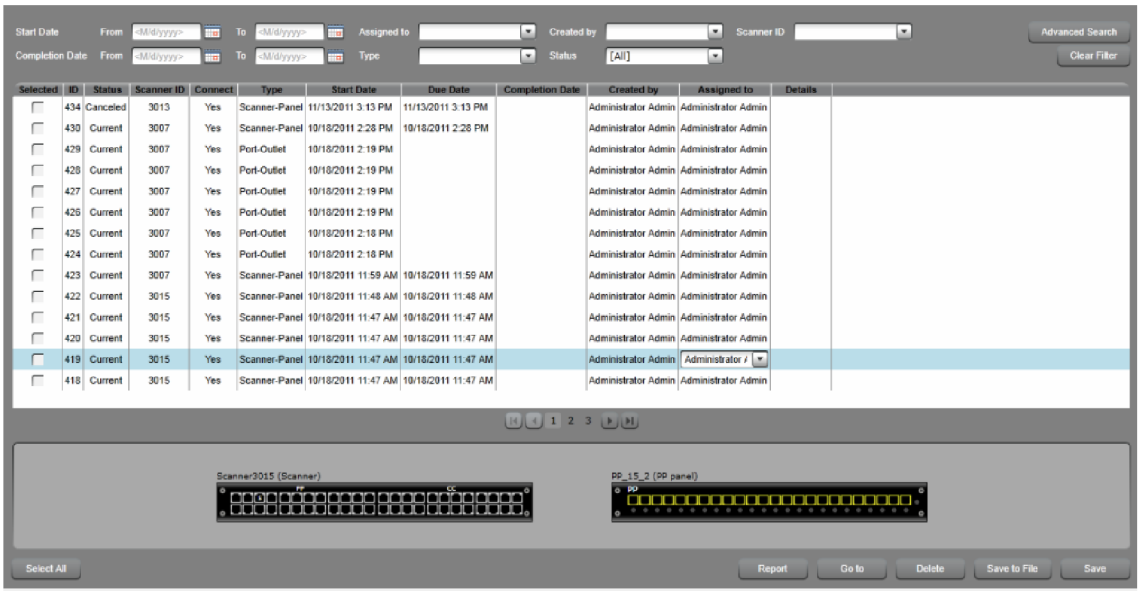
Díky informacím, které systém pro management sítě uchovává v databázi, tak můžeme vytvářet velké množství výkazů, statistik a reportů, což ukáže IT správcům například vytížení aktivních prvků, seznamy nevyužitých portů, záznamy o změnách v sítí a pracovních úlohách. Pro vedení firmy můžou být naopak klíčové informace jako například výkazy o počtu změn v síti, výkazy o počtu pravidelných prací vykonané jednotlivými techniky, výkazy o včasném plnění úkolu.

Některé systémy umožňují spolupráci s aplikacemi pro management na vyšších vrstvách od výrobců třetích stran. Spolupráce systémů managementu na fyzické vrstvě s dalšími systémy managementu na vyšších vrstvách je užitečná, jelikož v případě dosavadního používání takové aplikace nemusíme udržovat společné informace ve dvou databázích, což šetří čas IT správcům a minimalizuje zatížení sítě.

3.5.1 Pracovní úlohy

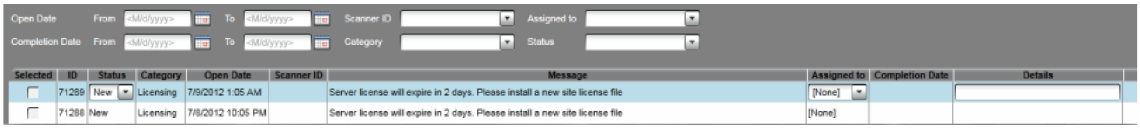
Pro většinu větších firemních sítí je užitečné sledovat, jak fyzická infrastruktura vypadá, ale je nutné i provádět změny organizovaně. K tomu slouží část systému určená pro plánování úloh.

Při obdržení požadavku na změnu v síti tak s asistencí systému pro management nalezneme vhodný bod pro připojení. Tato informace je následně vložena do pracovní úlohy pro technika, který má danou změnu realizovat v propojovací zóně. Úloha obsahuje informaci, které porty a na kterých panelech má technik propojit, nebo do které koncové zásuvky připojit zařízení a v jakém časovém intervalu úlohu provést. Následně systém příslušnému technikovi asistuje. V propojovací zóně se tak rozsvítí pomocná LED u požadovaných portů. Dále je tato úloha zaznamenána do databáze. Zároveň se tak kontroluje správnost práce technika a eliminuje se možné chyby při změnách v síti.



Obr. 3.12 Příklad zobrazení úloh v systému MIIM od Molex

V případě neplánovaných spojů či rozpojení systém okamžitě tuto událost zaznamená a upozorní IT správce. Systém může nabízet různé možnosti alarmů, které v případě neplánových událostí zašlou správci IT upozornění emailem nebo SMS.



Obr. 3.13 Příklad seznamu upozornění v systému MIIM od Molex

4 PŘÍKLAD SYSTÉMU PRO MANAGEMENT SÍTĚ FYZICKÉ VRSTVĚ

Tato kapitola bude zaměřena na konkrétního zástupce systému pro management fyzické vrstvy. Jedná se o systém MIIM, jejímž výrobcem je společnost Molex. Pro seznámení s funkcemi a analýzu systému byl použit prezentační MIIM kit, který se skládá ze skeneru, kombinace dvou propojovacích panelu, přepínače Cisco, panelu s osazenými MIIM terminátory a MIIM serveru (viz obr.4.1).

Obr. 4.1 Prezentační MIIM kit

Obr. 4.2 Pohled ze zadní strany MIIM kitu

4.1 Společnost Molex Premise Networks Limited

Molex PN je společnost založená roku 1985, která dodává úplná řešení síťové kabeláže pro komunikační průmysl. Jedná se o druhého největšího výrobce produktů propojovacích řešení na světě s ročními příjmy ve výši 3 miliard dolarů. V současné době sídlí v Portsmouth ve Velké Británii. Molex PN je dceřinou divizí společnosti Molex Electronics. Jejich portfolio produktů zahrnuje řešení jak pro metalické, tak i pro optické datové sítě.

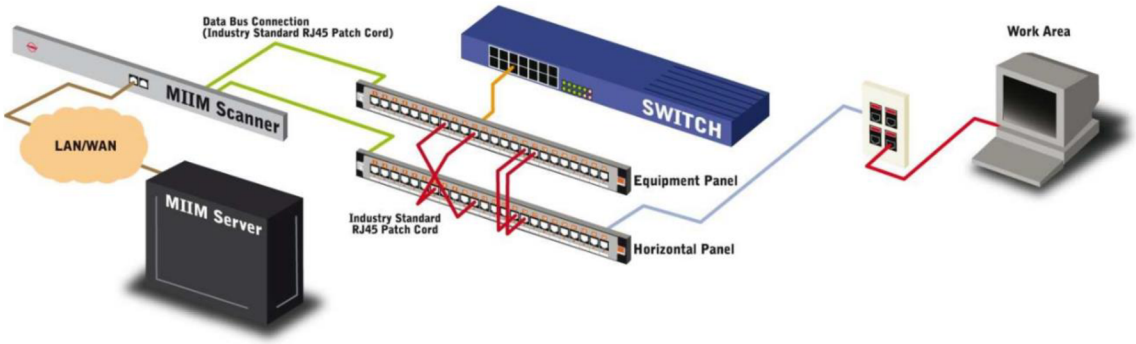
Společnost Molex Premise Networks Limited byla dříve známá jako Mod-Tap Limited a v červenci 1999 změnila název na společnost Molex Premise Networks Limited. Parametry veškerých jejich produktů a systémů splňují požadavky stanovené průmyslovými standardy, jako například ISO 11801, EN50173 a EIA/TIA 568B.

Obr. 4.3 Logo společnosti Molex PN [14]

Samostatná společnost Molex vznikla v roce 1938 a je výrobcem elektronických, elektrických a optických propojovacích systémů. Molex nabízí více než 100 000 produktů v celé řadě průmyslových odvětví (letectví, obrana, automobilový průmysl, alternativní energie, spotřební elektronika, domácí spotřebiče, užitková vozidla, výpočetní technika, průmyslová automatizace, průmyslová elektrotechnika, medicína, věda, smartphony a mobilní zařízení, polovodičové osvětlení a telekomunikace). Molex se dále například podílel na vývoji prvního autorádia, prvního mobilního telefonu a první HDTV [14].

4.2 Systém MIIM

MIIM je systém, který umožňuje kompletní správu fyzické vrstvy při současné integraci s dalšími nástroji určenými pro správu sítě. Správcům IT infrastruktury tak poskytuje kompletní viditelnost informací o fyzické vrstvě, což nese za výsledek výkonnější a efektivnější správu sítě.



Obr. 4.4 Schéma systému MIIM od Molex [7]

MIIM je ucelené řešení pro pokročilou správu fyzické vrstvy, která se primárně zaměřuje na vylepšenou správu sítě a jejího zabezpečení, správu majetku, zvýšenou produktivitu a viditelnost důležitých informací. MIIM umožňuje nejen spravovat přesuny, rozšíření, změny v sítí a správu pracovních úloh, ale také navíc nepřetržitě provádí monitoring a mapování fyzické vrstvy včetně neporušitelnosti kabeláže od telekomunikační místnosti až po koncovou datovou zásuvku, detekuje připojení a odpojení síťových zařízení, porovnává reálně nasazené prvky sítě s jejich návrhem a umožňuje technikům realizovat pracovní úlohy pomocí řízeného propojování. Klíčovým rozdílem je schopnost sledování stavu fyzických kanálů i za hranicemi telekomunikačních skříní. Řešení MIIM je jedním z mála ucelených řešení pro správu fyzické vrstvy s množstvím jedinečných funkcí zajišťující úplnou viditelnost informací pro správce sítí.

Řešení MIIM je navrženo s cílem zachovat jednoduchost, tedy ovládání jednoduché pro správce sítě, jednoduchá instalace a jednoduché používání bez potřeby speciálních propojovacích kabelů nebo LCD displejů. Zároveň díky okamžité funkční integraci s ostatními nástroji pro správu sítí jsou tak náklady na nasazení daného řešení výrazně nižší než v případě systémů inteligentního propojování, které jsou na trhu od dalších dodavatelů [7] [15].

V jednotlivých bodech níže jsou uvedeny základní klíčové vlastnosti řešení MIIM:

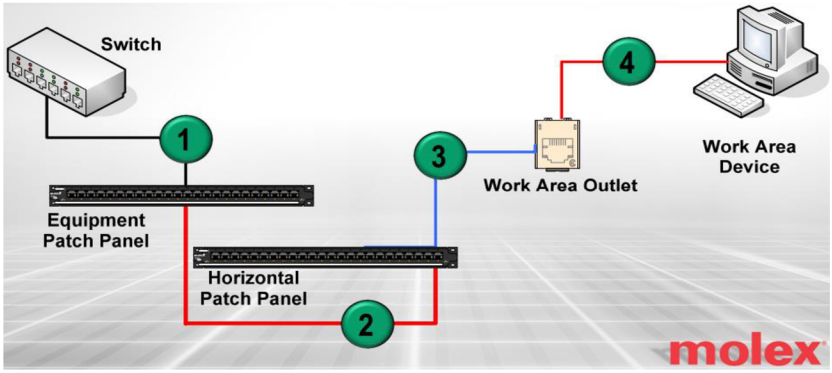
- Možnost řízeného propojování, kdy jsou na propojovacích panelech umístěné LED diody, které indikují porty s nevyřízenými pracovními úlohami a navádějí tak správce sítě.
- Usnadnění správy, včetně plánování a zaznamenávání přesunů, rozšíření a změn v sítí, včetně ověřování správného provedení pracovních úloh.
- Dotazování připojených zařízení řízených na základě událostí zajišťuje poskytování aktuálních informací ze všech zařízení připojených k datovým zásuvkám.
- Nepřetržitý monitoring fyzické vrstvy včetně kabelů a síťových zařízení.

- Ověřování neporušenosti horizontální kabeláže od propojovacího panelu až po datové zásuvky na pracovišti, detekce přerušeného spojení a poruchy izolace.
- Nepřetržitý monitoring na přítomnost zařízení připojených k datové zásuvce na pracovišti, a to i pokud je dané koncové zařízení vypnuté. Lze též konfigurovat výstrahy, které upozorňují správce sítě na neoprávněné odpojení zařízení nebo neoprávněné připojení do datové zásuvky.
- Porovnávání reálně nasazených prvků sítě s jejich návrhem a zvýraznění odchylek od návrhu.

4.2.1 End-to-end monitoring kanálu

Systém MIIM současně využívá pro monitoring princip postavený na kombinaci mikrospínače a měření impedančních vlastností. Datovým kanálem se v systému MIIM rozumí všechny kabely a konektory od přepínače až k připojenému koncovému zařízení. Jak znázorňuje obr. 4.5, tak systém Molex MIIM je schopný monitorovat celý datový kanál od koncového zařízení až po aktivní prvek, tedy:

1) Kanál od přepínače k panelu reprezentující aktivní prvek (equipment patch panel),
2) kanál mezi propojovacími panely,
3) kanál horizontální kabeláže (od horizontálního panelu k datové zásuvce),
4) kanál koncového zařízení.



Obr. 4.5 Zobrazení end-to-end monitoringu systému MIIM [1]

Systém MIIM je v rámci zmíněného čtvrtého případu schopen detekovat připojení nebo odpojení zařízení i v takové situaci, že dané koncové zařízení je vypnuté. Toto je aktuálně jeho konkurenční výhoda, kterou zatím ostatní systémy pro management neaplikují.

Většina konkurenčních řešení monitoruje často pouze propojovací oblast, tedy spojení mezi propojovacími panely. Případný monitoring koncových zařízení řeší prostřednictvím vyšších vrstev, často díky SNMP informaci z přepínače, které porty má aktivní. Aby však port na přepínači byl aktivní, musí koncové zařízení být zapnuté. Tuto situaci právě systém MIIM umí řešit. Kromě detekce přerušení kanálu, jsme schopni detekovat [1]:

- Neautorizované připojení neschválených zařízení,
- nedefinované zapojení nebo propojení mezi propojovacími panelu
- odebrání kriticky důležitých síťových zařízení (jako přepínač) ze sítě,
- odebráni drahých síťových zařízení připojené k síti (například tiskárny).

Obr. 4.6 Zobrazení kompletního kanálu v systému MIIM

4.2.2 Architektura propojovacích panelů MIIM

Systém MIIM podporuje obě zmíněné architektury zapojení propojovacích panelů:

- Jednoduchá reprezentace (Inter-Connect),
- Dvojité reprezentace (Cross-Connect).

Pro plné využití systému a schopnosti monitorovat celý kanál musíme výhradně využít dvojitého zapojení (Cross-Connect). V případě dvojitého zapojení systém MIIM zavádí vlastní označení CC a PP pro propojovací panely. Porty CC panelu reprezentují porty přepínače a porty PP panelu reprezentují porty datových zásuvek. CC a PP panely jsou navzájem propojovány běžnými propojovacími kabely. V jednom kanálu nelze mít připojené více než dva MIIM propojovací panely [9].

4.2.3 Snímání NIC

Počítače, tiskárny, IP a další zařízení obsahují karty síťového rozhraní NIC pro připojení k sítím založeným na architektuře Ethernet. MIIM detekuje standardní elektrické vlastnosti ve většině NIC síťových zařízení se zásuvkou pro RJ-45 konektor a zjistí, zda je zařízení připojeno či nikoliv bez ohledu na to, zda je toto zařízení napájeno. Systém MIIM využívá pro detekci princip Smith-termination na síťových rozhraních. Jedná se o patentované zakončení ethernetových síťových rozhraní, který využívá většina výrobců. Naměřený odpor síťové karty odpovídá přibližně 150 Ω.

Systém MIIM má jedinečný detekční mechanismus, který poskytuje významné výhody pro detekci zařízení a monitorování kanálů nad rámec toho, co je možné v jakémkoli jiném řešení. MIIM umožňuje detekovat většinu IP zařízení (se standardními Ethernet síťovými kartami) na trhu připojených k jednomu konci kanálu (koncová datová zásuvka) bez ohledu na to, zda je toto zařízení napájeno [1].

4.3 Prvky systému MIIM

V této podkapitole jsou popsány základní prvky pro kompletní funkci řešení MIIM od společnosti Molex.

4.3.1 MIIM skener kanálu

Skenery MIIM monitorují aktivitu systémů s podporou MIIM řešení. MIIM skener (obr. 4.7) spolupracuje s MIIM serverovým softwarem (prostřednictvím TCP/IP protokolu) a MIIM inteligentními propojovacími panely, aby koordinovali řízení pracovních úloh, poskytovali vodítko na propojovacích panelu pomocí LED, snímali a zprostředkovávali informace o stavu připojení v hlídané oblasti. Skenery MIIM lze konfigurovat a aktivovat nezávisle na softwaru. Jakmile je aplikační software MIIM připojen ke skeneru, zjistí skener aktivní zařízení v síti a tyto data zašle do serverového aplikačního softwaru MIIM. Skener sleduje stav připojených kanálů MIIM a předává data o změně stavu do serverového aplikačního softwaru MIIM. Tím dochází ke spuštění funkce inteligentního dotazování řešení MIIM, které zasílá dotazy konkrétním datovým zásuvkám a aktualizuje databázi.

Obr. 4.7 Přední strana MIIM skeneru [9]

Ke skeneru, o velikosti v racku 1U, lze připojit až 48 propojovacích panelů, což umožňuje monitorovat až 576 samostatných fyzických kanálů v jedné Cross-Connect zóně. První polovina portů je určeno pro CC panely a druhá polovina portů

pro PP panely. Neomezený počet skenerů (cross-connect zón) může být spravováno jedním serverem. Pro spojení datové sběrnice mezi skenerem a propojovacím panelem se využívá běžný ethernetový kabel kabel se standardizovaným konektorem RJ45.

V situaci, kdy MIIM server nemůže komunikovat se skenerem, tak skener si transakce poznamená do fronty pro pozdější doručení serverové aplikaci. V případě výpadku elektrického napájení nebude skener shromažďovat data. Z tohoto důvodu je vhodné mít skener připojený k záložnímu zdroji UPS, aby byl aktivní minimálně po dobu provozu přepínače. Konfigurace však budou neporušené a při obnově napájení skener automaticky začne shromažďovat data o všech propojovacích kabelech a stavech koncových zásuvek. Systém MIIM neovlivňuje ani nečte Ethernetovou komunikaci. MIIM skener spotřebovává malé množství elektrické energie, což může být v zásadní v prostředích, které mohou být náročné na napájení, například datová centra. O provoz skeneru se stará operační systém Windows Embedded Compact. Konfigurace skeneru probíhá prostřednictvím jeho webového rozhraní [16] [17].

Zde jsou uvedené základní vlastnosti skeneru MIIM:

- Sledování kanálů až po umístění zařízení.
- Výstraha v případě odpojení kabelu od portů.
- Automatické zjišťování aktivního zařízení, automatické plnění databáze.
- Inteligentní dotazování umožňuje nepřetržité aktualizace systému MIIM s minimálním vlivem na šířku pásma a výkon sítě.
- Díky nízké spotřebě odpadá nutnost externích ventilátorů a chlazení.
- Vysoká hustota portů: Skener v rackové skříni zabírá minimální prostor (1U) a podporuje až 576 kanálů.
- Datová sběrnice mezi skenerem a propojovacím panelem je realizován prostřednictvím propojovacích kabelů se standardizovaným konektorem RJ45.
- Skener MIIM může být připojen k MIIM inteligentním propojovacím panelům a testován správnou funkčnost řešení bez nutnosti připojení k aplikačnímu serveru MIIM.
- Fronty transakcí zaznamenávají události pro pozdější doručení v případě, že dojde k narušení komunikace se aplikačním serverem MIIM.
- Automatická synchronizace s aplikačním MIIM serverem v případě výpadku nebo selhání systému
- Webové rozhraní pro administraci.
- Snadná konfigurace skeneru.

Obr. 4.8 Pohled na MIIM skener ze zadní strany [17]

4.3.1.1 Skenování

Skenování je proces, který zajišťuje skener a hlídá, zda k portu panelu je připojený propojovací kabel, popřípadě dosah datového kanálu. Pravděpodobný princip skenování systému MIIM je takový, že vystaví malé napětí (v řádech mV) na portu PP propojovacího panelu a toto napětí se snaží naměřit na portu CC panelu pro určení propojení a zároveň za PP panelem změří impedanci pro zjištění kontinuity horizontální linky a případně připojeného zařízení k datové zásuvce (viz kapitola o terminátoru datové zásuvky MIIM). Společnost Molex z konkurenčních důvodu, jako většina výrobců, nezveřejňuje přesný způsob a popis skenování, či detekce. Popsaný způsob detekce tak vychází ze zkušenosti při práci se systémem. MIIM skener provádí následující typy skenování [17]:

- **Fast scan**
  - Probíhá neustále.
  - Tento typ skenování probíhá pouze v rámci stávajících datových kanálů (propojení mezi panely CC a PP, horizontální linka, připojené koncové zařízení), které má systém nadefinované v databázi.
  - Pokud během skenování zapojíme do panelů propojovací kabel nebo ho odpojíme, tak systém tuto událost zjistí na základě sepnutého spínače uvnitř portu panelu a skener provede skenování nového propojení. Zároveň systém upozorní na novou událost.
  - Trvání rychlého skenování může trvat několik sekund, maximálně až 1 minutu. Konkrétní doba trvání závisí na velikosti síťové infrastruktury.
- **Full Patch Panel Scan**
  - Tento typ skenování zjišťuje, zda nebyl ke skeneru připojen nový propojovací panel.
  - Probíhá po uplynutí určitého počtu fast scan cyklů.
  - Počet cyklů fast scanu, po kterých se má provést full patch panel scan, můžeme měnit v nastavení skeneru.

- **Full Patchcord Scan**
    - Pro ověření správnosti zapojení propojovacích panelů.
    - Při tomto typu skenování dochází k postupné kontrole jednotlivých portů PP panelu vždy vůči všem portům CC panelu a určí propoj na konkrétních portech mezi panely, který skener posléze uloží do své databáze, zároveň kontroluje kontinuitu horizontální kabeláže i připojení zařízení ke koncové datové zásuvce.
    - Doba trvání skenování je časově náročná a může trvat několik minut až několik hodin. Doba se odvíjí od velikosti síťové topologie.
    - Nejčastěji si provádí při počáteční implementací systému managementu, po určité době po provedení fast scan cyklů nebo po obnovení ze stavu offline (např. po přerušení napájení) – kontroluje stav před a po výpadku na základě databáze.
    - V případě detekce nového propojení nebo změny v propojovací zóně v průběhu full patch cord scanu je při dalším cyklu full patchcord scanu pozastaven a proběhne fast scan nového propojení, následně pokračuje ve full patchcord scanu. Událost změny je detekována na základě tlačítka v portu panelu. Časté změny v propojovací zóně mohou prodloužit dobu trvání full patchcord scanu. Zároveň však dochází k mírnému zpoždění upozornění na případné události, jelikož systém čeká na doběhnutí skenování portu PP panelu vůči všem CC, následně provede fast scan na vyvolanou událost. Posléze pokračuje ve full patch panel scanu na dalším portu PP.
    - Počet cyklů fast scanu, po kterých se má provést full patchcord scan, můžeme měnit v nastavení skeneru.

4.3.2 MIIM terminátor datové zásuvky

Terminátor MIIM (obr. 4.9) se využívá v koncové datové zásuvce a umožňuje systému MIIM monitorovat kontinuitu horizontálního kabelu do dané datové zásuvky. Terminátor MIIM použijeme místo klasické vložky (RJ45 keystone jacku), který se dnes běžně využívá v datových zásuvkách.

Rozdíl v nich je, že řešení MIIM využívá speciální krytky (tzv. stuffer cap), obsahující velmi vysoký odpor (1 MΩ), který je systém schopen změřit a určit, že horizontální linka je v pořádku. V případě přerušení horizontální linky by systém naměřil odpor blížící se nekonečnu a upozornil, že daná linka není v pořádku. Kontinuální měření se provádí na bílo-hnědém a oranžovém pinu. Dané dva kontakty stuffer capu tak přiléhají k příslušným kontaktům keystone jacku.

V případě připojení koncového zařízení, tak systém MIIM využívá standardizovaného zakončení Smith-termination u ethernetových síťových rozhraní. Naměřený odpor zařízení na zmíněných pinech je přibližně 150 Ω. Systém je schopen odpor detekovat a zjistit, že zařízení je připojeno. Tato detekce je unikátní u společnosti Molex a jeho systému oproti ostatním konkurentům.

Komunikace mezi terminátorem MIIM a skenerem MIIM je transparentní pro datový kanál a operuje mimo šířku pásma architektury Ethernet. Systém MIIM může fungovat nezávisle na terminátoru MIIM. Nicméně terminátor však poskytuje vylepšené funkcionality, co s týče monitorování náhradních nebo nepoužívaných kanálů [9] [18].

Obr. 4.9 MIIM terminátor

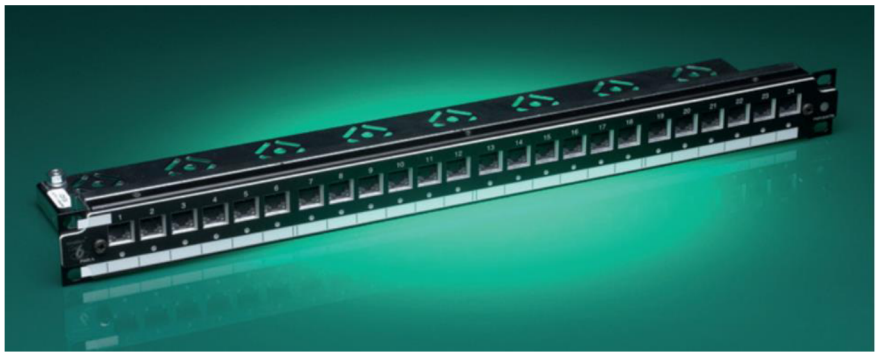
Zde jsou uvedené základní vlastnosti terminátoru datové zásuvky MIIM:

- Potvrzení integrity obvodu mezi inteligentním propojovacím panelem MIIM a datovou zásuvkou.
- Transparentní pro datové kanály.
- Umožňuje monitorovat změnu a detekuje přítomnost zařízení připojeného k datové zásuvce.
- Neinterferuje s Ethernet signálem nebo PoE.

4.3.3 MIIM inteligentní propojovací panel

V rámci řešení MIIM jsou využívány 24portové propojovací panely UTP kategorie 6 nebo 6A. Ke každému MIIM panelu (obr. 4.10) je ze zadní strany zasunutý e-modul (viz obr. 4.11), pomocí kterého je panel řízen. Bez tohoto zásuvného modulu, se panel chová jako běžný propojovací panel. Na e-modulu se nachází port (viz obr. 4.12), který je určený pro připojení do datové sběrnice systému MIIM. Tento propojovací port datové sběrnice spojuje propojovací panel se skenerem MIIM prostřednictvím standardního propojovacího kabelu RJ45 a zároveň zajišťuje napájení e-modulu. Jednotlivé moduly portů (keystony) jsou pak k samotnému e-

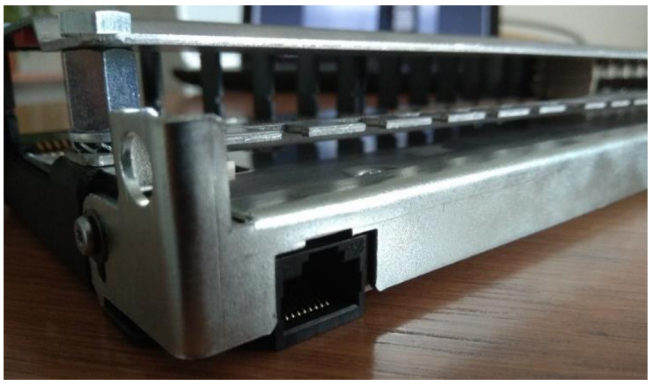
modulu připojeny prostřednictvím speciálního rozhraní (viz Obr. 4.13). Každý port panelu obsahuje mikrospínač, pomocí kterých hlídá obsazenost panelu.



Obr. 4.10 MIIM inteligentní propojovací panel [19]

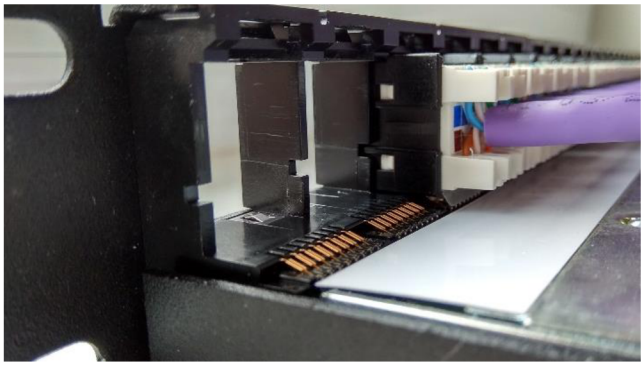
Obr. 4.11 MIIM e-modul [9]

Propojovací panel je schopen detekovat připojení na straně propojovacího panelu i na straně datové zásuvky na pracovišti. Dva vestavěné indikátory napájení na panelu zajišťuji indikaci napájení ze skeneru.



Obr. 4.12 Port na zadní straně panelu pro připojení skeneru

Pokud propojovací panel není připojen k systému MIM, tak funguje jako klasický propojovací panel. Propojovací panel MIIM vyhovuje požadavkům na kategorii 6, 6A a splňuje kabelové normy pro výkon dané kategorie.



Obr. 4.13 Rozhraní mezi keystone jacky a e-modulem

Zde jsou uvedeny základní vlastnosti propojovacího panelu MIIM:

- Možnost ukončování za použití standardních zatlačovacích nástrojů.
- Vestavěná přihrátka pro správu kabelů zajišťující požadavky na ohyb kabelů.
- Konfigurovatelnost pole dle kategorie 6 nebo 6A pro standard 586A/B.
- Propojení datové sběrnice se skenerem MIIM pomocí standardních propojovacích kabelů s konektorem RJ45.
- Dva indikátory stavu napájení pro zajištění řádného přívodu energie ze skeneru.

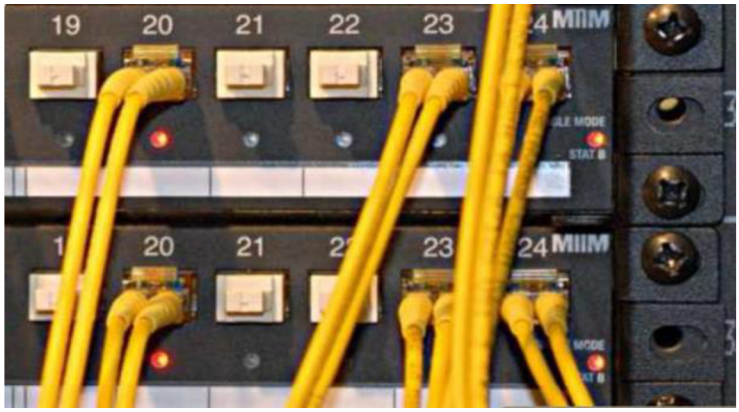
4.3.4 MIIM Duplex LC Fiber propojovací panel

Molex v rámci svého systému MIIM nabízí pro propojovací část i řešení pro optickou kabeláž. Řešení však nenabízí úplně stejné vlastnosti jako v případě systému pro metalickou kabeláž a zjištění připojení kabelu je také řešeno odlišně. Z tohoto

důvodu je nutné využít také speciální propojovací panel (viz obr. 4.14), a navíc také i speciální propojovací kabel. Monitoring neprobíhá end-to-end, ale pouze v propojovací zóně mezi panely. Je nutné tedy využívat dvojitou reprezentaci. Optické panely nesledují stejné vlastnosti jako u metalické kabeláže.

Obr. 4.14 MIIM optický propojovací panel [20]

MIIM optický panel obsahuje 24 duplexních LC adaptérů. Každý MIIM optický panel o velikost 1U má na zadní straně propojovací port datové sběrnice. Propojovací port datové sběrnice spojuje optický panel MIIM se skenerem prostřednictvím standardního propojovacího kabelu s konektorem RJ45. Dva zabudované indikátory v panelu zajišťují viditelnost stavu napájení panelu ze skeneru. Při připojení ke skeneru MIIM panely detekují aktivitu připojení na každém duplexním LC portu. Pokud panel není připojený ke skeneru, tak pracuje jako běžný propojovací panel. Stejně jako u panelu pro metalickou kabeláž, tak každý port má LED diodu, která navádí správce IT při přepojování (viz obr. 4.15) [9] [20].



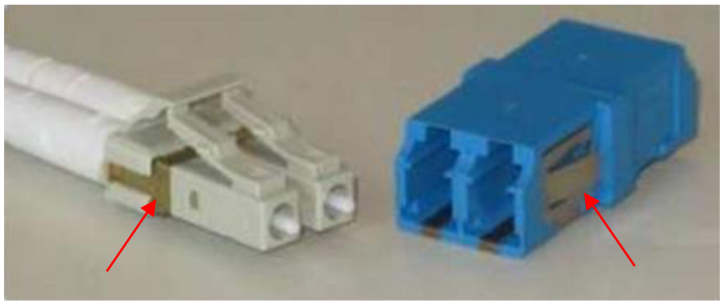
Obr. 4.15 Přední strana MIIM Fiber propojovacího panelu [9]

Zde jsou uvedené základní vlastnosti optického panelu MIIM:

- Dva indikátory pro zjištění stavu správného připojení napájení ze skeneru.
- Využívá standardní propojovací kabely s konektorem RJ45 pro připojení datové sběrnice ke skeneru MIIM.
- Vysunovací police pro vedení kabelu.
- Panel lze využít pro single mode i multi mode vedení.

4.3.5 MIIM Fiber propojovací kabel

Jak již bylo zmíněno v předchozí části, tak řešení pro optickou kabeláž funguje na jiném principu a je omezenější než v případě metalické kabeláže. Zde je nutné využívat speciální optický propojovací kabel (obr. 4.17). MIIM Fiber optický propojovací kabel se využívá pro propojení MIIM optických panelů v rámci systému MIIM. MIIM FIber propojovací kabely obsahují metalický monitorovací kabel spolu s kontaktními piny na konektorech propojovacích kabelů (viz obr. 4.16), které aktivují detekční mechanismus v propojovacím panelu MIIM. Při použití se zbytkem systému MIIM budou propojovací kabely poskytovat informace o připojení k systému MIIM [9] [21].



Obr. 4.16 Kontaktní piny pro detekci kabelu [9]

Zde jsou uvedené základní vlastnosti MIIM optického propojovacího kabelu:

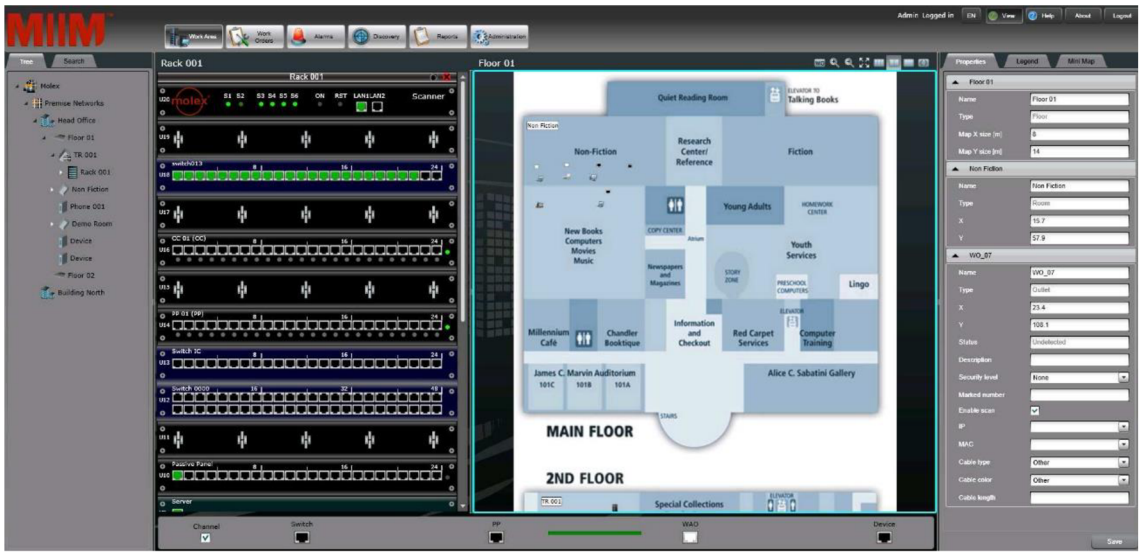
- Robustní vlákna.
- Dostupné single mode (OS1, OS2) a multi mode (OM1, OM2, OM3, OM4) provedení.
- Standardní materiál pláště je LSOH.
- MIIM optické propojovací kabely jsou konstruovány ze dvou vláken obsažených ve vnějším plášti.
- Monitorovací kontaktní rozhraní pro propojovací MIIM panely.

Obr. 4.17 MIIM Fiber propojovací kabel [21]

4.3.6 Aplikační software MIIM

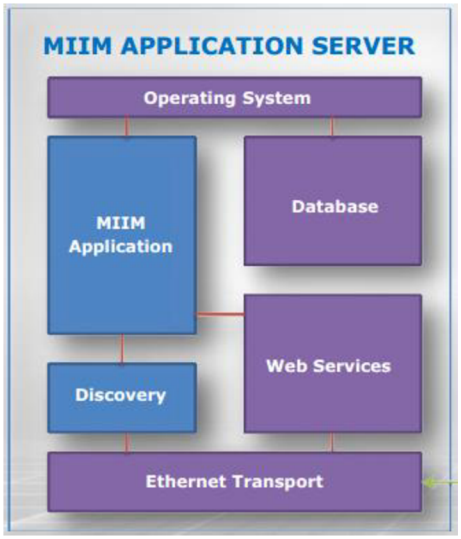
Aplikační software pro řešení MIIM je program typu klient – server, který slouží k centrální správě dat systému MIIM. Spravuje aktiva fyzické vrstvy a poskytuje okamžité informace IT správcům ohledně konektivity kanálů podporující řešení MIIM. Daný software dokumentuje plánované i neplánované změny v síti. Umožňuje nepřetržitý monitoring kanálu od datové zásuvky až po aktivní síťový prvek. Aplikace využívá inteligentní dotazování k automatizovanému sledování událostí o připojení a odpojení, aktualizace veškerých změn do databáze, identifikace a potvrzení volného portu a oznámení správci IT o všech neplánovaných a neautorizovaných změnách v síti. Inteligentní dotazování je vyvoláno aktualizacemi ze skeneru. Software tak umožňuje globální přístup k síti a cenově dostupnou pokročilou správu sítě. MIIM server podporuje neomezený počet skenerů, avšak skener může být nakonfigurován pouze pro komunikaci s jedním MIIM serverem. Skener nemusí být přímo připojen k serveru, ale server se tak může nacházet kdekoliv v rámci lokální sítě.

Pro správu MIIM se využívá aplikace postavená na webovém rozhraní (viz obr 4.18). MIIM server tak funguje jako rozhraní webové služby pro centrální databázi a aplikaci. Klient tak k rozhraní systému MIIM přistupuje prostřednictvím svého webového prohlížeče odkudkoliv z lokální sítě. Server pro svou činnost vyžaduje spojení se skenerem. Server se dotazuje skeneru a získané informace si poznamenává do databáze. Zpracování dat zahrnuje integraci s pracovními úlohami (work orders) a upozornění na nesrovnalosti navržené síti v MIIM oproti skutečnému stavu sítě.



Obr. 4.18 Prostředí aplikace MIIM [22]

Na obr. 4.19 vidíme blokové schéma aplikačního serveru MIIM. Modré bloky znázorňují součástí poskytnuté řešením MIIM, tedy samotná MIIM aplikace a modul Discovery pro dotazování. Ostatní fialové bloky reprezentují součásti poskytnuté další stranou (např. databáze, atd.). Příklad konkrétních součástí nutné pro provoz systému MIIM je popsán v následující podkapitole [22] [23].



Obr. 4.19 Struktura MIIM serveru [22]

Zde jsou uvedené základní vlastnosti aplikačního softwaru řešení MIIM:

- neomezený počet uživatelů na licenci,
- k dispozici sada pro tvorbu reportů o správě,
- otevřená systémová architektura umožňuje propojení s dalšími aplikacemi pro správu sítě,
- aktiva L1 vrstvy lze propojit s mapou budovy,
- logy událostí pro záznamy auditu,
- funkce pro snadné vyhledávání aktiv a informací,
- umožňuje řízené propojování,
- monitorování konektivity a zařízení, i když je koncové zařízení vypnuté,
- inteligentní dotazování udržuje data aktuální a minimalizuje zatížení šířky pásma sítě,
- monitoring událostí o připojení a odpojení,
- hierarchický pohled na podnikovou infrastrukturu v rámci L1 vrstvy až k datové zásuvce.

4.3.6.1 HW a SW nároky MIIM aplikačního serveru

Jak je zřejmé z textu výše, tak softwarové řešení MIIM obsahuje serverovou a klientskou část. Klient k aplikaci přistupuje prostřednictvím webového prohlížeče. Nutností je mít i nainstalované rozhraní Silverlight od společnosti Microsoft. Z tohoto důvodu jsme však omezení na webový prohlížeč Internet Explorer. Většina ostatních prohlížečů ukončila podporu rozhraní Silverlight z důvodu ukončeného vývoje samotnou společností Microsoft. V následující tab. 4.1 jsou zmíněné doporučené HW a SW nároky pro provoz MIIM serveru [23].

Tab. 4.1 HW a SW nároky MIIM aplikačního serveru

Operační systém	Microsoft Windows (Server 2008 R2 nebo 2012)
Procesor	Intel Core Duo nebo AMD řady Athlon/X2/Opteron nebo kompatibilní s frekvencí 2 GHz nebo vyšší
Paměť	4 GB nebo více
Místo na HDD	50 GB
Síť	síťová karta 10/100/1000 Mb/s
Databáze	Microsoft SQL Server (Express)
Služba	Microsoft IIS
Rozhraní	Microsoft .NET Framework 4, Crystal Reports Developer Edition for Visual Studio, Java 6 Std Edition v1.6 Update 24 (nebo novější)

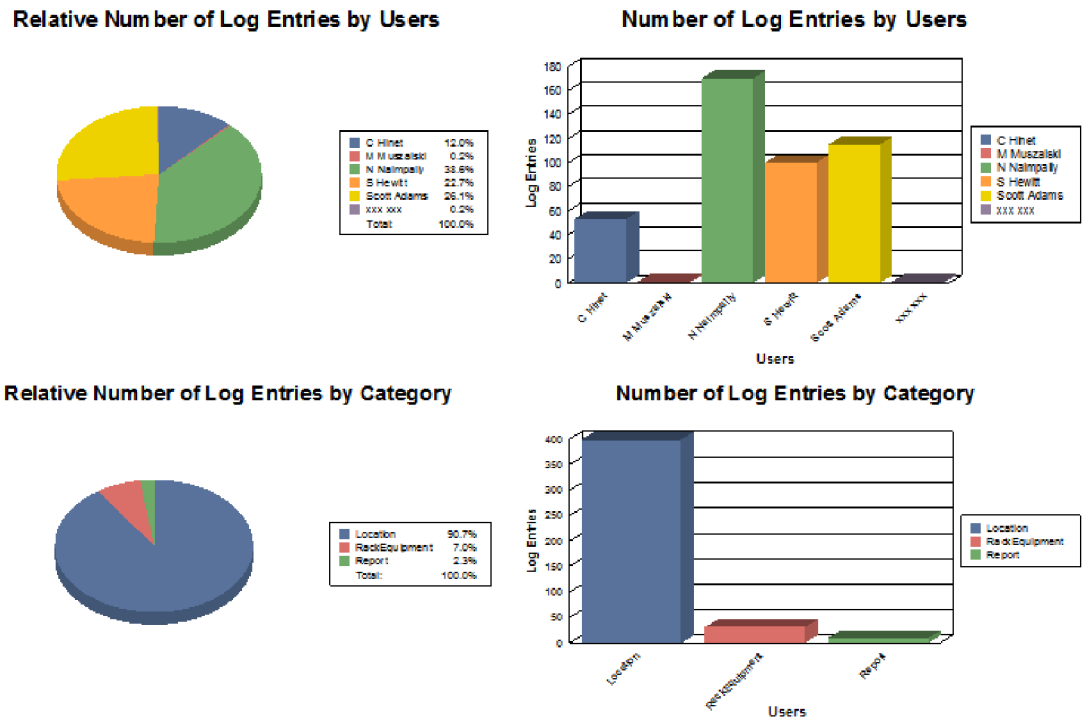
4.3.6.2 MIIM reporty

Systém MIIM obsahuje modul pro poskytnutí reportů různých událostí. Data jsou základním prvkem systému MIIM a správci sítě poskytuje tyto data ve srozumitelné podobě prostřednictvím různých typů grafů (viz obr. 4.20). Systém umožňuje nastavit, jak často se má provádět reporting událostí (např. denně, týdně, měsíčně). Lze tedy definovat přesné datum a čas reportingu. Samozřejmostí je i možnost reportování vypnout. Reporting systému MIIM je vhodnou utilitou, která správců sítí poskytuje důležité informace například pro monitoring nebo při dalším plánování návrhu sítě. Aplikace má v základu několik typů sestav, které však můžeme upravovat dle vlastních potřeb:

- Work Orders Report,
- Alarms Report,
- Log Report,
- Rack Equipment Report,

- Outlets Report,
- Devices Report,
- Channel Report.

Každý typ šablony má různá filtrovací kritéria a různé typy grafů, které si lze vybrat.



Obr. 4.20 Příklad výstupních grafů z reportovacího modulu

Výstupními formáty reportovacího modulu systému MIIM jsou následující:

- Crystal Report (SAP),
- Excel,
- Word,
- PDF.

4.3.7 Discovery Engine

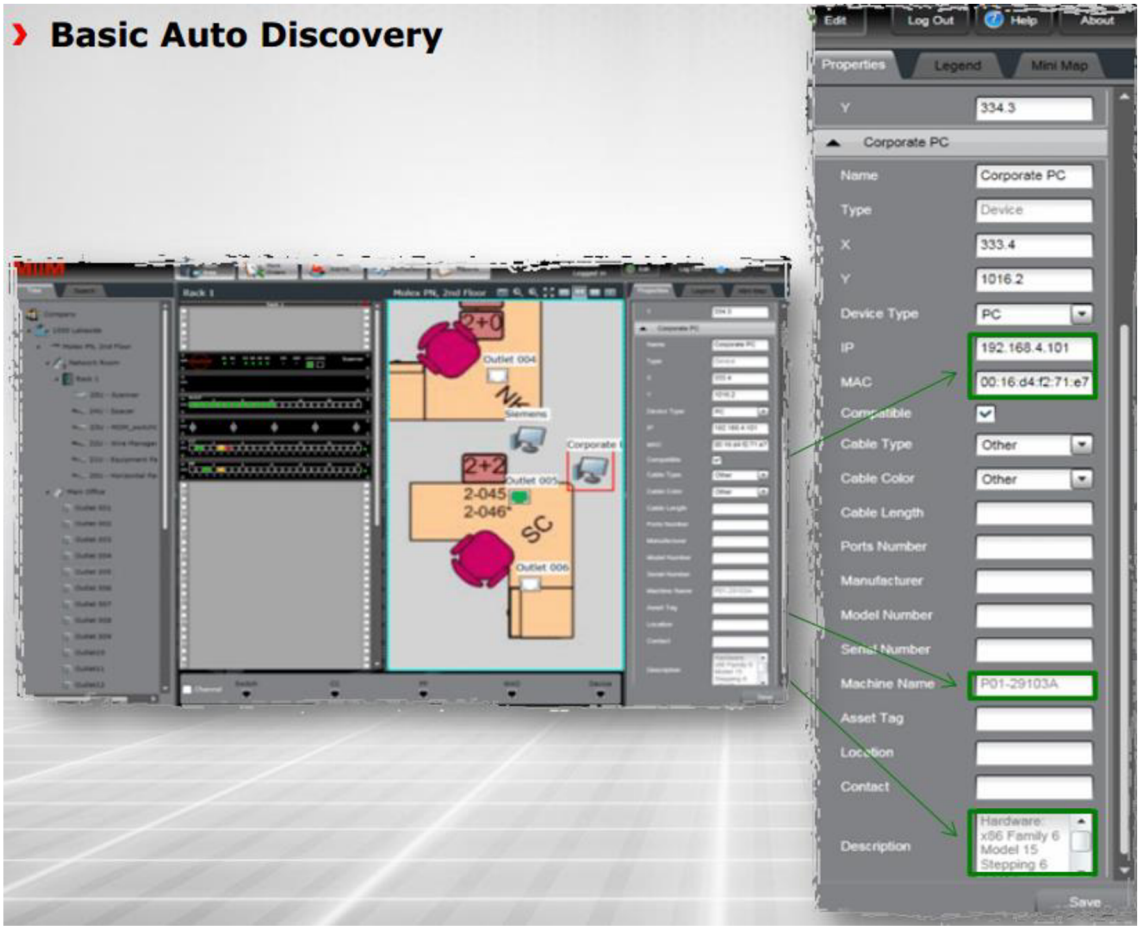
MIIM Discovery Engine sdružuje objevená zařízení s fyzickými kanály a místy v mapách budov a zjištění aktuálních dat z tabulek přepínačů.

Metoda Discovery se používá k dotazování zařízení v sítí využitím ARP tabulek, položek DNS a tabulek přepínačů. LAN podsítě a plánované oblasti, které mají být dotazovány, jsou definovány uživatelem. MIIM Discovery Engine spravuje tabulku všech

zařízení spolu s jejich MAC adresami, IP adresami a místem v plánu, kde jsou ve vaší síti připojeni. Metody použité Discovery Engine zahrnují Auto-Discovery a Event-Driven Discovery (EDD). Metoda EDD je právě v rámci řešení MIIM unikátní od ostatních výrobců [24].

4.3.7.1 Metoda Auto-Discovery

Metoda Auto-Discovery identifikuje informace týkající se síťového zařízení připojeného ke koncovým datovým zásuvkám. Auto-Discovery se na vyžádání dotazuje síťových zařízeních k logickému mapování sítě (viz obr.4.21). Tyto informace zahrnují IP, MAC adresu a název zařízení (je-li povolen protokol SNMP). Každá položka je spojena s fyzickou polohou a mapou připojení. Metodě můžeme definovat LAN podsíť, na které budeme provádět identifikaci zařízení. Auto-Discovery může také hlásit více aktiv v jedné zásuvce (PC+ VoIP telefon) [24].



Obr. 4.21 Aplikace Discovery metody [24]

4.3.7.2 Metoda Event-Driven Discovery

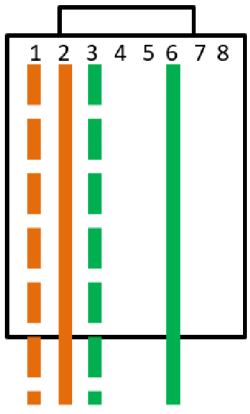
Metoda EDD se realizuje pouze, když je zařízení přidáno k úplnému kanálu. Po zjištění připojeného zařízení systém MIIM automaticky zjišťuje z aktivního prvku adresu IP, MAC adresu a název zařízení a přidružuje tyto informace k datovému kanálu. EDD bude se bude pouze dotazovat kanálů, které se změnily, tím tak šetří šířku pásma sítě. Změna na propojovacím panelu nebo koncové zásuvce vyvolá EDD. Pouze částečně navázané kanály dotazování EDD nespouštějí.

EDD se realizuje ve stavu kompletního kanálu a používá změnu fyzické konektivity k cílení k dotazování konkrétního přepínače pro adresy MAC a IP, po němž následuje dotazování samotného zařízení pro jeho název [24].

5 SLABINY SYSTÉMU MIIM

Společnost Molex spolu se svým systémem MIIM poskytuje i soubor zásad, které je nutné při implementaci a provozu dodržovat tak, aby systém poskytoval plnou funkcionalitu. Příkladem takové zásady může být způsob propojování v rámci propojovacích panelů. Systém MIIM dovoluje pouze propojení mezi CC a PP panelem. Další možnosti jako například propojení pouze v rámci PP nebo CC panelu, propojení jednoho panelu (PP nebo CC) přímo s aktivním prvkem, propojování s jinou propojovací zónou obsluhovanou jiným skenerem nejsou v rámci těchto zásad dovoleny. Případné porušení některé z těchto zásad systém MIIM nedokáže rozpoznat, pouze detekuje stav připojeného kabelu v portu panelu, ale nedokáže detekovat propojení, ani zbytek datového kanálu. Je nutné využívat ethernetové kabely se všemi zapojenými čtyřmi páry. Využití kabelů se dvěma páry (typicky standard 10BaseT a 100BaseT) vede opět k neúplné detekci a stavu, který systém neočekává.

MIIM vykazoval problémy s detekcí připojení nestandardních zařízení. Konkrétně se může jednat o zařízení s upraveným portem síťové kartě, které má vyvedené pouze piny zeleného a oranžového páru postačujícího pro 100megabitovou konektivitu. Jelikož systém pro detekci připojeného zařízení využívá měření odporu na kombinaci bílo-hnědého a oranžového pinu, tak systém toto zařízení není schopen detekovat, i když je aktivní. Stejná situace nastane i při použití kabelu mezi datovou zásuvkou a koncovým zařízením se zapojeným oranžovým a zeleným párem. Společnost Molex na tuto situaci v instalačních zásadách systému MIIM poukazuje tak, že systém je určen pouze pro připojování ethernet zařízení a kabelů minimálně Cat5e se všemi osmi vodiči zapojenými v konektoru.



Obr. 5.1 Zapojení konektoru dle standardu 100BaseT

Tab. 5.1 Význam pinů zapojení 100BaseT

Pin	Popis	Význam
1	TD+	Transmit+
2	TD-	Transmit-
3	RX+	Receive+
4	-	-
5	-	-
6	RX-	Receive-
7	-	-
8	-	-

U první generace systému MIIM, který neobsahoval v propojovacích panelech mikrospínače, byla problematická detekce nových propojení portů při skenování. To bylo způsobeno využitím levných přepínačů, které pro snížení nákladů využívají společné zakončení pro více portů. Jelikož porty přepínače měly společný obvod, tak v rámci skenování při vystavení napětí PP panelem na CC panel často docházelo k tomu, že se dané napětí vystavilo na společně zakončených portech přepínače zpět na CC a systém MIIM napětí detekoval na jiných portech CC panelu, než byl fyzicky připojen kabel a vedlo to k neúplné a nesprávné detekci systému. Molex tento problém u nové generace panelů řeší zavedením mikrospínačů do jednotlivých portů. Při zapojení kabelu a sepnutí tlačítka tak systém už předpokládá dopředu, na kterém portu CC detekovat napětí.

Zároveň u systému první generace detekce nového datového kanálu možná až při dalším cyklu full patchcord scanu, jelikož panely neobsahovaly mikrospínače a systém tak po určitou dobu nevěděl o případných nových kanálech. Systém MIIM tento nedostatek vyřešil taktéž za pomocí mikrospínačů, které při sepnutí okamžitě vyvolají událost a skener provede fast scan nového kanálu.

Při využití zařízení napájené typem PoE se stává implementace systému MIIM komplikovanější. V současnosti existují způsoby řešení PoE, které zařízení využívají: režim A a režim B. Bližší popis těchto režimů je nad rámec této práce. Při implementaci systému MIIM a PoE musíme prostřednictvím MIIM serveru definovat na propojovacích panelech, v jakém režimu budou pracovat. Panely nemohou pracovat zároveň v obou režimech. Je tedy nutné v rámci implementace panely rozdělit na více skupin, kde každá bude podporovat zařízení pro jeden daný režim PoE. Zároveň nelze v rámci implementace systému MIIM zapojit do datové zásuvky zapojit zdroj PoE [9].

5.1 Další možnosti bezpečnosti fyzické vrstvy

Spousta společností se snaží řešit kybernetické útoky pouze softwarovými řešeními, ale neuvědomují si, že riziko napadení může přejít i zevnitř organizace. Většina společnosti řeší situaci zavřenými dveřmi od serverové místnosti, ale neuvědomují si, že nejsou chráněná další místa, kde se může útočník připojit do síťové infrastruktury (např. volné datové zásuvky v kanceláři). Kromě použití managementu fyzické vrstvy můžeme rozšířit bezpečnost horizontální a páteřní (vertikální) kabeláže i o další její prvky. Tím i zároveň eliminujeme riziko připojení upraveného kabelu (viz předchozí kapitola) [25].

Implementaci lze provést dvěma způsoby:

- Implementovat zabezpečení rovnou do datových zásuvek a rozvaděčů.
- Doplnit stávající kabeláž o prvky zabezpečení.

5.1.1 Přímá implementace prvků

Volbu přímé implementace zvolíme tehdy, pokud návrh a budování sítě řešíme od samotného začátku. Prvky můžeme použít jak pro metalickou, tak i optickou kabeláž. Tyto prvky reprezentují nejčastěji konektory v datové zásuvce nebo propojovacím panelu. Mezi největší výrobce těchto prvků pro bezpečnější fyzickou vrstvu patří například společnost Commscope. Metalická kabeláž založena na konektoru RJ-45 s mechanickou úpravou. Použít lze tak pouze speciální propojovací kabel. Konektory jsou dostupné pro různé kategorie (např. Cat5e, Cat6A), v nestíněném i stíněném provedení. Existuje celá řada hardwarových variant (hardwarových klíčů), které se často odlišují barevným kódováním. Nelze například připojit klíčovaný kabel do konektoru s odlišnou barvou. Připojením klasickým propojovacím kabelem tak není umožněno z důvodu fyzického rozdílu. V případě optických rozvodů (horizontální i páteřní) je situace například u konektorů LC a MP0 stejná.

Obr. 5.2 Klíčované kabely [25]

Obr. 5.3 Barevné klíčování [26]

5.1.2 Dodatečná implementace prvků

V případě již instalované kabeláže lze využít řešení prvků pro dodatečnou ochranu. Propojení mezi porty propojovacích panelů v datovém rozvaděči nebo od datové zásuvky po koncové zařízení lse realizovat pomocé zamykacího propojovacího kabelu. Tento kabel může být ve dvou variantách:

- Zamykání na obou stranách (přímé fixní propojení dvou zařízení).

Obr. 5.4 Propojovací kabel se zamykáním na obou stranách [25]

- Zamykání na jedné straně (propojení zafixované klíčem na straně datové zásuvky, druhá strana může být fixována uvnitř propojovacího zařízení např. IP kamera s krytem).

Obr. 5.5 Propojovací kabel se zamykáním na jedné straně [25]

Místem ohrožením mohou být instalované zásuvky ve veřejných prostorech s větším přístupem osob. Zde může například použít například zamykací dvouportové zásuvky, které vyhovují krytí IP44.

Obr. 5.6 Zamykací dvouportová zásuvka [25]

Podobným příkladem ohrožení mohou být zasedací místnosti, kde je předinstalován propojovací kabel. Zde můžeme využít dodatečné hardwarové krytí za pomocí zamykací koncovky.

Obr. 5.7 Zamykací koncovka [25]

V případě volných portů na aktivních prvcích nebo datových zásuvkách můžeme použít pro jejich zaslepení zamykací konektor nebo blokátory. Ty zabrání případnému útočníkovi k přímému připojení vlastního zařízení.

Obr. 5.8 Zamykací konektor [25]

Obr. 5.9 Blokátory portů [26]

6 SROVNÁNÍ ŘEŠENÍ MIIM S KONKURENCÍ

Trh s výrobci systému managementu sítě fyzické vrstvy je poměrně rozsáhlý. Důvodem je rok od roku zvětšující se poptávka po systémech managementu fyzické vrstvy napříč všemi kontinenty. Největší růst poptávky je hlavně ve finančním sektoru a datacentrech. Mezi největší výrobce těchto systémů patří následující: Commscope, iTracs, RiT, Panduit, popřípadě další jejich smluvní partneři.

V rámci této diplomové práce byla provedena i základní analýza řešení některých konkurenčních výrobců systémů pro management sítě fyzické vrstvy s různými principy monitoringu, hlavně co se týče schopnosti monitoringu datového kanálu. Cílem je tak porovnat výhody řešení MIIM od řešení ostatních konkurentů na trhu.

6.1 Situace pro srovnání s konkurencí

Porovnání monitoringu na následujících situacích:

- **Falešné propojení**
  - Situace, kdy v plánovaném propojení portů mezi panely je do jednoho portu panelu zapojen jeden propojovací kabel a do portu druhého panelu další kabel. Oba tyto kabely na druhém konci zůstanou nepřipojeny.
- **Přestřižení propojení**
  - Situace, kdy v realizovaném propojení mezi propojovacími panely daný kabel přestřihneme.
- **Horizontální kabeláž**
  - Jedná se o kabel mezi propojovacím panelem reprezentující datové zásuvky (panel PP) a samotnou datovou zásuvkou. Situace určuje, zda systém je schopen reagovat na případné přerušení dané linky.
- **Detekce zapnutého koncového zařízení**
  - Schopnost detekovat odpojení/připojení zapnuté koncové stanice.
- **Detekce vypnutého koncového zařízení**
  - Schopnost detekovat odpojení/připojení koncové stanice i v případě, že je vypnuté.

6.2 Výsledné srovnání

V tab. 6.1 můžeme vidět porovnání jednotlivých řešení při různých situacích popsaných v předchozím textu.

Tab. 6.1 Srovnání různých řešení pro management fyzické vrstvy

Výrobce řešení	Princip monitoringu	Falešné propojení	Přestřižení propojení	Horizontální kabeláž	Zapnuté koncové zařízení	Vypnuté koncové zařízení
Commscope imVision/Systimax	Senzor (mikrospínač)	✗	✗	✗	✓ SNMP	✗
Panduit PanView IQ	9-pin	✓	✓	✗	✓ SNMP	✗
Belden Patch Pro	RFID čip	✗	✗	✗	✓ SNMP	✗
Molex MIIM	impedanční vlastnosti/ mikrospínač	✓	✓	✓	✓	✓

V případě Commscope imVision a Panduit PanView IQ využívající princip senzoru v portu a čipu na propojovacím kabelu nejsme schopni detekovat falešné propojení nebo jeho přestřižení. To je způsobeno tím, že tyto řešení monitorují stav, zda jsou příslušné porty fyzicky na panelech obsazeny, nikoliv nekontroluje propojení samotné. U systému Panduit s principem devátého pinu v propojovacím kabelu bychom v případě falešného propojení nevytvořili monitorovací smyčku a v případě přestřižení bychom tuto smyčku přerušili.

První jasnou výhodu nad uvedenými má systém MIIM v monitoringu kontinuity horizontální kabeláže. Ostatní výrobci by případné přerušení této linky nebyli schopni detekovat.

Všechny uvedená řešení umí detekovat koncová zařízení, ale společnost Molex se svým řešením MIIM je unikátní v tom, že dokáže připojené koncové zařízení v datové zásuvce detekovat i vypnuté. Ostatní výrobci monitorují připojené koncové zařízení na základě aktivity portu přepínače. Tuto informaci získává prostřednictvím SNMP protokolu. V případě vypnutého koncového zařízení je port na přepínači neaktivní a systém není schopen monitorovat to, zda koncové zařízení nebylo odpojeno.

Princip postavený na RFID čipu a 9-pinu lze také poměrně snadno podvrhnout. Při připojení klasického propojovacího kabelu do propojovacích

panelů postavených na těchto principech, systém tuto událost nedetekuje a v softwaru pro management realizovaný propoj nevidíme, i když spojení je aktivní.

Další unikátnost řešení MIIM je v metodě Event-Driven Discovery. Ostatní systémy konkurenčních společností se na informace (IP, MAC, název) dotazují v pravidelných cyklech a více tak zatěžují síťovou infrastrukturu.

7 ZÁVĚR

Bezpečnost je často jen iluzí, jejíž důvěryhodnost zvedá zejména naivita a nevědomost pracovníků organizace. Bezpečnostním produktům se nesmí slepě a bezmezně důvěřovat. Jinak bychom se v opačném případě nechali unést pouhou iluzí bezpečnosti, která nebude nikdy 100%. Každý bezpečnostní proces je nutné implementovat, a to jak samotnou technologii, tak i pravidla. Zmíněná pravidla musí dodržovat například všichni zaměstnanci společnosti. Navíc je nutné provádět nahodilé testy bezpečnostní kontroly, při nichž například zjistíme, zda určité osoby pravidla neopomíjí a neporušují.

Přirozené je domnívat se, že bezpečnostní technologie nás ochrání před zlomyslným narušením bezpečnosti. V takovém případě chápeme význam bezpečnosti pouze z části, jelikož zapomínáme na ten vůbec nejslabší článek – lidský faktor.

Systémy pro management fyzické vrstvy je vhodný a užitečný pro správu a organizaci podnikové sítě. Tyto systémy monitorují propojovací zónu, popřípadě některé systémy jsou schopny monitorovat i celý kanál jako například uvedený systém MIIM. Unikátnost tohoto systému je i v jeho dotazovací metodě Event-Driven Discovery, která se dotazuje pouze v případě události v rámci kompletního kanálu a nezatěžuje infrastrukturu periodickými dotazy. Software, spravující daný systém, poskytuje správců možnost sledovat virtuální obraz fyzické sítě, plánovat změny v síti a hlídat jejich realizaci. Z bezpečnostního hlediska systém přispívá ke zvýšení bezpečnostní úrovni sítě, a to díky možnosti upozornění na neautorizované zásahy do firemní sítě (například neočekávané odpojení počítače z datové zásuvky v kanceláři). Nelze však tyto systémy považovat za úplný bezpečnostní prvek sítě sám o sobě, který je schopen ochránit síť před útoky. Poskytuje pouze informační hodnotu pro bezpečnost, kdy jsme schopni určit, že například ve firmě bylo provedeno útočníkem neautorizované připojení koncového zařízení, kdy a ve které místnosti tato událost nastala Pro účinnější ochranu a prevenci před případným útokem je nutné kombinací využít dalších prvků fyzické vrstvy (např. klíčované kabely) a služeb vyšších vrstev (např. omezení portu přepínače na připojení zařízení s určitou MAC adresou, umístění nevyužitých portů do speciální VLAN). Samozřejmostí by mělo být i striktní omezení přístupu do telekomunikační místnosti, která by měla být nejlépe hlídána elektronickým zabezpečovacím systémem v případě násilného vniknutí. Zároveň by v rámci neobsazených koncových zásuvek nemělo být realizované propojení v rámci propojovacích panelů.

Při implementaci systému je i důležité striktně dodržovat zásady pro instalaci, které můžou definovat požadovaný hardware a způsob práce se systémem, tak by poskytoval plnou funkcionalitu a vyhnuli jsme se případným slabinám.

Z ekonomického hlediska při budování sítě se systémem pro management fyzické vrstvě jsou náklady navýšeny. Tyto navýšení na výstavbu sítě se pohybují v rozmezí 20–50 %. Přesné navýšení nákladu se odvíjí od velikosti a rozložení síťové infrastruktury. Samozřejmě cena se odvíjí i od konkrétního výrobce systému. Mnoho výrobců systémů zdůvodňuje, že se jedná investici, která se určitě vrátí v podobě bezpečnější a spolehlivější sítě i mzdové náklady.

Počátkem roku 2018 však byla pozastavena distribuce systému MIIM samotným výrobcem. Důvodem jsou patentové spory s izraelskou startupovou firmou, která vlastní patenty na detekci zařízení měřením impedančních vlastností v síti. Společnost Molex by měla v blízké budoucnosti přijít s novým řešením a zároveň upustit od předchozího. Nový systém by měl nést název MIIM-lite a bude postaven pouze na principu podobnému mikropřepínačů/senzorů v portech propojovacích panelů, které využívali i u stávajícího řešení. Systém se tedy srovná se svou konkurencí a zaměří se pouze na monitoring propojovací zóny. Zároveň by měl probíhat vývoj vlastního řešení, který jim umožní opět monitorovat celý kanál. Bližší podrobnosti v době psaní této práce zatím nejsou známy.

V rámci přílohy k této diplomové práci byla zpracována i laboratorní úloha, která studenta seznámí se základní administrací systému, simulací možných scénářů přerušení kabeláže a jejich detekci systémem a realizaci prosté slabiny systému, kterou není schopen detekovat. Tato úloha najde uplatnění zejména v předmětech zabývající se správou a bezpečností podnikových sítí.

Na úplný závěr je vhodné dodat, že „skutečnou“ bezpečnost nelze zakoupit v nějakém jednom produktu. Je to ve skutečnosti celá řada procesů, do něhož je kromě produktů zapojen i lidský faktor (například zaměstnanci společnosti).

Literatura

[1] MOLEX. *Module 03 MIIM Design* [online]. USA: Molex, 2015, 76 s. [cit. 2017-11-15].

[2] DEBENEDICTS, Damon. Integrating Physical Layer Management Systems into Today's Networks. *DataCenterKnowledge* [online]. 2014 [cit. 2017-11-115]. Dostupné z: http://www.datacenterknowledge.com/archives/2014/11/03/integrating-physical-layer-management-systems-todays-networks

[3] Intelligent Patching: DCIM, IPLMS, IIMS, or AIM?. POULOS, Kirsten. *Belden* [online]. 2015 [cit. 2017-11-15]. Dostupné z: https://www.belden.com/blog/data-centers/Intelligent-Patching-DCIM-IPLMS-IIMS-or-AIM

[4] NACHMONI, Oded. The Security Advantage of Intelligent Physical Layer Management. *Advancing Information Transport Systems* [online]. 2016, , 2 [cit. 2017-11-15]. Dostupné z: http://www.rittech.com/_Uploads/dbsAttachedFiles/Security-Advanced-IPLM.pdf

[5] Moves, adds and changes (MAC). ROUSE, Margaret. *SearchDataCenter* [online]. 2015 [cit. 2017-11-115]. Dostupné z: http://searchdatacenter.techtarget.com/definition/moves-adds-and-changes-MAC

[6] CARL, Lea. What is Automated Infrastructure Management?. *NetworksAsia* [online]. 2016 [cit. 2018-04-16]. Dostupné z: https://www.networksasia.net/article/what-automated-infrastructure-management.1472343848

[7] NETWORK GROUP, S. R. O. MIIM. NETWORK GROUP, S. R. O. *NWG* [online]. b.r. [cit. 2017-11-15]. Dostupné z: http://www.nwg.cz/index.php?module=shop_catalog&action=list_products&id=132

[8] Inteligentní sítě – management na fyzické vrstvě. HELÁN, Radek. *NetGuru* [online]. 2010 [cit. 2017-11-15]. Dostupné z: http://netguru.cz/component/content/article?id=615

[9] MOLEX. *Module 04 MIIM Hardware Installation / Hands on* [online]. USA: Molex, 2015, 34 s. [cit. 2017-11-15].

[10] AMPTrac - Systém pro monitorování a management fyzické vrstvy. FLEISCHNER, Michal. *Svět sítí* [online]. 2005 [cit. 2017-11-15]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=AMPTrac-System-pro-monitorovani-a-management-fyzicke-vrstvy-252005

[11] KELINE. KELine® Intelligent system for monitoring and management of physical layer network. KELINE. *KELine* [online]. b.r. [cit. 2017-11-15].

Dostupné z: http://www.keline.com/a/36/keline-intelligent-system-for-monitoring-and-management-of-physical-layer-network

[12] PANDUIT PVQ-PM inteligentní skener portů patch panelu PViQ. *Lancomat* [online]. b.r. [cit. 2017-11-15]. Dostupné z: https://www.lancomat.cz/pvq-pm-inteligentni-skener-portu-patch-panelu-pviq-p18437/

[13] Quareo ICM - Monitoring fyzické vrstvy. *Category* [online]. b.r. [cit. 2017-11-15]. Dostupné z: http://www.category.cz/oblasti/provoz-siti/quareo-icm-monitoring-fyzicke-vrstvy

[14] MOLEX. About us. MOLEX. *Molex* [online]. b.r. [cit. 2017-11-15]. Dostupné z: http://www.molex.com/molex/about/about-us.jsp

[15] MOLEX. MIIM. MOLEX. *Molex CES* [online]. b.r. [cit. 2017-11-15]. Dostupné z: http://www.molexces.com/webfoo/wp-content/uploads/MIIM-Flyer-USA-2012-1ec69e09-6a01-402f-aa89-d8ae84a59e14-4.pdf

[16] MOLEX. *Module 05 Recognizing the MIIM Scanner* [online]. USA: Molex, 2015, 42 s. [cit. 2017-11-15].

[17] MOLEX. MIIM 576 Channel Scanner. MOLEX. *Molex CES* [online]. 2016 [cit. 2017-11-15]. Dostupné z: http://www.molexces.com/product/ims-00100-miim-576-channel-scanner/

[18] MOLEX. PowerCat 6 MIIM Outlet Terminator – pack of 24. MOLEX. *Molex CES* [online]. 2016 [cit. 2017-11-15]. Dostupné z: http://www.molexces.com/product/imt-00100-powercat-6-miim-outlet-terminator-pack-of-24/

[19] MOLEX. MIIM G2 Category 6, 1U, 24 Port Patch Panel 568A/B. MOLEX. *Molex CES* [online]. 2016 [cit. 2017-11-15]. Dostupné z: http://www.molexces.com/product/miim-g2-category-6-1u-24-port-patch-panel-568ab/

[20] MOLEX. MIIM Single Mode 24P Duplex LC Fiber Patch Panel. MOLEX. *Molex CES* [online]. 2016 [cit. 2017-11-15]. Dostupné z: http://www.molexces.com/product/rfr-00300-miim-single-mode-24p-duplex-lc-fiber-patch-panel/

[21] MOLEX. MIIM Fiber Optic Patch Cord. MOLEX. *Molex CES* [online]. 2016 [cit. 2017-11-15]. Dostupné z: http://www.molexces.com/product/91-pp-4a2-00300-miim-fiber-optic-patch-cord-ofpc-lc-lc-dup-mm-om4-3m-ls0h/

[22] MOLEX. *Module 07 MIIM Application Overview* [online]. USA: Molex, 2015, 45 s. [cit. 2017-11-15].

[23] MOLEX. *Module 06 MIIM Application Installation on 2008R2 Platform for your MIIM KIT* [online]. USA: Molex, 2015, 126 s. [cit. 2017-11-15].

[24] MOLEX. *Module 11 Event-Driven Discovery and Auto-Discovery* [online]. USA: Molex, 2015, 28 s. [cit. 2017-11-115].

[25] TŘÍSKA, Zdeněk. Kybernetická bezpečnost: pasivní vrstva, často podceňovaná součást. *NetGuru* [online]. b.r. [cit. 2018-04-01]. Dostupné z: http://www.netguru.cz/novinky/3635-kyberneticka-bezpecnost-pasivni-vrstva-casto-podcenovana-soucast

[26] SEDLÁK, Petr. Management bezpečnosti fyzické vrstvy. *Vut-vsb.cz* [online]. 2013 [cit. 2018-04-18]. Dostupné z: https://vut-vsb.cz/home/get-file?file=203&amp%3Bportal=Portal2

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AIM	-	Automated Infrastructure Management
ANSI	-	American National Standards Institute
DCIM	-	data center infrastructure management
EDD	-	Event-Driven Discovery
EIA	-	Electronic Industries Alliance
EN	-	European Standards
GUI	-	Graphic User Interface
HDD	-	Hard Disk Drive
HDTV	-	High-Definition television
HW	-	Hardware
IDS	-	Intrusion Detection System
IIMS	-	Intelligent Infrastructure Management Solution
IMAC	-	Instalation, Move, Add & Change
IMACD	-	Instalation, Move, Add, Change & Delete
IP	-	Internet Protocol
IPLMS	-	Intelligent physical layer management solutions
ISO	-	International Organization for Standardization
IT	-	Informační technologie¨
L1	-	Layer 1
LC	-	Lucent, Local Connector
LED	-	Light-Emitting Diode
LSOH	-	Low Smoke Zero Halogen
MAC	-	Media Access Control
MACs	-	Moves, Adds & Changes
NIC	-	Network Interface Card
PDF	-	Portable Document Format
PN	-	Permise Networks
PoE	-	Power over Ethernet
RFID	-	Radio Frequency Identification
RIA	-	Rich Internet Application
RJ45	-	koncovka síťových kabelů
SNMP	-	Simple Network Management Protocol
SP	-	Service Pack
SW	-	Software
TCP	-	Transmission Control Protocol
TIA	-	Telecommunications Industry Association
U	-	Unit, jednotka pro velikost v rozvodné skříni

UPS	-	Uninterruptible Power Supply
UTP	-	Unshielded Twisted Pair
VLAN	-	Virtual Local Area Network
VoIP	-	Voice Over IP

SEZNAM PŘÍLOH

A LABORATORNÍ ÚLOHA – MANAGEMENT SÍTĚ NA FYZICKÉ VRSTVĚ

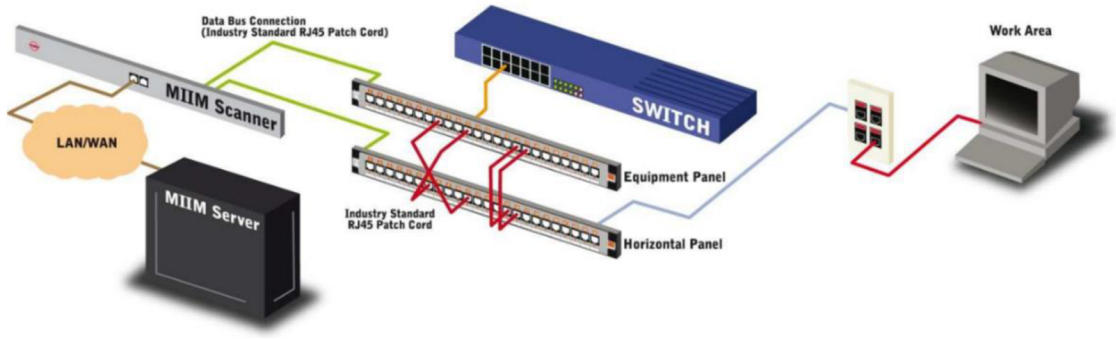
Cílem této úlohy je studenty seznámit se základní administrací systému pro management fyzické vrstvy, vyzkoušet si jeho možnosti detekce a realizovat danou slabinu systému.

Zadání úlohy

1. Seznámit se základní administrací a vytvoření infrastruktury v systému MIIM.
2. Otestovat všechny možné scénáře pro schopnost detekce systému MIIM.
3. Realizovat slabinu v detekci systému MIIM prostřednictvím UTP kabelu.

Teoretický úvod

V prostředí rozsáhlých ethernetových sítí s vysokým počtem a koncentrací prvků bylo nutné zavést automatizované systémy správy infrastruktury (AIM), které poskytují aktuální přehled o aktuální databázi map portů s monitorováním sítě v reálném čase, propojení portů jednotlivých zařízení v síti, plánování změn v síti, zvýšení bezpečnosti sítě a časovou úsporu při řešení poruch. Typicky se jedná o prostředí datacenter, ale v poslední době se AIM zavádí i do prostředí podnikových sítí. V současné době neexistuje standard, kterého by se výrobci systémů drželi, a tak jsou všechny systémy proprietární a navzájem nekompatibilní. Mezi klíčové výrobce patří například společnosti Molex, Tyco a CommScope [1].



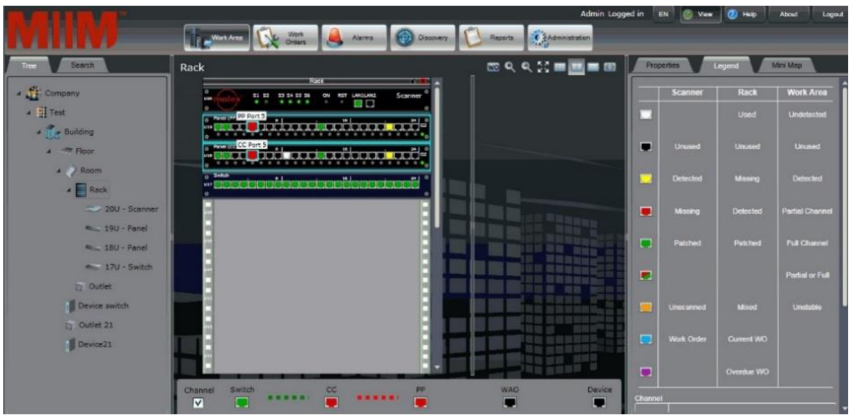
Obr. A.1 Schéma systému MIIM [2]

V současnosti existuje několik principů detekce propojení. Mezi nejvíce využívané patří princip devátého vodiče (9-pin), princip očipovaných zásuvek (RFID) a měření impedančních vlastností. V této úloze se zaměříme na poslední zmíněnou, která je aktuálně nejpokrokovější v možnostech detekce ze všech

zmíněných. Díky ní není nutné používat žádné speciální komponenty jako propojovací kabely s devátým pinem nebo čipem. Výhodou tohoto principu je, že při dotazování dostupnosti stanic nevyužívá SNMP protokol a zároveň umožňuje detekci připojeného koncového zařízení i ve vypnutém stavu. Jsme navíc schopni monitorovat celý kanál, tedy od aktivního prvku až po koncové zařízení. Konkrétně se jedná o systém MIIM od společnosti Molex.

Systém se skládá ze dvou inteligentních propojovacích panelů, kde jeden panel (tzv. **CC panel**) reprezentuje porty aktivního prvku (přepínače) a druhý panel (tzv. **PP panel**) reprezentuje porty koncových datových zásuvek. Tyto panely pro každý port obsahují signalizační LED, pomocí které můžeme být navedeni, jaké porty panelů máme propojit. Jednotlivé koncové zásuvky obsahují speciální **terminátor** (tzv. stuffer cap), obsahující odpor (1 MΩ), podle kterého je systém schopen hlídat kontinuitu horizontální linky. Detekci připojeného koncového zařízení pak provádí na základě odporu síťové karty (150 Ω). Systém odpor měří prostřednictvím bílo-hnědého a oranžového pinu ethernetového kabelu.

Všechny propojovací panely jsou datovou sběrnicí připojeny ke **skeneru**, který sbírá v reálném čase stavové info ze všech portů propojovacích panelů. Získané informace pak skener ukládá a porovnává je s databází na MIIM serveru. V databázi se nacházejí údaje, jako například umístění racků, propojovacích panelů, aktivních prvků, zobrazení jednotlivých spojů v propojovací zóně, údaje o koncových zařízeních a jejich uživatelích. V návaznosti můžeme také uložit i další informace (IP, MAC adresa) o koncových stanicích získané z vyšších vrstev prostřednictvím SNMP protokolu. **MIIM server** pak nashromážděné informace a o stavu jednotlivých datových kanálů prezentuje uživateli prostřednictvím webové aplikace, zároveň uživatel jejím prostřednictvím může vytvářet jednotlivé pracovní úlohy a plánovat změny v síti a dohlížet na jejich realizaci. Díky získaným datům v databázi může IT pracovník vytvářet statistiky a grafy poskytující přehled o využití portů aktivních prvků, změnách v síti, využitých a volných zásuvkách a mnohé další.



Obr. A.2 Hlavní obrazovka MIIM serveru

Systém tedy poskytuje důležitou informační hodnotu pro bezpečnost, díky možnosti upozornění na neautorizované zásahy (např. připojení útočníka k volné datové zásuvce či odpojení tiskárny). Pokud by došlo k realizaci neplánovaných událostí, systém tuto událost zaznamená a upozorní povolanou osobu (např. e-mailem, SMS) [1][3].

Postup pro vypracování úlohy

Úloha bude provedena na prezentačním MIIM kitu od společnosti Molex, který obsahuje všechny prvky důležité systému MIIM pro management sítě na fyzické vrstvě (viz teoretický úvod). Prezentační kit (Obr.A.3) je složen z panelu koncových datových zásuvek (WAO), PP panelu, CC panelu, MIIM skeneru a přepínače Cisco Catalyst 2950. Přepínač CISCO najdeme na zadní straně MIIM kitu. Prvních 12 portů WAO panelu je osazeno MIIM terminátorem.

Obr. A.3 Prezentační MIIM Kit

Tab. A.1 Přístupové údaje k zařízením

Název zařízení	IP adresa	Login/Heslo
Lenovo - Windows login	192.168.1.100	Administrator/molex12#
MIIM server (Lenovo)	192.168.1.100	admin/admin
MIIM scanner	192.168.1.10	admin/admin
Cisco Switch(SW_01)	192.168.1.9	admin/molex12#

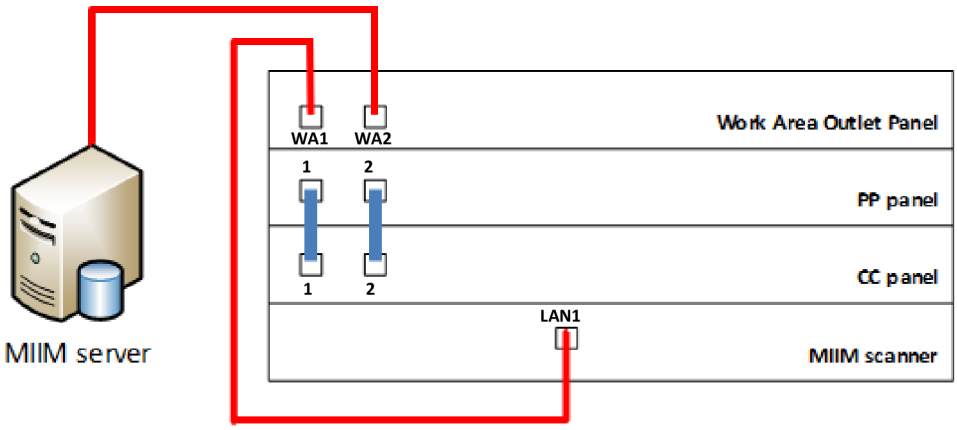
1) Zapojení pracoviště

V první části zapojíme pracoviště pro zajištění komunikace mezi skenerem a MIIM serverem. Připojení jednotlivých panelů ke skeneru, portů CC panelu k přepínači a porty PP panelu ke koncovým zásuvkám (horizontální linka) už je realizováno

uvnitř MIIM kitu. Porty přepínače i CC panelu jsou zapojeny 1:1, stejně tak i porty WAO panelu vůči portům PP panelu.

Postačí nám tedy proto realizovat propojení portu skeneru **LAN1** do portu **WA1** a následně realizovat propoj **prvního portu PP panelu** a **prvního portu CC panelu.**

Následně připojíme stanici hostující **MIIM server** do **WA2** a realizujeme propoj **druhého portu PP panelu** s **druhým portem CC panelu**.



Obr. A.4 Zapojení systému

2) Tvorba databáze

V dalším kroku už můžeme přejit k samotné konfiguraci systému MIIM prostřednictvím **MIIM serveru**. Na stanici hostující MIIM server otevřeme webový prohlížeč Internet Explorer a do URL řádku zadáme **192.168.1.100/miimserver** pro přístup do webové aplikace **MIIM** serveru. Následně zadáme přihlašovací údaje a přihlásíme se do webového rozhraní.

Na úvod musíme vytvořit databázi pro naši celou infrastrukturu. V pravé horní části obrazovky klikneme na tlačítko **Edit**  pro přepnutí do editačního režimu, abychom mohli měnit konfiguraci systému. Na hlavním panelu v horní časti obrazovky klikneme na **Administration ->** záložka **Database** -> v podokně **Database list** klikneme na tlačítko **Create** -> zadáme jméno databáze (např. „VUT_AIM_MIIM“). Poté v podokně **Database Management** v části **Server Configuration** nastavíme **Database Name** na námi vytvořenou databázi. Dále se můžeme povšimnout možnosti zálohování databáze i možnosti exportu/importu. Klikneme na tlačítko **Save.** Dvakrát potvrdíme tlačítkem **OK** a znovu se přihlásíme do systému.

3) Tvorba logické infrastruktury

V následující části si vytvoříme logickou infrastrukturu naší sítě. Opět se přepneme do editačního režimu prostřednictvím tlačítka **Edit**. V levé části okna v záložce **Tree** klikneme na **Company** a v pravé části okna -> záložka **Properties** -> část **Company** -> změníme položku **Name** například na **„VUT“** -> potvrdíme tlačítkem **Save**.

V okně **Tree** klikneme pravým tlačítkem myši na nápis **VUT** -> **New** -> **Building** -> zvolíme jméno budovy v řádku **Name** například jako **„FEKT“** -> potvrdíme tlačítkem **Save**.

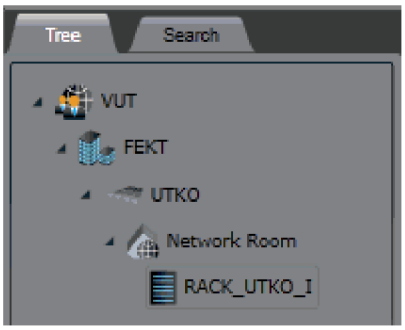
Rozevřeme celý strom **VUT.** Pravým tlačítkem myši klikneme na název vytvořené budovy **FEKT** -> **New** -> **Floor** -> a zvolíme například **„UTKO“** jako jméno v řádku **Name** a potvrdíme tlačítkem **Save**.

Nyní si přiřadíme mapu pro lepší specifikaci umístění jednotlivých zařízení. Pravým tlačítkem myši klikneme na **UTKO** -> **Assign map** -> klikneme na tlačítko **Upload** -> v rámci řádku **File** zvolíme obrázek **simple_office**, který je uložen na **Ploše** -> potvrdíme tlačítkem **OK**.

Pravým tlačítkem myši klikneme na **UTKO** -> **New** -> **Network Room** -> řádek **Name** můžeme ponechat jako **„Network Room“** -> potvrdíme tlačítkem **Save**.

Následně pravým tlačítkem myši klikneme na vytvořenou **Network Room** -> **New** -> **Rack** -> do řádku **Name** zvolíme například jméno **„RACK_UTKO_I“** -> potvrdíme tlačítkem **Save**.

Na závěr si zobrazíme vytvořený rack kliknutím pravého tlačítka na **RACK_UTKO_I** -> **Show**. Prozatím je však prázdný. Výsledná stromová struktura by měla vypadat stejne jako na obr. A.5.

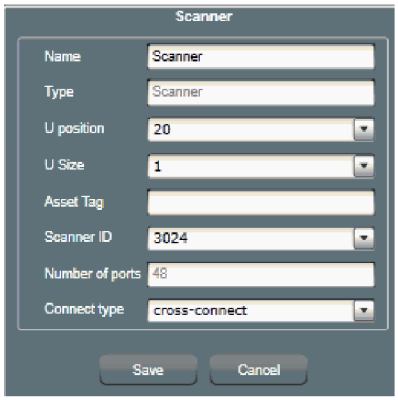


Obr. A.5 Strom infrastruktury

4) Implementace zařízení do systému MIIM

Nejprve je nutné je na server MIIM nahrát licenci pro skener. To provedeme prostřednictví tlačítka **Administration** na hlavním panelu -> záložka **Scanners** -> v podokně **Scanners List** kliknout na tlačítko **New** -> ve vedlejší podokně **Scanner** kliknout na tlačítko **Browse** -> najít cestu k licenčnímu souboru, který se nachází na Ploše ve složce miimserver_001 (Scanner_3024.lic). Pokud by se licence nenačtla hned, je nutné provést refresh stránky, znovu se přihlásit a přepnout se do editačního režimu. Následně zkontrolujeme, zda licence už je nyní nahraná. V podokně **Scanners list** by se měl nacházet záznam. Vrátíme se zpět kliknutím na tlačítko **Work Area** na hlavním panelu.

V záložce **Tree** pravým myši tlačítkem klikneme na **RACK_UTKO_I** -> **New** -> **Scanner** -> **576p scanner** -> zkontrolujeme, že **Connect Type** je nastavený na **cross-connect** a zbytek můžeme ponechat výchozí -> potvrdíme tlačítkem **Save**.



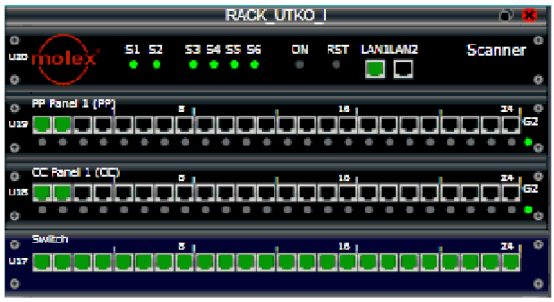
Obr. A.6 Nastavení skeneru

Nyní přidáme PP panel kliknutím pravého tlačítka myši na **RACK_UTKO_I** v podokně **Tree** -> **Panel** -> **G2** -> do pole **Name** zadáme například „**PP panel 1**“, zkontrolujeme, že **Panel type** je **PP** a zbytek ponecháme výchozí -> potvrdíme tlačítkem **Save**.

Znovu klikneme pravým tlačítkem myši na **RACK_UTKO_I** -> **New** -> **Panel** -> **G2** -> do pole **Name** zadáme například „**CC panel 1**“ -> **Panel type** nastavíme na **CC** a zbytek ponecháme výchozí -> potvrdíme tlačítkem **Save.**

Naposledy pravým tlačítkem myši klikneme na **RACK_UTKO_I** -> **New** -> **SW_01** -> pro naše účely vše můžeme nechat výchozí a potvrdíme tlačítkem **Save**. Klikneme pravým tlačítkem myši na **RACK_UTKO_I** -> **Show**.

Nyní nám náš virtuální rack přibližně odpovídá obsazení našeho fyzického MIIM kitu (viz obr. A.7).



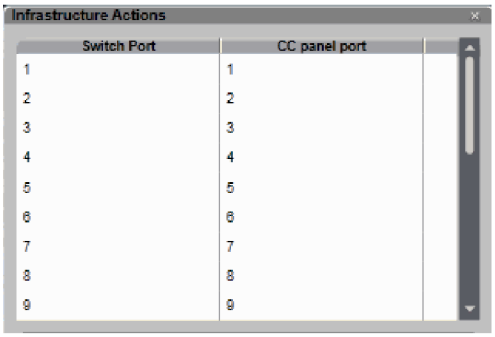
Obr. A.7 Virtuální rack v systému MIIM

5) Logické propojení zařízení

Aktuálně máme všechny zařízení v systému nachystaná, takže postačí je pouze logicky prpojit. V okně našeho racku **RACK_UTKO_I** v pravé horní části klikneme na ikonku **WO** 

, kterou se přepneme do pracovního režimu (Work Order), abychom mohli provádět logické úpravy v našem racku**.**

Nejprve je nutné provázat přepínač s CC panelem. To provedeme jedním klikem levého tlačítka myši na panel **přepínače** -> objevíme se nám stín přepínače, na který klikneme a přetáhneme jej na **CC panel** -> v zobrazeném okně zaškrtneme tlačítko **Connect All** pro logické spojení portů **přepínače** a **CC panelu** 1:1 (viz obr. A.8) -> potvrdíme tlačítkem **Submit**.



Obr. A.8 Zapojení portu přepínače a CC panelu

Posléze klikneme pravým tlačítkem myši na **Scanner** v racku -> zvolíme **New Instalation** pro realizaci zcela nové instalace -> potvrdíme tlačítkem **OK**. Provede se restart skeneru a vyčkáme, dokud porty na skeneru nebudou v žlutém stavu.

Následně je nutné oba panely (CC a PP) připojit ke skeneru. To provedeme dvojklikem na panel **Scanner**. Ukáže se nám zádní část skeneru s porty určenými pro PP panely (levá část) a porty pro CC panely (pravá část). Klikneme jednou na **první PP port** skeneru -> objeví se nám nad ním stínový port, na který klikneme a přetáhneme na **PP Panel 1** -> v zobrazeném okně potvrdíme tlačítkem **Submit**.

Podobně opakujeme pro CC panel. Klikneme tedy na **první CC port** skeneru -> poté klikneme na jeho stínový port a přetáhneme jej na **CC panel 1** -> opět potvrdíme tlačítkem **Submit**. Vybrané porty na skeneru by měli přejit do oranžového stavu a je tedy nutné je aktivovat

Vypneme pracovní režim kliknutím na tlačítko **WO** a pro pravým tlačítkem myši klikneme na oranžové porty skeneru -> **Activvate**. Na **CC** a **PP** panelu vidíme červené porty z důvodu toho, že nejsou nadefinované. Proto klikneme pravým tlačítkem myši na **PP panel 1** -> **Confirm panel patch cords**. Tím potvrdíme, že víme, o jaký propoj se jedná a porty přejdou do zeleného stavu.

Obr. A.9 Porty skeneru

6) Tvorba monitorované místnosti

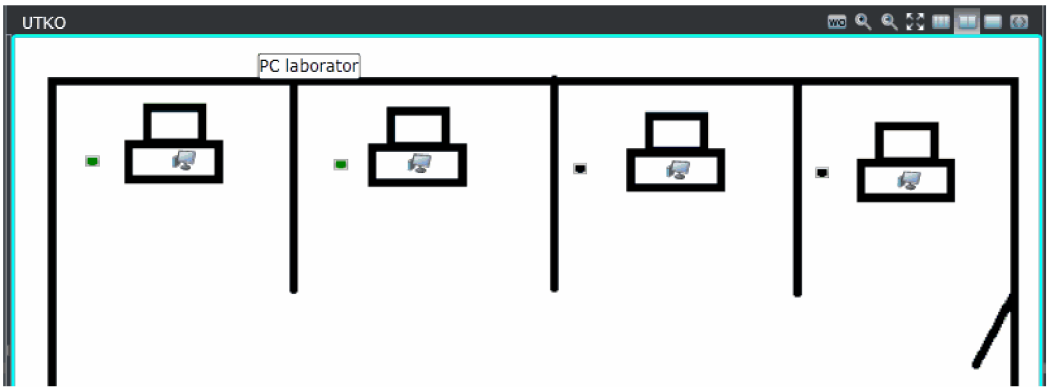
V této části si vytvoříme mísnost, ve které budeme chtít provádět monitoring a měla by odpovídat místnosti fyzické.

V okně **Tree**, ve stromové struktuře klikneme pravým tlačítkem myši na **UTKO** -> **New** -> **Room** -> do pole **Name** zadáme například **„PC laborator 1“** -> potvrdíme tlačítkem **Save**.

Následně přidáme koncové datové zásuvky, které budeme chtít monitorovat. Klikneme proto tedy pravým tlačítkem myši ve stromové struktuře na vytvořenou **PC laborator 1** -> **New** -> **Outlet** -> v novém okně v poli **Name** ponecháme **„Outlet“** -> počet vytvořených zásuvek (**Number of Objects to Create**) nastavíme například na **4**. Zbytek můžeme ponechat výchozí -> potvrdíme tlačítkem **Save.** Pravým tlačítkem myši v okně **Tree** klikneme na **PC laborator 1** -> **Locate on Map**.

Zásuvky pak můžeme ve zjednodušeném plánku rozmístit vedle počítačů. Jednotlivé datové zásuvky musíme provázat s porty **PP panelu**. Přepneme se opět do pracovního režimu prostřednictvím tlačítka **WO** a pomocí CTRL a levého tlačítka myši označíme všechny porty a přetáhneme je na **PP panel 1** -> v nově otevřeném okně zaškrtneme **Connect All** pro zapojení 1:1 -> potvrdíme tlačítkem **Submit**

Dále přidáme i samotné koncové stanice. Pravým tlačítkem myši opět klikneme na **PC laborator 1** -> **New** -> **Device** -> v novém okně do pole **Name** zadáme například **„PC“** -> počet počítačů (**Number of Objects to Create**) nastavíme například na **4** -> potvrdíme tlačítkem **Save**. Ikony počítačů rozmístíme do mapy.

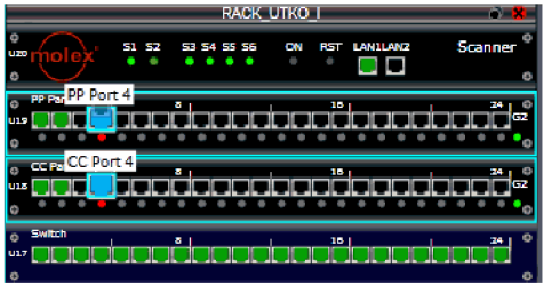


Obr. A.10 Rozmístění prvků

Nakonec propojíme logicky vytvořené porty a počítače. Přepneme se do pracovního režimu prostřednictvím tlačítka **WO**. Klikneme na ikonu portu na mapě a přetáhneme je na ikonu počítače -> v novém okně potvrdíme tlačítkem **Submit**. Provedeme tak stejně u zbývajících.

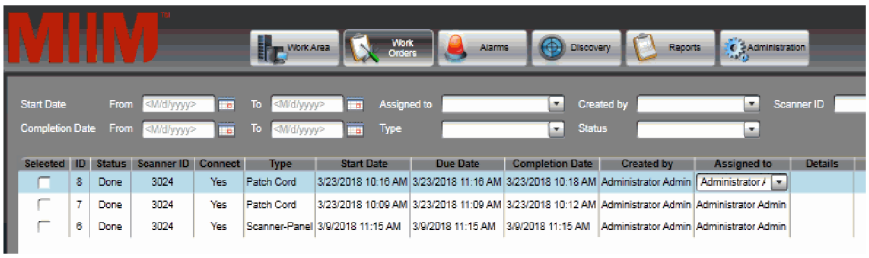
7) Naplánování pracovní úlohy

Nejprve je nutné se přepnout do pracovního režimu prostřednictvím tlačítka **WO**. Pote vybereme libovolný port na **PP panel 1**, například čtvrtý**,** a klikneme na něj. Objeví se nám nad ním stínový port, na který klikneme a přetáhneme jej na čtvrtý port **CC panelu** -> a v novém okně potvrdíme tlačítkem **Submit**. Nyní se nám na obou panelech rozsvítí námi zvolené porty, takže realizujeme spojení propojovacím kabelem. Porty nám v systému přejdou do zeleného stavu. Můžeme nyní i připojit koncové zařízení do čtvrtého portu WAO panelu (např. přiložený domácí přepínač).



Obr. A.11 Identifikace portů k propojení

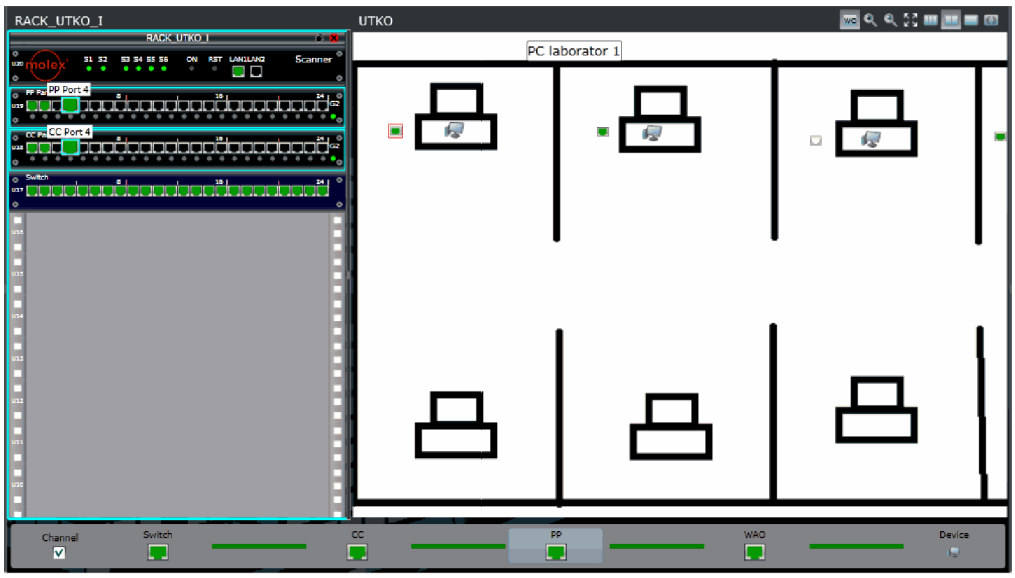
Přehled o jednotlivých pracovních úlohách najdeme na hlavním panelu pod tlačítkem **Work Orders**.



Obr. A.12 Seznam pracovních úloh v MIIM

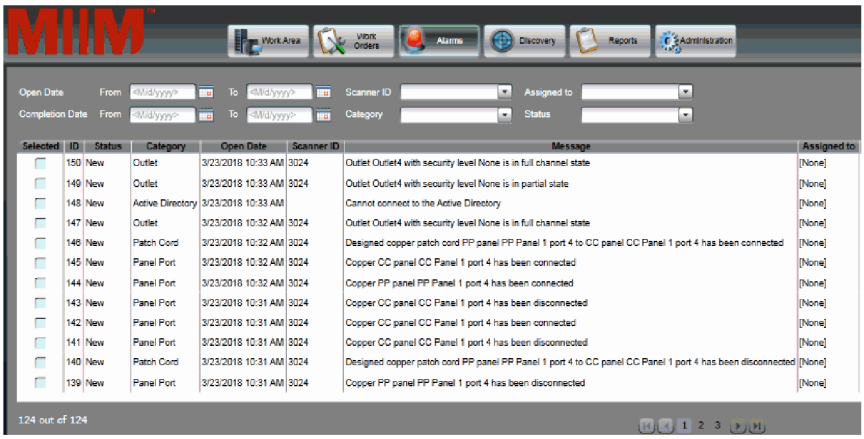
8) Sledování datového kanálu

Nejprve vypneme **WO** režim a klikneme například na čtvrtý port na **PP** panelu. Ukáže se nám pod virtualním rackem panel **Channel**. V případě zaškrtnutí checkboxu se nám zobrazí kontinuita daného kanálu od přepínače až po koncové zařízení. V tomto případě by měl být kanál kompletní. Může nastat situace, že se kanál okamžitě nezobrazí, proto stačí kliknout na jakýkoliv jiný port a posléze kliknout zpět na námi zvolený. Info o jednotlivých významech barev portů a datových portů nalezneme v pravé části okna v záložce **Legends**.



Obr. A.13 Datový kanál v systému MIIM

Seznam veškerých událostí ať už plánovaných či neplánovaných můžeme najit pod tlačítkem **Alarms** na hlavním panelu. Můžete vyzkoušet rozpojení a znovuzapojení propojovacího kabelu ve čtvrtém portu **PP** panelu, odpojení a znovuzapojení koncového zařízení či provést propojení do nenaplánovaných portů a připojení koncového zařízení.



Obr. A.14 Přehled událostí v systému MIIM

9) Samostatné úkoly

Vyzkoušejte možnosti detekce událostí v rámci datového kanálu dle následujících scénářů. Použijte již vytvořený datový kanál, popřípadě vytvořte nový (viz 6. a 7. krok).

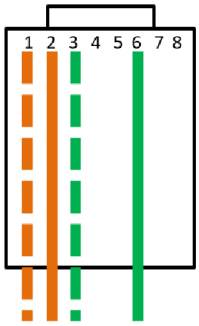
- **Falešné propojení**
  - Situace, kdy v rámci realizace plánovaného propojení portů mezi panely je do jednoho portu panelu zapojen jeden propojovací kabel a do portu druhého panelu další kabel. Oba tyto kabely na druhém konci zůstanou nepřipojeny.
- **Přestřižení propojení**
  - Situace, kdy v realizovaném propojení mezi propojovacími panely daný kabel „přestřihneme“. Realizujeme za pomocí dvou kabelů a spojky.
- **Horizontální kabeláž**
  - Jedná se o linku mezi propojovacím panelem reprezentující datové zásuvky (panel PP) a samotnou datovou zásuvkou (WAO panel). Situace určuje, zda systém je schopen reagovat na případné přerušení dané linky. Využijte port WA12 a port 12 na PP panelu pro realizaci kompletního kanálu v rámci MIIM kitu. Přerušení linky realizujte za pomocí kabelu a portů (viz obr. A.15) ze zadní části MIIM kitu.

Obr. A.15 Porty pro realizaci horizontální linky

- **Detekce zapnutého koncového zařízení**
  - Schopnost detekovat odpojení/připojení zapnuté koncové stanice. Realizujte pomocí přiložené koncové stanice.
- **Detekce vypnutého koncového zařízení**
  - Schopnost detekovat odpojení/připojení koncové stanice i v případě, že je vypnuté. Nemusíte vypínat stanici. Postačí místo stanice připojit přiložený aktivní prvek (např. domácí přepínač).

10) Připojení do sítě bez detekce systému

Jelikož systém MIIM měří impedanci prostřednictvím **oranžového** a **bílo-hnědého** pinu. Vytvořte nový kabel vyhovující standardu 10BaseT/100BaseT (popřípadě použijte už předpřipravený), aby možné se připojit přes koncovou datovou zásuvku (WAO) do sítě bez detekce systému MIIM. Připojte se tímto kabelem do koncové zásuvky (např. WA4) a pozorujte daný datový kanál náležející k danému portu, zda zobrazí připojené koncové zařízení. Pro jistotu můžeme zkontrolovat seznam událostí v položce **Alarms** a Následně nastavte na stanici statickou IP adresu z rozsahu 192.168.1.0/24 (např. **192.168.1.200**/24). Vyzkoušejte ping na MIIM server.



Obr. A.16 Zapojení konektoru dle standardu 100BaseT

Tab. A.2 Význam pinů zapojení 100BaseT

Pin	Popis	Význam
1	TD+	Transmit+
2	TD-	Transmit-
3	RX+	Receive+
4	-	-
5	-	-
6	RX-	Receive-
7	-	-
8	-	-

11) Smazání databáze

Na závěr této úlohy vymažte vytvořenou databázi na MIIM serveru. Na hlavním panelu klikněte na položku **Administration** -> záložka **Database** -> v řádku **Server Configuration** zvolte jinou databázi (např. **MIIM2**) -> klikněte na tlačítko **Save** -> **OK**. Po načtení databáze se přihlásíme do systému, zapneme **Edit** režim a opět přejdeme do nastavení databáze. V podokně **Database List** zvolíme naší předchozí vytvořenou databázi -> klikneme na tlačítko **Delete** -> potvrdíme **OK**.

Volitelné úkoly

1) Prozkoumejte další možnosti systému na MIIM serveru.
2) Prozkoumejte konfiguraci MIIM skeneru v rámci jeho webového rozhraní.

Otázky k úloze

1. Jmenujte další možná komerční řešení pro management na fyzické vrstvě.
2. Existuje kompatibilita mezi prvky od různých výrobců pro management sítě na fyzické vrstvě?
3. Jaké jsou výhody systémů pro management z hlediska bezpečnosti?
4. Z jakého důvodu se převážně používá dvojí reprezentace propojovacích panelů (tzv. Cross-connect)?
5. Jakými dalšími mechanismy lze zabránit případnému útočníkovi přístupu do sítě (na fyzické vrstvě a vyšší)?

Reference

[1] ROZSYPAL, O. Fyzická bezpečnost a management sítě na fyzické vrstvě. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 70 s.

[2] NETWORK GROUP, S. R. O. MIIM. NETWORK GROUP, S. R. O. NWG [online]. b.r. [cit. 2017-11-15]. Dostupné z:http://www.nwg.cz/index.php?module=shop_catalog&action=list_products&id=132

[3] CARL, Lea Ann. What is Automated Infrastructure Management?. *NetworksAsia* [online]. 2016 [cit. 2018-04-16]. Dostupné z: https://www.networksasia.net/article/what-automated-infrastructure-management.1472343848

B OBSAH PŘILOŽENÉHO CD

- Elektronická verze práce ve formátu PDF.