PROJEKT KONCEPCYJNY

Temat zadania: **Zintegrowany System Miejskiego Transportu Publicznego – Zaprojektowanie i Budowa Systemu Zarządzania Ruchem w Lublinie w ramach zadania pt. "Zintegrowany System Miejskiego Transportu Publicznego w Lublinie" współfinansowany w ramach Programu Operacyjnego Rozwój Polski Wschodniej 2007 – 2013**

Temat projektu: **Podsystem Telekomunikacyjny.**

ZAMAWIAJĄCY:	**Gmina Lublin** **Zarząd Dróg i Mostów w Lublinie** ul. Krochmalna 13j 20-401 Lublin
GENERALNY WYKONAWCA:	**Aeronaval de Construcciones e Instalaciones S.A.** Ul. Dekerta 24 30-703 Kraków

Funkcja	Imię i nazwisko autora	Data	Podpis
Autor	D. Gustavo A. Molina Méndez *Dyrektor Techniczny ACISA S.A.*	21/02/2013	
Dyrektor Projektu	Carlos Blázquez Alonso *Dyrektor Projektu ACISA S.A*	21/02/2013	

SPIS TREŚCI

1.- Akronim

1.1.- A

ABR- Area Border Router
ACL- Access Control List
AF- Assured forwarding
ASBR- Autonomous System Boundary Router

1.2.- B

BA- Behavior Aggregate
BDR- Backup Designated Router
BGP- Border Gateway protocol

1.3.- C

CBT- Center Based trees

1.4.- D

DEP- Database Exchange Process
DHCP Server- Dynamic Host Configuration Protocol server
DoS Prevention- Denial of Service Prevention
DR- Designated Router
DSCP- Differentiated Services Code Point
DVMRP- Distance Vector Multicast Routing Protocol

1.5.- E

EF- Expedited Forwarding

1.6.- G

GPL- General Public License

1.7.- I

IGMP- Internet Group Management Protocol
IP- Internet Protocol
IPv6- Internet Protocol version 6
IRDP- ICMP Router Discovery Protocol
IS-IS- Intermediate system to Intermediate system

1.8.- L

LAN- Local Area Netwok
LSNAT- Load Sharing Network Address Translation
LSR- Link State Request
LSU- Link State Update

1.9.- M

MAC- Media Access Control
MOSPF- Multicast Open Shortest Path First
MRP- Media Redundancy Protocol

1.10.- N

NLA - Network Log Analyzer

1.11.- O

OSPF-Open Shortest Path First

1.12.- P

PBR- Policy Based Routing
PBX - Private Branch Exchange
PHB- Per Hop Behavior
PIM-DM- Protocol Independent Multicasts- Dense Mode
PIM-SM- Protocol Independent Multicasts- Sparse Mode

1.13.- Q

QoS- Quality Of Service

1.14.- R

RFC- Request For Comments
RIP v1/v2- Routing Information Protocol version 1 and 2
RLA- Remaining Life Assessmen
RP- Rendevous Ponit

1.15.- S

SLA- Software License Agreement
SNMP- Simple Network Management Protocol

1.16.- T

TC- Traffic Conditioning
TCP- Transfer Control Protocol

1.17.- V

VLAN- Virtual Local Area Network
VLL- Virtual Leased Line
VRRP- Virtual Router redundancy protocol

1.18.- W

WAN- Wide Area Network

2.- Wyznaczanie sieci

2.1.- TOPOLOGIA

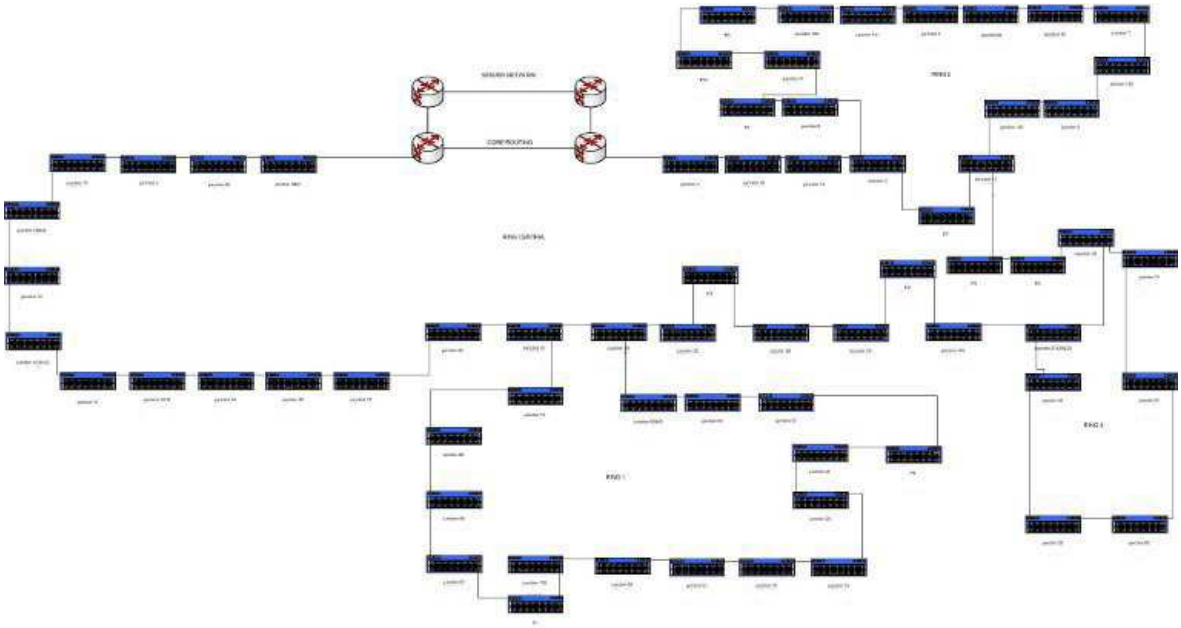
Firma ACISA zaprojektowała topologię tej sieci skupiając się głównie na jej wysokiej dyspozycyjności i solidnej architekturze.

Struktura sieci złożona będzie z 3 podpierścieni zagnieżdżonych w jednym wielkim pierścieniu głównym, co znane jest pod nazwą topologii wielu pierścieni.

Zaprojektowana sieć światłowodowa zasadniczo opiera się na rozprowadzeniu w mieście przewodów światłowodowych, o 16 i 12 włóknach jednomodowych dla najważniejszych odcinków oraz o 8 włóknach jednomodowych dla drugorzędnych odcinków obsługi kamer, central ruchu, sterowników, paneli itd.

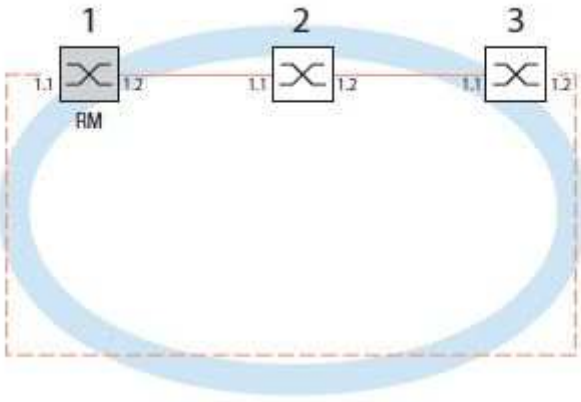
Architektura wielu pierścieni oparta jest na topologii pierścieni.

Jedna topologia pierścienia składa się z tylko jednego zamkniętego pierścienia złożonego z węzłów i łączy, w którym każdy węzeł połączony jest jedynie z dwoma sąsiadującymi węzłami. Ta topologia zostanie skonfigurowana z zastosowaniem protokołu MRP, który pozwoli nam wdrożyć strukturę pierścienia o wysokiej dyspozycyjności.



2.1.1 TOPOLOGIA PIERŚCIENIA

Za pomocą Ring Managera dwa krańcowe węzły będą mogły zamknąć strukturę redundantnego pierścienia, bez tworzenia pętli. Węzeł pełniący rolę Ring Managera utrzymuje otwarte połączenie redundantne zawsze gdy struktura pierścienia jest nienaruszona. Jeśli któryś segment/ ęzeł nie działa, Ring Manager natychmiast zamyka linię redundantną, a struktura sieci pozostaje nienaruszona.

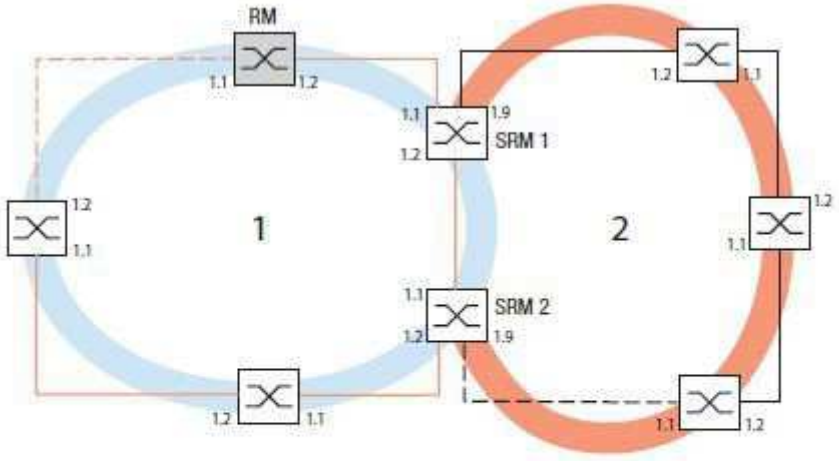


Pierścień jest najpowszechniejszą topologią, ponieważ dostarcza alternatywną drogę komunikowania się między dowolnymi dwoma węzłami.

2.1.2 TOPOLOGIA WIELU PIERŚCIENI

Topologia wielu pierścieni składa się z jednego głównego pierścienia i jego zagnieżdżonych podpierścieni.

Zasada podpierścienia umożliwia łatwe podłączenie nowych segmentów sieci do odpowiednich urządzeń w istniejących redundantnych pierścieniach (głównych pierścieniach). Urządzenia głównego pierścienia, do którego został podłączony nowy podpierścień, są odsyłane do Sub-Ring Managera (SRM).



Sub-Ring-Struktur
1 blueRing = Base -Ring
2 orangeRing = Sub-Ring
SRM = Sub-Ring-Manager
RM = Ring-Manager

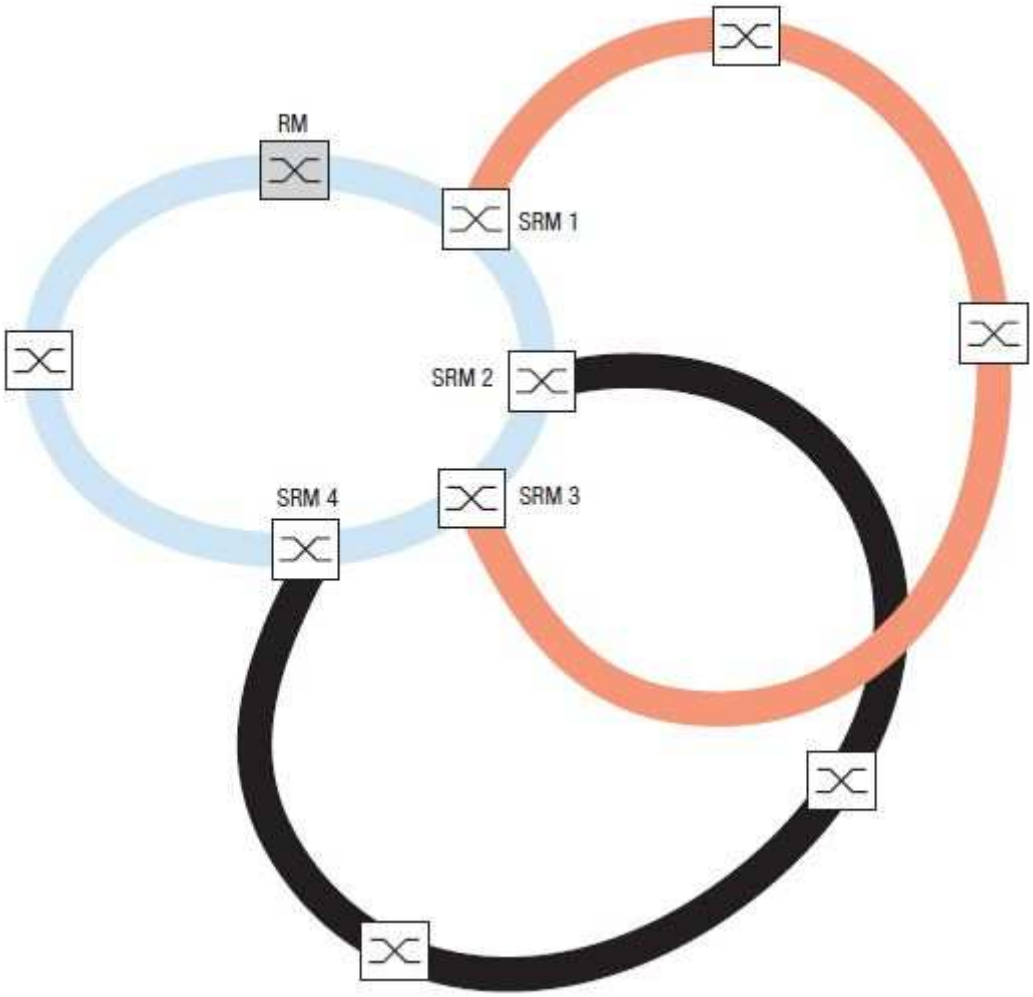
Do podpierścienia można włączyć jako uczestników urządzenia obsługujące protokół MRP; działanie Sub-Ring Managera nie jest wymagane.

Ustanowienie podpierścieni daje następujące korzyści:

Poprzez proces podłączania włącza się nowy segment sieci do redundantnego układu.

W łatwy sposób można sporządzić mapę struktury organizacyjnej systemu w topologii sieci.

Przy MRP-Ring czasy przełączania podpierścieni w przypadkach redundancji wynoszą zasadniczo < 100 ms.



Można również podłączyć podpierścienie do istniejących głównych pierścieni za pomocą protokołu MRP.

Jeśli podłącza się podpierścień do pierścienia głównego za pomocą MRP, należy skonfigurować obydwa pierścienie w różnych sieciach VLAN. Konfiguruje się którykolwiek z portów podpierścienia jako Sub-Ring Manager oraz urządzenia podpierścienia w oddzielnej sieci VLAN. Różne podpierścienie mogą używać tej samej sieci VLAN lub urządzeń pierścienia głównego, łącznie z portami głównego pierścienia Sub-Ring Manager w osobnej sieci VLAN. Zmniejsza to wysiłek włożony w konfigurację, gdy do pierścienia głównego podłącza się wiele podpierścieni.

2.2.- VLAN

W celu segregacji ruchu sieci według jego rodzaju (zarządzanie, video, dane itd.), z zastosowaniem tych samych fizycznych przewodów w przełącznikach konfiguruje się wirtualne sieci lokalne (VLAN), co pozwoli nam selektywnie wyznaczyć fizyczne porty każdego swicha do jednego VLAN'a, w zależności od ruchu generowanego przez podłączone do niego urządzenie.

Wirtualna sieć lokalna (VLAN) jest grupą logiczną stacji roboczych, serwerów i urządzeń sieciowych, które widoczne są w tej samej sieci LAN bez względu na ich geograficzne umiejscowienie. VLAN pozwala sieci komputerów i użytkowników na komunikację w sztucznym środowisku, jakby znajdowały się w pojedynczej sieci LAN i współdzieliły broadcastowy i multicastowy obszar.

VLAN pozwala różnym sieciom, by pracowały wirtualnie jako LAN. Jedną z największych korzyści sieci VLAN jest to, że eliminuje stan bezczynności sieci, co chroni zasoby sieci oraz zwiększa jej efektywność. Dodatkowo sieci VLAN stworzone są do dostarczania segmentacji oraz pomagają w takich kwestiach jak bezpieczeństwo, zarządzanie siecią oraz skalowalność. Ponadto, używając sieci VLAN, w łatwy sposób można kontrolować schematy ruchu.

Główne korzyści wdrożenia sieci VLAN są następujące:

Pozwala administratorom sieci na zastosowanie dodatkowego zabezpieczenia łączności sieci.

W łatwy sposób dokonuje się rozszerzenia oraz przemieszczenia sieci lub urządzeń sieciowych.

Zapewnia elastyczność, gdyż administratorzy mogą dokonywać konfiguracji w scentralizowanym środowisku, podczas gdy urządzenia mogą być zlokalizowane w różnych miejscach geograficznych.

Zmniejsza bezczynność oraz obciążenie ruchem w sieci i w urządzeniach sieciowych oraz zwiększają wydajność.

2.3.- Wyznaczenie planu przekierowania IP

Nazewnictwo ostatecznych urządzeń będzie następujące:

10.VLAN Pvid. nr skrzyżowania. Rodzaj urządzenia

Gdzie urządzenie posiadające IP 10.10.83.20 będzie swichem (czwarty oktet "20"), który będzie zlokalizowany na skrzyżowaniu 83 (trzeci oktet "83") i który będzie przynależał do VLAN 10 (drugi oktet "10"). Poniżej podajemy stosowane nazewnictwo.

2.3.1 Wyznaczanie zakresów sieci VLAN i jej ruchu:

W chwili wyznaczania zakresów VLAN wzięto pod uwagę, by numer VLAN zrównał się z drugim oktetem zakresu adresu IP.

Zarządzanie urządzeniami sieci VLAN 1:	10.1.0.0 /16
Zarządzanie Pierścieniem Centralnym VLAN 2:	10.2.0.0 /16
Zarządzanie Pierścieniem 1 VLAN 3:	10.3.0.0 /16
Zarządzanie Pierścieniem 2 VLAN 4:	10.4.0.0 /16
Zarządzanie Pierścieniem 3 VLAN 5:	10.5.0.0 /16
Kamery CCTV VLAN 11:	10.11.0.0 /16
Monitoring video incydentów VLAN 12:	10.12.0.0 /16
Visioways VLAN 13	10.13.0.0 /16
Kamery ARTR VLAN 14:	10.14.0.0 /16
Regulatory VLAN 15:	10.15.0.0 /16
PMV VLAN 16:	10.16.0.0 /16
Telefonia VLAN 17:	10.17.0.0 /16

2.3.2 Wyznaczanie rodzaju urządzeń według ich ostatniego oktetu adresu IP:

W celu ułatwienia rozróżniania urządzeń tylko po ich IP, zdecydowano o ich pogrupowaniu według rodzaju, tak, że czwarty oktet ich adresu kończy się na tę samą liczbę.

Gateway : 1, 2

Routery : 10

Switche : 20

Kamery CCTV :11, 21, 31, 41, 51, 61, 71, 81, 91, 101, 111, 121, 131, 141, 151, 161, 171, 181, 191, 201, 211, 221, 231, 241, 251.

Monitoring wideo zdarzeń : 12, 22, 32, 42, 52, 62, 72, 82, 92, 102, 112, 122, 132, 142, 152, 162, 172, 182, 192, 202, 212, 222, 232, 242, 252.

Monitoring wideo osób : 13, 23, 33, 43, 53, 63, 73, 83, 93, 103, 113, 123, 143, 153, 163, 173, 183, 193, 203, 213, 223, 233, 243, 253.

Kamery ARTR - (czas przejazdów) : 14, 24, 34, 44, 54, 64, 74, 84, 94, 104, 114, 124, 134, 144, 154, 164, 174, 184, 194, 204, 214, 234, 244, 254.

Sterowniki : 15, 25, 35, 45, 55, 65, 75, 85, 95, 105, 115, 125, 135, 145, 155, 165, 175, 185, 195, 205, 215, 225, 235, 245.

VMS : 16, 26, 36, 46, 56, 66, 76, 86, 96, 106, 116, 126, 136, 146, 156, 166, 176, 186, 196, 206, 216, 226, 236, 246.

2.4.- ROUTING

Do routingu pakietów używane będą dwa switche warstwy 3, które zostaną skonfigurowane z protokołami OSPF i VRRP. Pierwszy jest protokołem stanu łącza (Link-State) o dynamicznym routingu, drugi jest protokołem, na którym spoczywa dynamiczne przypisywanie funkcji wirtualnego routera jednemu z routerów VRRP w sieci LAN.

2.4.1 Protokół OSPF

Open Shortest Path First (OSPF) jest protokołem routingu stanu łącza. OSPF jest protokołem routingu bezklasowego, który do przeprowadzania skalowalności wykorzystuje koncepcję obszarów. RFC 2328 określa metrykę OSPF jako arbitralną wartość nazywaną kosztem.

Głównymi zaletami OSPF w porównania z protokołami routingu wykorzystującymi wektor odległości są jego szybka konwergencja i skalowalność przy implementacji do dużo większych sieci.

2.4.1.1 Właściwości protokołu OSPF

OSPF jest protokołem dynamicznego routingu typu link state (modyfikacji stanu), który wykrywa i zapamiętuje najlepsze ścieżki do miejsc przeznaczenia (dostępne). OSPF może szybko wyłapać zmiany w topologii systemu autonomicznego (SA), a po krótkim okresie konwergencji obliczyć nowe ścieżki. OSPF nie enkapsuluje pakietów IP, tylko sprawia, że przemieszczają się one w oparciu jedynie o adres przeznaczenia.

OSPF jest zaprojektowany by dostarczać usługi niedostępne z protokołem RIP. Jego zaawansowane właściwości zawierają w sobie:

●Mniej kosztowny routing. Pozwala konfigurować koszty ścieżki w oparciu o jakąkolwiek kombinację parametrów sieci, na przykład szerokość pasma, opóźnienie i koszt.

●Brak ograniczeń w metryce routingu. Podczas gdy RIP ograniczał metrykę routingu do 16 skoków, OSPF pod tym względem nie ma żadnych ograniczeń.

●Routing wielościeżkowy. Pozwala na wykorzystywanie wielu ścieżek o tym samym koszcie, łączących te same punkty. Można używać tych ścieżek do osiągnięcia równowagi (zrównoważenie obciążenia), co daje efektywniejsze wykorzystanie szerokości pasma sieci.

● Routing z wydzieleniem obszaru. Zmniejsza zasoby (pamięć i szerokość pasma sieci) wykorzystywane przez protokół i dostarcza dodatkowy poziom zabezpieczenia routingu.

●Maski podsieci o zmiennej długości. Pozwalają na dzielenie adresu IP na podsieci o zmiennej wielkości, z zachowaniem przestrzeni adresu IP.

●Uwierzytelnienie routingu. Daje dodatkowe zabezpieczenie routingu.

Protokół OSPF wspiera następujące rodzaje sieci fizycznych:

●**“Point-to-Point”**. Są to sieci wykorzystujące jedną linię komunikacji do połączenia jednej pary routerów. Jest to rodzaj sieci domyślnie wybierających interfejsy takie jak PPP, HDLC, TNIP.

●**“Broadcast”.** Są to sieci mogące mieć przyłączonych więcej niż dwa routery, zdolne do przekierowania jednej fizycznej wiadomości do wszystkich podłączonych routerów. Jest to rodzaj sieci domyślnie wybierających interfejsy Ethernet i Token-Ring.

●**“Non-Broadcast”(NBMA).** Są to sieci mogące mieć przyłączonych więcej niż dwa routery, lecz które nie mają zdolności broadcastu, choć dzięki konfiguracji są w stanie go emulować. Jest to rodzaj sieci domyślnie wybierający interfejs X25.

●**“Point-to-Mpoint broadcast”.** Są to sieci z więcej niż dwoma routerami, z częściową topologią siatki, zasadniczo o topologii gwiazdy. Poza tym sieć podtrzymuje bądź emuluje ruch broadcast, dzięki czemu nie ma potrzeby konfiguracji sąsiadów.

●**“Point-to-Mpoint non-broadcast”.** Są to sieci z więcej niż dwoma routerami, z częściową topologią siatki. Przepływ ruchu musi przechodzić przez punkt centralny. Poza tym sieć nie przytrzymuje ani nie emuluje ruchu broadcast, przez co niezbędna jest konfiguracja sąsiadów. Jest to rodzaj sieci domyślnie wybierający interfejs Frame-Relay. ROUTER

2.4.2 Działanie protokołu OSPF

Podstawowa sekwencja działań wykonywanych przez ten protokół jest następująca:

- Wykrywanie sąsiadów OSPF
- Wyznaczanie DR
- Tworzenie obszarów przylegających
- Synchronizacja baz danych
- Obliczanie tablicy routingu
- Ogłaszanie stanu łączy

Routery wykonają wszystkie te kroki podczas swojej aktywacji i powtórzą je w odpowiedzi na zdarzenia sieciowe.

Każdy router musi wykonać te kroki dla każdej sieci, do której jest podłączony, z wyłączeniem obliczania tablicy routingu.

Każdy router generuje i utrzymuje tylko jedną tablicę routingu dla wszystkich sieci.

Poniżej opisanych jest wszystkich sześć kroków działania OSPF.

2.4.2.1.1 Wykrywanie sąsiadów OSPF

Gdy routery OSPF się aktywują, nawiązują i utrzymują powiązanie ze swoimi sąsiadami za pomocą protokołu Hello. Dodatkowo protokół zapewnia, że komunikacja między sąsiadami jest dwukierunkowa.

Pakiety Hello wysyłane są okresowo na zewnątrz przez wszystkie interfejsy routerów. Komunikacja dwukierunkowa pojawia się gdy sam router pojawia się w pakiecie Hello swojego sąsiada.

2.4.2.1.2 Wyznaczanie DR

Używa się protokołu Hello. Router bada listę swoich sąsiadów, odrzuca tych, z którymi nie ma komunikacji dwukierunkowej lub które nie mają widocznego RP i zapisuje DR, BDR i RP zgłoszone przez każdego z nich. Router samoczynnie dodaje się do listy, używając wartości RP skonfigurowanej dla interfejsu zero (nieznany) dla DR i BDR, w przypadku gdyby proces był w momencie aktywacji. Wyznacza się BDR i DR.

Zamiar mechanizmu jest następujący: gdy router się aktywuje, nie powinien uzurpować pozycji obecnego BDR, choćby miał wyższy RP. BDR zastępuje DR w sposób uporządkowany. Wymagane jest, by BDR przejął jego obowiązki.

Algorytm nie zawsze sprawia, że router o największym priorytecie jest DR, ani że drugi pod względem ważności będzie DR.

2.4.2.1.2.1 Funkcje DR i BDR

DR generuje do sieci ogłoszenia stanu łączy obejmujących obszar oraz opisuje tę sieć wszystkim routerom ze wszystkich sieci obszaru.

DR staje się przyległy do innych routerów sieci.

BDR staje się przyległy do wszystkich pozostałych routerów sieci. Gwarantuje to, że gdy będzie zajmował miejsce DR, będzie mógł to uczynić szybko.

2.4.2.1.3 Tworzenie obszarów przylegających

Następna decyzja dotyczy tego czy należy utworzyć obszar przylegający do jednego z sąsiadów:

W sieciach wielodostępowych wszystkie routery stają się przyległe do DR i BDR. W przypadku łączy typu punkt- punkt (wirtualnych), każdy router zawsze tworzy obszar przylegający z routerem z drugiego końca.

Jeśli podejmie się decyzję by nie tworzyć obszarów przylegających, stan komunikacji z sąsiadem pozostaje w stanie “2-way”.

Obszary przylegające tworzy się z wykorzystaniem pakietów DD (“Database Description”).

W celu opisania bazy danych stosuje się procedurę zapytania-odpowiedzi.

Router o największym ID staje się routerem dominującym, a drugi- podrzędnym. Pakiety DD wysyłane przez router dominujący (zapytanie) rozpoznawane są przez DD routera podrzędnego (odpowiedź). Pakiet zawiera liczbę sekwencji zapewniającą zgodność między zapytaniem a odpowiedziami. Ten proces nazywa się DEP (“Database Exchange Process”).

2.4.2.1.4 Synchronizacja baz danych

Po zakończeniu DEP (“Database Exchange Process”), każdy router posiada listę tych ogłoszeń, dla których sąsiad ma najwięcej zaktualizowanych zapytań, które składa się za pomocą pakietów LSR (“Link State Request”).
Odpowiedzią na LSR jest LSU (“Link State Update”), zawierający niektóre lub wszystkie ogłoszenia, o które poproszono.

Jeśli odpowiedź się nie powtórzy, żądanie się powtarza. Ogłoszenia przychodzą w następnych pięciu formatach.

Gdy odpowie sie na pakiety LSR, bazy danych się synchronizują, a routery opisują się jako całkowicie przylegające.

Obszar przyległy dodaje się do ogłoszenia obu odpowiednich routerów.

2.4.2.1.5 Obliczanie tablicy routingu

Router, używając jako punktu wyjścia baz danych o stanach łączy obszarów, z którymi jest połączony, wykonuje algorytm SPF, w celu stworzenia swojej tablicy routingu.

Obliczenie polega na następujących krokach:

- Ścieżki wewnątrzobszarowe obliczane są tworząc minimalne drzewa dla każdego podłączonego obszaru, z zastosowaniem routera jako podstawy drzewa. Poza tym router oblicza czy obszar może być obszarem tranzytowym dla wirtualnych łączy.

- Ścieżki wewnątrzobszarowe obliczane są sprawdzając SLA. Dla ABR (które tworzą część pnia drzewa) używane są tylko ogłoszenia odpowiadające pniowi.

- Jeśli router podłączony jest do jednego lub więcej obszarów tranzytowych, router zastępuje ścieżki, które obliczył, ścieżkami przechodzącymi przez obszary tranzytowe, o ile są one lepsze.

- Ścieżki zewnętrzne obliczane są poprzez badanie zewnętrznych ogłoszeń AS. Lokalizacje ASBR są już znane, gdyż wyznaczane są tak jak każda ścieżka wewnątrz lub międzyobszarowa.

2.4.2.1.6 Ogłaszanie stanu łączy

Router okresowo ogłasza stan swojego łącza, dlatego brak nowych ogłoszeń wskazuje sąsiadom, że router nie jest aktywny. Wszystkie routery, które nawiązały dwukierunkową komunikację z sąsiadem, w celu wykrycia tego zdarzenia dokonują obliczenia bezczynności.
Komunikację należy nawiązywać od zera, łącznie z ponowną synchronizacją baz danych. Router ponownie wysyła swoje ogłoszenia gdy zmienia się stan.

Router może wysłać różne ogłoszenia dla każdego obszaru. Te rozpowszechniają się w obszarze w procesie zalewania. Każdy router wysyła RLA. Jeśli dodatkowo router jest DR dla jednej lub więcej sieci w obszarze, wytwarza dla nich NLA. ABR generują SLA dla każdego znanego międzyobszarowego punktu docelowego. ASBR wytwarzają ASL dla każdego znanego zewnętrznego punktu docelowego. Miejsca docelowe ogłaszają się zawsze w taki sposób, że zmiana choćby jednej ścieżki może zalać sieć bez konieczności wysyłania pozostałych ścieżek. Podczas procesu zalewania jeden LSU może mieć wiele ogłoszeń.

2.4.3 Protokół VRRP

VRRP (Virtual Router Redundancy Protocol) jest protokołem, który zajmuje się dynamicznym przypisaniem funkcji wirtualnego routera jednemu z routerów VRRP wewnątrz sieci LAN. Router VRRP kontrolujący kierunek przypisany do wirtualnego routera nazywa się Master. Bierze na siebie zadanie nakierowania pakietów wysyłanych poprzez ten adres IP. Gdy Master przestaje być dyspozycyjny, inny z routerów VRRP bierze na siebie odpowiedzialność za trasowanie w adresie wirtualnego routera, co pozwala na dynamiczną rekuperację w przypadku zaistniałego błędu. Dzięki temu każdy z adresów IP przypisanych do wirtualnego routera może być użyty jako adres pierwszego skoku (lub automatycznie ścieżki) urządzeń będących w sieci LAN.

Główną zaletą uzyskiwaną z użytkowania VRRP jest większa automatyczna dyspozycyjność routera, bez potrzeby konfigurowania trasowania dynamicznego lub protokołów wykrywających routery w każdym końcowym urządzeniu. VRRP zaprojektowany jest do eliminowania właściwego punktu błędu w obszarach skonfigurowanych z automatyczną ścieżką statyczną.

VRRP opisany jest dokładnie w dokumencie RFC 3768 “Virtual Router Redundancy Protocol (VRRP)”.

2.4.3.1 Właściwości Protokołu VRRP

VRRP dostarcza wyżej opisaną funkcjonalność wirtualnego routera.

Poniżej podane są definicje i pojęcia związane z protokołem VRRP:

●Router VRRP: Router używający protokołu VRRP. Router VRRP może uczestniczyć w jednym lub więcej routerów wirtualnych.

●Router wirtualny: Element abstrakcyjny sterowany przez routery VRRP, działający jako router automatycznie, gdy nie wybierze się urządzeń z sieci LAN. Router VRRP może równocześnie zrobić backup kilku routerów wirtualnych.

●Właściciel adresu IP: Router posiadający wirtualny adres IP (przypisany do routera wirtualnego) jako rzeczywisty adres na którymś ze swoich interfejsów.

●Główny adres IP: Adres IP wybrany spośród całości adresów rzeczywistych interfejsów. Wiadomości o ogłoszeniu protokołu VRRP (Advertisements) zawsze wysyłane są z zastosowaniem głównego adresu IP jako adresu IP pochodzenia pakietu.

●MASTER routera wirtualnego: Router VRRP bierze na siebie przetwarzanie pakietów trasowanych poprzez adres IP przypisany do routera wirtualnego oraz odpowiadanie na petycje ARP tego wirtualnego IP.

●Jeśli WŁAŚCICIEL adresu IP jest dyspozycyjny i gotowy do pracy, to routerem wirtualnym ZAWSZE będzie MASTER.

●BACKUP routera wirtualnego: Wszystkie routery VRRP z sieci LAN gotowe do wzięcia na siebie odpowiedzialności routera wirtualnego w przypadku błędu Mastera.

2.4.3.2 Działanie Protokołu VRRP

Działanie protokołu VRRP opiera się na symulacji routera wirtualnego między różnymi routerami VRRP. Routerowi wirtualnemu przypisuje się wirtualny adres IP oraz wirtualny adres MAC. Te wirtualne adresy pozostają niezmienne i niezależne od routera rzeczywistego, który bierze na siebie trasowanie pakietów przypisanych do routera wirtualnego.

Protokół VRRP używa ogłoszeń (Advertisements) w celu wskazania, że router pełniący rolę Mastera jest aktywny. Te wiadomości wysyłane są na adres IP multicast 224.0.0.18 przyznany przez Internet Assigned Numbers Authority (IANA). Numer protokołu IP ustanowiony przez IANA dla VRRP to 112. Advertisements zawierają informacje o routerze wirtualnym, ich priorytetach itd.

Jeśli w trakcie określonego okresu czasu (Master_Down_Interval) routery zapasowe (Backup) przestają otrzymywać wiadomości od Mastera, wtedy router backup o największym priorytecie staje się nowym Masterem routera wirtualnego.

Automatycznie, jeśli któreś z urządzeń zapasowych miałoby większy priorytet niż obecny Master, może pozbawić go swych funkcji i stać się nowym Masterem. Takie działanie gwarantuje, że Masterem zawsze będzie router o największym priorytecie. Jednakże jeśli z jakiegoś powodu zajdzie taka konieczność, będzie można administracyjnie odebrać zdolność do pozbawiania routera wirtualnego jego funkcji.

2.5.- REDUNDANCJA

ACISA zaprojektowała topologię tej sieci z myślą głównie o jej wysokiej dostępności oraz solidnej architekturze. Fizycznie zaprojektowano zdublowany system łączności pomiędzy skrzyżowaniami (topologia wielokrotnych pierścieni) bazujący na łączności TCP/IP, wdrożonej w sieci światłowodowej.

Zgodnie z wymogami PFU zdecydowano o użyciu trzech protokołów rezerwowych, które spełniają wszystkie wymagane cechy takie, jak: MRP, Ring-Coupling oraz protokół VRRP. Dwa pierwsze są z poziomu 2 (Switching), a trzeci z poziomu 3 (Routing).

Za pomocą tych 3 protokołów gwarantujemy ciągłości dzięki bardzo krótkiemu czasowi zbieżności (regeneracja interfejsu), pomiędzy 200 i 500 milisekund. Wdrożenie 2 protokołów rezerwowych poziomu 2 gwarantuje automatyczne przełączanie węzłów.

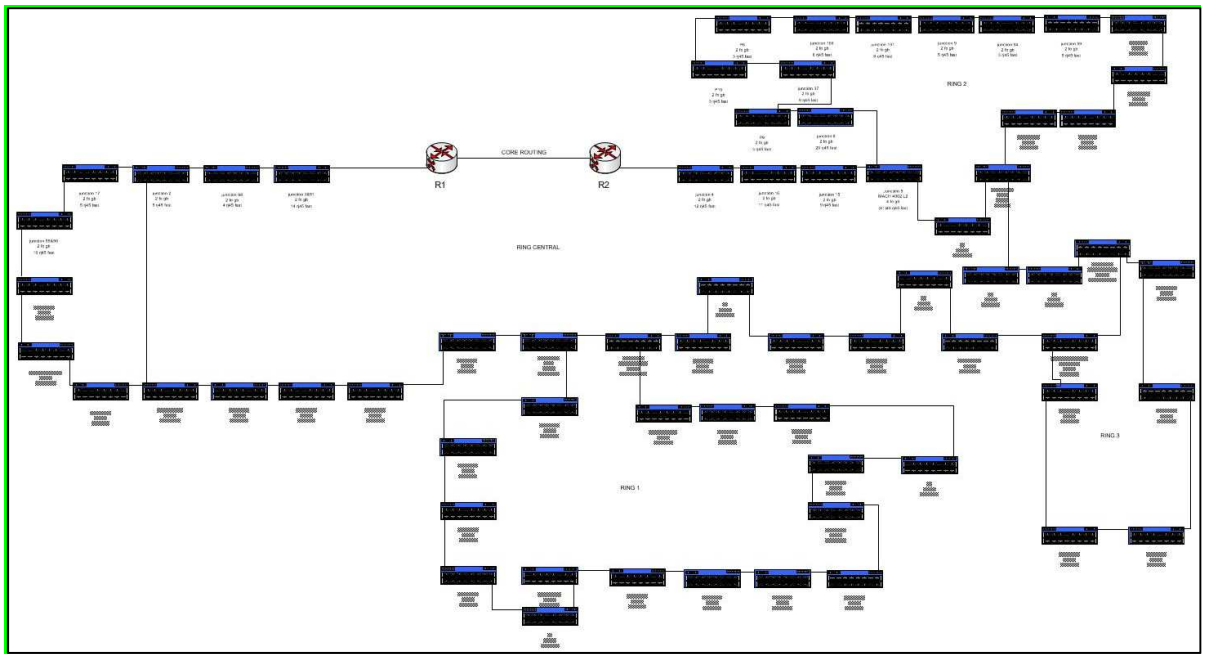
Następnie wyjaśnimy działanie każdego z protokołów oraz różnych przypadków awarii sieci, w których działać będzie ich system rezerwowy.

2.5.1 REDUNDANCJA FIZYCZNA

2.5.1.1 WIELE PIERŚCIENI ŚWIATŁOWODOWYCH

Sieć została zbudowana w taki sposób, że jest możliwe skonfigurowanie środkowego pierścienia, do którego dołączone zostaną 3 pierścienie podrzędne. Ta topologia jest również znana jako topologia wielokrotnych pierścieni. Architektura wielokrotnych pierścieni bazuje na topologii pierścienia.

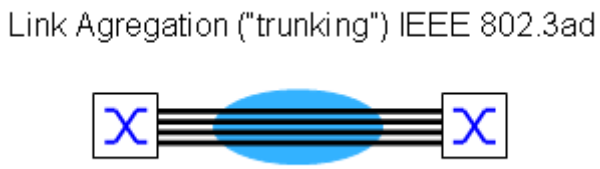
Topologia pierścienia składa się z pierścienia zamkniętego złożonego z węzłów i łączników, w którym każdy węzeł jest połączony jedynie z dwoma węzłami przyległymi. Ponieważ istnieje połączenie pomiędzy dwoma węzłami sprawia, że można wysłać/odebrać informację za pośrednictwem tych dwóch węzłów (decyzję o wysłaniu/odbiorze przez każdy z tych węzłów podejmie protokół zarządzający siecią).



2.5.1.2 Agregacja Łączy

Możliwa jest agregacja łączy, tzw. *link aggregation*, w celu zwielokrotnienia przepustowości.

Agregacja łączy, często określana terminem „*trunking*", jest częścią standardu IEEE 802.3. Standard zwany był wcześniej 802.3ad. Zapewnia redundancję będącą zabezpieczeniem na wypadek awarii łącza, a jednocześnie łączy wiele fizycznych połączeń do utworzenia jednego logicznego połączenia. Czas regeneracji według standardu wynosi ≤1 s.



Połączenia muszą być w trybie full-duplex i z tą samą szybkością transmisji danych. Możliwa jest agregacja różnych nośników.
The Link Aggregation Control Protocol LACP wykorzystywany jest do szybkiej aktywacji/dezaktywacji wszystkich dołączonych portów, również tych z innymi przełącznikami. Wykorzystuje się do tego multicast do 01:80:c2:00:00:02. Jeśli jeden z obydwu przełączników nie obsługuje LACP, można zastosować statyczną agregację.
Algorytm podziału ruchu jest - w zależności od konkretnego producenta- oparty na innym kryterium.
Transport danych jest zorganizowanym równoległym połączeniem, np.: połączenie pomiędzy dwoma urządzeniami może wykorzystywać tylko jedno z dodanych łączy!

2.5.2 REDUNDANCJA LOGICZNA

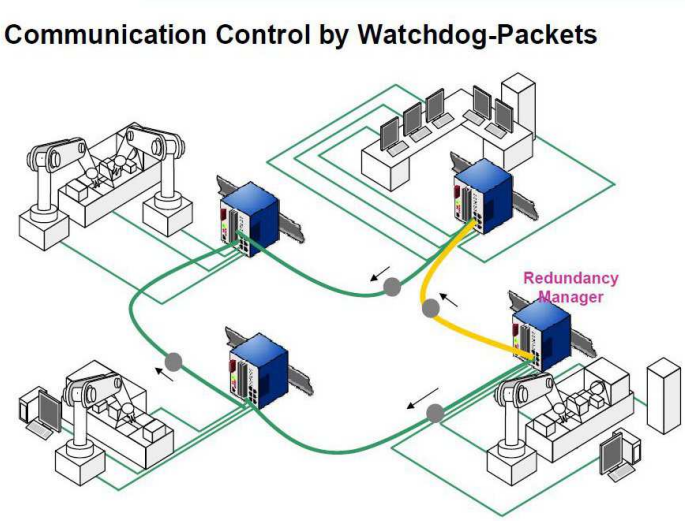
2.5.2.1 MRP (MEDIA RING PROTOCOL)

MRP jest protokołem poziomu 2 switching bazującego na adresach MAC. Zapobiega utracie łączności, jeśli połączenie jest zerwane. Umożliwia zarządzania rezerwą ruchu na pierścieniach Ethernet.
Ten protokół umożliwia również, by w przypadku zerwania jakiegoś połączenia, łączność była nawiązywana ponownie za pośrednictwem innego połączenia pierścienia w czasie nie krótszym niż 200ms, ale nie dłuższym niż 500ms.

2.5.2.1.1 Działanie protokołu

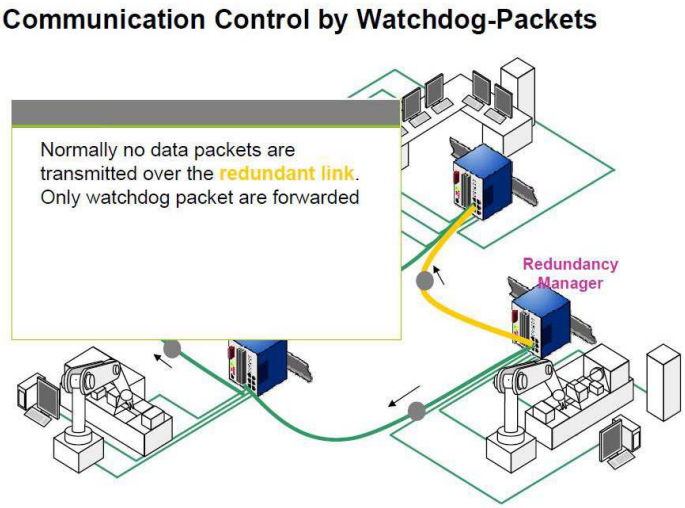
W sieci skonfigurowanej przy pomocy MRP jeden z przełączników należy skonfigurować jako Ring Manager (Redundancy Manager).

Ten sprzęt będzie wysyłał pakiety watchdog za pośrednictwem sieci w celu przetestowania integralności pierścienia.



Sterowanie komunikacją przy pomocy pakietów Watchdog

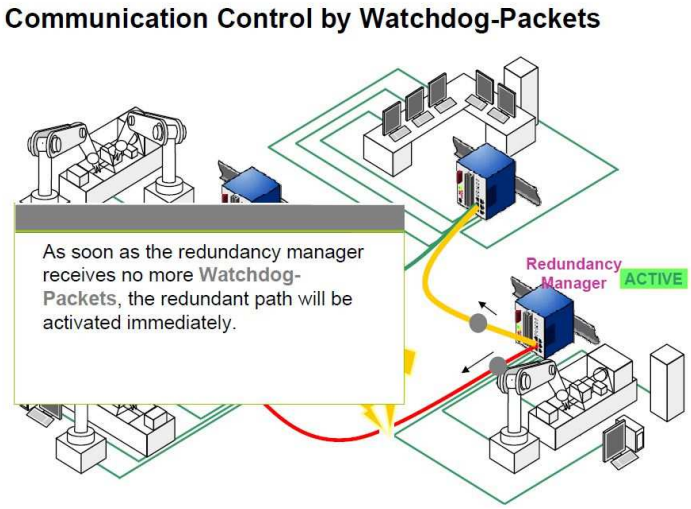
Pakiety watchdog przechodzą za pośrednictwem połączenia rezerwowego, podczas gdy normalne pakiety sieci Ethernet nie mogą tego uczynić.



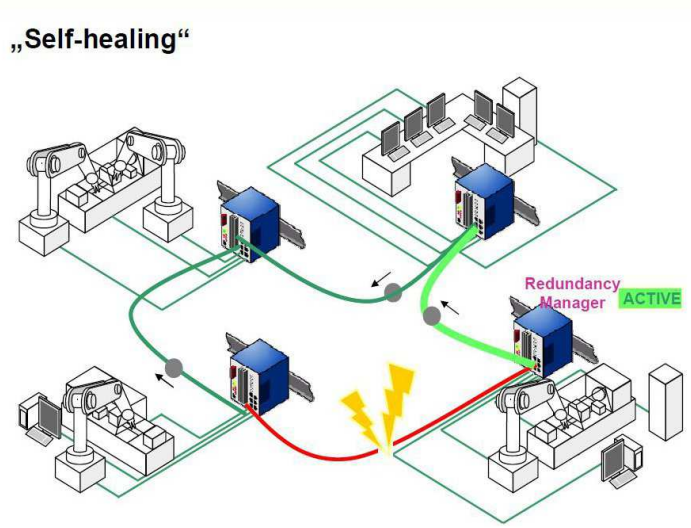
Sterowanie komunikacją przy pomocy pakietów Watchdog

Zazwyczaj żadne pakiety danych nie są przesyłane przez redundant link (złącze nadmiarowe). Przesyłane są wyłącznie pakiety watchdog

Jeśli Ring Manager/Redundancy Manager nie otrzymuje pakietów watchdog, ten włącza natychmiast połączenie rezerwowe.

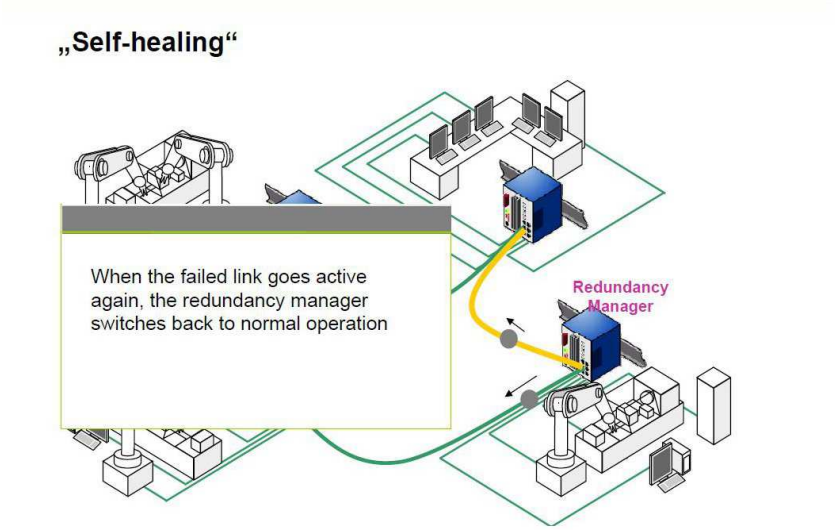


„Sterowanie komunikacją przy pomocy pakietów Watchdog
Jeśli Ring Manager/Redundancy Manager nie otrzymuje Pakietów Watchdog, ten włącza natychmiast połączenie rezerwowe”

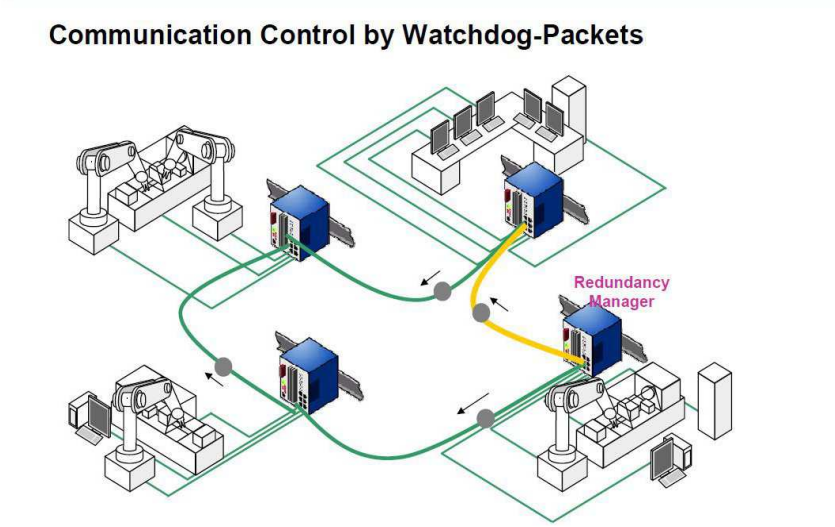


„Automatyczna naprawa”

Wszystkie switche pierścienia ponownie nawiązują swoje połączenia a ich łączność zostaje ponownie nawiązana w czasie pomiędzy 200 i maksymalnie 500 milisekund.
W przypadku naprawy zerwanego połączenia, Ring Manager ponownie pozostawia sieć w jej normalnym trybie działania.



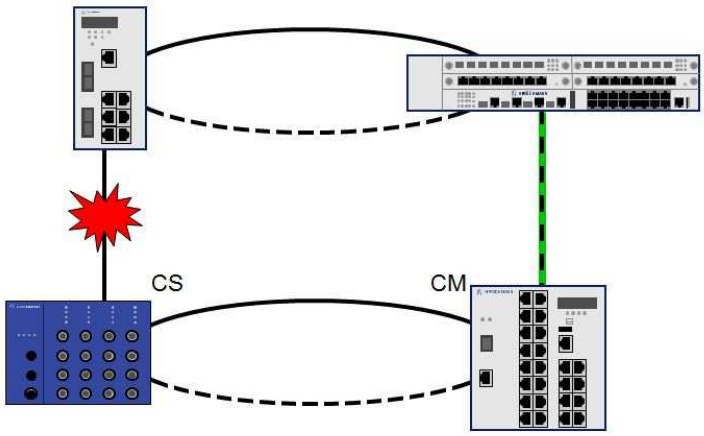
„Automatyczna naprawa”
W przypadku naprawy zerwanego połączenia, Ring Manager ponownie przełącza sieć do jej normalnego trybu pracy”



Sterowanie komunikacją przy pomocy pakietów Watchdog

2.5.2.2 RING-COUPLING

Ring Coupling/ Network Coupling: Pierścień lub sieć połączeniowa umożliwiają sprzężenie rezerwowe pierścieni rezerwowych oraz segmentów sieci. Network Coupling jest kompatybilny ze sprzężeniem pierścienia MRP z drugim pierścieniem MRP lub dla segmentu sieci wszelkiej struktury.
Ten protokół umożliwia nam połączenie trzech przyległych pierścieni do głównego pierścienia oraz zwiększenie tolerancji do awarii nawet 4 odcięć w sieci jednocześnie (jedno na pierścień).



2.5.2.2.1 Działanie RING-Coupling

Ten protokół będzie używany w celu zagwarantowania wysokiej dostępności podwyższonego systemu rezerwowego oraz tolerancji.

W tym celu należy skonfigurować dwa ze switchy pierścienia głównego jeden jako Coupling Manager "CM" a drugi jako Coupling Switch "CS".

Jeśli pierwsze połączenie (które łączy CS ze switchem drugiego pierścienia) wyłącza połączenie rezerwowe (które łączy CM do drugiego switcha drugiego pierścienia) natychmiast się włącza.

Kontrola rezerwy jest wykonywana przez dwa urządzenia, które się łączą między sobą pierścienie: CS oraz CM.

CS i CM łączą się ze sobą w celu kontroli rezerwy Ring Coupling, aby w ten sposób uniknąć zapętleń w czasie działania ustanawiania połączeń.

Po awarii połączenia głównego, CM otwiera połączenie rezerwowe. Jak tylko ponownie zacznie działań połączenie główne, CS podłączony do tej linii głównej poinformuje o tym CM. Połączenie rezerwowe zostanie ponownie zablokowane przez CM, a połączenie główne zostanie wznowione przez CS.

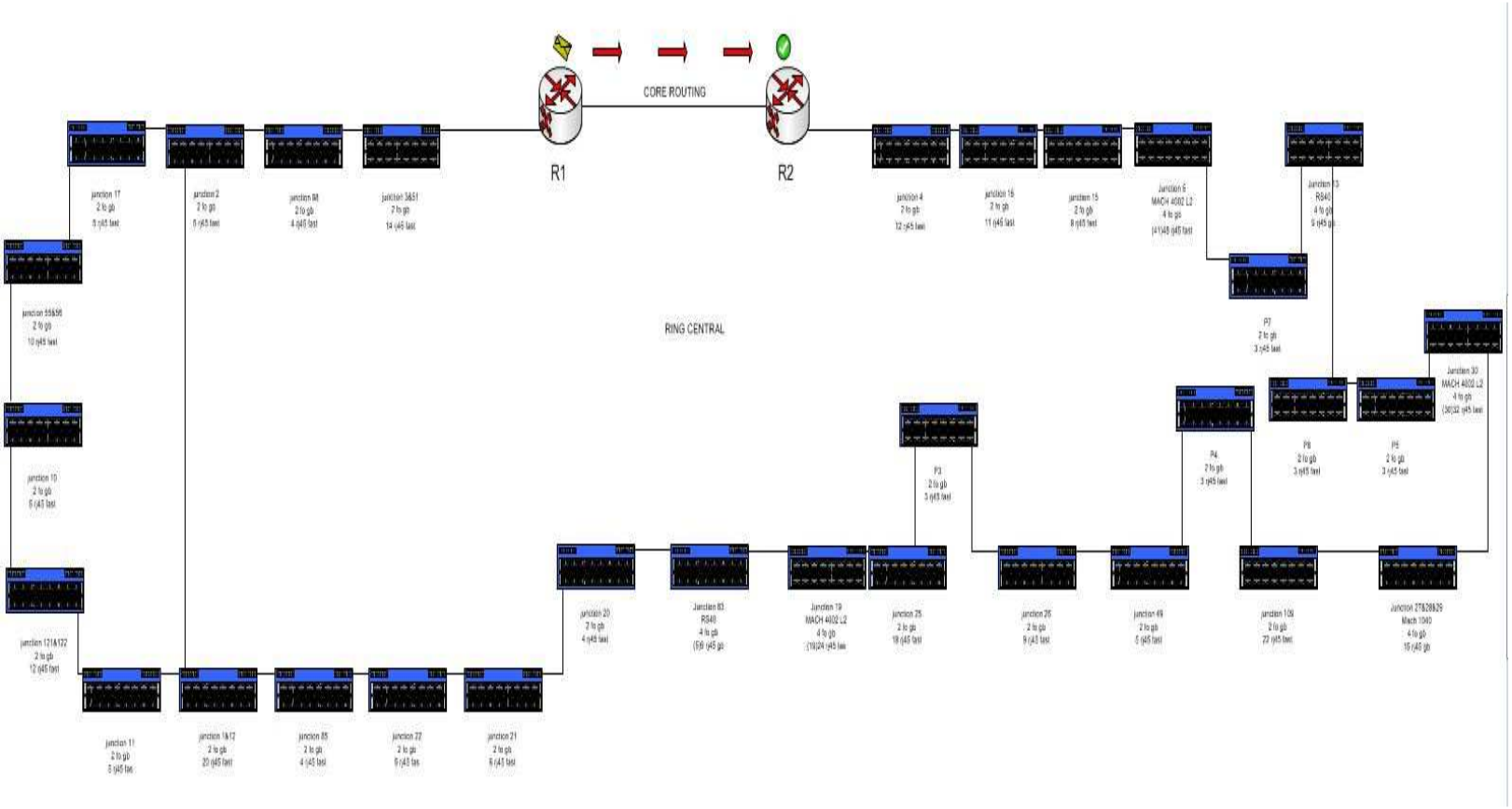
2.5.2.3 Błędy/Awarie, które mogą wystąpić w sieci

2.5.2.3.1 Pęknięcie światłowodu na pierścieniu

W przypadku pęknięcia na odcinku na jednym z pierścieni światłowodu czas zbieżności powinien wynieść pomiędzy 200 a 500 ms, a sieć powinna nadal działać bez żadnych anomalii.

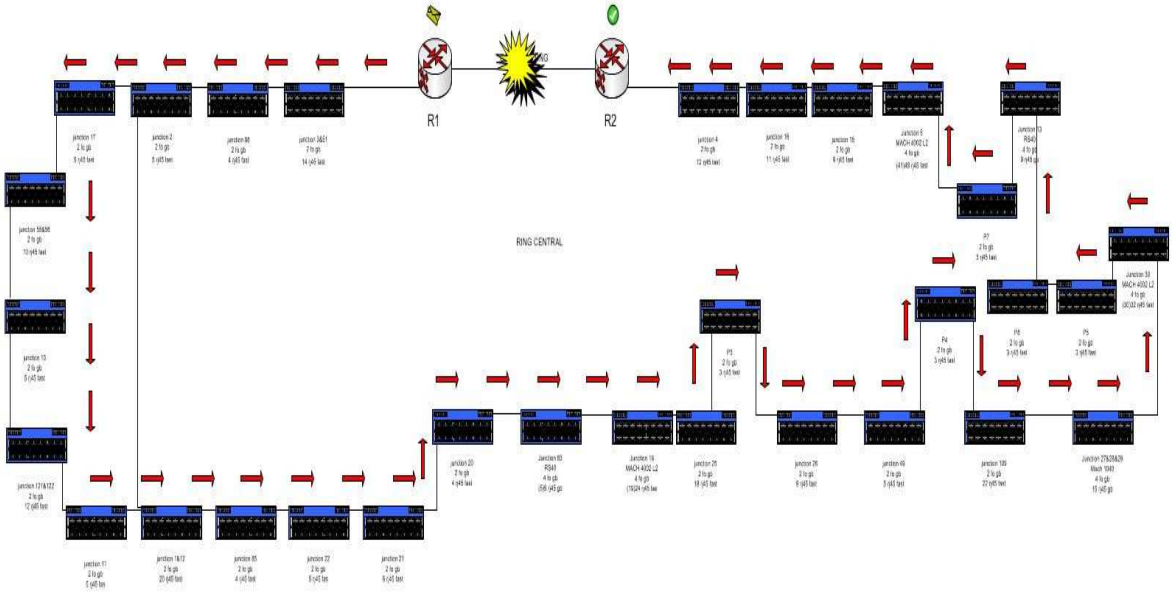
2.5.2.3.1.1 PIERŚCIEŃ CENTRALNY

W następnym przykładzie pokażemy, jak wygląda łączność pomiędzy R1 i R2, kiedy sieć jest w normalnym stanie.
Protokół MRP wybiera najkrótszy odcinek w celu wykonania połączeni



Junction – węzeł
Ring central – pierścień centralny
Core routing – główny przesył

W przypadku zaistnienia pęknięcia na odcinku, który łączy R1 i R2 łączność powinna następować drogą alternatywną. Tak, jak to przedstawiono na następującym obrazku:

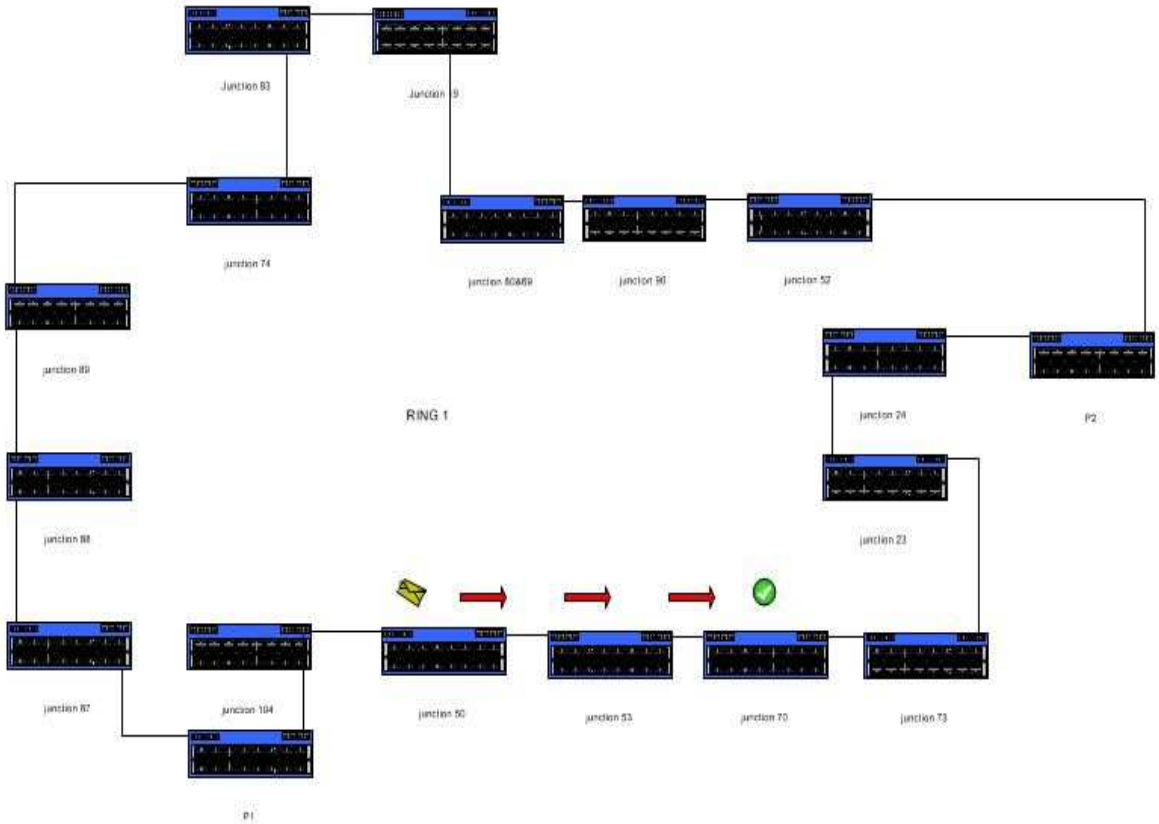


Junction – węzeł
Ring central – pierścień centralny

Ponieważ jest to pęknięcie fragmentu światłowodu żadne urządzenie końcowe nie przestanie pracować, gdyż istnieje alternatywna droga i wszystkie urządzenia nadal będą podłączone do sieci i będą działały za jej pośrednictwem.
Tak, jak to pokazaliśmy na pierścieniu głównym, pierścienie przylegle również wykonają ten sam proces.

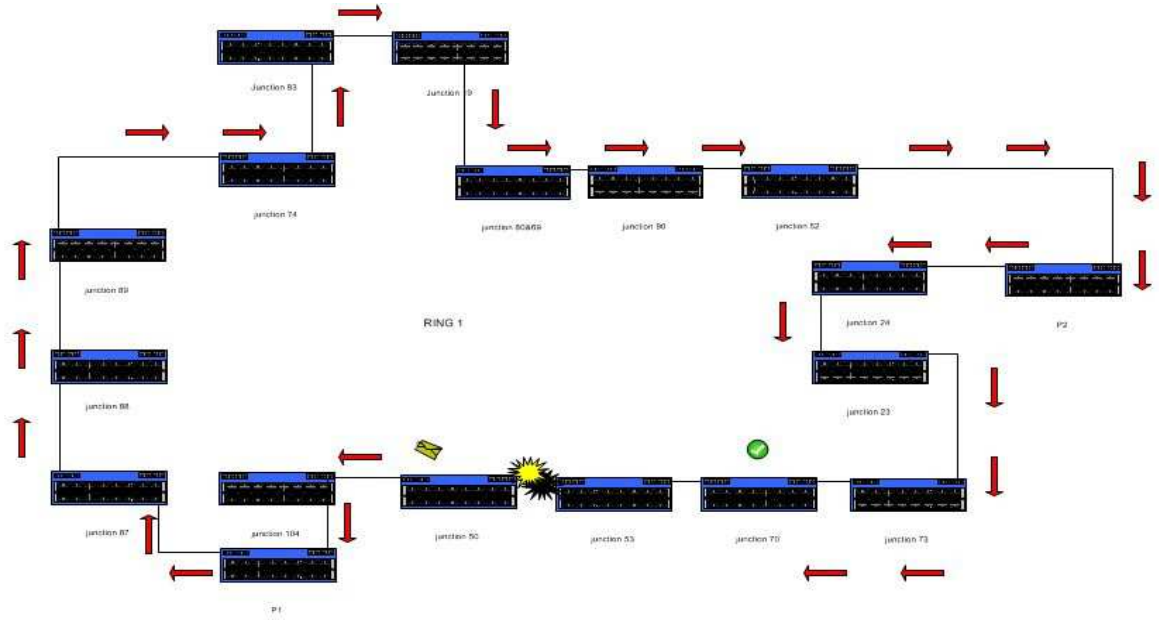
2.5.2.3.1.2 PIERŚCIEŃ 1

Na następnym schemacie pokażemy, jak działa łączność pomiędzy węzłem 50 a węzłem 70, kiedy sieć jest w stanie normalnym.



Junction – węzeł
Ring - pierścień

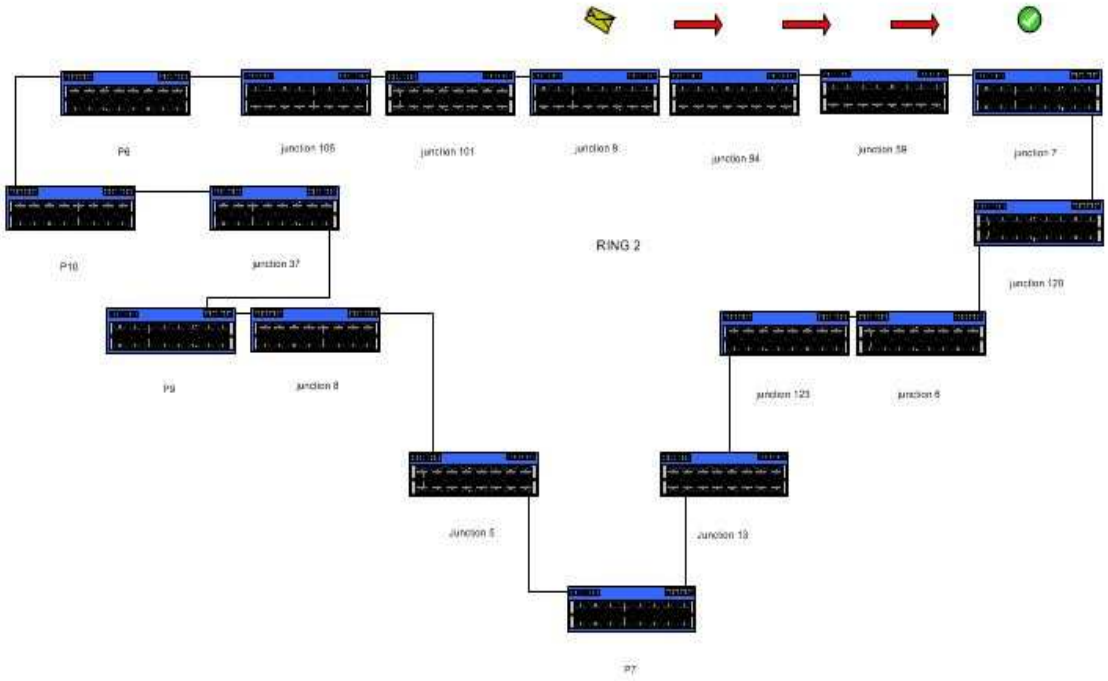
Symulując zerwanie na odcinku łączącym węzeł 50 z węzłem 53, łączność będzie się odbywała drogą alternatywną, jak to pokazano w dalszej części.



Junction – węzeł
Ring - pierścień

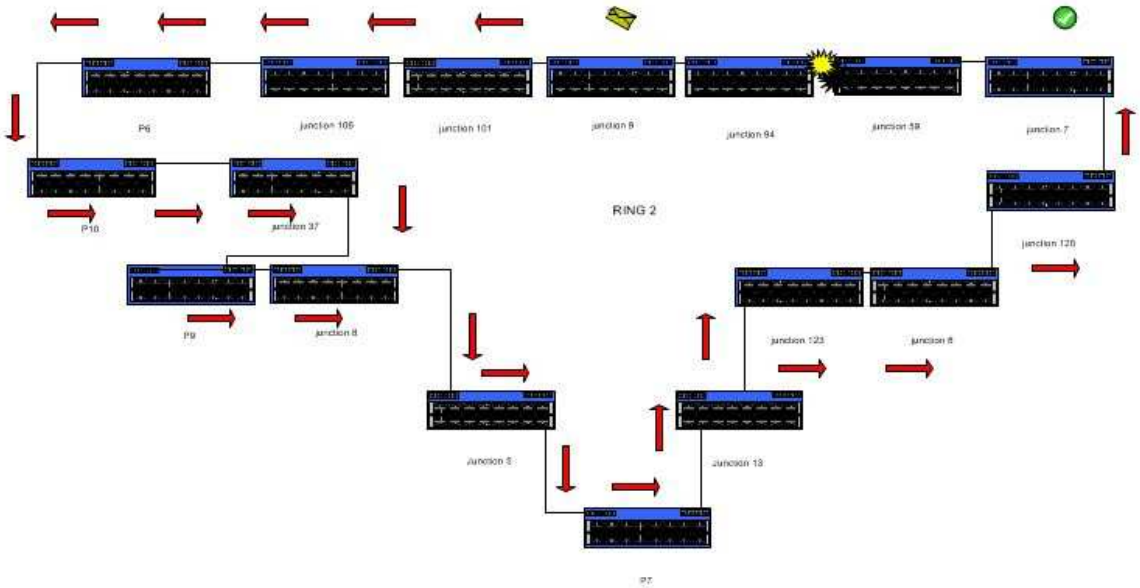
2.5.2.3.1.3 PIERŚCIEŃ 2

Na następnym schemacie pokażemy, jak działa łączność pomiędzy węzłem 50 a węzłem 70, kiedy sieć jest w stanie normalnym.



Junction – węzeł
Ring - pierścień

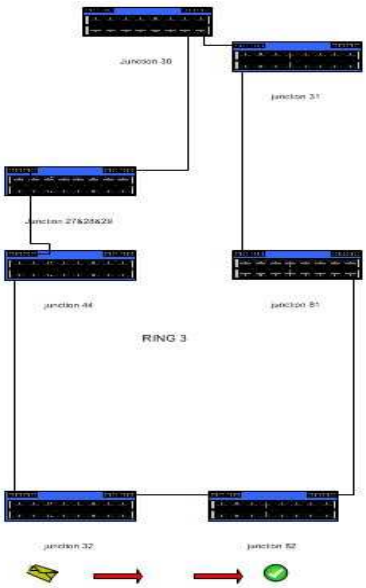
Prowokując zerwanie na odcinku łączącym węzeł 94 z węzłem 59, łączność będzie się odbywała drogą alternatywną, jak to pokazano w dalszej części.



Junction – węzeł
Ring - pierścień

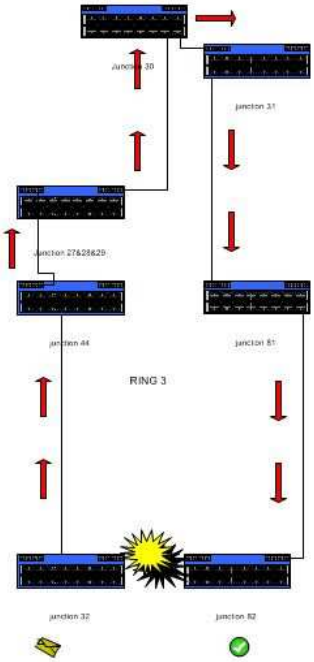
2.5.2.3.1.4 PIERŚCIEŃ 3

Na następnym schemacie pokażemy, jak działa łączność pomiędzy węzłem 32 a węzłem 70, kiedy sieć jest w stanie normalnym.



Junction – węzeł
Ring - pierścień

W przypadku zerwania na odcinku łączącym węzeł 32 z węzłem 82, łączność będzie się odbywała drogą alternatywną, jak to pokazano w dalszej części.

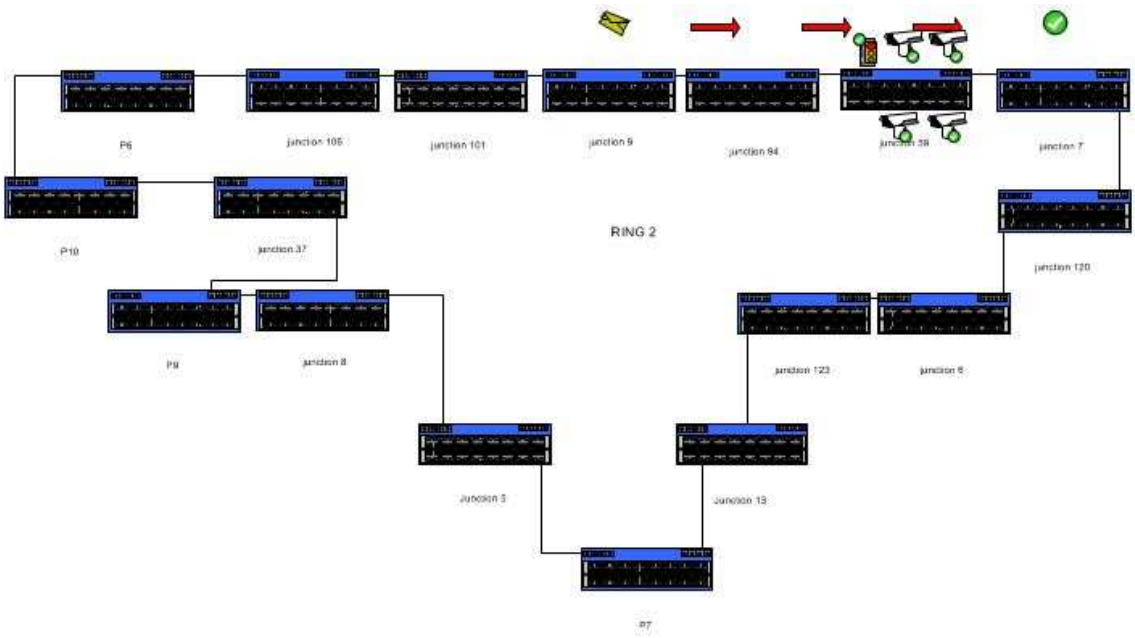


Junction – węzeł
Ring - pierścień

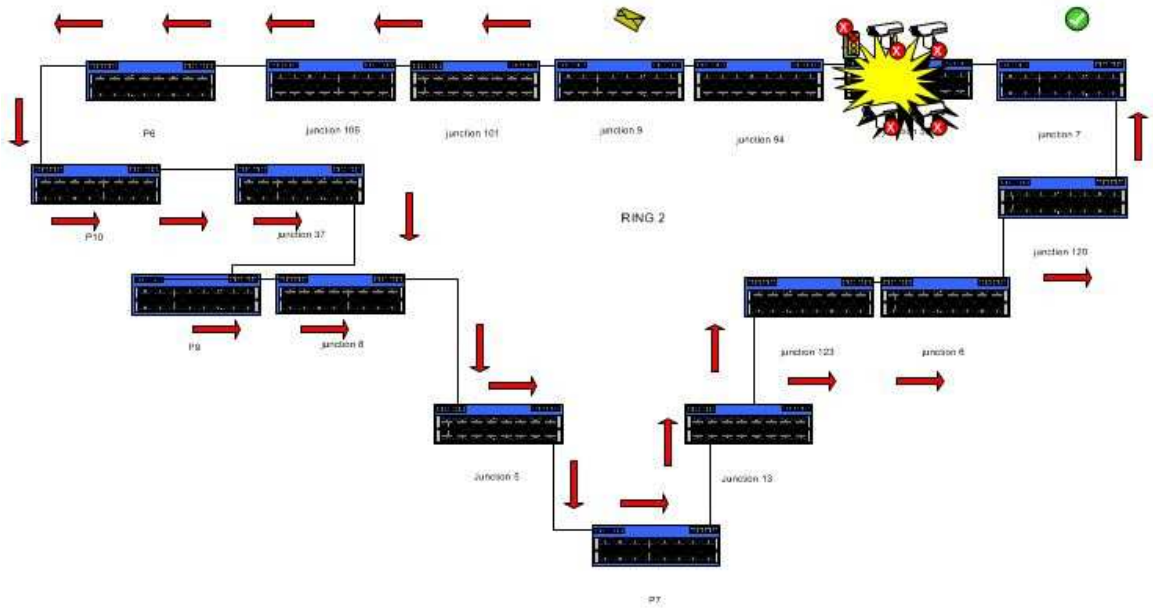
2.5.2.3.2 Zerwanie urządzenia sieciowego

W przypadku wystąpienia błędu tego rodzaju protokół łączności wykonuje ten sam proces, co w przypadku poprzednim, z jedyną różnicą, że sprzęt końcowy (kamery, sygnalizacja świetlna, itd…), które są podłączone do niego, przestają się łączyć za pośrednictwem sieci do czasu, kiedy przełącznik nie zostanie naprawiony lub wymieniony.

W następnym schemacie pokażemy, jak wygląda łączność pomiędzy urządzeniami sieci różnych pierścieni w stanie normalnym.



Junction – węzeł
Ring - pierścień



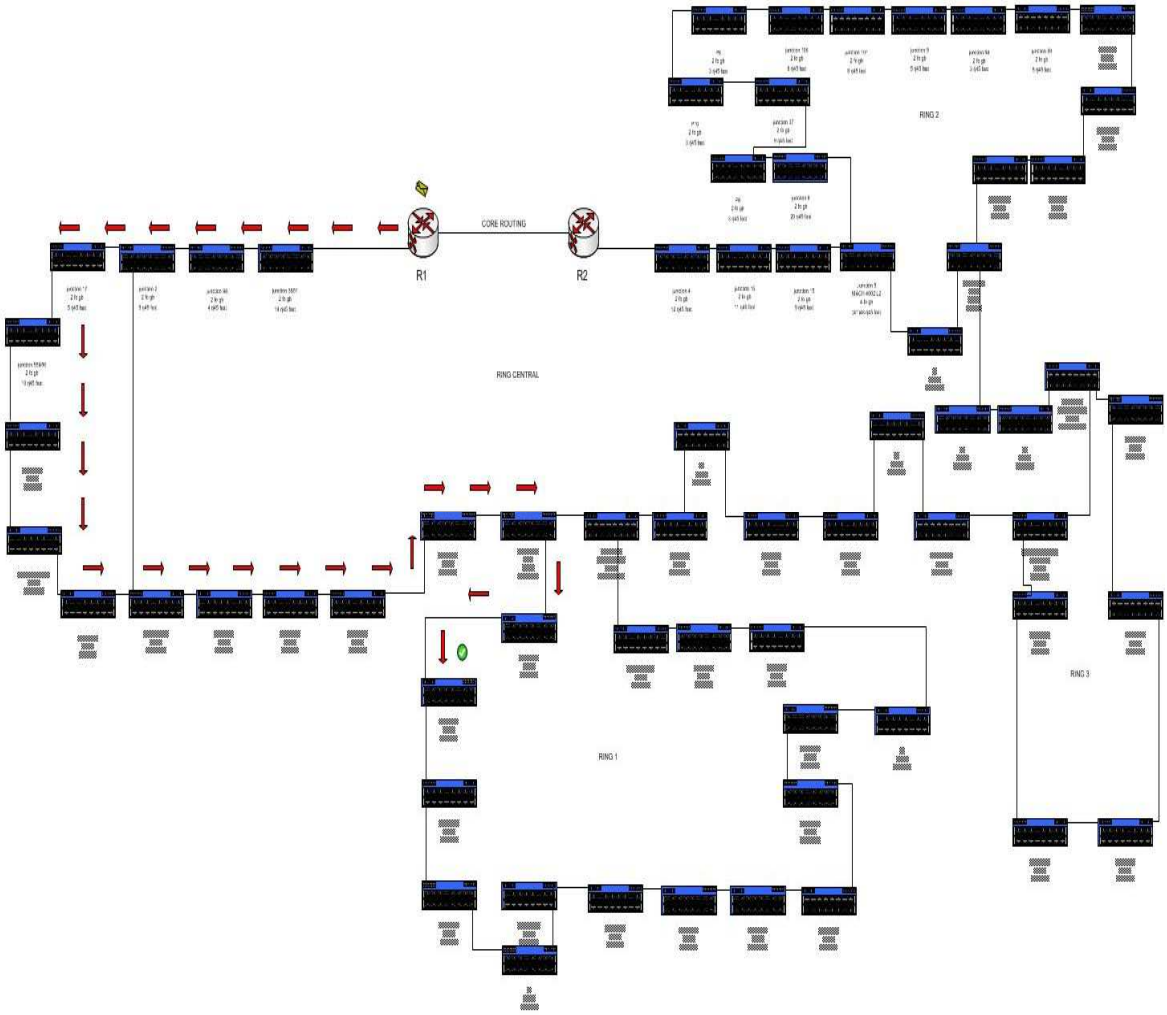
Junction – węzeł
Ring - pierścień

2.5.2.3.3 Pęknięcie światłowodu na odcinku Ring Coupling

Tak, jak to wyjaśniono poprzednio, połączenie 4 pierścieni ma miejsce za pomocą protokołu Ring-Coupling.

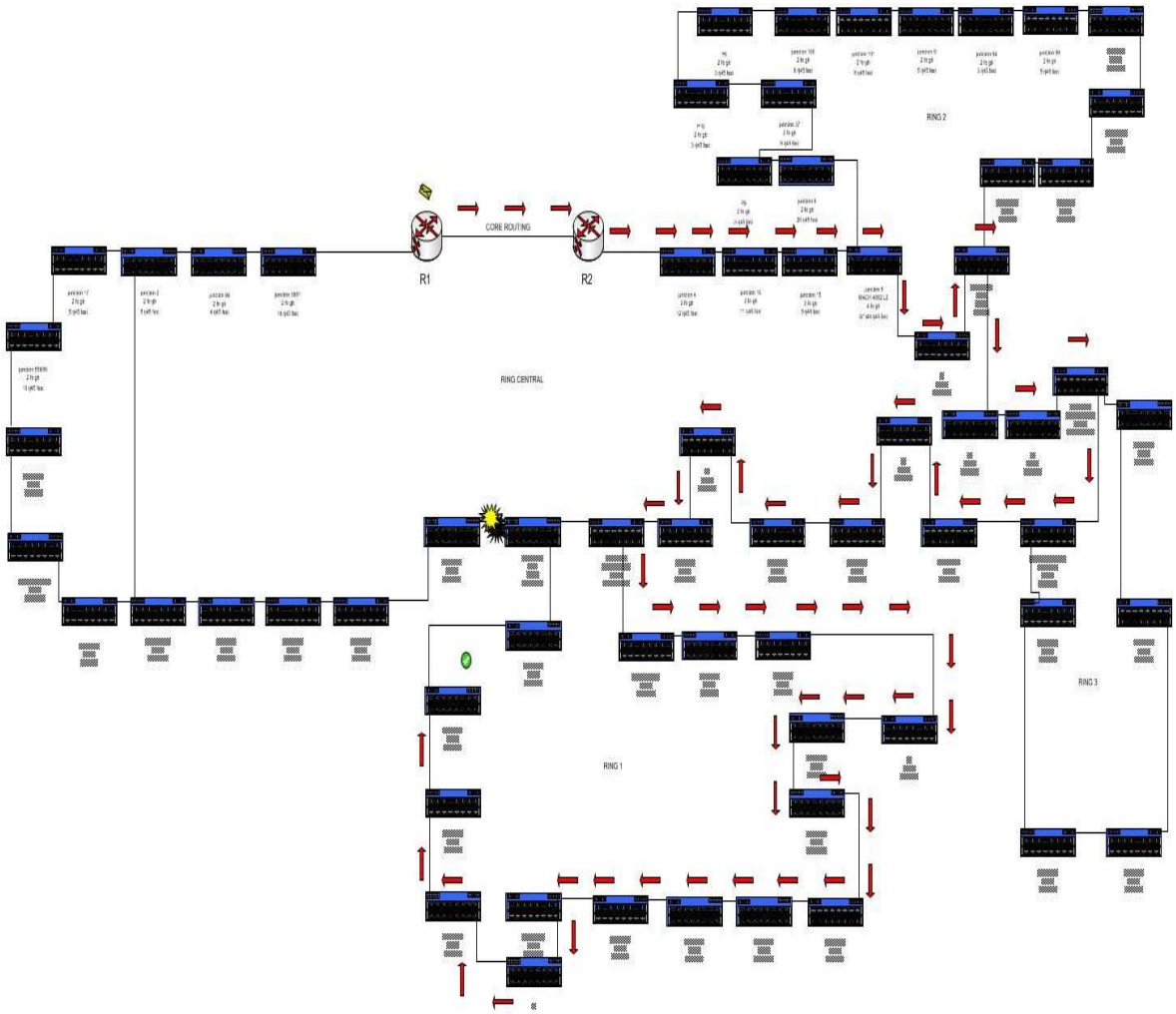
W przypadku wystąpienia awarii na jednym z dwóch połączeń, łączących jeden pierścień z pierścieniem centralnym, w sposób automatyczny włączone zostanie połączenie rezerwowe przekazując cały ruch do czasu, aż zostanie przywrócone połączenie główne.

Na następnym schemacie pokażemy, jak wygląda łączność pomiędzy urządzeniami sieci różnych pierścieni w stanie normalnym.



Junction – węzeł
Ring central – pierścień centralny
Core routing – główny przesył

Na następnym schemacie pokazujemy ruch alternatywny, który wykonują dane w przypadku, kiedy odcinek na którym łączą się pierścienie ulegnie awarii.



Junction – węzeł
Ring central – pierścień centralny
Core routing – główny przesył

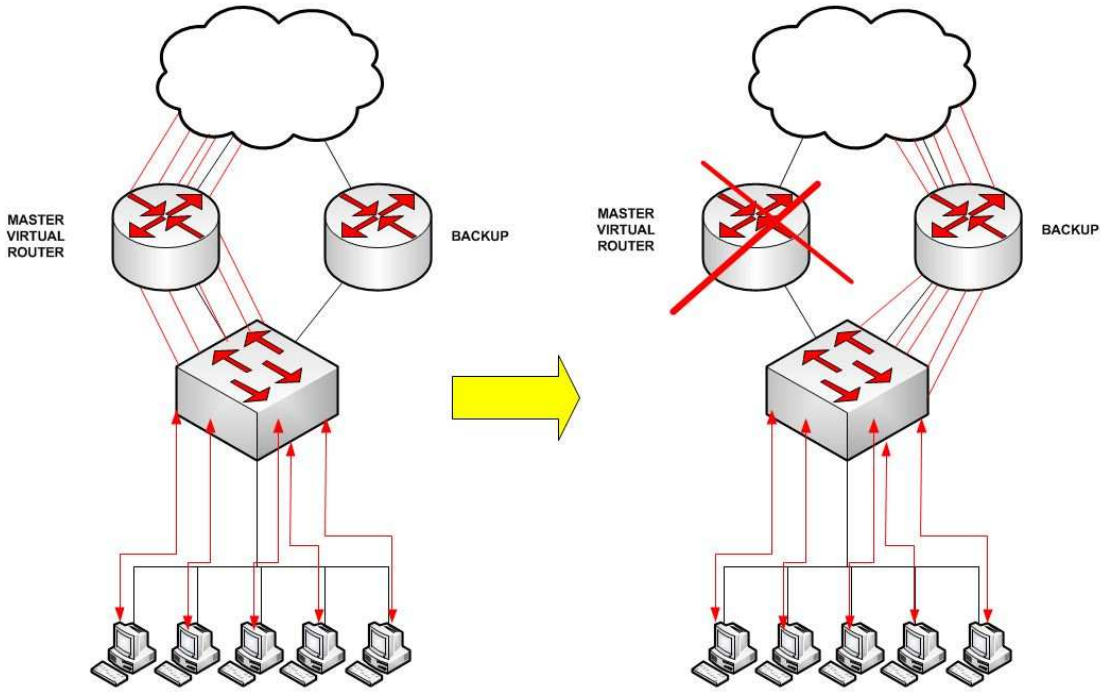
2.5.2.4 VRRP

Głównym celem niniejszego protokołu jest ochrona przed utratą danych i ich bezpieczna transmisja pomiędzy dwoma urządzeniami. Powszechnie jest nazywany systemem switching i działa jako układ zapasowy w przypadku przerwanego połączenia.

Jedną z głównych i bardzo ważnych zalet jest to, że VRRP zapewnia niezawodną pracę przez wykonywanie kopii zapasowych plików.

2.5.2.5 Błąd połączenia na ruterze Głównym

W przypadku, kiedy ruter główny lub połączenie łączące go do sieci ulegnie awarii, ruter zapasowy przejmie wszelkie zapytania sprzętu w sposób automatyczny tak, jak to pokazano na następującym obrazku.


MASTER
VIRTUAL
ROUTER
BACKUP
MASTER
VIRTUAL
ROUTER
BACKUP

2.6.- MULTICAST

Do prawidłowego działania sieci wielousługowej Lublina muszą zostać skonfigurowane usługi zarządzania multicastem. Te usługi są do dyspozycji na różnych poziomach zarządzania (L2 i L3).

Zaproponowany system spełnia wszystkie wspólne normy zarządzania multicastem sieci systemów kontroli ruchu miejskiego.

2.6.1 WPROWADZENIE

W chwili przekierowania hosta (interfejsu) wewnątrz sieci można użyć trzech różnych rodzajów transmisji:

•Transmisja unicast. Ten rodzaj transmisji odnosi się do tylko jednego hosta (interfejsu) wewnątrz podsieci. Przykładem unicastowego adresu IP jest 192.168.100.9. Unicastowym adresem MAC jest, na przykład, 80:C0:F6:A0:4A:B1.

• Transmisja broadcast. Za pomocą tej transmisji można przekierować wszystkie hosty (interfejsy) wewnątrz jednej sieci. Broadcastowym adresem IP jest 192.168.100.255, a broadcastowym adresem MAC jest FF:FF:FF:FF:FF:FF.

• Transmisja multicast. Ten rodzaj transmisji pozwala przekierować konkretną grupę hostów (interfejsów) wewnątrz jednej podsieci. Transmisji multicastowej używa się wtedy, gdy odbiorcą informacji ma być nie tylko jedna maszyna, lecz także gdy nie chce się wykonywać broadcastu do całej sieci. Takie działanie jest typowe w sytuacjach, w których wymagana jest wysyłka informacji multimedialnych (audio lub video w czasie rzeczywistym) do wielu hostów sieci. W przypadkach takich jak omawiany, biorąc pod uwagę szerokość pasma, wysyłka unicastowa do każdego z klientów chcących odbierać emisję multimedialną nie jest optymalnym rozwiązaniem. Ustanowienie transmisji broadcatowej także nie jest dobrym rozwiązaniem, szczególnie, gdy któryś z klientów znajduje się poza lokalną podsiecią, z której dokonuje się wysyłki. Jeśli host łączy się do grupy mulicastowej, otrzymuje całą transmisję unicastową do niego skierowaną, broadcast skierowany do całej podsieci oraz transmisję mulicastową skierowaną do grupy, do której się przyłączył.

2.6.2 DZIAŁANIE MULTICASTU

Zawartość transmisji dociera w któryś z dwóch następujących sposobów: unicast punkt do punktu lub multicast. W przypadku unicastu dane wysyłane są w oddzielnych transmisjach od źródła do każdego użytkownika, który ich zażąda. Ta metoda dobrze działa w sytuacji, gdy każdy z użytkowników pragnie zawartości innej niż pozostali, lecz nie gdy wielu ludzi chce tej samej zawartości w tym samym czasie. Dostarczenie tej samej treści do tysięcy użytkowników byłoby niewykonalne, gdyż z powodu kosztu nie pozwoliłaby na to szerokość pasma potrzebna dla serwera. Stosując metodę “jeden do wielu”, transmisja multicastowa rozwiązuje ten problem. Zamiast wysyłać setki informacji, serwer wysyła tylko jedną. Transmisja rozprzestrzenia się pomiędzy różnymi użytkownikami, którzy jej zażądali.

W ten sposób zmniejsza się potrzebna szerokość pasma, zarówno dla serwera, jak i dla sieci.

Jak widzimy, jest to skuteczne rozwiązanie dla poprawy wydajności sieci. Multicast pracuje wychodząc od architektury sieci hierarchicznej. Multicastowy przepływ danych IP wychwytywany jest przez routery tylko wtedy, gdy któryś z podłączonych komputerów zapisany jest do tej transmisji danych. Routery wysyłają dane tylko do tych przekaźników i koncentratorów, których klienci żądają transmisji.

W przypadku gdy chcemy pracować z multicastem w WAN, potrzebne są routery ze wsparciem multicastowym, które łączą się ze sobą za pomocą któregoś z protokołów trasowania dopuszczalnych w multicaście. Gdy jakiś proces w którymś hoście w podsieci przyłącza się do grupy multicastowej, ten host wysyła wiadomość IGMP do wszystkich routerów multicastowych swojej podsieci, informując je, że gdy otrzymają wiadomość multicastową przeznaczoną do grupy, do której się on przyłączył, to wysyłają ją do podsieci, aby on mógł ją odebrać. Te routery przekazują tę informację do pozostałych routerów multicastowych w taki sposób, by wszystkie routery wiedziały do kogo mają przetrasować docierające do nich wiadomości multicastowe.

Poza tym routery okresowo wysyłają wiadomość IGMP do grupy 224.0.0.1, żądając od hosta informacji na temat grup, do których są przypisane. Host, po otrzymaniu tej informacji załącza timer z przypadkową wartością i nie odpowiada aż ten timer osiągnie zero. Dzięki temu unika się tego, że wszystkie hosty odpowiadają równocześnie i wywołują niepotrzebne przeciążenie w sieci. Gdy timer któregoś z hostów osiągnie zero, host wysyła swoją odpowiedź na adres konkretnej grupy multicastowej, o której jest informowany, przez co pozostałe hosty przyłączone do tej grupy zobaczą odpowiedź i wyłączą swój timer, nie generując w ten sposób odpowiedzi. Dzieje się tak dlatego, iż jeden odpowiadający host jest wystarczający, router musi tylko wiedzieć, że w określonej grupie tej podsieci istnieje jakiś zainteresowany host. To mu wystarcza do przekierowania wiadomości multicastowych przeznaczonych do grupy, pozostałe routery je otrzymają i dlatego nie ma potrzeby, by one także udzielały odpowiedzi.

Jeśli wszystkie hosty znajdujące się w określonej grupie wychodzą z niej, wtedy żaden nie odpowie na wiadomości routera. Ten, widząc, że w określonej grupie podsieci nie ma już nikogo zainteresowanego, przestanie trasować do tej podsieci wiadomości przeznaczone do tej grupy. Inna opcja wdrożona w IGMPv2 jest taka, że sam host wskazuje routerom, że opuścił określoną grupę, wysyłając w tym celu wiadomość na adres 224.0.0.2.

Multicast cieszy się dużym zainteresowaniem w zastosowaniach multimedialnych. Firmy poważne rozważają tę możliwość do takich zastosowań jak nauka na odległość, rozpowszechnianie wiadomości na pulpicie oraz wirtualne zebrania w firmach. Inną rozważaną możliwością jest dystrybucja oprogramowania.

2.6.2.1 PROTOKÓŁ IGMP

IGMP jest stosowany przez maszyny i routery wspierające multicast. Informuje sieć fizyczną o tym, które maszyny obecnie przynależą do grupy multicastowej. Tej informacji wymagają routery, aby wiedzieć kiedy przesłać datagramy multicastowe.

Chociaż protokół IGMP do przesyłania wiadomości używa datagramów IP, uważamy go za nieodłączną część IP, a nie jako osoby protokół.

2.6.2.1.1 Działanie Protokołu IGMP

Do transmisji multicastowej przypisuje się adres klasy D. Każde urządzenie chcące otrzymywać przepływ danych umieści adres IP klasy D tego przepływu we wszystkich interfejsach używanych do IP. Jako że wszyscy klienci transmisji mają ten sam adres klasy D, multicast wysyłany jest tylko na jeden adres i do wielu klientów. W celu odszukania urządzeń podłączonych do podsieci, routery multicastowe używają protokołu przynależności do grupy, na przykład IGMP (Internet Group Management, protokół zarządzania grupami internetowymi). Gdy jakieś urządzenie chce dołączyć do którejś grupy, wysyła wiadomość IGMP do routera multicastowego, wskazując mu sesje, które pragnie otrzymywać. Router multicastowy zaczyna rozsyłać żądane sesje do członków podsieci, a każdy członek, aby rozpocząć odbieranie danych, dodaje adres identyfikacyjny grupy do swojego interfejsu. Skalowalność wzrasta w miarę jak dołącza coraz więcej członków, gdyż jest więcej możliwości zlokalizowania routera multicastowego w pobliżu sieci o transmisji od klienta.

2.6.2.1.2 Wiadomości IGMP

Wiadomości IGMP wysyłane są w datagramach IP. Nagłówek IP zawsze zawiera liczbę protokołu 2, wskazując IGMP oraz typ usługi zero (rutyna). Pole danych IP zawiera wiadomość IGMP o długości 8 bajtów.

Istnieją trzy główne rodzaje wiadomości:

1.- Zapytanie członków grupy:

Wiadomość wysyłana z mroutera do hostów swojej podsieci, w celu zapytania czy chcą dołączyć do grupy. Używa się sieci ze zdolnością multicastową, z zastosowaniem adresu IP 224.0.0.1, aby zapytać wszystkie systemy multicastowe podsieci. Ten rodzaj wiadomości mrouter wysyła okresowo i oczekuje na odpowiedzi hostów podsieci, konfigurując tablice routingu multicastowego za pomocą otrzymanych informacji. W tablicach utrzymuje się ustaloną grupę dopóki, dopóty otrzymuje się odpowiedź od któregoś z hostów tej grupy.

Dane datagramów IP i IGMP zapytania są następujące:

Typ IGMP = 1
IGMP adres grupy = 0

IP TTL = 1IP adres docelowy = 224.0.0.1 (do wszystkich hostów podsieci)
IP adres źródłowy = adres routera

2.- Raport członków grupy:

Wiadomość odpowiadająca na zapytanie, wysyłana z hostów do mroutera, w celu poinformowania, że chce się zostać członkiem grupy. Aby mrouter się nie zawiesił, przed udzieleniem odpowiedzi na zapytanie członków hosty czekają dowolny czas (od 0 do 10 sekund). Poza tym, jeśli jeden host widzi, że inny host z jego grupy wysłał już raport do mroutera, nie ma potrzeby wysyłania swojego raportu, gdyż istotne jest to, by mrouter dowiedział się, że w podsieci jest ktoś, kto przynależy do określonej grupy. Adres docelowy datagramu raportu jest adresem grupy, dzięki temu informacja dociera nie tylko do mroutera, ale i do wszystkich członków grupy w podsieci.

Dane datagramów IP i IGMP raportu są następujące:

Typ IGMP = 2
IGMP adres grupy = adres grupy
IP TTL = 1
IP adres docelowy = adres grupy
IP adres źródłowy = adres IP hosta3)

3.- Wiadomość DVMRP (Distance Vector Multicast Protocol):

Wiadomość wysyłana przez mroutery do swoich sąsiadów, aby poinformować ich o zmianach zaistniałych wśród członków grupy. Te wiadomości mogą być wysyłane w dwóch różnych sytuacjach:

Mroutery sąsiadujące połączone bezpośrednio z podsiecią multicastową: używają zarezerwowanego adresu 224.0.0.4.

Mroutery sąsiadujące połączone poprzez tunel: przesyłają multicastowe datagramy IP enkapsulowane wewnątrz unicastowych datagramów IP, które w nagłówku zawierają unicastowy adres docelowy z drugiego końca tunelu.

Można używać innych protokołów multicastowych, takich jak PIM i MOSPF, do których przypisane są ich własne rodzaje wiadomości. Te trzy rodzaje wiadomości nie rozsyłają się poza swoją podsieć. Mają czas życia (TTL) o wartości 1. Jeśli datagram ma pole TTL na zero, oznacza, że jest zarezerwowany dla hostu źródłowego, jeśli TTL wynosi 2, wszystkie hosty będące członkami grupy oraz wszystkie routery multicastowe otrzymują datagram, a datagramy z innymi wartościami dla adresu docelowego wysyłane są przez router multicastowy jako normalne: wartość TTL spada do czasu krótszego niż jedna sekunda.

2.6.3 PROTOKOŁY ROUTINGU MULTICASTOWEGO

Multicast stosuje jedną z dwóch technologii Spanning–Tree: Dense mode (tryb gęsty) lub Sparse mode (tryb rozsiany).

2.6.3.1 TRYB GĘSTY:

Członkowie grupy są gęsto pogrupowani w sieci. Ten tryb używany jest przy dużej dystrybucji, gdy wiele urządzeń umieszczonych w tej samej sieci lub podsieci otrzymuje dane z tej samej lokalizacji. Tryb gęsty zakłada również, że szerokość pasma jest wystarczająco duża do podtrzymania transmisji. Protokoły trasowania do dystrybucji danych w sieciach w trybie gęstym są następujące: DVMRP, PIM-DM oraz MOSPF.

DVMRP (Distance Vector Multicast Routing Protocol, czyli protokół trasowania grupowego na podstawie wektorów odległości): Stosuje zalanie jako metodę służącą do doprowadzenia danych multicastowych do ich celu, choć może wymagać dużej szerokości pasma. Routery DVMRP przyjmują, że wszyscy, którzy są podłączeni do podsieci, chcą otrzymywać dane. Ten rodzaj rozszerzenia drzewa przenosi informacje do wszystkich “liści drzewa” w najlepszy i najszybszy sposób. W miarę jak członkowie przyłączają się do grupy lub ją opuszczają, routery usuwają gałęzie drzewa, na których nie ma członków, zmniejszając w ten sposób używaną szerokość pasma.

DVMRP zależy od najkrótszej drogi rozprowadzania. Routery DVMRP sprawdzają swoje tablice routingu, w celu ustalenia czy nie posiadają lepszej drogi do następnego routera multicastowego. Sprawdzając swoje tablice routingu routery DVMRP tworzą efektywną drogę do transmisji danych. Jeśli któryś router ustali za pomocą protokołu IGMP, że nie posiada członków, do których może przekazać dane albo że nie ma lepszej drogi, poprosi o usunięcie z transmisji. Ten protokół do aktualizacji wszystkich routerów sieci stosuje technikę broadcastu.

PIM-DM (Protocol Independent Multicast Dense Mode, czyli protokół multicastowy niezależny- tryb gęsty): W ogólnym działaniu podobny do DVRMP. PIM-DM jest wersją trybu gęstego protokołu PIM, stworzonego w celu dostarczenia standardowego i skalowalnego protokołu routingu multicastowego. Sposób przesyłania pakietów danych PIM-DM polega na tym, że gdy pakiet dociera do routera, PIM-DM określa czy stosowana jest najkrótsza droga do źródła. Jeśli tak jest, pakiet wysyłany jest w sposób opadający do wszystkich interfejsów, aż dotrze do członków, a nieużywane gałęzie są usuwane. Działanie jest proste, lecz może spowodować przeciążenie i powielanie pakietów.

MOSPF (Multicast Open Shortest Path First, czyli pierwsza otwarta najkrótsza ścieżka w wersji multicast): jest to rozbudowana wersja OSPF nastawiona na ruch multicastowy, w miejsce obsługi jedynie ruchu unicastowego. MOSPF ukierunkowuje dane przez połączenia o najniższym koszcie, przy będącej do dyspozycji szerokości pasma. Najmniejsza ilość skoków używana jest jako kryterium wyznaczania najlepszej drogi. Stosując tę metodę można ominąć najbardziej zatarasowane drogi, jeśli przypisze im się najwyższy koszt.

Każdy router MOSPF utrzymuje pełną wizję całej sieci, stworzoną wychodząc od informacji o stanie łączy, jakimi wymieniają się między sobą routery. Może to ograniczyć skalowalność, jak również sprawić, że routery, poza wymianą informacji na temat stanu łączy, wyślą dane IGMP na temat członków, zmniejszając w ten sposób szerokość pasma do dyspozycji dla transmisji w sieciach z wieloma grupami członków. W miarę jak tworzy się drzewo multicastowe, każdy router MOSPF przeprowadza szereg obliczeń, w celu wyznaczenia najlepszej drogi dla pakietów. Jednak robi się raz dla każdej grupy, co utrzymuje przeciążenie sieci na niskim poziomie. W miarę jak pakiet przechodzi przez sieć, każdy router przeprowadza te same obliczenia i tworzy ostateczne drzewo dla członków.

2.6.3.2 TRYB ROZSIANY:

Celem jest znalezienie skutecznych metod przesłania danych do wielu ludzi rozsianych po dużych obszarach. W przeciwieństwie do trybu gęstego, który zakłada, że w każdym zakątku sieci jest jakiś członek, tryb rozsiany przyjmuje, że dla wyspecjalizowanych transmisji członkowie są podzieleni na niewielkie grupy sieci. Protokoły Sparse Mode zaprojektowano również do skutecznego działania przy przeciążonych połączeniach lub wspólnej, niewielkiej szerokości pasma.

Istnieją dwa protokoły trybu rozsianego: CBT i PIM-SM. Obydwa tworzą drzewo routingu prosząc routery, by uczestniczyły w jego tworzeniu. Gdy któryś z członków poprosi o przyjęcie, routery trybu rozsianego łączą się w jednej sesji multicastowej.

CBT (Center-Based Trees, czyli drzewa oparte na jednym centrum): Upraszcza nakierunkowanie, tworząc jedno drzewo używane przez wszystkie grupy oraz stosuje konstrukcję drzewa opartą na routerze centralnym, z którego przepływają dane, poza samym źródłem danych (serwerem). Jest to korzystne, gdyż dzięki temu, że wszystkie grupy używają tego samego drzewa, informacja o stanie łącza się zmniejsza. W przeciwnym razie router centralny przeciąża się w miarę jak dołączają kolejni członkowie.

PIM-SM (Protocol Independent Multicast Sparse Mode, czyli protokół multicastowy niezależny- tryb rozsiany): W swej topologii podobny jest do CBT, lecz jest bardziej elastyczny. W miejsce centralnego routera PIM-SM używa RP (Rendevous Point, czyli miejsce spotkania), w którym schodzące routery się “spotykają”. To pozwala PIM-SM na tworzenie drzewa dzielonego lub opartego na najkrótszej ścieżce. W ten sposób każda grupa może posiadać inną strukturę drzewa, w zależności od tego które działa najlepiej.

CBT utrzymuje niską ilość informacji na temat stanu łączy, choć może nie dostarczać najlepszej ścieżki do członka. Jeśli potrzeba jest niskiego stanu utajenia, PIM-SM może tworzyć lepsze ścieżki.

Jako że PIM jest protokołem standaryzowanym, możliwe jest wspólne działanie pomiędzy PIM-DM i PIM-SM.

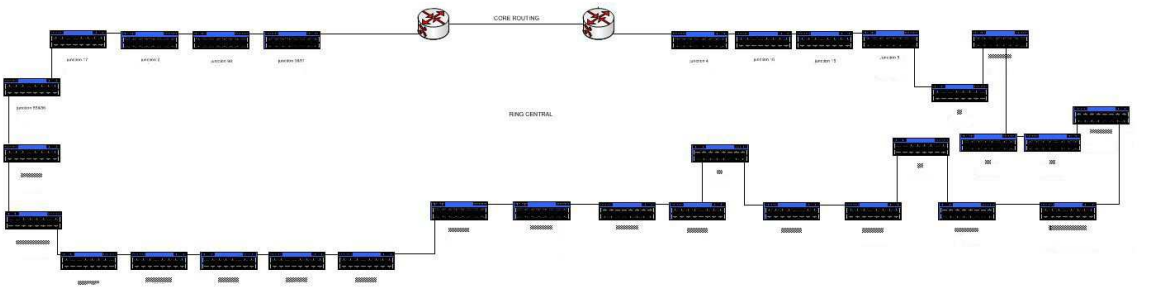
2.7.- PIERŚCIENIE

W tym rozdziale pokazany jest schemat każdego z pierścieni z odpowiadającymi im skrzyżowaniami, łącznie z pomiarem okablowania i jego lokalizacją.

2.7.1 PIERŚCIEŃ CENTRALNY

2.7.1.1 Topologia logiczna

Schemat logiczny pierścienia głównego.



2.7.1.2 Pomiary długości pierścienia

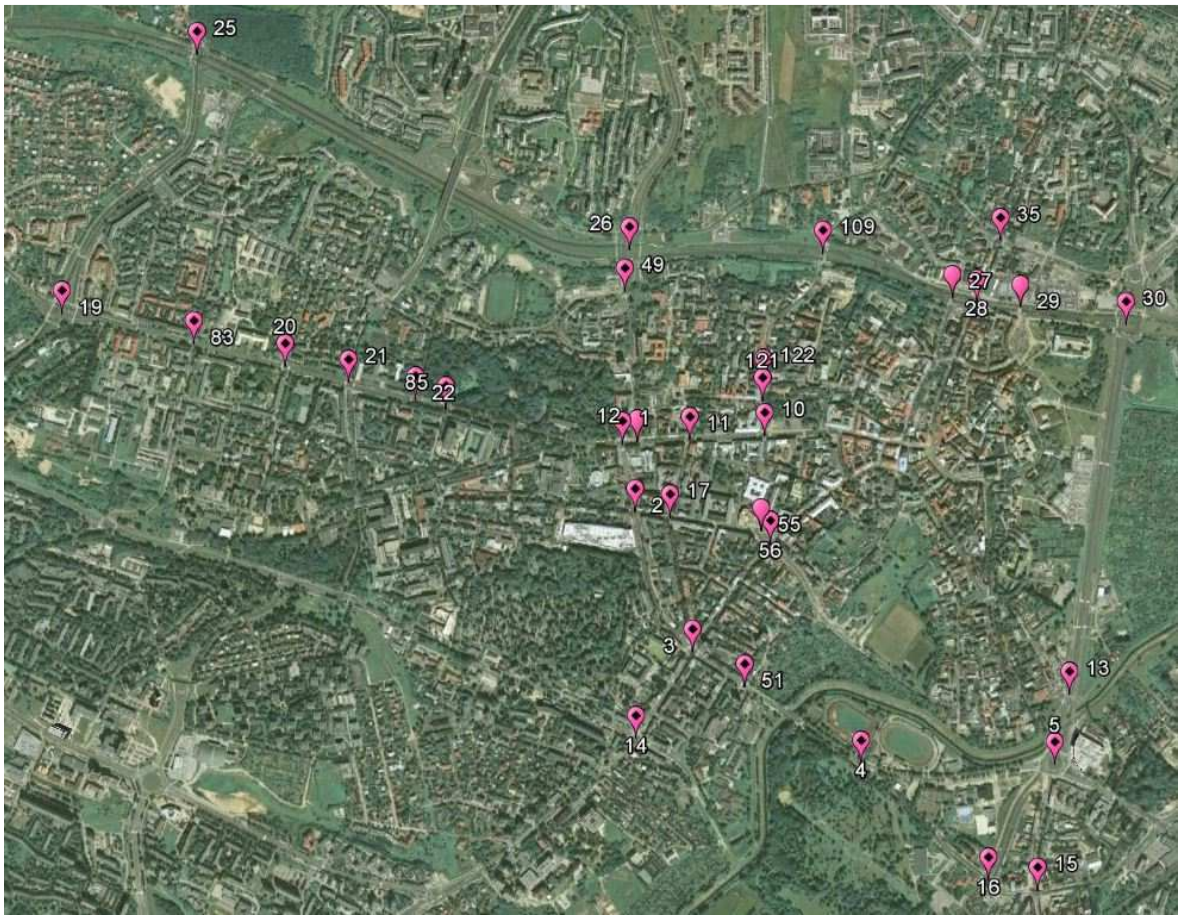
Tabela pomiarów odległości między skrzyżowaniami pierścienia głównego.

PIERŚCIEŃ CENTRALNY

NR SKRzYŻOWANIA	SĄSIEDNIE SKRZYŻOWANIE				ODLEGŁOŚĆ OD SĄSIEDNIEGO SKRZYŻOWANIA (m)			
	Północ	Południe	Wschód	Zachód	Północ	Południe	Wschód	Zachód
1			12	85			47,5	580,9
2		98	17			124,1		
3	98	14	51			336,5	204,3	
4			16	51		562,9		
5	13	16	123		217,0			
10	121	55		11	108,5	327,7		
11			10	12			243,2	
12			11	1			172,5	
13	30	5			1225,4			
14	3							
15				16				
16	5		15	4	498,4		169,6	
17			55	2			108,4	
19	25	52	83	69			440,0	
20			21	83			213,1	
21			22	20			220,9	
22			85	21			99,8	
25		19	26			976,7		
26		49		25		131,6		1602,6
27			28	109				450,6
28	35		29	27	216,1			72,9
29			30	28				160,3
30		13		29				341,1
35		28						
49	26							
51			4	3			453,6	
55			56	17		55,9	296,6	
56				55				
83			20	19			300,2	
85			1	22			580,9	
98	2	3				381,4		
109			27	26				629,5
121	122	10						
122		122				67,4		
					DŁUGOŚĆ PIERŚCIENIA			12037,2

2.7.1.3 Lokalizacja pierścienia

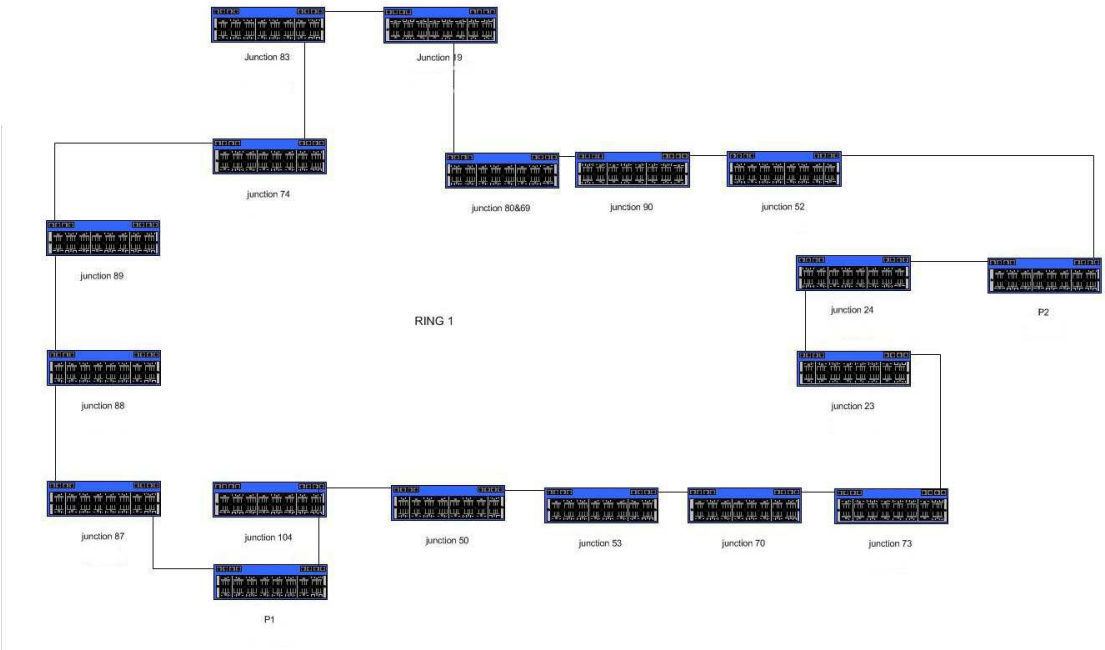
Lokalizacja usytuowania skrzyżowań pierścienia głównego pokazana za pomocą Google Earth.


25
26
109
35
49
27
28
29
30
19
83
20
21
85
22
12
1
11
10
17
2
55
56
3
51
13
14
4
5
16
15

2.7.2 PIERŚCIEŃ 1

2.7.2.1 Topologia logiczna

Schemat logiczny pierścienia 1.



2.7.2.2 Pomiary długości pierścienia

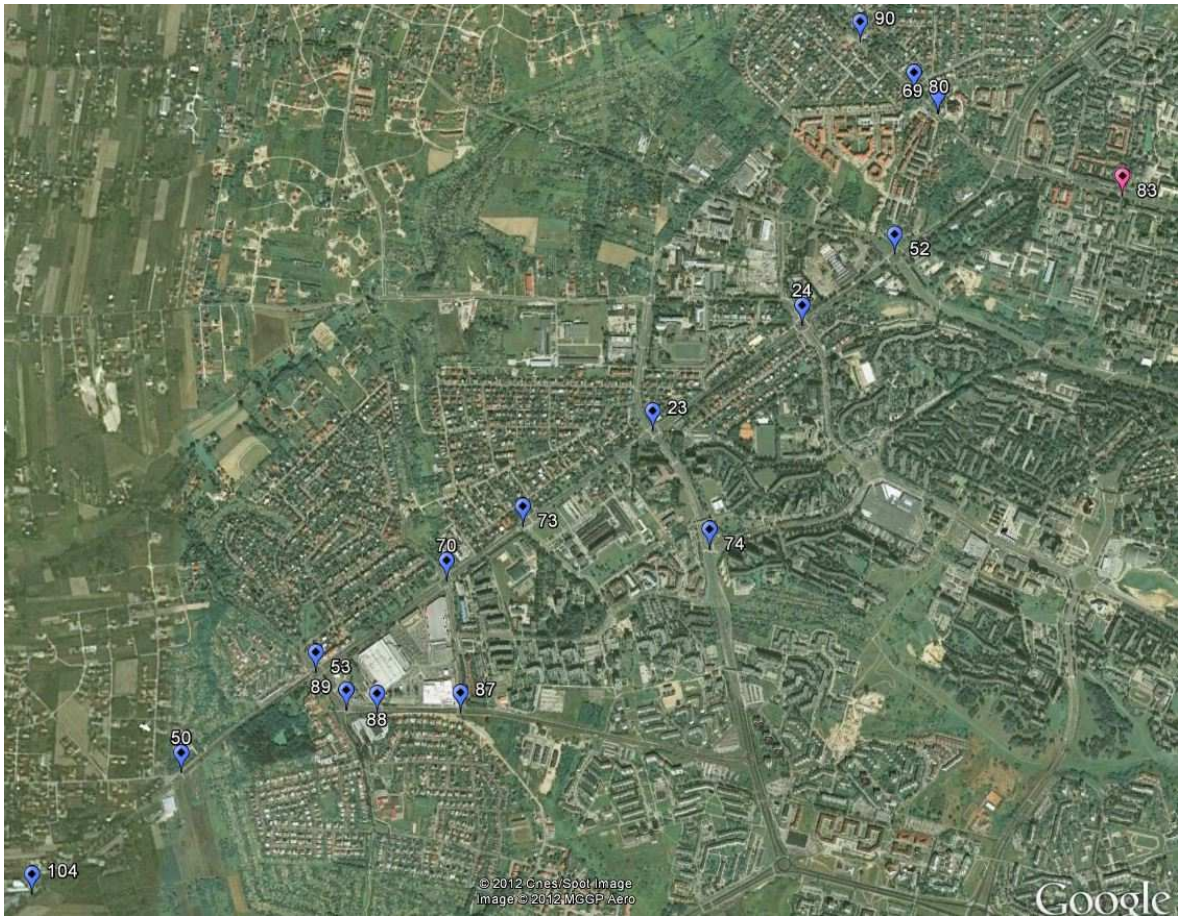
Tabela pomiarów odległości między skrzyżowaniami pierścienia 1.

PIERŚCIEŃ 1

R SKRzYżOWAN	SĄSIEDNIE SKRZYŻOWANIE				ODLEGŁOŚĆ OD SĄSIEDNIEGO SKRZYŻOWANIA			
	Północ	Południe	Wschód	Zachód	Północ	Południe	Wschód	Zachód
19	25	52	83	69		520,0		350,1
23		74	24	73		481,0		591,0
24			52	23				668,1
50			53	104				637,2
52			19	24				425,9
53		89	70	50		163,6		659,8
69			19	80				91,8
70			73	53				580,8
73			23	70				347,3
74	23							
80			69	90				288,2
83			20	19				
87				88				
88			87	89			320,8	
89			88	53			114,2	
90			80					
104			50					
				DŁUGOŚĆ PIERŚCIENIA				6239,7

2.7.2.3 Lokalizacja pierścienia

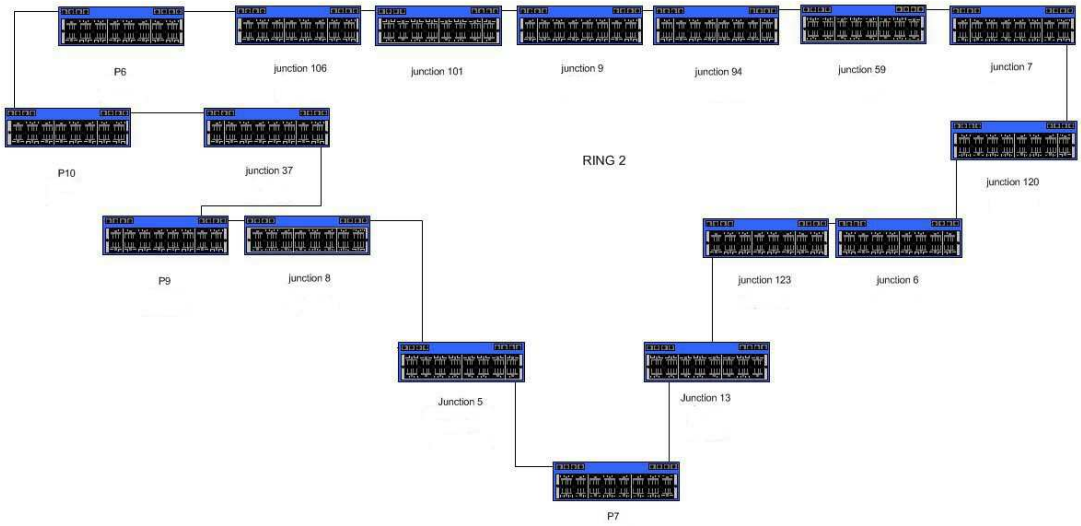
Lokalizacja usytuowania skrzyżowań pierścienia 1 pokazana za pomocą Google Earth.



2.7.3 PIERŚCIEŃ 2

2.7.3.1 Topologia logiczna

Schemat logiczny pierścienia 2.



2.7.3.2 Pomiary długości pierścienia

Tabela pomiarów odległości między skrzyżowaniami pierścienia 2.

PIERŚCIEŃ 2

R SKRzYżOWAN	SĄSIEDNIE SKRZYŻOWANIE				ODLEGŁOŚĆ OD SĄSIEDNIEGO SKRZYŻOWANIA (m)			
	Północ	Południe	Wschód	Zachód	Północ	Południe	Wschód	Zachód
5	13	16	123				197,4	
6			120	123			430,0	
7			8	120			382,7	
8	59	106	94	7	360,3	751,3	257,6	
9			101	94			554,7	
13								
37								
59								
94			9	8			161,2	
101				9				
106	8	37				697,1		
120			7	6			335,3	
123			6	5			206,1	
					DŁUGOŚĆ PIERŚCIENIA			4333,6

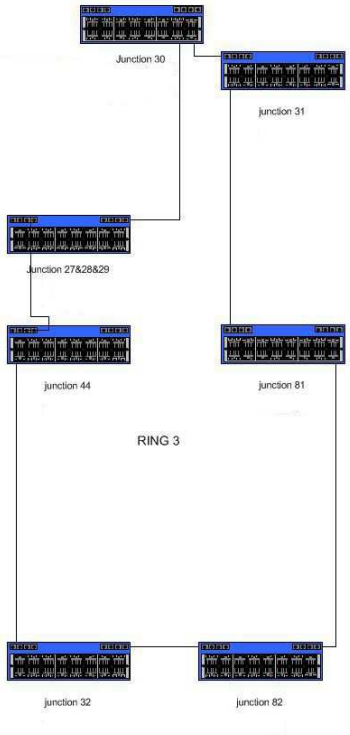
2.7.3.3 Lokalizacja pierścienia

Lokalizacja usytuowania skrzyżowań pierścienia 2 pokazana za pomocą Google Earth.

2.7.4 PIERŚCIEŃ 3

2.7.4.1 Topologia logiczna

Schemat logiczny pierścienia 3.



2.7.4.2 Pomiary długości pierścienia

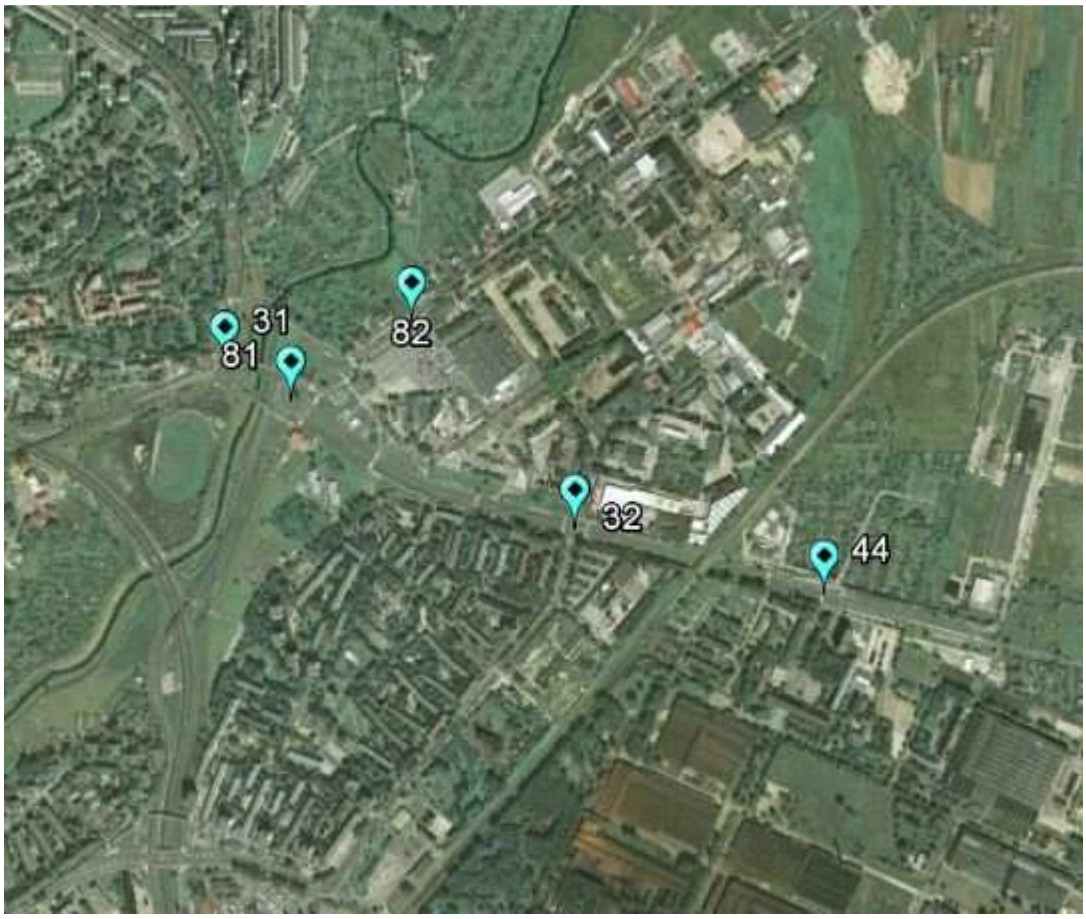
Tabela pomiarów odległości między skrzyżowaniami pierścienia 3.

PIERŚCIEŃ 3

NR SKRzYżOWANIA	SĄSIEDNIE SKRZYŻOWANIE				ODLEGŁOŚĆ OD SĄSIEDNIEGO SKRZYŻOWANIA (m)			
	Północ	Południe	Wschód	Zachód	Północ	Południe	Wschód	Zachód
30		13	31	29			1336,6	
31			81	30			144,7	
32			44	81				1236,8
44				32				
81	82		32	31	409,6		615,2	
82		81						
					DŁUGOŚĆ PIERŚCIENIA			3742,9

2.7.4.3 Lokalizacja pierścienia

Lokalizacja usytuowania skrzyżowań pierścienia 3 pokazana za pomocą Google Earth.



3.- Bezpieczeństwo i jakość usługi

3.1.- Cele

Miejska sieć komunikacyjna jest strategicznym elementem każdego miasta i z tego powodu musimy poświęcić wiele uwagi jej bezpieczeństwu oraz odporności na działanie czynników zewnętrznych. Zagrożenia dla bezpieczeństwa dzielą się na wewnętrzne i zewnętrzne. W tym paragrafie zostały zdefiniowane poszczególne strategie w ramach systemu łączności pod kątem jego zabezpieczenia przed działaniem czynników zewnętrznych.

Aby zapewnić sieci bezpieczeństwo, zostaną wykorzystane różne metody, które podzielimy na dwa rodzaje bezpieczeństwa:

Bezpieczeństwo fizyczne:

- Dostęp fizyczny do urządzeń.

Bezpieczeństwo logiczne

- Wyłączenie portów nieużywanych.
- MAC Filtering
- Uwierzytelnienie 802.1X
- Strong Password
- SNMP 3
- ACL
- QoS

W kolejnych punktach opiszemy metody, które zostaną wdrożone do systemu.

3.2.- Bezpieczeństwo fizyczne

3.2.1 Dostęp do urządzeń

Główną drogą dostępu do danej sieci jest sposób lokalny, to znaczy, że ktoś podłączy się bezpośrednio do urządzeń. Z tego powodu, a także z przyczyn o charakterze meteorologicznym, przełączniki będą zainstalowane w szafach zamkniętych na klucz utrudniający dostęp do nich przez osoby niepowołane.

3.3.- Bezpieczeństwo logiczne

Po uwzględnieniu podstawowych środków bezpieczeństwa fizycznego powinniśmy przystąpić do wdrażania środków bezpieczeństwa logicznego.

3.3.1 Filtrowanie według portów

Na początek ograniczymy dostępność portów, które będą puste w urządzeniach sieciowych, to znaczy porty te zostaną wyłączone w taki sposób, że jeśli ktoś spróbuje podłączyć jakiś terminal do pustego portu, nie dostanie linku i nie będzie mógł podłączyć się do sieci. Porty te będą mogły zostać włączone tylko przez administratora sieci w trybie zdalnym, z centrum sterowania lub lokalnie z portu konsoli.

3.3.2 Filtrowanie według adresu MAC

Kolejnym krokiem do wykonania będzie konfiguracja urządzeń sieciowych, ograniczając połączenia do tylko tych urządzeń, których adres MAC będzie znany. Jakakolwiek prośba o podłączenie urządzenia z nieznanym MAC zostanie odrzucona. Tak samo jak włączenie/wyłączenie portów, zmiana konfiguracji filtra MAC Address i pozostałych środków bezpieczeństwa logicznego będzie możliwa do wykonania tylko przez administratora sieci w trybie zdalnym, z centrum sterowania lub lokalnie z portu konsoli.

3.3.3 Uwierzytelnienie 802.1x

W celu jeszcze lepszego zabezpieczenia dostępu do sieci przez urządzenia niepożądane zostanie zastosowana standardowa metoda uwierzytelnienia 802.1x dla wszystkich terminali podłączonych do sieci.

Jej funkcjonowanie przedstawia się następująco:

Kontroler dostępu (Serwer Radius), po otrzymaniu prośby o połączenie od użytkownika, wysyła prośbę o uwierzytelnienie.

Użytkownik wysyła odpowiedź do kontrolera dostępu, który przekierowuje odpowiedź do serwera uwierzytelnienia.

Serwer uwierzytelnienia wysyła "challenge" do kontrolera dostępu, który przekazuje go do użytkownika. “Challenge” jest metodą służącą do ustalenia tożsamości. Jeżeli klient nie może ocenić “challenge”, serwer próbuje z innym i tak dalej.

Użytkownik odpowiada na “challenge”. Jeżeli tożsamość użytkownika jest prawidłowa, serwer uwierzytelnienia wysyła zatwierdzenie do kontrolera dostępu, który pozwala użytkownikowi na wejście do sieci lub jej części, zgodnie z przyznanymi uprawnieniami. Jeżeli nie można było sprawdzić tożsamości użytkownika, serwer uwierzytelnienia wysyła wiadomość odmowną i kontroler dostępu odmawia użytkownikowi dostępu do sieci.

3.3.4 Strong Passwords

Wszystkie urządzenia sieciowe będą konfigurowane z użytkownikami i hasłami innymi niż te dostarczane domyślnie przez producenta. Jeśli chodzi o hasła, beda wykorzystywane takie, które składają się z 14 znaków (co najmniej), między którymi będą się znajdować symbole, wielkie i małe litery, postępując według procedur tworzenia Strong Passwords.

3.3.5 SNMP

Protokół SNMP, jak mówi jego nazwa, jest prostym protokołem do administrowania siecią i zostanie przez nas wdrożony dla potrzeb administrowania i monitorowania sieci. Użyjemy do tego wersji 3 protokołu, ponieważ w odróżnieniu od swoich poprzedników wprowadza funkcje bezpieczeństwa chroniące przed:

Integralność-->manipulowanie informacją.
Spoofing--> Fałszowanie IP
Sniffing-->Prywatność

3.3.6 Filtrowanie ruchu za pośrednictwem ACL

Jedną z najpowszechniejszych metod filtrowania ruchu jest korzystanie z list kontroli dostępu (ACL). ACL mogą być stosowane do administrowania i filtrowania ruchu wchodzącego do sieci, jak również ruchu z niej wychodzącego.
Będziemy używać ACL do:

Identyfikacji lub klasyfikacji ruchu dla takich funkcji jak QoS i kolejki.
Kontroli dostępu do terminali w określonych strefach sieci.

ACL ma zastosowanie do ruchu wchodzącego lub wychodzącego poprzez interfejs. Jeśli dany pakiet jest zbieżny z zezwoleniem, może wejść lub wyjść z routera. Jeżeli jest zbieżny z odmową, nie może postępować dalej.
Kiedy dany pakiet dociera do interfejsu, router sprawdza, czy istnieje ACL powiązany z tym interfejsem. Jeśli jest, sprawdza czy wchodzi czy też wychodzi, a w końcu sprawdza, czy ruch jest zbieżny z kryteriami zezwalającymi lub zakazującymi.

3.3.7 QoS

Ze względu na ilość i różnorodność ruchu, który będzie transmitowany za pośrednictwem sieci, zostanie zastosowana technologia QoS, która zapewnia transmisję określonej ilości informacji w danym czasie i która pozwala nam nadawać priorytet i regulować strumień pasma przenoszenia sieci lokalnej.

3.3.7.1 Definicja QoS

Jakość usługi (QoS - Quality of Service) odnosi się do zdolności Sieci do zapewnienia usług wyższego priorytetu, włączając dedykowane pasmo, kontrolowanie drgania i opóźnień (wymagane przez niektóre typy ruchu interaktywnego i ruchu w czasie rzeczywistym) oraz ulepszoną charakterystykę strat, w określonym ruchu sieci w poszczególnych technologiach WAN, LAN oraz MAN. Jednocześnie, upewniając się, że priorytetowe traktowanie jednej klasy ruchu w sieci, nie ma drastycznych efektów na inne przepływy.

Zazwyczaj wyróżniamy trzy poziomy / klasy QoS:

Usługa Best-effort - Zapewniająca podstawową łączność bez gwarancji dostarczenia danych, prędkości, ani kolejności dostarczenia.

Usługa zróżnicowana (Klasa usługi) – Niektóre ruch jest traktowany lepiej niż inny (szybsza obsługa, lepsza średnia przepustowość i mniejsza wskaźnik średnich strat). Jest to tylko statystyczna preferencja, a nie gwarantowana usługa, która jest zazwyczaj zapewniania przez klasyfikację ruchu.

Usługa gwarantowana – Jest to całkowita rezerwacja zasobów sieci dla określonego ruchu. Jest świadczona przez narzędzia QoS RSVP w sieci pakietowej. Tradycyjna sieć PSTN wykorzystuje przełącznik obwodu z gwarantowanym łączem i alokacją przepustowości w celu zapewnienia QoS.

Acisa wdroży model zasobów gwarantowanych w sposób rodzajowy, a nie poprzez strumienie czy sesje. Umożliwi to zapewnienie zróżnicowanych warunków obsługi dla różnych rodzajów ruchu, w sposób skalowalny i skuteczny, poprzez całą sieć. Podstawowe zalety to:

- Nie wymaga wcześniejszej sygnalizacji.
- Nie pozwala na zapewnienie krańcowych warunków ruchu.
- Jest bardzo elastyczny i skalowalny.
- Dzieli ruch na klasy w zależności od wymogów organizacji.
- Każdy pakiet otrzymuje obsługę, która została zdefiniowana dla tej klasy, do której należy dany pakiet.
- Do każdej klasy można przypisać inny poziom obsługi, a wraz z nim inne zasoby.
- Przypisanie zasobów odbywa się skokowo w każdym urządzeniu sieci, a nie dla określonej trasy.

Usługi Zróżnicowane, które są także znane pod nazwą DiffServ, eliminują konieczność stanu per-flow oraz sygnalizowania przy każdym przeskoku. Architektura diffserv przyciska całą złożoność do krawędzi sieci i w ten sposób eliminuje obciążenie związane z obsługą ruchu per-flow w rdzeniu sieci.
Właśnie to jest powodem, dla którego zaproponowano DiffServ: aby przezwyciężyć problem skalowalności narzucony przez zintegrowane usługi, wymagające stanu per-flow oraz sygnalizowania. Celem DiffServ jest podział ruchu na kilka klas i traktowanie każdej klasy w określony, inny sposób; każda klasa posiada inne zasady klasyfikacji, kontroli, kształtowania i kolejkowania.

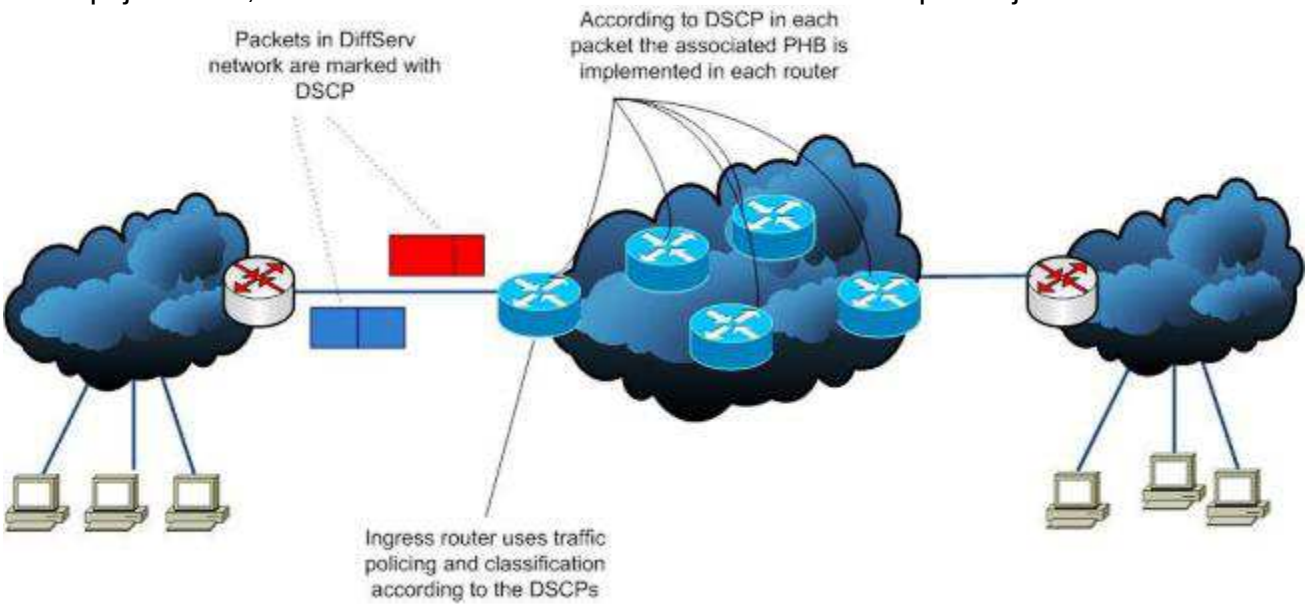
Usługi Zróżnicowane są realizowane poprzez mapowanie punktu kodowego, zawartego w polu TOS, w nagłówku pakietu IP do określonego zachowania

przeskoku (PHB), przy każdym węźle sieci wzdłuż jego drogi. DiffServ określa układ bajta TOS (zwanego polem DS.), w celu zamiany istniejącej metody definicji bajta TOS.

Sześć z ośmiu bitów pola DS (2 bity są obecnie nieużywane) używa się jako punktu kodowego (DSCP), w celu wyboru zachowania przeskoku (PHB), którego pakiet doświadczy na każdym węźle. PHBy zazwyczaj kolejkują dziedziny zaimplementowane na interfejsach wyjściowych urządzeń sieciowych (routerów). Pomimo, że od standardu DSCP oczekuje się wywołania odpowiadającego mu standardu PHB, mapowanie DSCP do PHB jest implementowane w każdym urządzeniu sieciowym i jest konfigurowane przez dostarczyciela sieci. Przynajmniej wewnątrz danej sieci dostarczyciela lub domeny, mapowanie DSCP do PHB powinno być skonfigurowane konsekwentnie.

Ważne jest, aby zauważyć, że w zależności od umowy pomiędzy dostarczycielem oraz klientem, DSCP może być oznaczone przez klienta, zanim pakiety zostają przekazane do Siecie. Jeżeli klient nie oznaczy pakietów, dostarczyciel sieci może sklasyfikować pakiety u wejścia sieci, na podstawie danej umowy z klientem.

Koncepcje DSCP, Warunkowania Ruchu oraz PHB zilustrowano poniżej:



3.3.7.2 Warunkowanie Ruchu oraz PHBs

Kontrola dostępu, klasyfikacja i warunkowanie pakietów są zaimplementowane w skrajnym węźle wejściowym, znanym jako krawędź sieci dostarczyciela. Niniejsze funkcjonalności są zapewnianie przez komponenty warunkowania ruchu (TC), które oznaczają lub odrzucają pakiety. Główne komponenty warunkowania ruchu są następujące:

• Klasyfikatory

Klasyfikatory, jak ich nazwa wskazuje, klasyfikują ruch. Celem klasyfikatora jest oddzielenie pakietów przybywających do węzła wejściowego, na poszczególne

klasy ruchu, zgodnie z kryterium klasyfikacji. Istnieją dwa typy klasyfikatorów: klasyfikatory zachowania globalnego (BA) oraz klasyfikatory wielopolowe (MF).
Klasyfikatory BA klasyfikują przychodzący ruch zgodnie z DSCP w nagłówkach pakietów. Niniejsze klasyfikatory są używane, kiedy przybywające pakiety zostały już oznaczone DSCP tj. w rdzeniu sieci, gdzie określony DSCP jest mapowany do odpowiadającego mu PHB w interfejsie wyjściowym urządzenia.
Klasyfikatory MF klasyfikują ruch zgodnie z pewnymi polami datagramowymi IP (adres źródłowy IP, adres docelowy IP, port źródłowy oraz port docelowy). Niniejsze klasyfikatory są zazwyczaj używane w węzłach wejściowych sieci DiffServ. Stamtąd natomiast, klasyfikatory BA są używane do obsługi ruchu.

• **Liczniki**
Liczniki są komponentami warunkowania ruchu, które mierzą szybkość przekazywanego ruchu i porównują ją z temporalnym profilem, który opisuje temporalne charakterystyki zgodnych strumieni ruchu. Liczniki dzielą przychodzący ruch na kilka strumieni wyjściowych, zgodnie z poziomem zgodności profilu mierzącego. Proste liczniki dzielą przychodzący ruch na zgodny i niezgodny ruch.

• **Znaczniki**
Znaczniki są używane do oznaczania określonego DSCP w nagłówku pakietu. W przypadkach, gdzie ruch przychodzący dociera do routera wejściowego nieoznaczony, wtedy klasyfikator MF klasyfikuje ruch, a następnie szereg znaczników jest używanych do oznaczenia odpowiedniego DSCP w polach nagłówka odpowiedniego ruchu.
W przypadku, gdy przychodzący ruch jest już oznaczony, wtedy znacznik jest używany wyłącznie, jeżeli przekazywany ruch jest niezgody i wymaga oznaczenia na niższy poziom usług.

• **Kształtowniki**
Kształtowniki opóźniają niektóre lub wszystkie pakiety w strumieniu ruchu, aby zmusić wspomniane pakiety do zgodności z profilem ruchu. Kształtowanie jest uzyskiwane przeze kolejkowanie pakietów w buforze o określonych wymiarach.

• **Dropery**
Dropery porzucają pakiety, które są przekazywane do sieci dostarczyciela, ale okazują się niezgodne (sprawdza je licznik).

• **Realizowanie Zachowań Przeskokowych**
Zachowania Przeskokowe (PHB) definiują kategorie ruchu obsługiwane przez sieć. Znormalizowano trzy grupy PHB. Są to: przekazywanie ekspresowe (EF), przekazywanie ubezpieczone (AF) oraz domyślne (Best-Effort) PHB bez jakichkolwiek gwarancji QoS.

• **Przekazywanie Ekspresowe PHB**
EF PHB zostało opracowane, aby zapewnić klientom usługę o niskim opóźnieniu, niskim drganiu, niskich stratach i pewnej przepustowości, która generuje ruch o stałej, maksymalnej prędkości transmisji danych (odpowiednią do nieelastycznego

ruchu). Ponieważ usługa ta pojawia się jako linia dzierżawiona, często określana jest jako usługa wirtualnej linii dzierżawionej (VLL).
Przekazywanie ekspresowe PHB gwarantuje minimalne odchylenie prędkości dla ruchu, który został oznaczony jako EF. Przekazywanie opóźnionych pakietów jest bez znaczenia w tej sytuacji, więc jeżeli w przypadku EF wystąpi przeciążenie, pakiety zostają odrzucone.

• Przekazywanie Ubezpieczone Grupy PHB
W przeciwieństwie do EF PHB, grupa AF PHB nie ma na celu zapewnić usługi, która ma limit opóźnienia. Używa się jej do zastosowań, które wymagają lepszej niezawodności, niż ta, którą może zapewnić usługa best-effort. Ponadto, AF określa cztery różne klasy ruchu, z których każdej przydziela się określoną ilość zasobów. Wewnątrz każdej z klas, pakiety mogą być oznaczone jednym z trzech poziomów prawdopodobieństwa odrzucenia. Grupa AF PHB ma na celu zapewnienie niezawodnej usługi, nawet w czasie przeciążenia, poprzez klasyfikację oraz nadzór nad głównym routerami. Specyfikacja grupy AF PHB jest względnie elastyczna i może być używana do budowy różnorodnych rozwiązań w zakresie usług.
Niemniej jednak, AF PHB zaleca, aby mechanizm typu losowe, wczesne wykrycie (RED) był używany do odrzucenia pakietu w razie potrzeby. RED jest buforowym schematem zarządzania. Przypadkowo odrzuca pakiety w oparciu o ich DSCP oraz średnią długość kolejki. Celem RED jest uniknięcie przepełnienia kolejki i odrzucenia ogona (w przypadku, gdy kolejka się przepełni, wszystkie nadchodzące pakiety są odrzucane) przy każdym routerze. Poprzez odrzucanie pakietów losowo, istnieje większe prawdopodobieństwo, że pakiety różnych połączeń TCP będą odrzucane w różnym czasie. Dlatego też, mechanizm kontroli przepływu TCP dla tych połączeń, będzie redukował ich prędkość przesyłania w różnym czasie. Pomaga to zapobiec przepełnieniu kolejek routera, a tym samym uniknąć odrzucania ogona oraz zwiększa to wydajność.

4.- System telefoniczny

4.1.- Cele

Proponowana Sieć Telefoniczna jest oparta na Asterisku. Asterisk jest potężnym i elastycznym frameworkiem, opartym na oprogramowaniu open-source (otwartym). Może być wykorzystany do utworzenia dostosowanego PBX w niemal każdym środowisku.

Asterisk jest odpowiednim wyborem dla Lublin TMS.

4.2.- Właściwości

Asterisk jest oprogramowaniem open-source (otwartym). Oznacza to, że setki, jeżeli nie tysiące programistów codziennie pracuje nad Asteriskiem, jego rozszerzeniami, dodatkowym oprogramowaniem i dostosowanymi instalacjami Asteriska. W dużym stopniu, elastyczność produktu jest wynikiem dostępności kodu źródłowego, co oznacza, że możemy modyfikować zachowanie Asteriska, aby spełniło nasze potrzeby.

Co najważniejsze, Asterisk jest frameworkiem, który pozwala na wybór i usunięcie poszczególnych modułów, pozwalając nam na stworzenie dostosowanego systemu telefonicznego dla instalacji Lublina. Dobrze przemyślana architektura zapewnia elastyczność, pozwalając nam stworzyć niestandardowe moduły, które rozszerzają nasz system telefonii lub nawet służą jako zamienniki domyślnych modułów.

4.2.1 Asterisk jako PBX

Asterisk jest prywatną centralą abonencką (PBX - Private Branch Exchange). PBX może być traktowana jako prywatna centrala telefoniczna, łącząca jeden lub więcej telefonów po jednej stronie i zwykle łącząca jeden lub więcej telefonów po drugiej stronie. Zazwyczaj jest to bardziej opłacalne, niż dzierżawa linii dla każdego potrzebnego telefonu.

4.2.1.1 Połączenia Stacja-Do-Stacji

Asterisk jako PBX oferuje połączenia stacja-do-stacji. Oznacza to, że użytkownicy mogą dzwonić z jednego telefonu do drugiego. Choć wydaje się to oczywiste, dostępne są elementarne systemy telefoniczne (często określane jako Systemy Kluczowe), które wspierają mnogie linie i pozwalają każdemu telefonowi na użycie jakiejkolwiek linii. W praktyce oznacz to, że aparaty telefoniczne nie mają indywidualnych rozszerzeń, do których można się dodzwonić, więc nie ma możliwości wybrania połączenia z jednego aparatu do drugiego. Niniejsze systemy mogą zazwyczaj być zidentyfikowane poprzez fakt, że wszystkie linie wychodzące na każdym telefonie posiadają migającą kontrolkę. W przeciwieństwie do Systemów Kluczowych, Asterisk pozwala na połączenia stacja-do-stacji, pozwalając na zorientowaną, wewnętrzną komunikację.

4.2.1.2 Trunking

Asterisk oferuje także trunking. W swojej najprostszej formie, trunking zapewnia dostęp do wielu linii telefonicznych. Niniejsze linie telefoniczne są zazwyczaj wykorzystywane do podłączenia do globalnej sieci telefonicznej, znanej jako Publiczna Komutowana Sieć Telefoniczna lub PSTN (Public Switched Telephone

Network), ale mogą także być wykorzystywane do linii prywatnych do innych systemów telefonicznych.

Niniejsze połączenia mogą być pojedynczym, analogowym łączem komunikacyjnym, mnogimi, analogowymi łączami komunikacyjnymi lub połączeniami cyfrowymi o dużej pojemności, które umożliwiają wykonywanie równoległych rozmów w jednym połączeniu.

4.2.1.3 Funkcje Telco

Asterisk wspiera wszystkie „standardowe" funkcje, których można oczekiwać po jakiejkolwiek firmy telefonicznej (lub telco). Asterisk wspiera wysyłanie i odbieranie usługi Caller ID (identyfikacja dzwoniącego numeru), a nawet pozwala na trasowanie połączeń w oparciu o Caller ID. Korzystanie z usługi Caller ID w PSTN wymaga subskrypcji tej funkcji z naszym dostawcą PSTN.

Asterisk wspiera również inne funkcje, takie jak połączenia oczekujące, automatyczne wybieranie ostatniego połączenia (*69), charakterystyczny dzwonek, przełączanie połączeń, przekazywanie połączeń itd. Niniejsze podstawowe funkcje oraz wiele więcej, są zapewniane przez Asteriska.

4.2.1.4 Zaawansowana Dystrybucja Połączeń

Asterisk może odbierać połączenia, sprawdzać ich atrybuty i na tej podstawie podejmować decyzje o trasowaniu. Jeżeli dostarczyciel PSTN nie zapewni wystarczającej ilości informacji, wtedy możemy prosić rozmówcę, aby wprowadził informacje za pomocą telefonu z wybieraniem tonowym.

Po podjęciu decyzji, w jaki sposób trasować połączenie, możemy przesłać numer wewnętrzny, grupę numerów wewnętrznych, nagranie, pocztę głosową lub nawet grupę telekonsultantów, którzy mogą wybierać pomiędzy telefonami. Możemy także używać kolejek połączeń, aby jeszcze skuteczniej służyć naszym klientom przy zachowaniu efektywności operacyjnej.

Ta elastyczność daje nam możliwość rozszerzenia zwykłego systemu telefonicznego do potężnego narzędzia dostępnego z poziomu naszego telefonu. Zaawansowana Dystrybucja Połączeń (ACD - Advanced Call Distribution) daje możliwość służenia naszym klientom w najlepszy możliwy sposób.

Jednym z głównych czynników odróżniających Asteriska od innych systemów PBX, które spierają ACD, jest to, że Asterisk nie wymaga zakupu specjalnej licencji udostępniającej niniejsze funkcje. Ograniczenie ilości kolejek połączeń jest na przykład, określane tylko i wyłącznie przez sprzęt, którego używamy.

4.2.1.5 Szczegółowa Ewidencja Połączeń

Asterisk prowadzi kompletną Szczegółową Ewidencję Połączeń (CDR - Call Detail Records). Możemy przechowywać te informacje w pliku lub preferowanie w bazie danych, dla bardziej przejrzystego widoku i przechowywania. W niniejszym Projekcie, wszelkie informacje będą przechowywane w głównej bazie danych. Używając tych informacji możemy monitorować wykorzystanie systemu Asterisk, szukać schematów lub nieprawidłowości, które mogą mieć wpływ na naszą działalność.

Możemy porównać niniejsze dane z rachunkiem otrzymanym od dostarczyciela telefonicznego. Pozwalają one na analizę ruchu połączeń i umożliwiają na przykład utworzenie raportu najczęściej wybieranych numerów.

Możemy także określić centralę telefoniczną, która dzwoni do nasz najczęściej, w celu ukierunkowania naszego marketingu na odpowiedni obszar.

Ponadto, możemy sprawdzić ile trwają połączenia telefoniczne. Umożliwia to zliczenie ile połączeń określony telekonsultant odbiera i możemy porównać to ze średnią. Istnieje bardzo wiele zastosowań tej funkcji.

Nie należy lekceważyć istotności ewidencji połączeń: ta informacja jest bezcenna dla wielu funkcji biznesowych. Ze względu na fakt, że w wielu państwach funkcjonuje lista do-not-call (lista abonentów nie życzących sobie połączeń z telemarketingu), możemy szybko określić, czy dzwoniliśmy do kogoś z takiej listy i zweryfikować poprawność naszych procesów sprawdzających.

4.2.1.6 Nagrywanie Rozmów

Asterisk daje nam możliwość nagrywania rozmów wykonywanych przez PBX. Możemy to wykorzystać w celach szkoleniowych, uzyskując przykłady rozmów, które przebiegły poprawnie oraz niepoprawnie. Można to także wykorzystać, aby udowodnić treść rozmowy, w celu usatysfakcjonowania klientów lub partnerów, może to także być pomocne w przypadku potencjalnej sytuacji prawnej. Ważne jest także, aby rozważyć tę funkcję w momencie zakładania usługi Asterisk, ponieważ trzeba dostosować sprzęt oraz pomyśleć o kwestii przechowywania, jeżeli Twój PBX ma obsługiwać i nagrywać dużą liczbę rozmów.

Ostrzeżenie: Nasz system zapewnia niniejszą funkcję, należy jednak określić czy korzystanie z niej jest legalne, odpowiednie oraz pomocne w poszczególnych warunkach.

4.2.1.7 System IVR

System IVR (Interactive Voice Response), czyli system umożliwiający interaktywną obsługę osoby dzwoniącej rewolucjonizuje prawie każdy biznes, który decyduje się z niego korzystać. Siła i elastyczność programowalnego

systemu telefonicznego daje możliwość odpowiadania naszym klientom w merytoryczny sposób.

Możemy użyć Asteriska, aby zapewnić 24-godzinną obsługę, jednocześnie zmniejszając obciążenie pracy naszym pracownikom. Asterisk pozwala odtwarzać pliki, czytać tekst, a nawet pobierać informacje z bazy danych. Jest to ten sam typ technologii, które można spotkać w bankowości telefonicznej lub systemach płatności za rachunki. Gdy dzwonisz do swojego banku słyszysz różne nagrania i prośbę o wprowadzenie określonych danych za pomocą wybierania tonowego. Na przykład możesz usłyszeć powitania i wiadomości o statusowe, proszące Cię o wprowadzenie numeru konta, danych osobowych lub danych uwierzytelniających. Często też możesz usłyszeć spersonalizowane informacje, które zostały pobrany z bazy danych, takie jak Twoje ostatnie transakcje, czy też saldo Twojego rachunku, Systemy tego typu mogą być i są implementowane przy użyciu Asteriska.

4.2.1.8 System Poczty Głosowej

Asterisk posiada w pełni funkcjonalny system poczty głosowej. System poczty głosowej jest bardzo wydajny. Wspiera konteksty poczty głosowej, więc wiele organizacji może być obsługiwanych z tego samego serwera. Obsługuje różne strefy czasowe, więc użytkownicy mogą śledzić, kiedy przychodzą ich połączenia. Zapewnia nawet funkcje powiadomienia odbiorcy o nowej wiadomość za pomocą emaila: a nawet przesyła audio wiadomość w załączniku.

4.2.1.9 System Voice over IP (VoIP)

Asterisk daje nam możliwość wykorzystania protokołu internetowego (IP) do wykonywania połączeń telefonicznych, łącznie z bardziej tradycyjnymi technologiami telefonicznymi.

Wybór Asteriska nie oznacza, że możemy używać wyłącznie technologii Voice over IP do wykonywania połączeń. W rzeczywistości, wiele instalacji Asteriska w ogóle z niej nie korzysta. Jednak każdy z tych systemów posiada możliwość łatwego dodatnia usługi Voice over IP, w każdym momencie i bez żadnych dodatkowych kosztów.

Większość firm posiada dwie osobne sieci: jedną dla telefonów i jedną dla komputerów. W naszym systemie, połączyliśmy dwie powyższe Siecie w jedną sieć Ethernet. Największe oszczędności wynikają z redukcji obciążenia administracyjnego dla personelu informatycznego w przyszłości. Teraz wystarczy, że będziemy mieli kilku ekspertów od komputerów i sieci, a ze względu, że telefonia będzie przebiegała łącznie z siecią IP, podstawowa wiedza wystarczy, aby personel był stanie obsługiwać system telefoniczny.

W dłuższej perspektywie, ma to również korzyści w kwestii kosztów zakupu sprzętu. Sprzęt komputerowy staje się coraz bardziej tańszy, podczas gdy opatentowane systemy telefoniczne wydają się być cały czas stałe w swojej cenie.

Dlatego też, możemy oczekiwać, że koszt przełączników sieciowych, routerów oraz innego sprzętu sieciowego będzie w dalszym ciągu się obniżać.
W większości obecnych systemów telefonicznych, rozszerzenia mogą występować tylko tak daleko, jak wynosi maksymalna długość okablowania dozwolona przez producenta systemu telefonicznego. Choć wydaje się to całkowicie uzasadnione, czasami jest to bardzo uciążliwe. W przypadku używania VoIP możemy mieć wielu użytkowników używających tej samej usługi Asteriska z różnych lokacji. Możemy mieć użytkowników w lokalnym biurze, używających telefonów PSTN lub telefonów IP i możemy mieć zdalnych użytkowników VoIP, a nawet możemy mieć systemy Asteriska obsługiwane zupełnie osobno, ale z zintegrowanym trasowaniem

To jednak nie wszystkie korzyści wynikające z używania Voice over IP. Wykorzystamy serwer Asteriska w LTMC oraz podłączymy go do centrali PBX (Siemens HiPath 4000/8000). Oznacza to, że każde biuro będzie miało własne lokalne linie, ale między biurowa komunikacja będzie tunelowana przez sieć centrali. Oszczędności wynikające z uniknięcia opłat za połączenia będą znaczące, ale jeszcze nie wszystko.
Połączenie biur w ten sposób, da nam możliwość jednolitego obsługiwania połączeń, bez względu na to, w którym biurze znajdują się pracownicy. Na przykład, jeżeli klient zadzwoni do Biura A, aby zapytać o swoje konto, a wydział kont znajduje się w Biurze B, w bardzo prosty sposób przełączymy rozmowę do odpowiedniej osoby w innym biurze. Nie musimy się przejmować, gdzie to biuro się znajduje, tak długo jak posiadają solidne połączenie internetowe, to biuro może nawet znajdować się w innym państwie.

Możemy trasować połączenia na podstawie kosztów. Jeżeli jest bardziej opłacalne, możemy przełączyć połączenia do innego biura, gdzie następnie zdalny serwer Asteriska połączy je z regularną siecią telefoniczną. Jest to powszechnie określane jako „Omijanie Opłat” ("Toll Bypass").

Kolejną korzyścią wynikającą z połączenia systemów telefonicznych jest to, że możemy trasować połączenia w oparciu o czas. Wyobraźmy sobie, że mamy dwa biura, każde w innej strefie czasowej. Każde biuro będzie prawdopodobnie otwarte w innych godzinach. Aby efektywnie obsługiwać naszych klientów, możemy przekazywać połączenia z zamkniętego biura do tego, które w danym momencie jest otwarte. Ponownie, jeżeli używamy połączenia internetowego do łączenia naszych biur, żadna dodatkowa opłata nie jest pobierana.

Łącząc nasze biura używając technologii Voice over IP, możemy zwiększyć efektywność obsługi klienta, jednocześnie zmniejszając nasze wydatku: prawdziwa sytuacja win-win.

Istnienie wszystkich tych funkcji, nie koniecznie oznacza, że musimy z nich korzystać, jednak wszechstronność Asteriska umożliwia nam korzystanie i ignorowanie funkcji, wedle naszych wymagań. Jeżeli zdecydowalibyśmy się na używanie każdego typu linii i funkcji, które Asterisk wspiera, mogłoby to prowadzić do stworzenia bardzo skomplikowanego i trudnego w aspekcie administrowania

systemu. Powinniśmy wybrać ten zbiór, który pasuje do naszych wymagań i który będzie dobrze funkcjonował w naszej obecnej konfiguracji komunikacyjnej.

4.2.2 Czym Asterisk nie jest?

Skoro omówiliśmy już, co Asterisk potrafi musimy jasno określić, czym Asterisk nie jest. Poprzez pogląd na funkcje, których Asterisk nie spełnia, możemy ocenić jak ważne są te aspekty, aby upewnić się, że Asterisk jest najlepszym wyborem dla Lublin TMC.

4.2.2.1 Asterisk Nie Jest Produktem Gotowym Do Użytku

Istnieją systemy telefoniczne, które są łatwe w instalacji, konfiguracji i implementacji, że ktokolwiek beż żadnego szkolenia mógłby to zrobić. Asterisk nie jest jednym z nim.

Elastyczność i wydajność Asteriska wymagają odpowiedniego ustawienia i konfiguracji. Najlepszy zestaw opcji będzie się różnił, w zależności od instalacji, a czasami nawet różnił przy tej samej instalacji, ale z innym zastosowaniem. Na przykład, niektóre aparaty powinny mieć funkcję połączenia oczekującego, podczas gdy dla innych to nic innego jak zakłócenie.

Z Asteriskiem możemy skonfigurować wszystko, czego tylko potrzebujemy, jednak wymaga to pewnej wiedzy. Czasami do zmian systemu telefonicznego wymagana jest znajomość programowania. ACISA oferuje swoją wiedzę oraz zapewnia szkolenie na temat jak dokonywać przeciętnych konfiguracji.

4.2.2.2 Asterisk Nie jest SIP Proxy

Asterisk obsługuje protokół inicjowania sesji (SIP - Session Initiation Protocol) dla VoIP. Połączenia mogą być wykonywane i odbierane przez SIP przy pomocy Asteriska.

W SIP, urządzenia rejestrują się na serwerze SIP. Niniejszy serwer zezwala urządzeniom zlokalizować się nawzajem, aby ustalić połączenie. Gdy duża ilość urządzeń SIP jest w użyciu, często korzysta się z SIP Proxy, aby obsłużyć rejestracje oraz połączenia w efektywny sposób.

Asterisk nie może jednak spełniać funkcji SIP Proxy. Urządzenia SIP mogą się rejestrować z Asteriskiem, ale jeżeli ilość tych urządzeń znacznie się zwiększy, Asterisk nie jest w stanie zbyt dobrze się skalować. Dlatego też, jeżeli mamy w planach używanie ponad 200 urządzeń SIP, Asterisk może być nieodpowiedni. W naszym Projekcie rozważyliśmy niniejszą kwestię i ilość naszych urządzeń SIP wynosi poniżej dwudziestu, poza tym zapewnimy zarządzanie dla 100 linii.

4.3.- Plan Projektu

Przed przedstawieniem projektu należy rozważyć kilka kwestii:

4.3.1 Rozważania

4.3.1.1 Publiczna Komutowana Sieć Telefoniczna (PSTN)

Większość telefonów na świecie jest podłączonych do szerokiej sieci, umożliwiającej każdemu telefonowi połączenie z jakimkolwiek innym. Ta sieć nazywa się Publiczną Komutowaną Siecią Telefoniczną (PSTN). Z telefonami, które się w niej znajdują można się połączyć poprzez wybranie numeru, który może zawierać numery dla danego państwa, numery kierunkowe oraz numery telefonu.
Chociaż istnieją przypadki, w których podłączenie do sieci PSTN jest niewłaściwe, większość użytkowników telefonów oczekuje, żeby w jego zasięgu był cały świat. Dlatego też będziemy rozważać połączenie z PSTN jako wymóg.

4.3.1.1.1 Metody Połączenia

Istnieje wiele różnych metod podłączenia do sieci PSTN. Każda ma swoje zalety i wady, o większości z nich wspomnimy. Ze względu na fakt, że koszty różnią się w zależności od miasta oraz państwa, nie podamy dokładnej ceny.
Zajmiemy się każdą metodą osobno.

4.3.1.1.1.1 Łącze POTS (Plain Old Telephone Service)

Najprawdopodobniej najbardziej popularną metodą podłączenia do PSTN jest łącze POTS. Jest to łącze analogowe, oferowane przez operatora telefonicznego. Każda linia POTS może obsługiwać tylko jedną rozmowę w danym momencie. Osiem linii jest zazwyczaj punktem, w którym powinniśmy poważnie zastanowić się nad inną technologią dla naszego podłączenia.

Łącza POTS z naszej LEC wymagają interfejsu Foreign eXchange Office (FXO), aby były możliwe do zastosowania w Asterisku.

4.3.1.1.1.2 Sieć Cyfrowa z Integracją Usług ISDN (Integrated Services Digital Network)

ISDN jest całkowicie cyfrową siecią, która jest dostępna od ponad dekady. Jest dostępna w dwóch głównych wersjach: Podstawowej BRI (Basic Rate Interface) oraz Pierwotnej PRI (Primary Rate Interface).

ISDN dzieli łącze na wiele kanałów. Każdy kanał może zawierać ładowność (Element nośny lub kanał B) lub sygnalizację (Dane lub kanał D). BRI posiada 3 kanały: 1 kanał D oraz 2 kanały B. Dlatego też, na jednym BRI mogą mieć miejsce dwa jednoczesne połączenia. PRI posiada 24 kanały: 1 kanał D oraz 23 kanały B, dając możliwość wykonywania 23 jednoczesnych połączeń.

ISDN nie jest ograniczone wyłącznie do przesyłania głosu. Każdy kanał może nieść 64k danych, jeżeli zostanie odpowiednio skonfigurowany z LEC. Daje to ISDN dużą przewagę nad POTS, skoro kanały mogą być w locie przekonfigurowane z głosu do danych.

Dzięki osobnemu kanałowi D, ISDN może wykonywać funkcje, jakich POTS nie jest w stanie obsługiwać, na przykład ustalanie własnego caller ID (identyfikator dzwoniącego), otrzymywanie wiadomości o wybieranym numerze, przekierowywanie połączeń w locie oraz cały zestaw innych funkcji. Oczywiście, wszystkie te funkcje wymagają współpracy z LEC.

4.3.1.1.1.3 T1 lub E1

Technicznie rzecz biorąc, kiedy zamawiamy usługę od LEC, zamawiamy DS1, które jest dostarczane przez łącze określane jako T1. Jednakże, ten szczegół jest zazwyczaj przeoczany. Dlatego też, będziemy odwoływać się do tego w odpowiedni sposób: T1.

T1 jest łączem z 24 kanałami. Każdy kanał może zawierać połączenie. Dlatego też, T1 może pomieścić jedno połączenie więcej w porównaniu z PRI. W Europie, E1 są bardziej popularne i różnią się od T1 tym, że posiadają 32 kanały. Łącza T1 muszą w jakiś sposób sygnalizować połączenie. Rozwiązane jest to sygnalizacją przy pomocy bitu „zrabowanego” (Robbed Bit Signaling). Oznacza to, że od czasu do czasu bit zostaje „zrabowany”, kiedy wymagany jest przepływ informacji o połączeniu. Choć jest to zazwyczaj niewychwytywane przez ludzkie ucho, może to być szkodliwe w przypadku transmisji danych.

Wykorzystywanie T1 do dostarczania zarówno danych jak i głosu jest bardzo powszechną praktyką. Niektóre z 24 kanałów są oznaczone jako kanały do przesyłania danych, a inne do przesyłania głosu. Mogą występować nawet kanały nieużytkowane. W ten sposób LEC (operator) może oferować niższe ceny w przypadku łączonych usług, ponieważ kilka kanałów będzie przypisanych przesyłaniu głosowemu, inne będą używane do połączenia z Internetem, a jeszcze inne mogą być wykorzystane do prywatnej transmisji danych do innego biura.

Lokalni operatorzy (LEC) są w stanie przesyłać informacje o numerze, który został wybrany już na początku połączenia. W ten sposób jedna z zalet PRI jest także spełniana przez łącza T1. Jeżeli zamierzamy mieć od 8 do 12 łączy, jak i również transmisję danych, T1 może być dobrym wyborem.

4.3.1.1.1.4 Połączenia Voice over IP

W ostatnich latach pojawił się nowy sposób podłączenia do sieci PSTN. Firmy używają PRI, T1 i innych technologii, aby połączyć się z PSTN, a następnie sprzedają te połączenia klientom. Użytkownicy łączą się z firmami oferującymi te

połączenia za pomocą technologii Voice over IP. W ten sposób, można całkowicie ominąć lokalnych operatorów (LEC).

Przez niniejsze usługi, możemy uzyskać prawdziwy numer telefonu, z numerem kierunkowym w zależności od tego, do którego nasz dostarczyciel ma dostęp. Nie wszyscy dostarczyciele mogą zaoferować numery w każdej okolicy. Oznacza to, że połączenie z naszego numeru może być rozmową na dużą odległość z naszym sąsiadem, a rozmową lokalną z kimś z innego województwa. Jednakże, zaletą tego jest to, że nasz dostarczyciel będzie trasował większość naszych połączeń przez infrastrukturę VoIP, a następnie użyje PSTN, kiedy uzyska najbardziej lokalny punkt w miejscu odbiorczym, co oznacza, że koszty za rozmowy na dużą odległość zostaną znacznie zredukowane. Jeżeli łączymy się z wieloma różnymi państwami, województwami lub miastami, znalezienie dostarczyciela, który oferuje lokalny dostęp PSTN do miejsc, do których dzwonimy najczęściej może nam zająć trochę czasu.

Stawki za minutę są zazwyczaj bardzo atrakcyjne. Często, stawki za rozmowy długodystansowe wynoszą tyle samo, co za rozmowy lokalne. Jedną rzeczą na którą należy uważać, jest to, że niektórzy dostarczyciele pobierają opłatę za połączenia przychodzące, podobnie jak w przypadku telefonów komórkowych. Zdarzają się też dostarczyciele, którzy pobierają opłaty za rozmowy lokalne.

Kolejną rzeczą, z której należy sobie zdawać sprawę, jest to, że niektórzy dostarczyciele wymagają korzystania z ich Bramki VoIP (ATA - Analog Terminal Adapter). W praktyce wygląda to tak, że przysyłają skrzynkę, która obsługuje Voice over IP i którą należy podłączyć do Internetu. Wtedy będziesz miał łącze POTS, do którego można podłączyć telefon (lub Asteriska).

Stosowanie technologii Voice over IP ma sens w wielu instalacjach. Jednak, aby jakość była akceptowalna, wymagane jest solidne połączenie internetowe o niskim opóźnieniu. Inną kwestią, na którą należy zwrócić uwagę jest drganie. Drganie odnosi się do różnic w opóźnieniach pomiędzy pakietami. Większość protokołów znacznie lepiej radzi sobie z opóźnieniem, jeżeli jest ono stałe w czasie połączenia.

Odpowiednim kandydatem na technologię Voice over IP jest więc miejsce, w którym przerwa w świadczeniu usługi nie będzie zagrażała życiu oraz nie zaszkodzi nieodwracalnie firmie. Podczas gdy dostarczyciele VoIP dążą do osiągnięcia jak najlepszej dyspozycyjności, będziemy musieli także polegać na Internecie w ogóle oraz na dostawcy usług internetowych naszego dostarczyciela VoIP, jak i na naszym własnym dostawcy usług internetowych.

Jeżeli nasze potrzeby telekomunikacyjne są tego typu, że okresowe przestoje są tolerowalne, technologia VoIP będzie najprawdopodobniej naszym najtańszym rozwiązaniem. Wymaga ona także mniej sprzętu w naszym systemie Asterisk, zwiększając oszczędności: aby korzystać z VoIP z Asteriskiem, wszystko czego potrzebujemy to solidny dostęp do Internetu; nie będziemy potrzebować żadnego wyspecjalizowanego sprzętu telefonicznego.

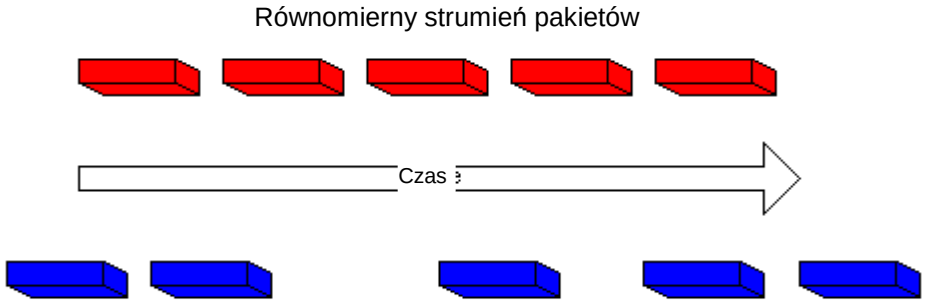
4.3.1.2 Połączenia Intranetu

Ze względu na wymagania centrali, niniejszy system będzie podłączony do Sieci Telekomunikacyjnej Centrali (Council Telecomunication Network). W Systemie Telefonicznym będzie to połączenie typu Ethernet w izolowanej sieci VLAN o wysokiej jakości usługi, aby uniknąć problemów z opóźnieniem i drganiem.

4.3.1.3 Drganie oraz Opóźnienie

Drganie definiuje się, jako różnicę pomiędzy opóźnieniami w otrzymywanych pakietach. Po stronie wysyłającej, pakiety są wysyłane w ciągłym strumieniu, z równymi odstępami pomiędzy kolejnymi pakietami. Ze względu na przeciążenie sieci, nieodpowiednie kolejkowanie lub błędy konfiguracyjne, ten równomierny strumień może zostać zniekształcony lub opóźnienie pomiędzy pakietami może zostać zmodyfikowane.

Poniższy schemat ilustruje, w jaki sposób obsługiwany jest równomierny strumień pakietów.

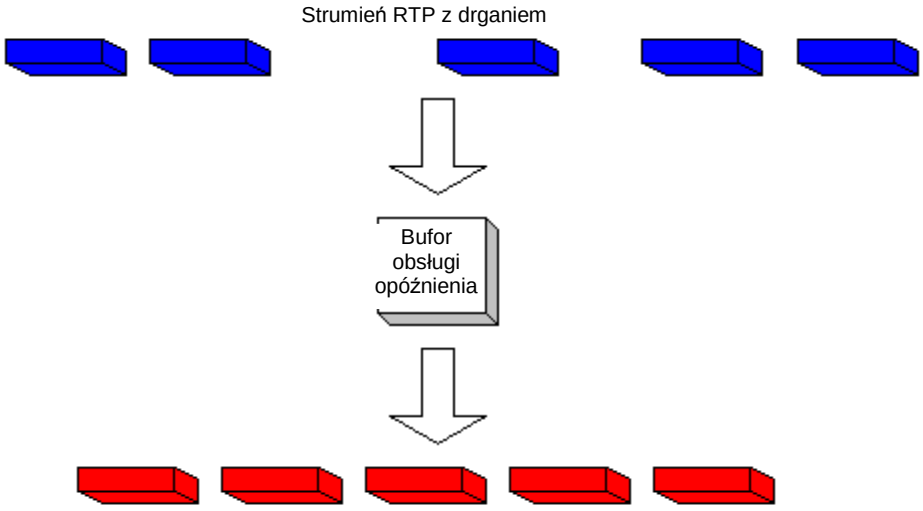


Ten sam strumień pakietów po przeciążeniu lub nieodpowiednim kolejkowaniu

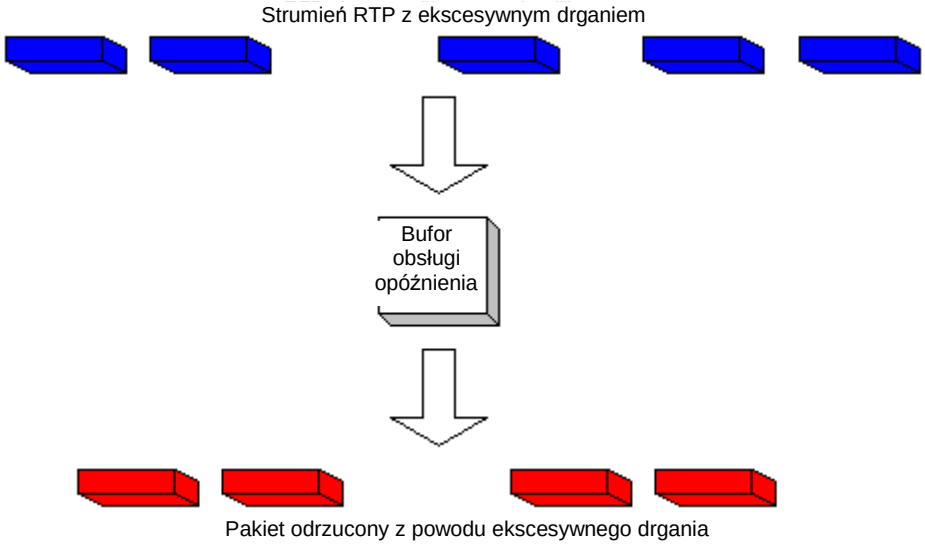
Gdy router otrzymuje strumień audio Protokołu Czasu Rzeczywistego (RTP) dla Voice over IP (VoIP), musi zrekompensować występujące drganie. Mechanizm, który się tym zajmuje to bufor obsługi opóźnienia.

Bufor obsługi opóźnienia buforuje takie pakiety, a następnie przekazuje je w równomiernym strumieniu do cyfrowego przetwarzania sygnałów (DSP), aby przekonwertować je ponownie do analogowego strumienia audio.

Poniższy schemat ilustruje, w jaki sposób obsługiwane jest drganie.



Jeżeli drganie jest tak duże, że powoduje, iż odebrane pakiety są poza zasięgiem tego bufora, pakiety poza zasięgiem są odrzucane i w strumieniu audio słychać zakłócenia. Jeżeli straty są tak małe jak jeden pakiet, DSP interpoluje przypuszczalny dźwięk i nie słychać żadnych zakłóceń. Jeżeli drganie przekracza możliwości rekompensacyjne DSP, problem jest słyszalny w strumieniu audio. Poniższy schemat ilustruje sposób, w jaki obsługiwane jest ekscesywne drganie.

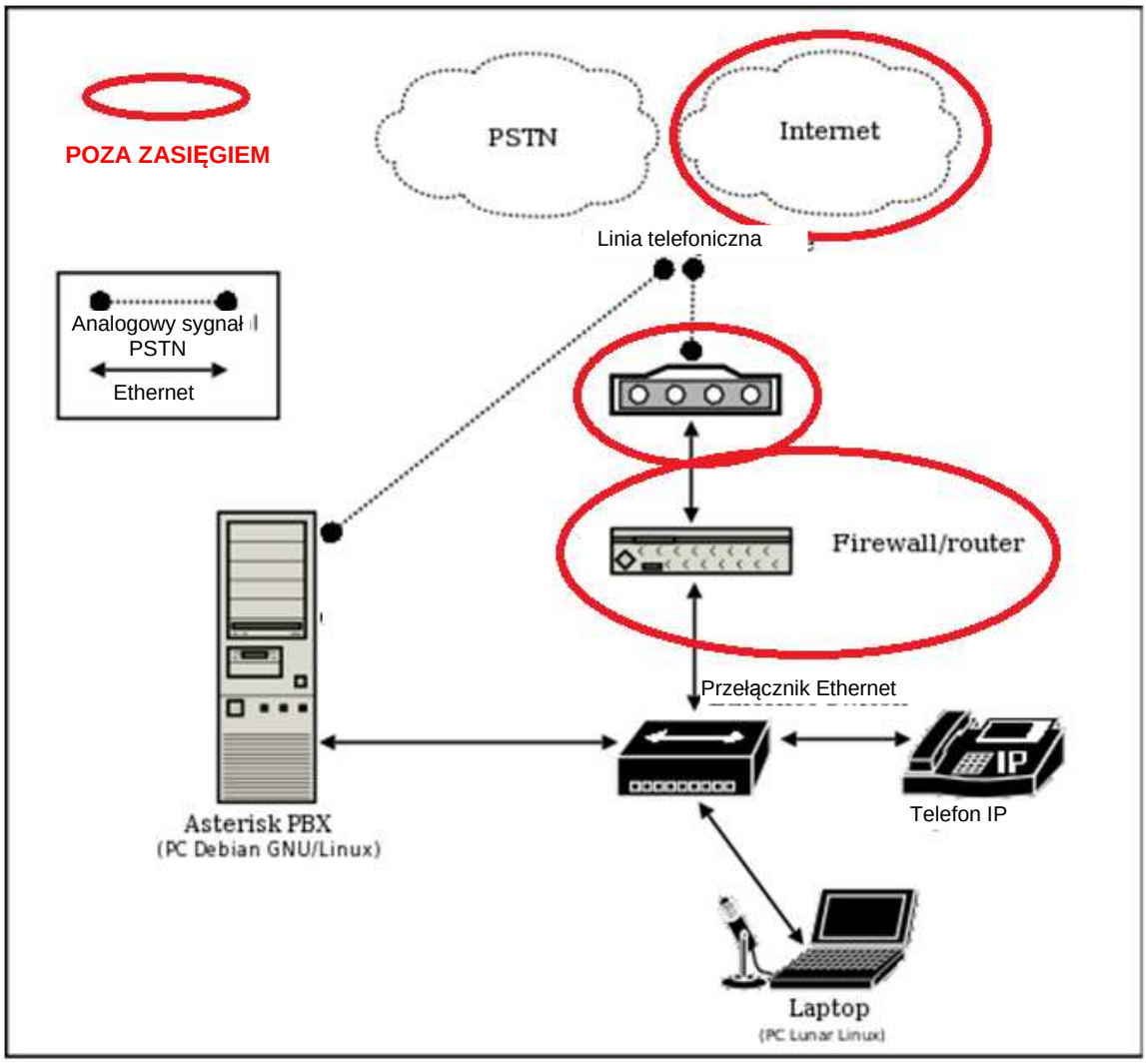


Jeżeli opóźnienie wynosi powyżej 30ms, występują przecieki transmisyjne.

Aby uniknąć takiej sytuacji, w sieci należy zaimplementować QoS, a ruch VoIP powinien być zawarty we własnej sieci VLAN oraz musi mu zostać przypisany wysoki priorytet w zarządzaniu ruchem.

4.4.- Architektura

Proponowany system ma poniższą architekturę:



Wszystkie elementy oznaczone czerwonym okręgiem są w zakresie istniejącej Sieci Telekomunikacyjnej Lublina (Lublin Telecomunication Network).

4.4.1 Linie równoległe

Będziemy obsługiwać maksymalnie 16 równoległych połączeń PSTN.

Jeżeli będziemy potrzebować więcej kanałów, niż posiadamy, ktoś będzie miał sygnał zajętości. Dlatego też, powinniśmy zaplanować maksymalną ilość kanałów, której używaliśmy, plus rozsądny margines. 125% obecnego maksimum jest zazwyczaj rozsądnym marginesem, to pozwala na przykład, na 20-25% wzrost, tak abyśmy mogli zagospodarować nagłe zwiększenie połączeń bez powodowania sygnału zajętości. Jeżeli zwiększymy połączenia do tego poziomu na względnie długi okres czasu, powinniśmy rozważyć rozszerzenie ilości linii, aby zapobiec przeciążeniu.

Niniejsze ilości są wytycznymi i mogą się zmienić w zależności od okoliczności. W centrum telefonicznym, gdzie głównym zadaniem jest odbieranie i wykonywanie

połączeń, 150% jest bardziej satysfakcjonującą ilością. Powinniśmy także wziąć pod uwagę czas, jaki trzeba przeznaczyć na założenie nowych linii. Jeżeli wydarzy się coś istotnego, co sprawi, że ilość połączeń znacząco się zwiększy, powinniśmy mieć zdolność do zapanowania nad taką sytuacją lub być w stanie szybko zwiększyć naszą wydajność.

Tak więc, ostatecznie będziemy obsługiwać 22 równoległe łącza.

4.4.2 Technologia Połączenia

Teraz, gdy mamy już ilość łączy, musimy określić jakich technologii będziemy używać. VoIP jest zazwyczaj najtańsza, w szczególności dla długodystansowych połączeń, ale nie nadaje się do niniejszego Projektu, ponieważ niezawodność nie jest wystarczająca dla Sterowania Monitoringiem Ruchu (Trafic Monitoring Control).

PRI jest z zasady najbardziej niezawodny. Także w przypadku PRI trunking jest bardziej efektywny, co może okazać się kluczowym aspektem. Pomimo, że PRI może mieć setki numerów telefonów, za każdy numer, co miesiąc pobierana jest opłata. Numery zwane DID (Directed Inward Dialing) są "wirtualnymi" numerami zazwyczaj sprzedawanymi w zestawach 10-20. Jeżeli na początku nie zamówi się odpowiedniej ilość, zazwyczaj nie ma problemu, by zamówić więcej numerów DID w późniejszym czasie; często mogą być dostępne w ciągu tygodnia, w zależności od firmy telefonicznej. Niniejsze numery przypisze się do poszczególnych urządzeń oraz grup urządzeń, gdy zostaną już przydzielone.

Oznacza to, że możemy zlikwidować lub ponownie przydzielić numery, jeżeli zajdzie taka potrzeba. Może zajdzie potrzeba przydzielania DID innym grupom, w zależności od danej sytuacji, osobistych DID dla kluczowego personelu lub głównych DID dla grupy osób, która byłaby odpowiedzialna za obsługę niniejszych połączeń.

Należy rozważyć, jakich linii wymagamy, jakich numerów telefonów potrzebujemy oraz wyraźnie zaznaczyć, jeżeli różnią się one od aktualnie zainstalowanych połączeń PSTN.

Zatem PRI jest wybraną metodą połączenia wzajemnego z PSTN.

4.4.3 Urządzenia Końcowe

Gdy już zdecydowaliśmy się na sposób podłączenia do PSTN, musimy podjąć decyzję odnośnie naszych wewnętrznych połączeń. Nasz PBX może posiadać podłączone modemy, faksy, telefony oraz inne jednostki PBX. Wszystkie te urządzenia będziemy określać mianem Urządzeń Końcowych.

4.4.3.1 Typy Urządzeń Końcowych

Istnieją cztery główne typy urządzeń końcowych: telefony sprzętowe, telefony softwarowe, urządzenia komunikacyjne oraz PBX. Poniżej krótko opiszemy każdy z tych typów.

4.4.3.1.1 Telefony Sprzętowe

Telefony sprzętowe są fizycznymi urządzeniami działającymi jak zwykły aparat telefoniczny. Telefony sprzętowe są dostępne dla POTS (jak te używane w typowym gospodarstwie domowym) lub VoIP.

4.4.3.1.2 Telefony Programowe

Jak sama nazwa wskazuje, telefony programowe są realizowane w oprogramowaniu. Używające wszystkich protokołów dostępnych dla telefonów sprzętowych, telefony programowe są znacznie tańsze w implementacji. Korzystając ze zwykłego komputera osobistego, można uniknąć kosztownej wymiany wszystkich telefonów w budynku.
Zanim przejdziemy dalej, należy zaznaczyć, że większość telefonów sprzętowych to tak naprawdę telefony programowe połączone z odrobiną specjalnego sprzętu. Moc obliczeniowa telefonu sprzętowego nie jest tak rozległa jak ta komputera osobistego, ale w przeciwieństwie do komputera osobistego jest specjalnie dostrojony do przenoszenia głosu. Dlatego też, nie powinniśmy od razu odrzucać możliwości zastosowania telefonów sprzętowych.

Prawdą jest, że niektórym użytkownikom będzie trudniej zaakceptować telefony programowe. Oprócz niechęci niektórych użytkowników do korzystania z komputera w celu rozmowy przez telefon, musimy zastanowić się również, jak poradzimy sobie w przypadku awarii prądu. Zasilenie komputera, który potrzebuje ponad 400 watów będzie znacznie trudniejsze oraz kosztowniejsze, niż zapewnienie napięcia dla telefonu sprzętowego, który pobiera 15 watów, szczególnie w przypadku dłuższych przestojów.
Najbardziej istotną zaletą telefonów programowych jest ich koszt. W większości firm, na każdym biurku stoi komputer i telefon. Jeżeli uda nam się wyeliminować telefon, będzie to oczywistą redukcją kosztów sprzętu. Jest wiele dostępnych produktów telefonów programowych, a większość systemów operacyjnych ma pakiet telefonu programowego w standardowej wersji. Istnieje również wiele dostępnych produktów open source. Wybór produktu, programowego, czy sprzętowego, jest równie ważny jak wybór PBX. Należy się upewnić, że użytkownicy będą korzystali z urządzenia oraz, że będzie ono solidne i niezawodne.

4.4.3.1.3 Urządzenia Komunikacyjne

Dedykowane urządzenia komunikacyjne, takie jak modemy i faksy, nadal są bardzo powszechne w dzisiejszym biznesie. Podczas gdy niniejsze urządzenia mogłyby być zastąpione przez nowocześniejsze i bardziej niezawodne technologie, nie zostały jeszcze one wyparte.

Większość z tych urządzeń będzie analogowa (co oznacza, że będą wymagały łącza POTS). Jak wspomniano wcześniej, T1 może obsłużyć 24 linii, a łącze POTS jest w stanie połączyć tylko 1 linię. Przy użyciu urządzenia zwanego bankiem kanałów, T1 można podzielić na 24 linie POTS.

Jeżeli potrzebujemy wielu linii POTS, banki kanałów mogą okazać się opłacalne.

Uwaga na temat faksowania: Asterisk obsługuje otrzymywanie oraz wysyłanie faksów poprzez dodatek o nazwie SpanDSP. Przy jego użyciu, Asterisk może odebrać faks i zamienić go w plik TIFF. Plik TIFF może być później dalej przekonwertowany do pliku PostScript lub PDF i wysłany emailem do odpowiedniego odbiorcy. Instalacja niniejszego dodatku nie została tutaj opisana, ze względu, że jest to kwestia podlegająca bardzo szybkim zmianom.

Niniejsze urządzenia komunikacyjne są zazwyczaj obsługiwane na zasadzie „dziedziczenia”. Powinniśmy jednak nieustannie dążyć do tego, aby zredukować przestarzałe technologie i zastąpić je bardziej aktualnymi rozwiązaniami.

4.4.3.1.4 Inny PBX

Możemy podłączyć więcej centrali PBX razem, aby zapewnić usługi użytkownikom znajdującym się na innej centrali PBX. Aby połączyć centrale PBX możemy użyć SIP, PRI, T1, H.323 lub IAX.

Jeżeli zamierzamy połączyć kilka centrali PBX z Asteriskiem, powinniśmy użyć IAX. Protokół IAX posiada kilka funkcji o określonym przeznaczeniu, takich jak możliwość trunkingu kilku rozmów do tego samego strumienia UDP, uzyskując lepszą wydajność.

W niniejszym Projekcie Asterisk będzie podłączony do Siemens Hipath PBX.

4.4.4 Długość Numerów Wewnętrznych

Tworząc nasz system telefoniczny powinniśmy utworzyć zestaw numerów wewnętrznych. Pomimo, że Asterisk tego nie wymaga, numery wewnętrzne powinny mieć taką samą długość dla wygody użytkowników. Należy, zatem określić długość, która będzie stosowana dla wszystkich numerów wewnętrznych.

W czasie tworzenia numerów wewnętrznych, zazwyczaj dobrze jest zgrupować pewne numery razem. Na przykład, wszystkie numery wewnętrzne sprzedaży powinny się znajdować w numerach 200, obsługi 300, a zarządzania 100 itd. Można nawet dokonać dalszego podziału i pierwszy poziom wsparcia umieścić w 3100, drugi poziom w 3200, trzeci 3300 itd.

W niniejszym Projekcie będzie 100 numerów wewnętrznych i będą one zdefiniowane przez lubelski wydział techniczny w kolejnej fazie Projektu.

4.4.5 Skalowalność i Awaryjny Tryb Pracy

Jako, że serwer Asterisk będzie prawdopodobnie bardzo ważny dla firmy, chcemy się upewnić, że przywrócenie z kopii zapasowych będzie rzadko się zdarzało, a w przypadku awarii, gdy administrator będzie niedostępny, będziemy mieli pewnego rodzaju tryb awaryjny. Aby to osiągnąć, stosuje się techniki redundancji oraz balansu obciążenia w celu upewnienia się, że nasza infrastruktura ma środki do obsługi danych, które wymagają przetworzenia.

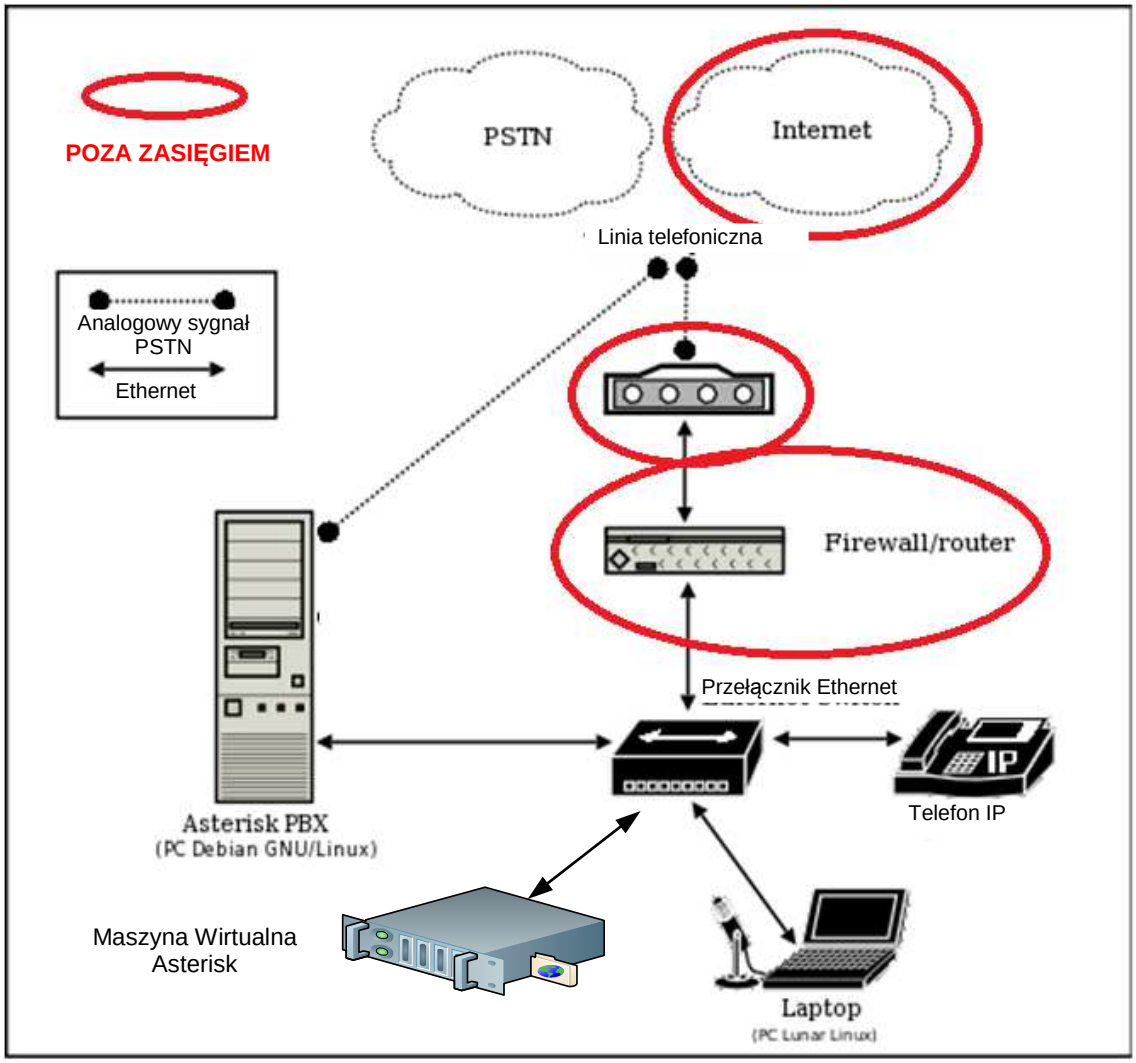
W przypadku awarii komponentu, chcielibyśmy się upewnić, że nie stracimy usług. Najlepiej byłoby, gdyby użytkownicy systemu nawet nie zauważyli, że miała miejsce jakakolwiek awaria, a administrator mógłby naprawić usterkę w najbliższym dogodnym momencie. Tego typu strategiczne planowanie jest niezbędne dla utrzymania usług, z których tak często się korzysta, jak to zazwyczaj ma miejsce w przypadku Asteriska.

Awaria jest nie tylko niepożądana, ale może mieć poważne skutki dla biznesu. Jest także możliwość takiej sytuacji, że system Asterisk będzie musiał pozostać offline na czas aktualizacji. Można tego uniknąć poprzez zaimplementowanie skalowalności do naszego projektu, upewniając się, że system będzie mógł rosnąć wraz z wymaganiami biznesu.

Ze względu na fakt, że Asterisk nie może być zainstalowany na klasterze, należy postarać się o balans obciążenia oraz skalowalność, które mogą być zaimplementowane bez użycia klasterów.

W niniejszym Projekcie system awaryjnego trybu pracy będzie zaimplementowany przez maszynę wirtualną i będzie zezwalał wyłącznie na połączenia do Siecie Telekomunikacyjnej Miasta Lublin (Lublin City Telecomunication Network.)

W miejsce systemu obciążenia balansu, zaimplementowany zostanie schemat Aktywno-Pasywny oraz programy wsadowe, które będą wykrywać awarię głównego systemu i minimalizować czas naprawy.



4.4.6 VoIP

Technologia Voice over IP używa różnych protokołów, w zależności od aparatu, centrali PBX oraz wymagań. Główne protokoły są następujące:

4.4.6.1 H.323

Protokół ten jest formalnie znany pod nazwą "ITU-T Recommendation H.323: Packet-based multimedia communications systems" (Systemy komunikacji multimedialnych oparte na pakietach), co jest wskazówką na to, jak uzyskać konferencje przez IP, włączając głos, wideo oraz dane. Niniejsza rekomendacja ukazała się mniej więcej w tym samym czasie, co SIP, jednak była znacznie szerzej implementowana.

Standard H.323 ma pełną wczesną kompatybilność. Obecnie najnowsza wersją jest H.323v5 oraz prowadzi się dyskusje na temat v6. Każda nowa wersja posiada

wszystkie elementy poprzedniej. To daje jasną ścieżkę modernizacji i zapewnienie, że sprzęt nie będzie szybko przestarzały.

Sprzęt H.323 jest szeroko dostępny. Od bramek po aparaty telefoniczne, wszelki sprzęt jest stosunkowo łatwo znaleźć. Większość aparatów telefonicznych posiada pełną funkcjonalność, ponieważ protokół H.323 ma bardzo wydajny zestaw funkcji.

Podczas, gdy standard H.323 nie były przeznaczony dla rozległych sieci, stworzono cały zestaw reguł pozwalających na międzydomenowe adresowanie. Opracowano także system raportowania jakości usług (QoS) z powrotem do serwera, pozwalając, aby takie informacje były wykorzystywane do trasowania przyszłych połączeń..

Wreszcie, H.323 jako standard obsługuje intruzje. Nowe punkty końcowe mogą być dynamicznie dodawane do jakiejkolwiek konferencji (tj. rozmowy).

Wsparcie Asteriska dla H.323 nie jest wbudowane. W tym celu należy zainstalować dodatkowy pakiet o nazwie asterisk-oh323. Po instalacji aparaty H.323 oraz bramki mogą być adresowania w taki sam sposób jak każdy inny kanał w Asterisku.

W niniejszym Projekcie ten protokół nie zostanie zaimplementowany.

4.4.6.2 SIP

Protokół Inicjacji Sesji lub SIP, jest kolejną metodą sygnalizowania połączeń VoIP. SIP jest częścią domyślnej instalacji systemu Asterisk.

Większość nowszego sprzętu VoIP obsługuje protokół SIP. Posiada on kilka zalet. Jedną z nich jest fakt, że kod jest mniejszy. Spowodowane jest to tym, że SIP obsługuje tylko bardzo podstawowe funkcje. Wszystkie zaawansowane funkcje są wspierane przez osobne standardy internetowe. Kolejnym powodem jego małych rozmiarów jest to, że kiedy funkcje stają się przestarzałe zostają usunięte z kodu.

Kolejną zaletą protokołu SIP jest jego modularna natura, a w takim przypadku rozszerzenie protokołu staje się łatwym zadaniem. Lepiej się również skaluje i został zaprojektowany z myślą o dużych sieciach.

SIP wydaje się być przyszłością VoIP. Istnieje jednak wiele funkcji dostępnych w H.323, których SIP nie oferuje. Obejmuje to sterowanie konferencją za pomocą aparatu, lepsze definicje bramki multimedialnej oraz dzielenie się danymi. Jednakże, SIP jest bardzo dobrym protokołem do prostych rozmów telefonicznych. Poza tym, w przypadku gdy używamy Asteriska, konferencje są kontrolowane właśnie przez Asteriska, a nie aparaty telefoniczne. Asterisk jest bramką multimedialną i kiedy jest używany w tej formie, nieoznaczoność w SIP nie jest problemem.

W niniejszym Projekcie ten protokół będzie obsługiwany.

4.4.6.3 IAX

Protokół IAX (Inter-Asterisk eXchange) jest protokołem opracowanym przez programistów, którzy stworzyli Asteriska. Ze względu na ograniczenia protokołu SIP oraz H.323, postanowiono stworzyć nowy standard, który pozwoli serwerom Asteriska wykonywać wiele operacji, które po prostu są niemożliwe przy użyciu innych standardów. Obsługuje on także pewne funkcje, które bardzo trudno wykonać w protokołach SIP oraz H.323.

Po pierwsze, IAX bardzo łatwo radzi sobie z tłumaczeniem adresów sieciowych (NAT - Network Address Translation). Większość firewalli oraz bramek Internetu korzysta z NAT. Protokoły SIP oraz H.323 bardzo ciężko pracowały, aby opracować standardy, które pozwolą im przedzierać się przez różne typy NAT; natomiast IAX bez problemu radzi sobie z większością urządzeń NAT.

IAX jest bardziej konfigurowalny niż inne protokoły, szczególnie przy współpracy z Asterskiem. Skoro kod źródłowy jest dostępny, możemy modyfikować go wedle własnego uznania, a następnie przedstawić te zmiany, aby zostały włączone do kolejnych wersji Asteriska. Ze względu na fakt, że IAX nie jest obecnie standardem Internetowym per se, nie jest pod tak ścisłym nadzorem, co sprzyja szybszemu rozwojowi i ulepszeniom.

IAX obsługuje trunking połączeń. Oznacza to, że wiele połączeń może być powiązanych w jednym strumieniu. Dzięki wydajności trunkingu, można zaoszczędzić znaczącą ilość pasma pozbywając się nadmiaru strumieni.
Połączenia IAX pomiędzy serwerami obsługują instrukcje przełączania, dzięki czemu informacje o trasowaniu połączenia mogą być efektywnie dzielone między serwerami Asteriska.

IAX obsługuje bardzo dużą ilość kodeków. Jakikolwiek kodek obsługiwany przez Asteriska może być używany z kanałami tego typu..

Ze względu na fakt, że IAX jest protokołem stworzonym przez Asteriska, nie ma zbyt wielu aparatów oraz bramek dostępnych. Jednakże, wraz z upływem czasu, coraz więcej i więcej urządzeń wspiera protokół IAX.

Czasami spotyka się podział na IAX oraz IAX2. IAX2 został włączony do IAX, dlatego jeżeli urządzenie obsługuje IAX2, będzie też obsługiwało IAX.

W niniejszym Projekcie ten protokół będzie obsługiwany.

5.- Obliczenia szerokości pasma

5.1.- Cele

W niniejszym rozdziale pzostaly zaprezentowane obliczenia odpowiadające ogólnej szerokośći pasm dla całego systemu.

5.2.- Uwagi ogólne

Przy obliczaniu szerokości pasma uwzględniono następujące uwagi ogólne:

- Inwentaryzacja podłączonych urządzeń do sieci (które nie są ostateczne ponieważ nie są wykonane projekty wykonawcze):

Urządzenie	**Ilość**
Sterowniki	57
Kamery ARTR	138
Wideodetektory	291
Panele Zmiennej Treści	10
Kamery CCTV	20

Rozdzielone w całości na 268 porty.

Wymagana szerokość pasma (BW) dla każdego urządzenia jest następująca:

- Sterowniki: 0,02 Mb.

- Panele Zmiennej Treści VMS: 0,01 Mb.

- Kamery CCTV: 2Mb

- Kamery ARTR: W tym wypadku PFU wymaga nagrania wszystkich obrazów, a tym samym ciągłego nadawania sygnału przez kamery. Każdy pakiet złożony ze zdjęć i innych danych (tablica rejestracyjna, data i godzina, miejsce …) jest mniejszy niż 120Kb.

Problem stanowi określenie rytmu dostarczania obrazów. W tym celu zbadamy jeden z odcinków pod kątem dostępnego przepływu ruchu w godzinach szczytu, określimy średnią liczbę zdjęć wykonanych przez kamerę i i rozszerzymy średni wynik na całkowitą liczbę kamer.

Na ul. Unii Lubelskiej, na przykład, między skrzyżowaniami 5 i 30, całkowity przepływ ruchu wynosi odpowiednio 1316 i 1824 pojazdów na godzinę. Te pojazdy

obsługuje sześć kamer. Co oznacza, że każda kamera powinna wykonywać średnio 523 zdjęć na godzinę.

Wymagana średnia szerokość pasma dla tej kamery wynosi:

BW = 523 (zdjęć) * 0,12 (Mb na zdjęcie) / 3600 (sekund na godzinę) = 0,018 Mb.

Dodatkowo strumień wideo z tych kamer również dociera do Centrum Sterowania zajmując szerokość pasma 0,5Mb.

Wynik całościowy na kamerę to 0,5+0,018=0,518.

Te informacje zostaną wykorzystane w 138 kamerach, które będą potrzebne zgodnie z danymi ogólnych projektów koncepcyjnych.

- Wideodetekcja

  Szerokośc pasma na każdym kanale wideo wynosi 2Mb.

- Administrowanie 268 portami wymaga BW o wartości 2 Mb

5.3.- Obliczenia szerokości Pasma

W tym rozdziale opisane są obliczenia szerokości pasma w całości oraz dla każdego z pierścieni tworzącego układ

5.3.1 Ogólne obliczenia szerokości Pasma

Bilans tych wyników jest następujący:

Urządzenie	Ilość	BW	Całość
Sterowniki	57	0,02	1,14
Kamery ARTR	138	0,518	71,5
Strumień Wideo z wideo detektorów	36	2	72
Panele Zmiennej Treści	10	0,01	0,10
Kamery CCTV	20	2	40
Zarządzanie Portami			4
			186,74

Jak będzie można zauważyć, liczbę przepływających z wideodetektorów obrazów, docierających równocześnie do Centrum Sterowania oszacowano na 36, z następujących powodów:

-Nie znaleźliśmy w PFU żadnego wymagania, które zobligowałoby nas do ciągłego przesyłu obrazów przez wideodetektory.

-Również nie istnieją w Centrum Sterowania środki do wizualizacji tak dużej liczby obrazów. Uznaliśmy, że każdy operator wyświetla obrazy z 6 kamer w danej chwili

-Normalnym działaniem podczas projektowania infrastruktury jest używanie parametrów równoczesności.

Podkreślamy, że to założenie jest wynikiem obliczeń. W Centrum kontroli mogą być odbierane w danym momencie jednocześnie obrazy z wszystkich wideodetektorów na skrzyżowaniu, jeśli jest to wymagane.

Zgodnie z PFU przewiduje się, że system będzie obsługiwał 160 skrzyżowań oraz 25 tablic zmiennej treści. Dla takich założeń uzyskano wartości:

Urządzenie	**Ilość**	**BW**	**Całość**
Sterowniki	160	0,02	3,2
Kamery ARTR	138	0,518	71,5
Strumień Wideo z wideo detektorów	48	2	96
Panele Zmiennej Treści	25	0,01	0,25
Kamery CCTV	49	2	96
Zarządzanie Portami			4
			270,95

Można zauważyć, że zwiększyliśmy również wielkość równoczesnego przesyłu obrazów z wideo detektorów i z ilośći kamer CCTV, która nie jest podana w PFU, a została uzyskana z proporcji do ilość przewidywanych skrzyżowań w przyszłości.

Cały strumień prowadzi do głównego pierścienia, rozpraszając się na jego krańce. Takie założenie mogłaby dodatkowo polepszyć wyniki, nie jest jednak wymagane, jeśli sporządzone zostały obliczenia wydajności sieci.

Otrzymane wyniki z przeprowadzonych obliczeń szerokości pasma gwarantują, że przepustowość zarówno dla stanu projektowanego jak i dla stanu w przyszłości będzie mieć zapas powyżej 70%.

Przy określeniu zaledwie nazw przyszłych zakładanych systemów, trudno jest wyznaczyć wymaganą szerokość pasma, niemniej jednak spróbujemy to określić:

- Informacja dotycząca uwarunkowań środowiskowych: Przewidywany system ma tworzyć sieć stacji meteorologicznych, najprawdopodobniej wraz z innymi dodatkowymi tablicami zmiennej treści, które będą musiały być instalowane zgodnie z warunkami umownymi. Brane jest pod uwagę odpowiednio 10 i 10 sztuk obydwóch urządzeń. BW 0,05 dla

każdego urządzenia jest wystarczająca, a nawet zawyżona. W tym podsystemie zostałaby założona BW 1MB.

- Zarządzanie i kontrola obsługi technicznej: Najczęściej jest zależne od umiejscowienia urządzeń oraz nadzoru postępu zadanych im prac. Komunikacja z tymi urządzeniami przebiega za pomocą GPRS i nie wpływa na obliczenia dotyczące sieci.

- Rozpoznawanie pojazdów stanowiących zagrożenie wraz z pomiarem dynamicznym. Przyjmuje się że jest 10 centrów kontroli, przez które przejeżdża 1000 kontrolowanych dziennie pojazdów, zakłada się że konieczne będzie przesłanie ich zdjęć w dobrej rozdzielczości, o wielkości 0,5 Mb. System zakłada szerokość pasma przesyłu o wartości:

BW = (10 * 1000 * 0,5)/(24*3600) = 0,012 Mb.

- Dostęp do parkingów na terenie Starego Miasta: System jest projektowany w formie serii urządzeń kontroli dostępów, najprawdopodobniej wraz z innymi dodatkowymi tablicami zmiennej treści, które będą musiały być instalowane zgodnie z warunkami umownymi. Brane jest pod uwagę odpowiednio 10 i 10 sztuk obydwóch urządzeń. BW 0,05 dla każdego urządzenia jest wystarczająca, a nawet zawyżona. W tym podsystemie zostałaby założona BW 1MB.

6.- TESTY SYSTEMU

6.1.- CELE

Integralność i poprawne działanie systemu zostanie sprawdzone za pomocą serii testów i badań opisanych niżej w tym dokumencie. Podczas tych czynności, zostaną sprawdzone i przetestowane wszystkie elementy systemu, zarówno fizyczne, takie jak okablowanie, jak i logiczne, czyli zdublowanie pierścieni, trasowanie, wirtualne sieci, itd.

Niniejszy dokument zawiera opis testów, które zostaną wykonane.

6.2.- Sprawdzenie Środowiska

Na początek, wykonamy pewne czynności i testy zwane Reflektometrią, potwierdzające, że przewód optyczny oraz instalacja spełniają minimalne wymagania w zakresie łączności i standardów przemysłowych. Montaż światłowodu jest skomplikowany i trudny, jednak techniki weryfikacji oraz kryteria montażu są wyraźnie i dostatecznie wyszczególnione

oraz znormalizowane, a same czynności sprawdzające opierają się na urządzeniach zaawansowanych technologicznie.

Światłowód ma wiele zalet w zakresie przekazu danych na duże odległości, w porównaniu do przewodów miedzianych, ale również przedstawia pewne niedogodności, związane przede wszystkim z jego delikatną strukturą i trudnościami podczas łączenia przewodów szklanych o średnicy nie większej niż 62, 5 μm.

Metody weryfikacji zgodności instalacji z określonymi normami są różnorodne i zależą od rodzaju instalacji.

6.2.1 Pomiar długości optycznej

Precyzyjny pomiar przewodu opiera się na współczynniku refrakcji zamontowanego światłowodu. Pomiar powinien być wykonany za pomocą OTDR, urządzenia odpowiednio wykalibrowanego i opatrzonego certyfikatem producenta lub upoważnionego dystrybutora, a uzyskane wartości pomiaru połączeń fuzyjnych nie mogą przekraczać średniej 0, 115 db dla połączeń dwukierunkowych oraz 0, 5 db dla złączenia zamontowanego na testowanym odcinku światłowodu.

Teoretyczne wartość utraty mocy na Km odcinka wynosi 0, 38 dla światłowodu w drugim ekranie (1310nm) i 0, 25 db dla światłowodu mierzonego w trzecim ekranie (1550 nm).
Pomiar należy wykonać z jak najlepszą rozdzielczością, to znaczy, wartość musi być jak najmniejsza dla określonej odległości i szerokości impulsu.

6.2.1.1 Testy szczelności skrzynek połączeniowych

Testy oparte na kontroli wzrokowej skrzynki i stwierdzeniu braku nieszczelności.

6.2.1.2 Norma jakości dla akceptacji połączeń

Niżej podane normy jakości stosowane są do akceptacji poszczególnych sekcji światłowodowych sieci miejskich, przy czym, sekcją określamy odcinek światłowodu znajdującego się między dwoma końcami dystrybutora światłowodu. Pauza akceptacji powinna być zachowana dla każdego światłowodu na poziomie sekcji.

Ustala się:

- Dla poszczególnych odcinków światłowodu zostaną zastosowane następujące normy jakości, w celu akceptacji średniego osłabienia sygnału na każdym łączeniu, które nie może przekraczać wartości 0, 10 db. Maksymalna wartość osłabienia sygnału na złączeniu może wynosić 0, 15 db, jeżeli przekroczy tą wartość, łączenie należy wykonać ponownie. W przypadku, gdy wartość osłabienia sygnału na łączeniu nie ulegnie zmniejszeniu po trzykrotnym

poprawieniu złączenia, zostanie przyjęta wartość uzyskana przy czwartym połączeniu.

- Większość pomiarów osłabienia sygnału powinna być wykonana przy długości fali 1310 nm, dokonując pomiaru w obu kierunkach, a maksymalną wartością utraty powinna być średnia uzyskana z obu pomiarów. Mimo tego, organ nadzorujący może wymagać dokonania pomiarów przy innych długościach fali.
- Podczas wykonywania pomiarów należy realizować protokół testowy połączeń oraz testy po ułożeniu światłowodu, załączone do niniejszego dokumentu, ponadto, dokumenty należy załączyć do certyfikatu jakości połączenia i okablowania.
- Jednostka miary i płatności za przetestowany światłowód obejmuje przygotowanie przewodu do badania, narzędzia, sprzęt i prace niezbędne do wykonania testów i przygotowania protokołu i raportów testowych, które zostaną przekazane w formacie drukowanym i elektronicznym.

6.2.1.3 Norma jakości do akceptacji przyłączeń

6.2.1.3.1 Pomiar osłabienia sygnału

Dla celów wdrożeniowych, określa się dwie konfiguracje zależne od zastosowania kabla przyłączeniowego do zakończenia w budynku lub wykonywane jest przyłączenie bezpośredni przewodu zewnętrznego do dystrybutora światłowodu.

6.2.1.3.2 Norma jakości dla akceptacji

Dostęp do budynku za pomocą przewodów przyłączeniowych i przewodu zewnętrznego: w tej konfiguracji, przyłączeniem na poziomie dystrybutora światłowodu do zestawu przerywników utraty, złożonego z utraty złącznika oraz połączenia pig tail (przewód przyłączeniowy) oraz połączenia przewodu przyłączeniowego (przewód zewnętrzny). Całkowita utrata pomiarów wykonanych w obu kierunkach, przy długości fali 1310 i 1550 nm, nie może przekraczać wcześniej ustalonych i podanych wartości.
Do pomiaru należy wykorzystać dwa zwoje światłowodu o długości nie mniejszej niż 1000 m, a każdy zwój będzie zawierał światłowód tej samej technologii, co zastosowany do odcinków pig tail.
Aby dokonać pomiaru, jeden koniec zwoju powinien być wstępnie podłączony do tego samego złącznika stosowanego na poziomie dystrybutora światłowodu.
Pomiar odbicia
Wartości utraty zwrotnej zmierzone na każdym zakończeniu światłowodu, na poziomie każdego dystrybutora światłowodu, powinny być zgodne z następującą normą akceptacji:

- 70% wartości zmierzonych > 40 db. (większy)
- 30% wartości zmierzonych < 38 db. (mniejszy)

6.2.1.3.3 Pomiar utraty całkowitej na odcinku przy określonej mocy optycznej

Całkowita utrata dla każdej sekcji (A) światłowodu powinna dostosować się do następującego równania:

A<a*L+En*ae+Nc*ac

Gdzie:

- ‘A’ = Całkowita utrata na odcinku (dB)
- ‘a’ = Nominalne osłabienie sygnału światłowodu dla określonej długości fali; (dB/km)
- ‘L’ = Całkowita długość optyczna odcinka; (Km)
- ‘En’ = całkowita ilość połączeń. Przyłączenia oraz połączenia pig tail nie będą brane pod uwagę, jeżeli istnieją.
- ‘ae’ = średnia wartość osłabienia na połączenie, (dB)
- ‘Nc’ = Liczba złączników.
- ‘ac’= utrata podłączenia na poziomie dystrybutora (dB)

W celach przeliczeniowych należy zastosować następujące wartości:

- ‘a’ = 0.25 dB/km dla 1550 nm i 0.38 dB/km dla 1310 nm. Światłowód mono w trybie standardowym

Te wartości osłabienia sygnału powinny być brane pod uwagę, jeżeli odpowiadają pomiarom wykonanym na przewodzie przed jego zainstalowaniem.

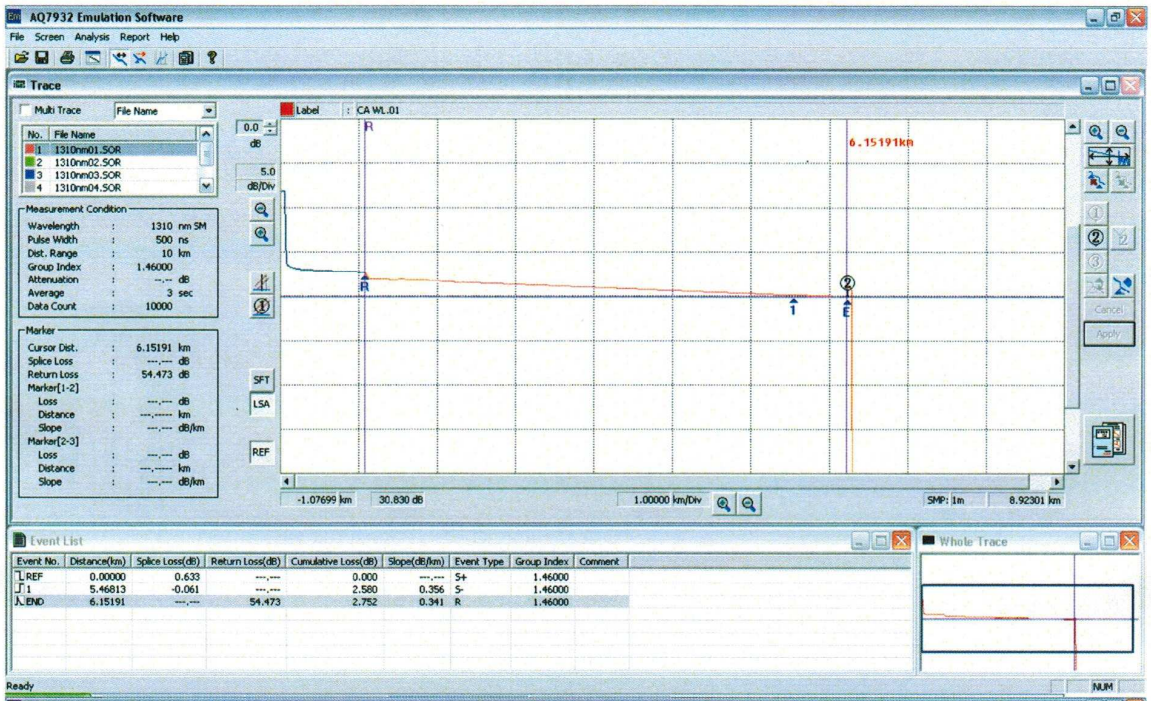
- ‘L’ = długość optyczna. Do pomiaru długości optycznej odcinka, należy dokładnie stosować współczynnik refrakcji odpowiedni dla zainstalowanego światłowodu.
- ‘ac’ = 0.25 dB dla złącznika LC; SC, ST, FC.

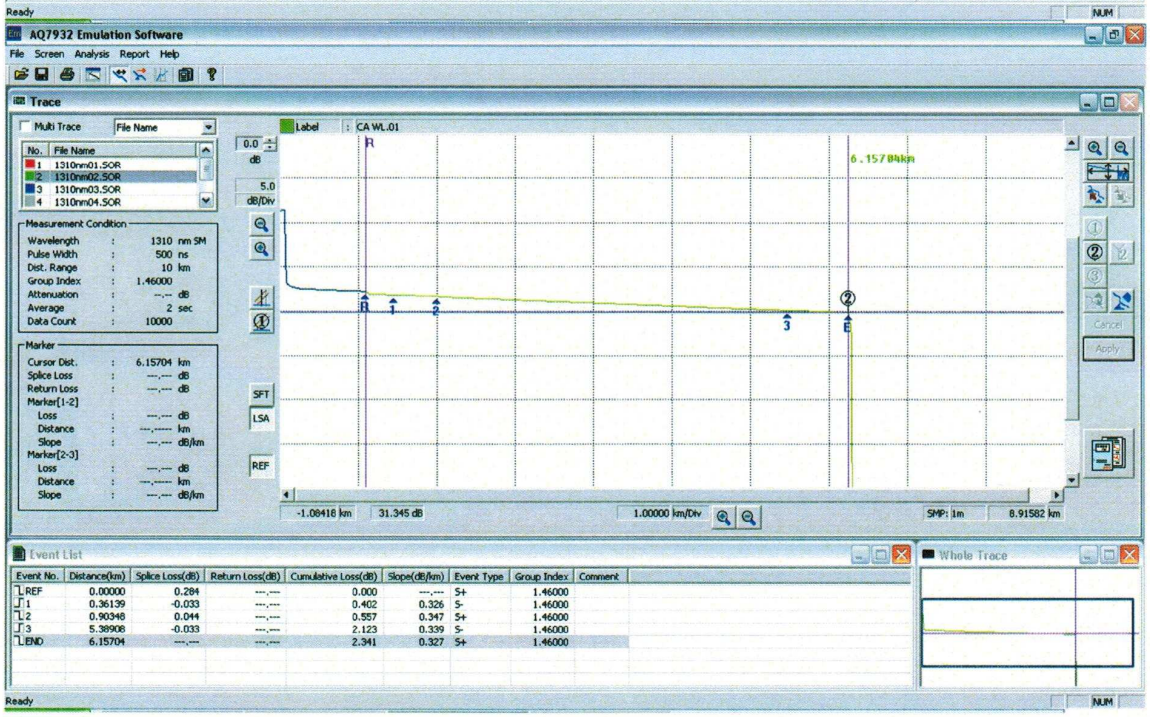
Mając na uwadze możliwość, że interfejs fizyczny instrumentu pomiarowego może być nie kompatybilny z zastosowanymi złącznikami na poziomie dystrybutora światłowodu, do pomiaru mocy należy zastosować następującą procedurę kalibracji, wymagającą przystosowania nadajnika i odbiornika.

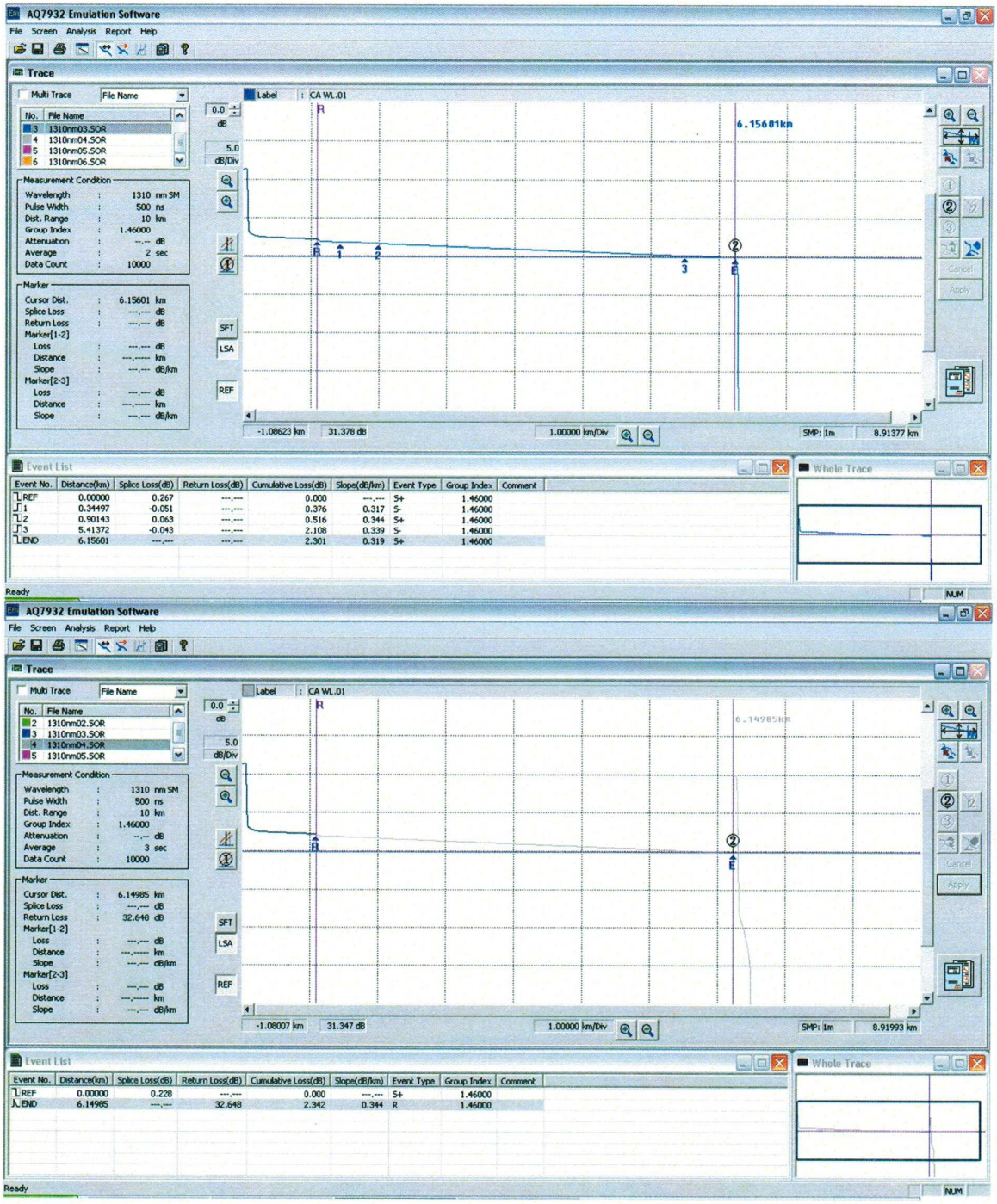
- Zmierzyć poziom mocy wyjściowej nadajnika, za pomocą przewody podłączonego zgodnie z interfejsem fizycznym instrumentu,
- Zmierzyć utratę wejściową przy odpowiednim zestawie przełączników do podłączenia 2 przewodów adaptacyjnych
- Utrata właściwa zostanie uzyskana z różnicy między pomiarami wykonanymi w powyższych przedmiotach, a wartość powinna być mniejsza niż 0, 4 db.
- Na podstawie powyższej konfiguracji, można wykonać kalibrację nadajnika i odbiornika.

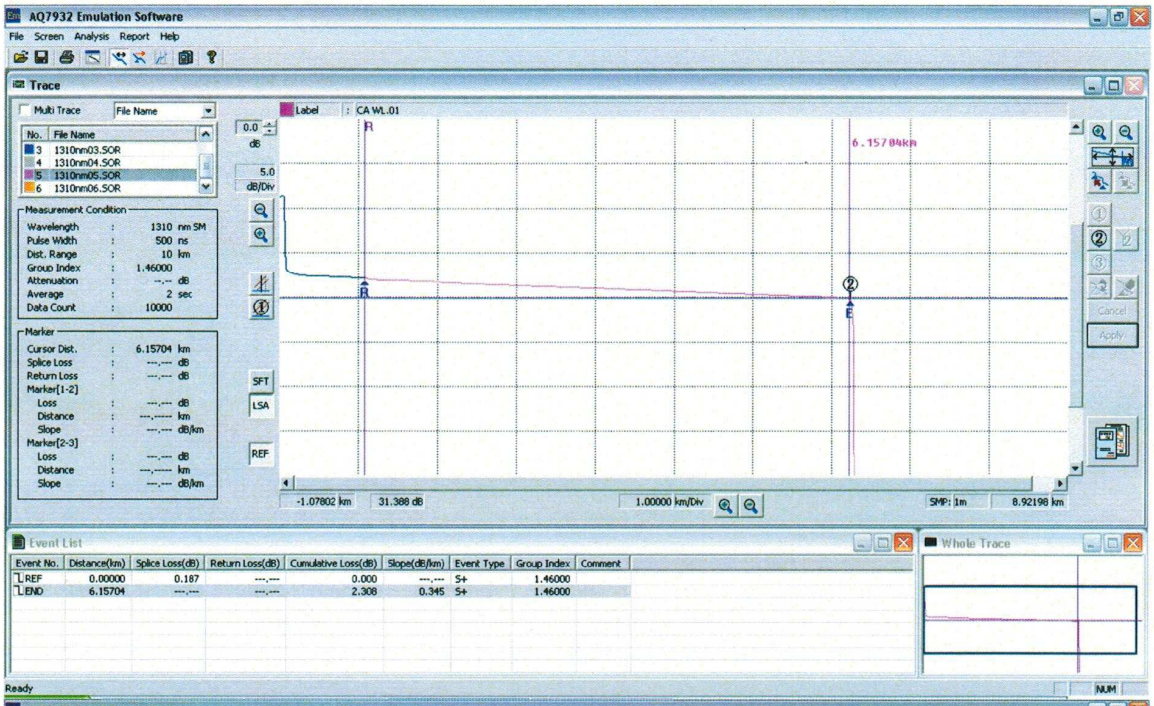
To urządzenie kalibracyjny wymaga zastosowani wartości ‘Nc’ = 1 podczas obliczania całkowitej utraty na odcinku.
Jeżeli urządzenie pomiarowe posiada interfejs kompatybilny ze złącznikami zastosowanymi na poziomie dystrybutora światłowodu, kalibracja zostanie wykonana bezpośrednio między nadajnikiem a odbiornikiem, bez stosowania przewodów adaptacyjnych.
Przejście pośrednie należy wykonywać za pomocą odłączenia przewodu referencyjnego na poziomie odbiornika. Aby wykonać pomiar, należy zastosować przewód przyłączeniowy między odbiornikiem a dystrybutorem światłowodu.
Ten rodzaj kalibracji wymaga zastosowania wartości ‘Nc’ = 2 przy obliczaniu wartości utraty całkowitej na odcinku. Pomiar będzie wykonywany przy długości fali 1550 nm oraz 1310 nm.
Absolutna wartość utraty będzie uzyskana jako średnia 3 pomiarów dokonanych po 3 procesach odłączenia - podłączenia.

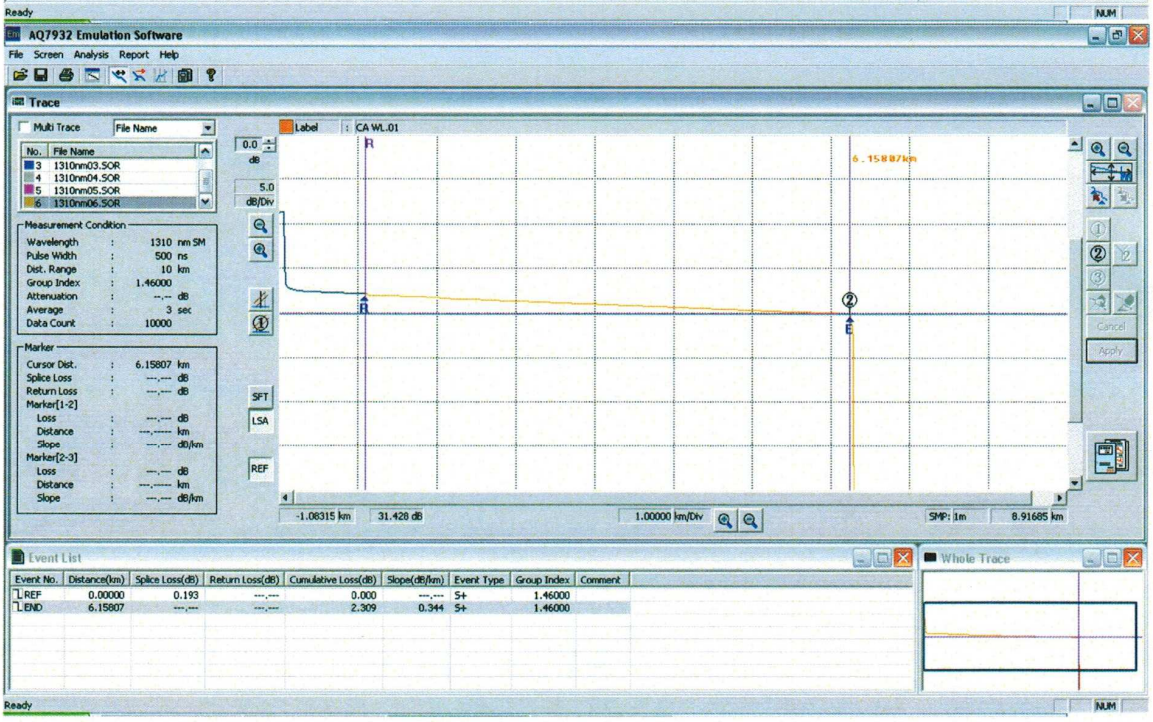
Zrzuty ekrany podczas reflektometrii:





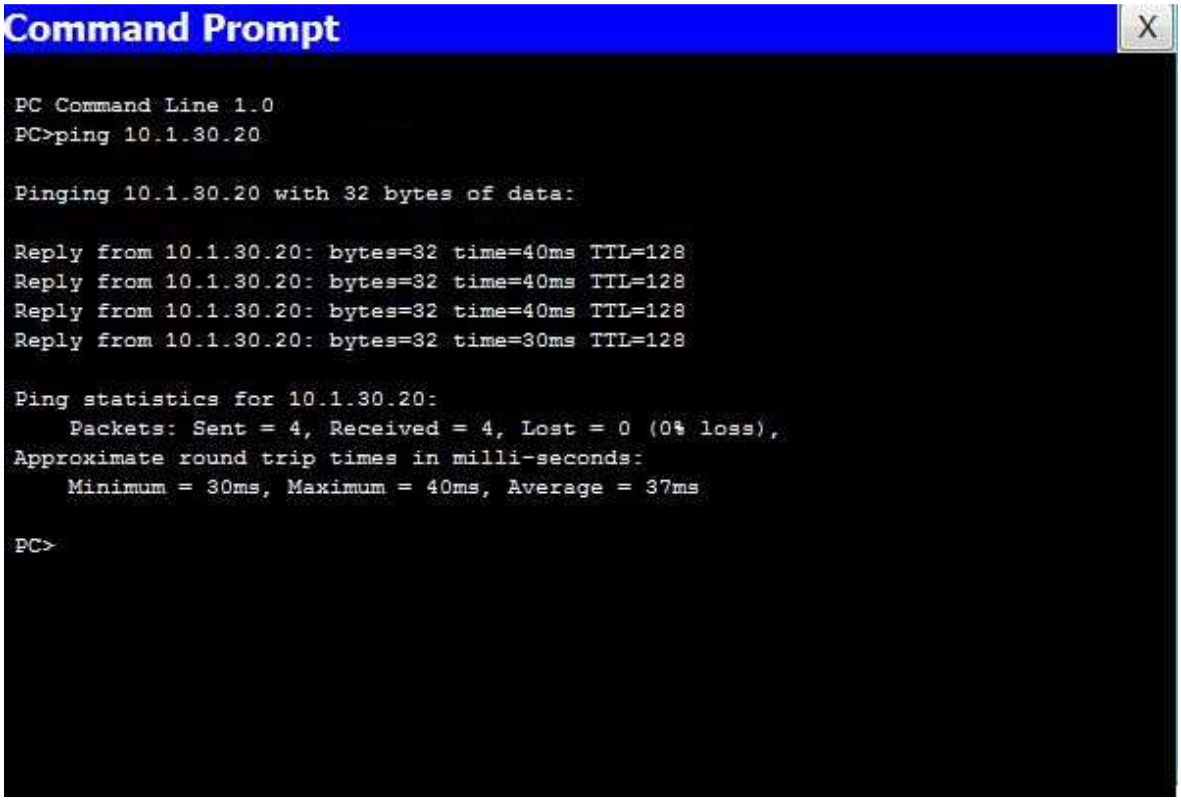

AQ7932 Emulation Software
File Screen Analysis Report Help
Trace
Multi Trace
File Name
No. File Name
3 1310nm03.SOR
4 1310nm04.SOR
5 1310nm05.SOR
6 1310nm06.SOR
Measurement Condition
Wavelength : 1310 nm SM
Pulse Width : 500 ns
Dist. Range : 10 km
Group Index : 1.46000
Attenuation : --.-- dB
Average : 2 sec
Data Count : 10000
Marker
Cursor Dist. : 6.15601 km
Splice Loss : ---.--- dB
Return Loss : ---.--- dB
Marker[1-2]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Marker[2-3]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Label : CA WL.01
6.15601km
SFT
LSA
REF
-1.08623 km
31.378 dB
1.00000 km/Div
SMP: 1m
8.91377 km
Event List
Event No. Distance(km) Splice Loss(dB) Return Loss(dB) Cumulative Loss(dB) Slope(dB/km) Event Type Group Index Comment
REF 0.00000 0.267 ---.--- 0.000 ---.--- S+ 1.46000
1 0.34497 -0.051 ---.--- 0.376 0.317 S- 1.46000
2 0.90143 0.063 ---.--- 0.516 0.344 S+ 1.46000
3 5.41372 -0.043 ---.--- 2.108 0.339 S- 1.46000
END 6.15601 ---.--- ---.--- 2.301 0.319 S+ 1.46000
Whole Trace
Ready
NUM
AQ7932 Emulation Software
File Screen Analysis Report Help
Trace
Multi Trace
File Name
No. File Name
2 1310nm02.SOR
3 1310nm03.SOR
4 1310nm04.SOR
5 1310nm05.SOR
Measurement Condition
Wavelength : 1310 nm SM
Pulse Width : 500 ns
Dist. Range : 10 km
Group Index : 1.46000
Attenuation : --.-- dB
Average : 3 sec
Data Count : 10000
Marker
Cursor Dist. : 6.14985 km
Splice Loss : ---.--- dB
Return Loss : 32.648 dB
Marker[1-2]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Marker[2-3]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Label : CA WL.01
6.14985km
SFT
LSA
REF
-1.08007 km
31.347 dB
1.00000 km/Div
SMP: 1m
8.91993 km
Event List
Event No. Distance(km) Splice Loss(dB) Return Loss(dB) Cumulative Loss(dB) Slope(dB/km) Event Type Group Index Comment
REF 0.00000 0.228 ---.--- 0.000 ---.--- S+ 1.46000
END 6.14985 ---.--- 32.648 2.342 0.344 R 1.46000
Whole Trace
Ready
NUM


AQ7932 Emulation Software
File Screen Analysis Report Help
Trace
Multi Trace
File Name
No. File Name
3 1310nm03.SOR
4 1310nm04.SOR
5 1310nm05.SOR
6 1310nm06.SOR
Measurement Condition
Wavelength : 1310 nm SM
Pulse Width : 500 ns
Dist. Range : 10 km
Group Index : 1.46000
Attenuation : --.-- dB
Average : 2 sec
Data Count : 10000
Marker
Cursor Dist. : 6.15704 km
Splice Loss : ---.--- dB
Return Loss : ---.--- dB
Marker[1-2]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Marker[2-3]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Label : CA WL.01
6.15704km
SFT
LSA
REF
-1.07802 km
31.388 dB
1.00000 km/Div
SMP: 1m
8.92198 km
Event List
Event No. Distance(km) Splice Loss(dB) Return Loss(dB) Cumulative Loss(dB) Slope(dB/km) Event Type Group Index Comment
REF 0.00000 0.187 ---.--- 0.000 ---.--- S+ 1.46000
END 6.15704 ---.--- ---.--- 2.308 0.345 S+ 1.46000
Whole Trace
Ready
NUM


AQ7932 Emulation Software
File Screen Analysis Report Help
Trace
Multi Trace
File Name
No. File Name
3 1310nm03.SOR
4 1310nm04.SOR
5 1310nm05.SOR
6 1310nm06.SOR
Measurement Condition
Wavelength : 1310 nm SM
Pulse Width : 500 ns
Dist. Range : 10 km
Group Index : 1.46000
Attenuation : --.-- dB
Average : 3 sec
Data Count : 10000
Marker
Cursor Dist. : 6.15807 km
Splice Loss : ---.--- dB
Return Loss : ---.--- dB
Marker[1-2]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Marker[2-3]
Loss : ---.--- dB
Distance : ---.----- km
Slope : ---.--- dB/km
Label : CA WL.01
6.15807km
SFT
LSA
REF
-1.08315 km
31.428 dB
1.00000 km/Div
SMP: 1m
8.91685 km
Event List
Event No. Distance(km) Splice Loss(dB) Return Loss(dB) Cumulative Loss(dB) Slope(dB/km) Event Type Group Index Comment
REF 0.00000 0.193 ---.--- 0.000 ---.--- S+ 1.46000
END 6.15807 ---.--- ---.--- 2.309 0.344 S+ 1.46000
Whole Trace
Ready
NUM

6.3.- Sprawdzenie topologii.

Do wykonania tego i pozostałych testów, skorzystamy z bardzo znanej aplikacji zwanej PING (Packet Internet Groper).
Ping jest narzędziem diagnostycznym siedzi komputerowych, które sprawdza stan podłączenia lokalnego hosta do jednego lub więcej urządzeń zdalnych sieci TCP/IP za pomocą przesyłania pakietów ICMP nadawczych i odbiorczych. Narzędzie umożliwia przeprowadzenie diagnostyki stanu, prędkości i jakości określonej sicie.
Wykonując Ping nadawczy, lokalny Host przesyła wiadomość ICMP zamieszczoną w pakiecie IP. Wiadomość nadawcza ICMP zawiera rodzaj i kod wiadomości, numer identyfikacyjny i sekwencję numerów, 32 bitową, która powinna być zgodna z wiadomością odbiorczą ICMP, ponadto, opcjonalnie zawiera miejsce na dane.
Niejednokrotnie, aplikacja jest stosowana do pomiaru latencji lub czasu opóźnienia w połączeniu dwóch odległych od siebie punktów sieci, z tego powodu termin PING stosowany jest do określenia laga lub opóźnienia połączenia w grach sieciowych. Aby sprawdzić działania topologii oraz wszystkich przekaźników, wykonany komendę ping z przełącznika switch skonfigurowanego jako Ring Manager do każdego przekaźnika pierścienia.



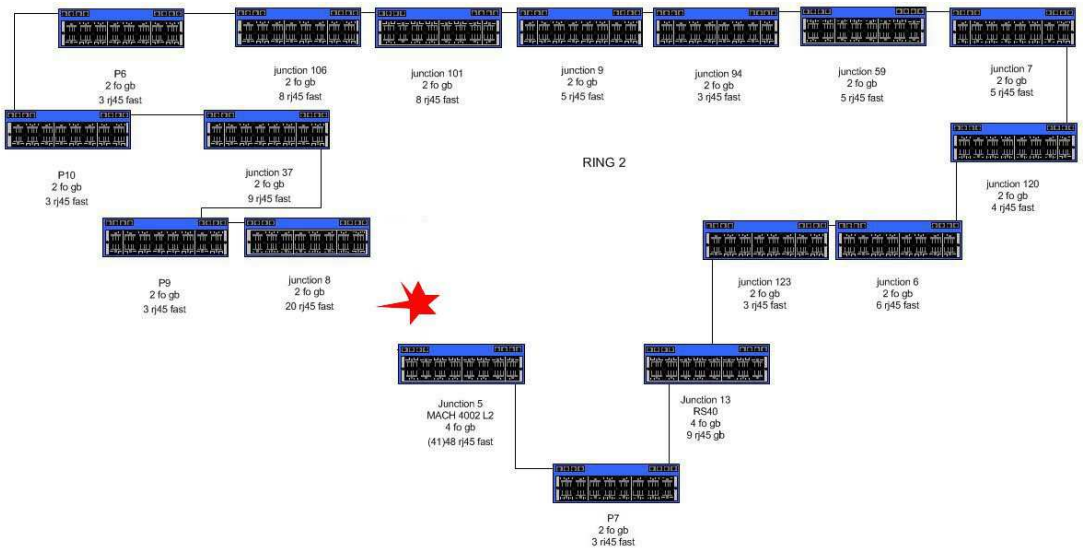
Jeżeli w każdym przypadku, komenda ping otrzyma odpowiedź od docelowego hosta, oznacza to, że między hostami jest łączność i możemy potwierdzić integralność struktury pierścienia.

```
Reply from 10.1.30.20: bytes=32 time=40ms TTL=128
Reply from 10.1.30.20: bytes=32 time=40ms TTL=128
Reply from 10.1.30.20: bytes=32 time=40ms TTL=128
Reply from 10.1.30.20: bytes=32 time=30ms TTL=128
```

Następujący krok polega na sprawdzeniu, czy integralność pierścienia jest zachowana pomimo przerwania połączenia (fizycznego lub logicznego) na jednym złączu. W tym celu, ponownie wykonamy komendę ping.

Czynności:

1. Wyłączyć jeden port lub odłączyć światłowód w porcie switch

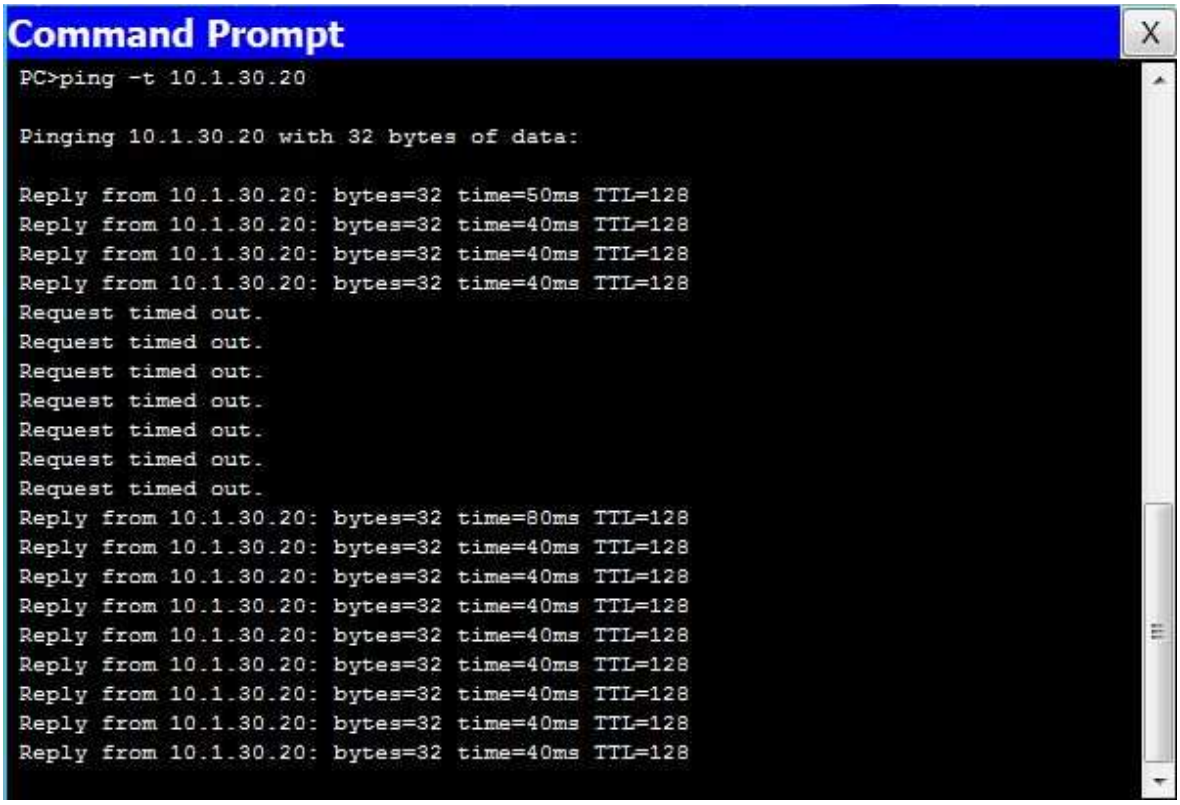


2. Wykonać komendę ping do pozostałych przekaźników sieci.
3. Sprawdzić poprawność odpowiedzi ping, jeżeli tak nie jest, sprawdzić konfigurację pierścienia i skorygować problem. Jeżeli odpowiedź jest poprawna, kontynuować test.
4. Wyłączyć kolejny port switch, odłączając światłowód łączący go z pierścieniem.
5. Zweryfikować, czy odpowiedź ping jest poprawna, jeżeli nie jest, sprawdzić konfigurację pierścienia i poprawić.
6. Wykonać ten proces dla każdego przekaźnika wchodzącego w skład każdego pierścienia, aby zagwarantować poprawne działanie zdublowanego systemu.

Po zagwarantowaniu poprawnego działania pierścienia, pozostaje sprawdzić czas zbieżności sieci, czyli czas wykrywania przez switch zerwanego połączenia i uruchomienia połączenia backup.
Test należy wykonać za pomocą narzędzi dostarczonych przez producenta urządzeń lub ponownie skorzystać z komendy ping.
Weryfikacja z pomocą komendy ping wykonywana jest podobnie od procesu kontroli zdublowania pierścienia, ale z pewnymi zmianami, które zostaną opisane poniżej.

Czynności:

1. Wykonać ping zwrotny do jednego z przełączników podłączonych bezpośrednio do switch z komputera podłączonego do tego samego przekaźnika.
2. Podczas kontroli ping zwrotnego, wyłączyć port sieciowy, do którego jest podłączonych bezpośrednio switch, do którego wysłaliśmy ping.
3. Po wyłączeniu portu, komenda ping spowoduje powrót kilku błędnych odpowiedzi, do czasu uruchomienia backup.

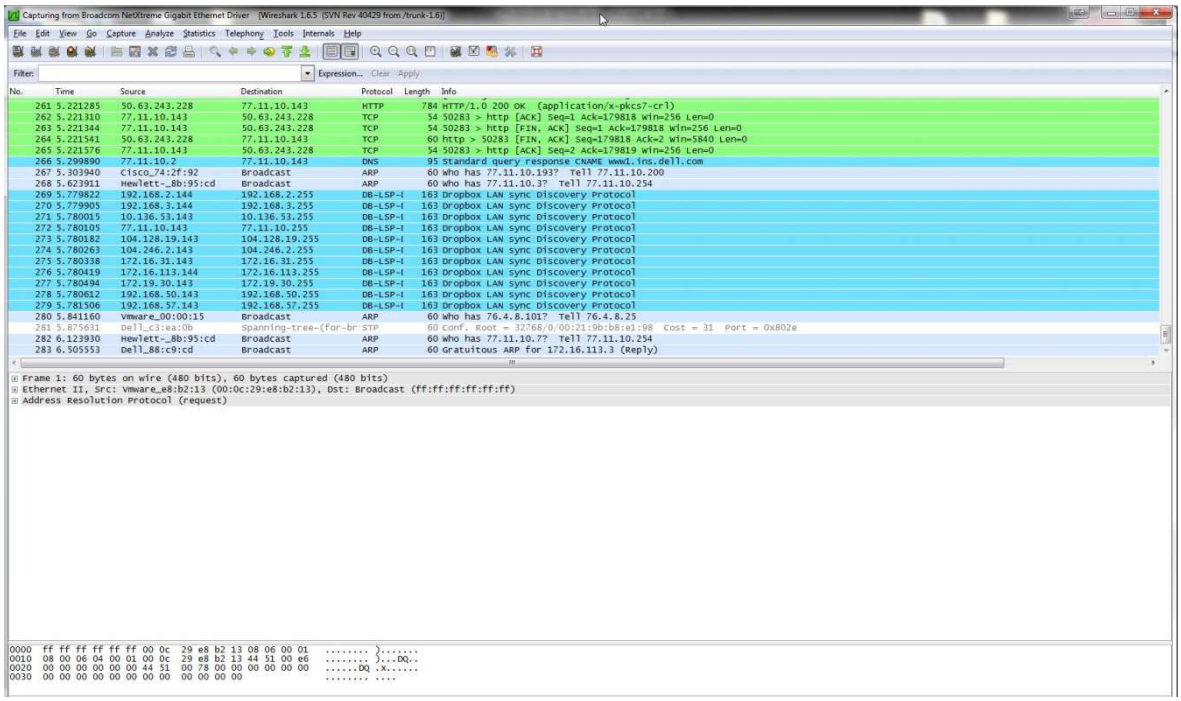


4. Po uruchomieniu backup, ping powróci do poprawnych wyników i sprawdzimy, czy czas skonfigurowany czas zbieżności zgadza się z rzeczywistym. Jeżeli tak nie jest, należy sprawdzić konfigurację dublowania wszystkich przekaźników, aby poprawić błąd.

6.4.- Weryfikacja VLAN's

Sprawdzenie poprawnego działania vlan wykonywane jest za pomocą następujących testów:
Podłączyć komputer do portu przypisanego dla vlan y wykonać komendę ping w kierunku każdego podłączonego IP należącego do tego vlan. Jeżeli odpowiedź jest poprawna przechodzimy do następnego testu, w przeciwnym razie, sprawdzamy, czy urządzenie końcowe zostały podłączone do odpowiednich portów. Jeżeli tak, sprawdzamy konfigurację VLAN wszystkich przekaźników i poprawiamy konfigurację.

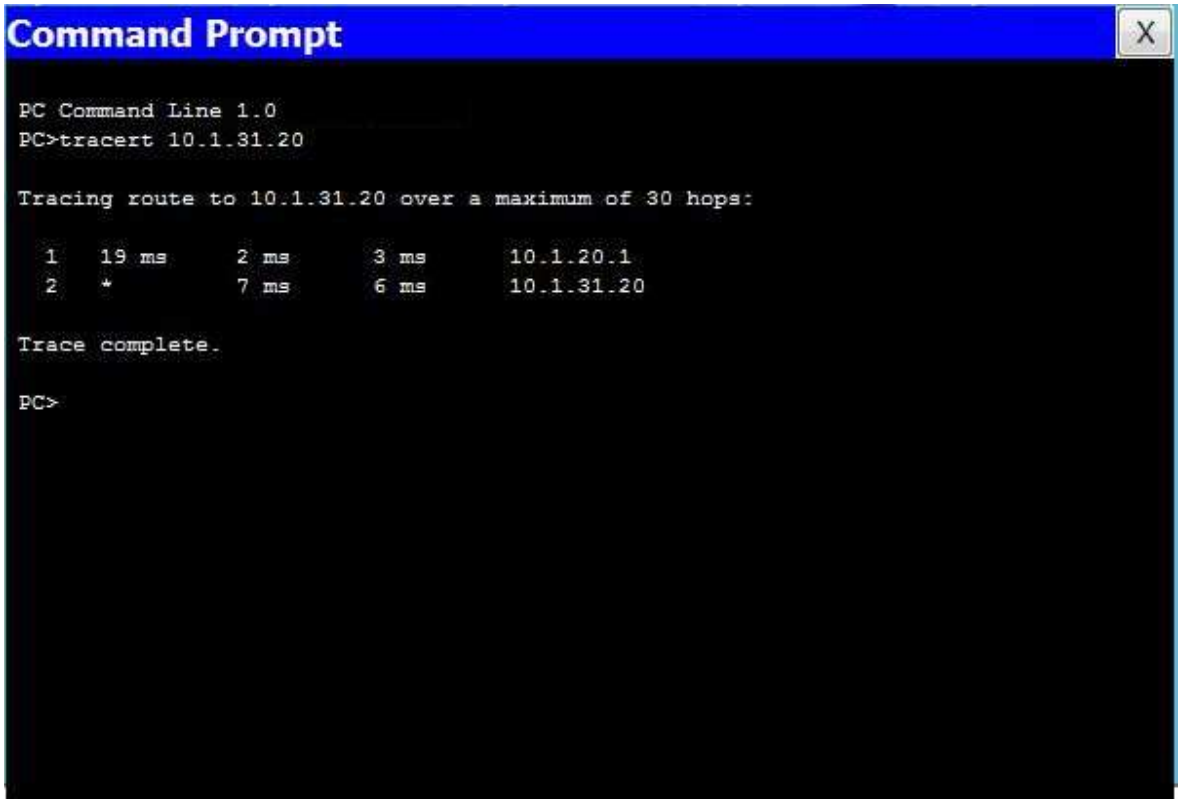
Po sprawdzeniu poprawnego podłączenie urządzeń końcowych w vlan, należy sprawdzić całkowitą integralność sieci wirtualnej, to znaczy, stwierdzamy brak nakładania się vlan (przez vlan przechodzi tylko informacja dla niego przeznaczona). W tym celu, skorzystamy z programu sniffer (program do wychwytywania odcinków sieci) zwanego WireShark.
Podłączyć komputer do portu vlan i za pomocą WireShark wychwycić odcinki, a następnie skontrolować przepływ danych dla tej sieci wirtualnej.



Do tego momentu, będzie możliwe skontrolowania całego przepływu danych przechodzących przez VLAN. Aby przyśpieszyć proces testowania, wykonać komendę ping zwrotnego między urządzeniami tego samego vlan, ale innego niż kontrolujemy w danym momencie (wykonać ping dla każdego vlan skonfigurowanego w sieci) i sprawdzić snifferem brak pakietów nieodpowiadających dla danego vlan.
Jeżeli WireShrek potwierdzi brak pakietów pochodzących z innych vlan, można stwierdzić, że sieć wirtualna działa poprawnie, w przeciwnym razie, sprawdzić konfigurację i rozwiązać problem.

6.5.- Weryfikacja Gateways

Aby sprawdzić, czy urządzenia końcowe, kamery, panele, regulatory, itd. wychodzą przez poprawne drzwi połączeniowe, należy wykonać komendę traceroute. Komenda wskazuje trasę konkretnego urządzenia do celu.
Podłączyć komputer do vlan i wykonać komendę traceroute do urządzenia podłączonego do innego vlan (nieobjętego ograniczeniami z list dostępu). Jeżeli wynik jest poprawny, pojawi się ilość skoków wykonanych do urządzenia docelowego, w tym przypadku 2 (drzwi połączeniowe oraz ip docelowe). W przeciwnym razie sprawdzić konfigurację urządzeń końcowych, a jeżeli są one poprawnie podłączone, sprawdzić konfigurację routerów.



6.6.- Sprawdzenie VRRP (Zdublowanie routerów)

Aby sprawdzić poprawne działanie systemu awaryjnego z VRRP, wykonać następujące czynności:
1. Wykonać ping do określonych drzwi połączeniowych, następnie wykonać ping do routera głównego i następny do router podporządkowanego, aby sprawdzić, czy wszystkie trzy są aktywne i połączone między sobą.
2. Następnie wykonać tracert do IP urządzenia podłączonego do innego vlan sieci, aby sprawdzić, przez jaki router przechodzi w danym momencie.
3. Wykonać 3 pingi zwrotne, dwa do IP routerów (głównego i podporządkowanego) i jeden do IP urządzenia innego vlan sieci.
4. Podczas wykonywania pingów, wyłączyć lub odłączyć router, przez który wychodzą komendy.
5. W okienku ping do routera, z którego wychodzi komenda, pojawią się błędy, a w okienku drugiego routera odpowiedź ping będzie nadal poprawna, w trzecim ping do urządzenia innego vlan, pojawią się pewne problemy ping, ale później ping zostanie odzyskany.
6. Wykonując nadal pingi zwrotne, wykonać komendę tracert, jak już opisano powyżej, uzyskując inne ip niż podane w pierwszym tracert, ponieważ jest aktywny inny router.
7. Pozostaje tylko przywrócić system do stanu początkowego, podłączając/włączając wcześniej odłączony/wyłączony router, stale kontrolując 3 pingi wykonane w punkcie 3. Zauważymy, że ping w podłączonym routerze zostaje przywrócony i pojawia się poprawna odpowiedź, natomiast ping podporządkowany utrzymuje bezbłędne połączenia, a trzeci ping urywa się na chwilę i ponownie działa poprawnie. Ta krótka chwila wskaże nam, że główny router ponownie stanowi główne drzwi połączeniowe.

7.- Architektura SW i Prezentacja

7.1.- CELE

Poprawne zarządzanie sieci łączności wymaga zastosowania dobrego systemu kontroli usług host i sieciowych.

Te narzędzia pozwalają rozwinąć strategię zapobiegawczą w obliczu określonych problemów, w przeciwieństwie do innych systemów pozwalających wyłącznie na reakcję po zdarzeniu.

Zwalnia administratorów od wykonywania regularnych kontroli określonych usług o krytycznym znaczeniu. Alarmuje w obliczu sytuacji, które w innych okolicznościach pozostają niespostrzeżone. Zapełnienie twardych dysków, utrata usługi, itd. Z tego powodu, proponujemy narzędzie kontrolne.

Proponowane narzędzie Nagios, dysponuje licencją na podstawie warunków GNU. Poniżej opisujemy cechy każdego z nich.

7.2.- Dlaczego należy stosować Nagios?

Nagios jest szeroko stosowanym systemem o charakterze open source do kontroli sieci, nadzorujący określone urządzenia (hardware) y usługi (software), ostrzegając w przypadku niepożądanego zachowania dowolnego elementu.

7.3.- Nagios

7.3.1 Co to jest Nagios

Nagios® to aplikacja do monitorowania usług. Oprogramowanie czuwa nad wykorzystaniem zasobów na hostach, wysyła sygnał alarmowy w przypadku niewłaściwego działania oraz w przypadku naprawy usterki.
Nagios miał działać w systemie Linux, ale współpracuje również z innymi systemami.

7.3.2 Cechy

Funkcje aplikacji Nagios:

- Monitorowanie usług sieciowych (SMTP, POP3, HTTP, NNTP, PING, itd.)

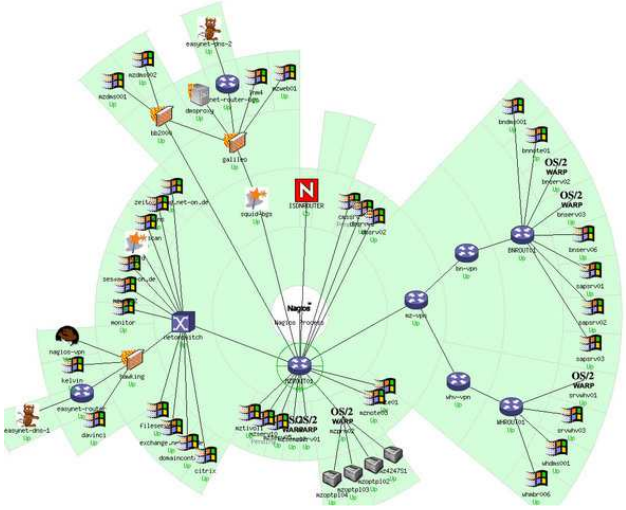
Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
AP-WIRELESE	PING	OK	2011-11-02 18:52:07	0d 21h 41m 20s	1/3	PING OK - Packet loss = 0%, RTA = 0.88 ms
BLOG-SERVER	HTTP	OK	2011-11-02 18:50:11	0d 4h 9m 27s	1/3	HTTP OK: HTTP/1.1 200 OK - 218664 bytes in 0,903 second response time
	MYSQL	OK	2011-11-02 18:52:31	0d 6h 57m 29s	1/3	Uptime: 25439 Threads: 1 Questions: 947 Slow queries: 0 Opens: 179 Flush tables: 1 Open tables: 43 Queries per second avg: 0,37
	PING	OK	2011-11-02 18:51:40	0d 21h 37m 35s	1/3	PING OK - Packet loss = 0%, RTA = 1.74 ms
	SSH	OK	2011-11-02 18:42:54	0d 21h 43m 10s	1/3	SSH OK - OpenSSH_5.5p1 Debian-6 (protocol 2.0)
LaFONERA	PING	OK	2011-11-02 18:52:04	0d 21h 40m 43s	1/3	PING OK - Packet loss = 0%, RTA = 2.70 ms
MAIL-SERVER	PING	OK	2011-11-02 18:51:37	0d 21h 36m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.90 ms
	POP3 Response Check	OK	2011-11-02 18:49:10	0d 18h 11m 54s	1/3	POP OK - 0,085 second response time on port 995 [+OK Qpopper (version 4.0.9) at SERVER-MAIL starting. <3030.1320255339@SERVER-MAIL>]
	SMTP Response Check	OK	2011-11-02 18:46:27	0d 19h 24m 32s	1/3	SMTP OK - 0,044 sec. response time
	SSH	OK	2011-11-02 18:49:34	0d 21h 41m 30s	1/3	SSH OK - OpenSSH_5.1p1 Debian-5 (protocol 2.0)
RTRobotics#1	DHCP	OK	2011-11-02 18:48:42	0d 11h 43m 47s	1/3	OK: Received 1 DHCPOFFER(s), 1 of 1 requested servers responded, max lease time = 86400 sec.
	PING	OK	2011-11-02 18:51:51	0d 21h 40m 5s	1/3	PING OK - Packet loss = 0%, RTA = 1.30 ms
WINDOWS7-ALEX	PING	OK	2011-11-02 18:47:07	0d 1h 55m 36s	1/3	PING OK - Packet loss = 0%, RTA = 2.76 ms
WINDOWS7-RUBEN	PING	CRITICAL	2011-11-02 18:46:12	0d 3h 16m 31s	1/3	CRITICAL - Host Unreachable (172.16.0.51)
WINDOWS7-XxX	PING	OK	2011-11-02 18:44:05	0d 21h 52m 4s	1/3	PING OK - Packet loss = 0%, RTA = 0.64 ms
WINDOWSXP-Portatil	PING	OK	2011-11-02 18:43:42	0d 21h 39m 34s	1/3	PING OK - Packet loss = 0%, RTA = 0.61 ms
nagios	HTTP	OK	2011-11-02 18:50:54	0d 3h 51m 49s	1/3	HTTP OK: HTTP/1.1 200 OK - 453 bytes in 0,002 second response time
	PING	OK	2011-11-02 18:51:48	0d 21h 36m 20s	1/3	PING OK - Packet loss = 0%, RTA = 0.06 ms
	SSH	OK	2011-11-02 18:50:45	0d 21h 47m 4s	1/3	SSH OK - OpenSSH_5.5p1 Debian-6+squeeze1 (protocol 2.0)

- Monitorowanie zasobów na hostach (obciążenie procesora, wykorzystanie dysku itd.)

WINDOWS7-XxX	ANTIVIRUS	OK	2011-11-04 17:37:11	0d 21h 21m 18s	1/3	msseces.exe: Running
	CPU LOAD	OK	2011-11-04 17:29:25	0d 21h 16m 19s	1/3	CPU Load 8% (5 min average)
	DRIVE SPACE C:	OK	2011-11-04 17:32:58	0d 21h 12m 51s	1/3	c: - total: 465,66 Gb - used: 228,31 Gb (49%) - free 237,35 Gb (51%)
	DRIVE SPACE D:	OK	2011-11-04 17:35:11	0d 21h 16m 7s	1/3	d: - total: 465,76 Gb - used: 270,81 Gb (58%) - free 194,95 Gb (42%)
	MEMORY USAGE	OK	2011-11-04 17:37:25	0d 21h 17m 57s	1/3	Memory usage: total:8188,37 Mb - used: 2137,82 Mb (26%) - free: 6050,55 Mb (74%)
	PING	OK	2011-11-04 17:29:38	2d 20h 37m 23s	1/3	PING OK - Packet loss = 0%, RTA = 1.31 ms
	UPTIME	OK	2011-11-04 17:33:11	0d 21h 18m 44s	1/3	System Uptime - 0 day(s) 20 hour(s) 48 minute(s)
WINDOWSXP-Portatil	ANTIVIRUS	OK	2011-11-04 17:35:25	0d 23h 24m 23s	1/3	msseces.exe: Running
	CPU LOAD	OK	2011-11-04 17:37:38	0d 23h 19m 21s	1/3	CPU Load 0% (5 min average)
	DRIVE SPACE C:	OK	2011-11-04 17:29:51	0d 21h 15m 16s	1/3	c: - total: 74,52 Gb - used: 27,91 Gb (37%) - free 46,61 Gb (63%)
	MEMORY USAGE	OK	2011-11-04 17:33:25	0d 23h 24m 4s	1/3	Memory usage: total:4440,87 Mb - used: 472,12 Mb (11%) - free: 3968,76 Mb (89%)
	PING	OK	2011-11-04 17:35:38	2d 20h 24m 53s	1/3	PING OK - Packet loss = 0%, RTA = 0.68 ms
	UPTIME	OK	2011-11-04 17:37:51	0d 23h 21m 33s	1/3	System Uptime - 1 day(s) 21 hour(s) 20 minute(s)

- Prosta wtyczka, która pozwala użytkownikom opracować własne testy
- Testy równoległe usług
- Możliwość definiowania hierarchii hostów za pomocą hostów macierzystych ‘parent’ pozwalające na wykrycie oraz wyróżnienie hostów, które są wyłączone i tych, które są nieosiągalne



- Powiadamianie w przypadku problemów z usługami i hostem oraz o ich naprawie (przez email, pager lub poprzez metodę zdefiniowaną przez użytkownika)

Contact Notifications
Last Updated: Sun Feb 1 12:07:59 NPT 2004
Nagios® - www.nagios.org
Logged in as *dhruba*

All Contacts

Latest Archive

Log File Navigation
Sun Feb 1 00:00:00 NPT 2004 to Present..

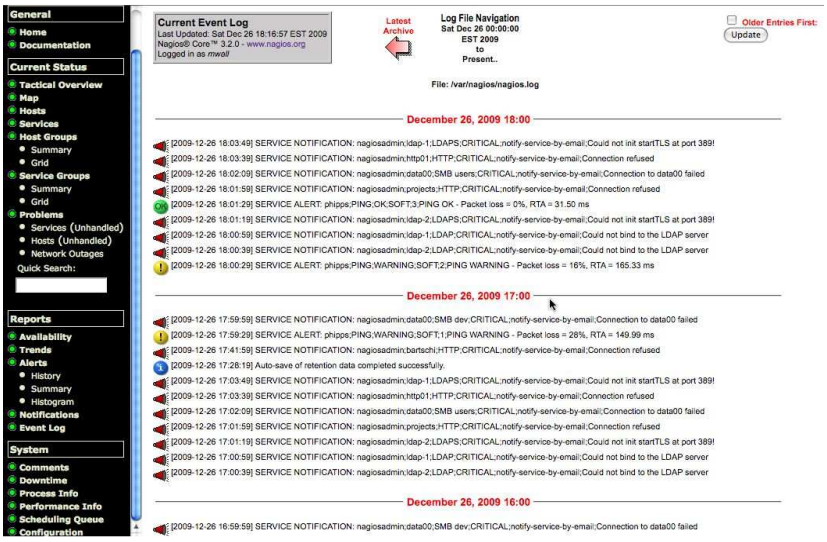
Notification detail level for all contacts: All notifications
Older Entries First:
Update

File: /usr/local/nagios/var/nagios.log

Host	Service	Type	Time	Contact	Notification Command	Information
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	NirajS	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Prabhu	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:10	Ravin	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:08	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Prabhu	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Hid-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Gyanu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Hid-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Ishwar	host-notify-by-email	PING CRITICAL - Packet loss = 100%

- Możliwość definiowania programów do obsługi zdarzeń, które pracują podczas uruchamiania usług lub hosta w przypadku rozwiązywania problemów

- Automatyczna rotacja pliku rejestratora



General
Home
Documentation

Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:

Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log

System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration

Current Event Log
Last Updated: Sat Dec 26 18:16:57 EST 2009
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as *mwal*

Latest Archive

Log File Navigation
Sat Dec 26 00:00:00 EST 2009 to Present..

Older Entries First:
Update

File: /var/nagios/nagios.log

December 26, 2009 18:00

[2009-12-26 18:03:49] SERVICE NOTIFICATION: nagiosadmin;ldap-1;LDAPS;CRITICAL;notify-service-by-email;Could not init startTLS at port 389!
[2009-12-26 18:03:39] SERVICE NOTIFICATION: nagiosadmin;http01;HTTP;CRITICAL;notify-service-by-email;Connection refused
[2009-12-26 18:02:09] SERVICE NOTIFICATION: nagiosadmin;data00;SMB users;CRITICAL;notify-service-by-email;Connection to data00 failed
[2009-12-26 18:01:59] SERVICE NOTIFICATION: nagiosadmin;projects;HTTP;CRITICAL;notify-service-by-email;Connection refused
[2009-12-26 18:01:29] SERVICE ALERT: phipps;PING;OK;SOFT;3;PING OK - Packet loss = 0%, RTA = 31.50 ms
[2009-12-26 18:01:19] SERVICE NOTIFICATION: nagiosadmin;ldap-2;LDAPS;CRITICAL;notify-service-by-email;Could not init startTLS at port 389!
[2009-12-26 18:00:59] SERVICE NOTIFICATION: nagiosadmin;ldap-1;LDAP;CRITICAL;notify-service-by-email;Could not bind to the LDAP server
[2009-12-26 18:00:39] SERVICE NOTIFICATION: nagiosadmin;ldap-2;LDAP;CRITICAL;notify-service-by-email;Could not bind to the LDAP server
[2009-12-26 18:00:29] SERVICE ALERT: phipps;PING;WARNING;SOFT;2;PING WARNING - Packet loss = 16%, RTA = 165.33 ms

December 26, 2009 17:00

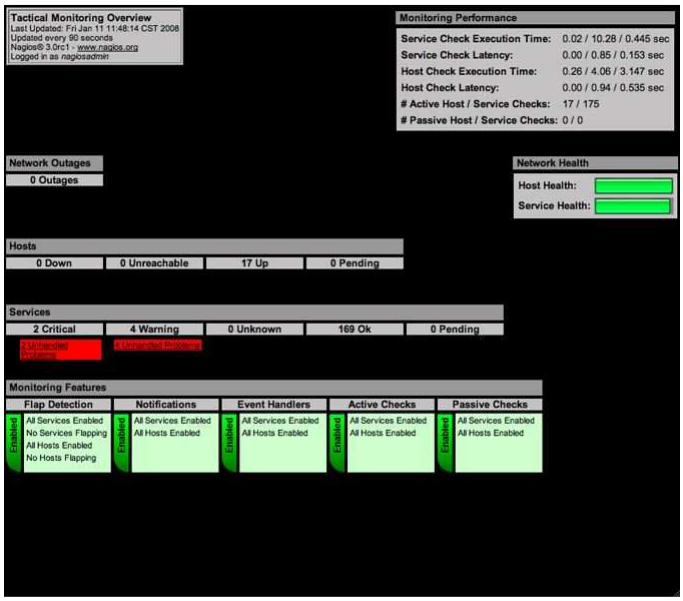
[2009-12-26 17:59:59] SERVICE NOTIFICATION: nagiosadmin;data00;SMB dev;CRITICAL;notify-service-by-email;Connection to data00 failed
[2009-12-26 17:59:29] SERVICE ALERT: phipps;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 28%, RTA = 149.99 ms
[2009-12-26 17:41:59] SERVICE NOTIFICATION: nagiosadmin;bartschi;HTTP;CRITICAL;notify-service-by-email;Connection refused
[2009-12-26 17:28:19] Auto-save of retention data completed successfully.
[2009-12-26 17:03:49] SERVICE NOTIFICATION: nagiosadmin;ldap-1;LDAPS;CRITICAL;notify-service-by-email;Could not init startTLS at port 389!
[2009-12-26 17:03:39] SERVICE NOTIFICATION: nagiosadmin;http01;HTTP;CRITICAL;notify-service-by-email;Connection refused
[2009-12-26 17:02:09] SERVICE NOTIFICATION: nagiosadmin;data00;SMB users;CRITICAL;notify-service-by-email;Connection to data00 failed
[2009-12-26 17:01:59] SERVICE NOTIFICATION: nagiosadmin;projects;HTTP;CRITICAL;notify-service-by-email;Connection refused
[2009-12-26 17:01:19] SERVICE NOTIFICATION: nagiosadmin;ldap-2;LDAPS;CRITICAL;notify-service-by-email;Could not init startTLS at port 389!
[2009-12-26 17:00:59] SERVICE NOTIFICATION: nagiosadmin;ldap-1;LDAP;CRITICAL;notify-service-by-email;Could not bind to the LDAP server
[2009-12-26 17:00:39] SERVICE NOTIFICATION: nagiosadmin;ldap-2;LDAP;CRITICAL;notify-service-by-email;Could not bind to the LDAP server

December 26, 2009 16:00

[2009-12-26 16:59:59] SERVICE NOTIFICATION: nagiosadmin;data00;SMB dev;CRITICAL;notify-service-by-email;Connection to data00 failed

- Obsługa opcji monitorowania hostów

- Opcjonalny interfejs sieciowy do wyświetlania bieżącego statusu sieci, powiadomień oraz historii wystąpienia problemu, dziennika, pliku, itd.



7.3.3 Nagios Core

7.3.3.1 Ogólnie

Nagios Core jest silnikiem monitorującym oraz powiadamiającym, stosowany jako podstawowa aplikacja, wokół której łączone są setki projektów Nagio. Aplikacja używana jest jako podstawowy program planujący zdarzenia, narzędzie do przetwarzania zdarzeń oraz manager alarmów dla monitorowanych elementów. Łączy kilka API, które stosowane są do rozszerzenia możliwości programu oraz wykonywania dodatkowych zadań, wdrażany jest jako deamon napisany w C, uruchamiany jest w systemie Linux/*nix.

7.3.3.2 Informacje o architekturze

Nagios Core zaprojektowano w architekturze warstwowej, która ma za zadanie zwiększyć jej elastyczność oraz skalowalność. Posiada kilka API, które pozwalają na łatwą rozbudowę aplikacji. Architektura jest wydajna i pozwala na tworzenie tysięcy dodatkowych projektów.

7.3.3.3 Zakres zastosowania

Nagios Core ma za zadanie planowanie testów, wykonanie testów, przetwarzanie testów, obsługę zdarzeń oraz alarmowanie. Przeprowadzanie testów, przesyłanie powiadomień, przetwarzanie danych oraz wiele innych zadań zwykle nie należy do podstawowych zadań Nagios Core, ale są obsługiwane przez inne projekty Nagio.

7.3.3.4 Frontends

Nagios Core dostarczała i wciąż dostarcza standardowego interfejsu CGI. CGI dostarcza użytkownikom aplikacje umożliwiające wyświetlanie i zarządzanie elementami, które są monitorowane przez Nagios Core. CGI stał się standardowym interfejsem w Nagios Core i często stosowany jest jako API przez wiele dodatkowych aplikacji Nagios. Wielu użytkowników rozmieszcza dodatkowe frontends w celu wykonania odpowiedniego wyglądu aplikacji i zapewnienia funkcjonalności Nagios UI. Nagios V-Shell to nowy frontends, który jest obecnie rozbudowywany jako oficjalny PHP frontend.

Nagios posiada wiele wydajnych Source frontends, które zostały opracowane przez społeczność Nagios.
Społeczność Nagios opracowała wiele frontend-ów dla Nagios Core, które są podzielone na kategorie jak Mobile Device Interface (który obsługuje iPhon-y, Android, Blackberries) interfejsy sieciowe, Windows oraz Linux.

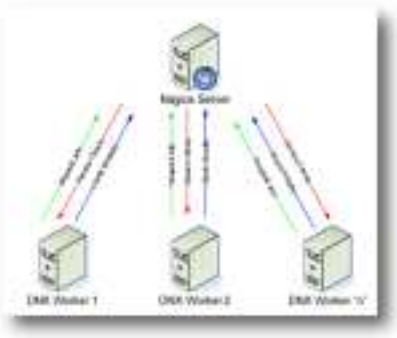
7.3.3.5 Rozbudowane funkcje

Aplikacja posiada wiele dodatków, dzięki którym jest więcej opcji w Nagios Core, wraz z frontendami, performance graphing, auto-discovery, wspólne monitorowanie i wiele innych. Funkcje te są dostępne w różnych projektach Nagios, które są wdrażane niezależnie, i znajdują się w Nagios Exchange.

Do najpowszechniejszych projektów Nagios należą:

7.3.3.5.1 DNX

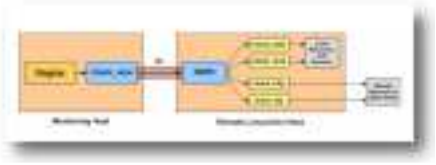
DNX to modułowa rozbudowa Nagios, która przejmuje znaczną część prac zwykle wykonywanych przez Nagios na dostępne sieci i hosty. Moduł DNX zapewnia, że operacje będą przydzielane równo pomiędzy zarejestrowanymi hostami klienckimi DNX.



7.3.3.5.2 NRPE

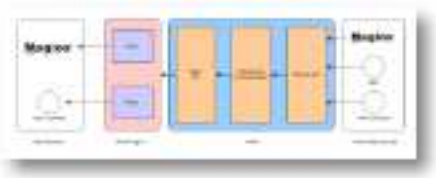
Agent NRPE umożliwia zdalne uruchamianie wtyczek Nagios w Linux/Unix. Umożliwia on monitorowanie metryki maszyny (wykorzystanie dysku, obciążenie

CPU itd.). Agent NRPE może również łączyć się z dodatkami agentów systemu Windows jak NSClinet++, więc można sprawdzać metryki w maszynach systemu Windows.



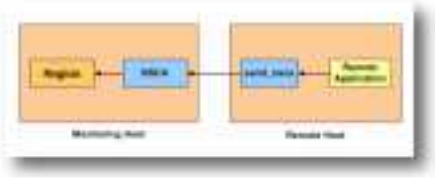
7.3.3.5.3 NRDP

NRDP jest elastycznym mechanizmem do przenoszenia danych. Utworzony jest na prostej i wydajnej architekturze, która pozwala na łatwą rozbudowę oraz dostosowanie do indywidualnych wymagań użytkowników. Używane są standardowe porty protokołów (HTTP(S) oraz XML), które mogą być wdrażane jako zamiennik NSCA.



7.3.3.5.4 NSCA

NCSA umożliwia integrowanie alarmów pasywnych oraz testów ze zdalnych maszyn i aplikacji z Nagios. Są użyteczne do przetwarzania alarmów bezpieczeństwa jak i rozmieszczania zbędnych i powszechnych konfiguracji Nagios.



7.3.3.5.5 NSClient++

NSClient++ jest to agent monitorujący/daemon do systemów Microsoft Windows, które pracują z Nagios. Umożliwa monitorowanie maszyn Windows.

7.3.3.5.6 Nagiosgraph

Nagiosgraph jest narzędziem do tworzenia grafiki, która analizuje wydajność oraz dane z wtyczek Nagios oraz przechowuje je w plikach RRD. Nagiosgraph wyświetla dane w trendach Nagio jako popup w hostach i usługach lub niezależnych raportach. Łatwo ją konfigurować i dostosować do własnych potrzeb.

7.3.3.5.7 NSTI

NSTI jest to dodatek do Nagios, który ułatwia zarządzenie sygnałami trap SNMP. NSTI zapewnia PHP frontend dla bazy danych SNMPTT backend i ułatwia szybkie i efektywne filtrowanie wyników SNMP, aby uzyskać obszerny przegląd potrzebnych informacji.

7.3.3.5.8 NConf

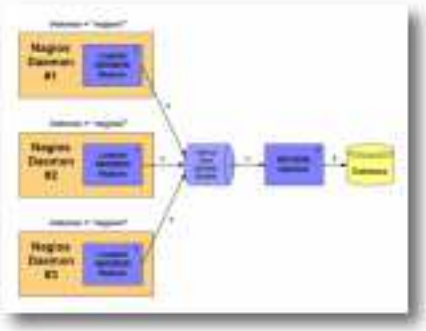
NConf jest to PHP frontend do konfigurowania Nagios. Różni się on od innych narzędzi, ponieważ oferuje oprogramowanie enterprises-class jak szablony, zależności oraz zdolność konfigurowania rozbudowaną typologię serwera Nagios.

7.3.3.5.9 NagEventLog

NagEventLog jest agentem dla Windows, który wysyła filtrowane wiadomości EventLog z maszyn Windows bezpośrednio do NSCA oraz pozwala otrzymywać alerty w Nagios, kiedy wykryte zostają wzory dziennika.

7.3.3.5.10 NDOUtils

NDOUtils pozwala eksportować bieżące i historyczne dane z jednej lub większej ilości Nagios do bazy danych MySQL. Kilka dodatków stosuje je jako źródło danych. NDOUtils składa się z niezależnego daemona, event broker Nagios oraz kilku programów użytkowych.



7.3.3.5.11 BPI

Nagios Business Process Intelligence (BPI) to zaawansowane narzędzie grupowania, które umożliwia ustalenie więcej zależności w celu określenia grup. Nagios BPI zawiera interfejs do efektywnego wyświetlania stanu sieci. Zasady stanu grup może określić użytkownik, zależności parent-child określane są w

przypadku, kiedy zachodzi potrzeba rozwiązania problemu. Narzędzia można używać w połączeniu z wtyczką do testowania, aby umożliwić wysyłanie powiadomień przez Nagios.

7.3.3.5.12 NagVis

Nagvis to wizualizacja dodatków do Nagios. Stosowany jest do przedstawiania danych, np. wyświetlenia procesów IT jak mail system lub infrastruktura sieciowa.

7.4.- Wymagania systemowe

Jedynym wymogiem do uruchomienia Nagios jest maszyna pracująca z systemem Linux (lub Unix) oraz kompilator C. Prawdopodobnie będziecie również chcieli konfigurować TCP/IP oraz wykonywać testy usług w sieci.
Nie jest wymagane zastosowanie CGI wraz z Nagios. Jednak, jeśli zdecydujecie się ich użyć, będziecie musieli zainstalować niezbędne oprogramowanie...
1. Serwer sieciowy (preferowany jest Apache)
2. Biblioteka Thomas Boutell gd wersja 1.6.3 lub nowsza (wymagana przez statusmap oraz trendy CGIs)

7.5.- Udzielanie licencji

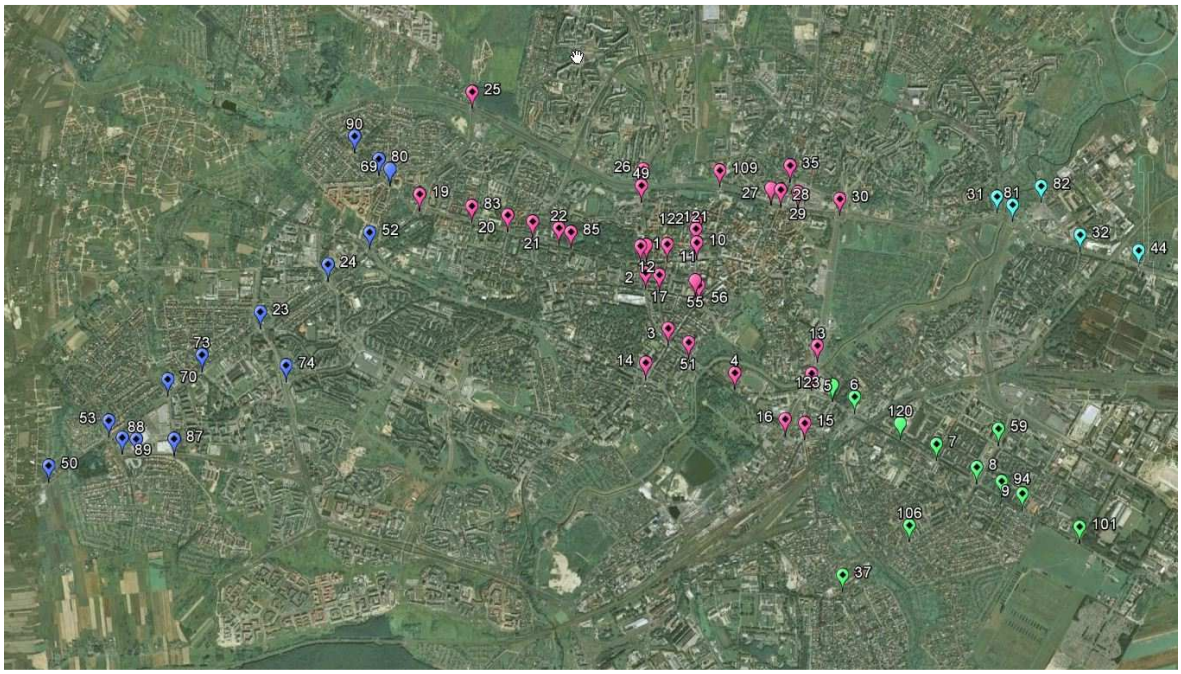
Aplikacja Nagios posiada licencję zgodnie z warunkami określonymi w Powszechnej Licencji Publicznej wersja 2, opublikowanej przez Free Software Foundation. Pozwala ona na legalne otrzymanie egzemplarza programu, rozpowszechnianie i/lub modyfikowanie go pod pewnymi warunkami. Należy przeczytać plik o nazwie „LICENSE” („LICENCJA”) oraz zapoznać się z wersją online.

8.- Umiejscowienie elementów

Na całym obszarze miasta Lublina rozplanowana została instalacja wszystkich elementów tworzących sieć telekomunikacji i ruchu drogowego.
W niniejszym dokumencie pokazano jakie elementy zostaną zainstalowane, jak również ich umiejscowienie.

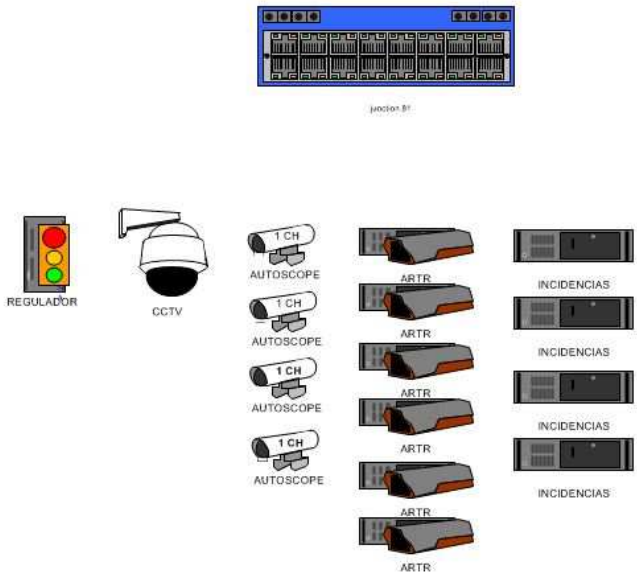
8.1.- Pierścienie

Zgodnie z tym, co zostało wyjaśnione w dokumencie definiujący sieć, wspomniana instalacja będzie się składać z licznych pierścieni, które w tym przypadku zostaną wykorzystane w celu umiejscowienia Urządzeń.
Wspomniane pierścienie składać się będą z kilku skrzyżowań, a te stanowić będą dokładne punkty umiejscowienia ww. urządzeń.



Wszystkie skrzyżowania wyposażone będą w odpowiednie urządzenia dostosowane do konkretnych potrzeb każdego z nich.

Na załączonym rysunku przedstawione zostały urządzenia, które stanowić będą wyposażenie większości skrzyżowań.



Na tym rysunku można obejrzeć urządzenia, jak również sprzęt wykrywający incydenty, regulatory, kamery CCTV, kamery ARTR, *Autoscopes* oraz switch[1]

[1] Legenda: REGULADOR= regulator; CCTV= CCTV; ARTR= ARTR; INCIDENCIAS= incydenty.

Na tym rysunku można obejrzeć urządzenia, które zostaną podłączone na skrzyżowaniach z zainstalowanymi panelami: switch i PMV.

8.1.1 Pierścień Centralny

Pierścień centralny złożony jest z 33 skrzyżowań, na każdym z nich zainstalowane zostaną regulatory, kamery, panele, itd., w zależności od potrzeb.

8.1.1.1 Skrzyżowanie 25

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'32.19"N
Długość geograficzna: 22°31'54.44"E

8.1.1.2 Skrzyżowanie 26

Współrzędne skrzyżowania to:

Szerokość geograficzna: 51°15'11.76"N
Długość geograficzna: 22°33'6.81"E

8.1.1.3 Skrzyżowanie 49

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'7.40"N
Długość geograficzna: 22°33'6.05"E

8.1.1.4 Skrzyżowanie 109

Współrzędne skrzyżowania::

Szerokość geograficzna: 51°15'11.41"N
Długość geograficzna: 22°33'39.23"E

8.1.1.5 Skrzyżowanie 122

Współrzędne skrzyżowania::

Szerokość geograficzna: 51°14'57.90"N
Długość geograficzna: 22°33'29.14"E

8.1.1.6 Skrzyżowanie 121

Współrzędne skrzyżowania::

Szerokość geograficzna: 51°14'55.90"N
Długość geograficzna: 22°33'29.03"E

8.1.1.7 Skrzyżowanie 10

Współrzędne skrzyżowania::

Szerokość geograficzna: 51°14'52.25"N
Długość geograficzna: 22°33'29.37"E

8.1.1.8 Skrzyżowanie 11

Współrzędne skrzyżowania::

Szerokość geograficzna: 51°14'51.82"N
Długość geograficzna: 22°33'16.89"E

8.1.1.9 Skrzyżowanie 12

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'51.57"N
Długość geograficzna: 22°33'8.11"E

8.1.1.10 Skrzyżowanie 1

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'51.35"N
Długość geograficzna: 22°33'5.64"E

8.1.1.11 Skrzyżowanie 2

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'44.31"N
Długość geograficzna: 22°33'7.76"E

8.1.1.12 Skrzyżowanie 17

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'43.74"N
Długość geograficzna: 22°33'13.59"E

8.1.1.13 Skrzyżowanie 55

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'42.31"N
Długość geograficzna: 22°33'28.78"E

8.1.1.14 Skrzyżowanie 56

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'40.98"N
Długość geograficzna: 22°33'30.33"E

8.1.1.15 Skrzyżowanie 3

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'29.62"N
Długość geograficzna: 22°33'17.35"E

8.1.1.16 Skrzyżowanie 14

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'20.55"N
Długość geograficzna: 22°33'7.88"E

8.1.1.17 Skrzyżowanie 51

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'25.95"N
Długość geograficzna: 22°33'26.08"E

8.1.1.18 Skrzyżowanie 4

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'17.88"N
Długość geograficzna: 22°33'45.65"E

8.1.1.19 Skrzyżowanie 16

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'5.62"N
Długość geograficzna: 22°34'6.97"E

8.1.1.20 Skrzyżowanie 5

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'17.71"N
Długość geograficzna: 22°34'18.15"E

8.1.1.21 Skrzyżowanie 15

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'4.56"N
Długość geograficzna: 22°34'15.23"E

8.1.1.22 Skrzyżowanie 13

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'25.09"N
Długość geograficzna: 22°34'20.64"E

8.1.1.23 Skrzyżowanie 30

Współrzędne skrzyżowania:

Szerokość geograficzna: 5 51°15'3.93"N
Długość geograficzna: 22°34'30.11"E

8.1.1.24 Skrzyżowanie 29

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'5.69"N
Długość geograficzna: 22°34'12.32"E

8.1.1.25 Skrzyżowanie 28

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'6.31"N
Długość geograficzna: 22°34'5.05"E

8.1.1.26 Skrzyżowanie 27

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'6.76"N
Długość geograficzna: 22°34'0.96"E

8.1.1.27 Skrzyżowanie 35

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'12.69"N
Długość geograficzna: 2 22°34'8.95"E

8.1.1.28 Skrzyżowanie 19

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'4.93"N
Długość geograficzna: 22°31'32.48"E

8.1.1.29 Skrzyżowanie 83

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'1.77"N
Długość geograficzna: 22°31'54.53"E

8.1.1.30 Skrzyżowanie 20

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'59.43"N
Długość geograficzna: 22°32'9.60"E

8.1.1.31 Skrzyżowanie 21

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'57.77"N
Długość geograficzna: 22°32'20.10"E

8.1.1.32 Skrzyżowanie 22

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'56.05"N
Długość geograficzna: 22°32'31.21"E

8.1.1.33 Skrzyżowanie 85

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'55.01"N
Długość geograficzna: 22°32'36.26"E

8.1.2 Pierścień 1

Pierścień 1 złożony jest z 15 skrzyżowań, na każdym z nich zainstalowane zostaną regulatory, kamery, panele, itd., w zależności od potrzeb.

8.1.2.1 Skrzyżowanie 69

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'11.65"N
Długość geograficzna: 22°31'19.89"E

8.1.2.2 Skrzyżowanie 80

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'14.22"N
Długość geograficzna: 22°31'15.31"E

8.1.2.3 Skrzyżowanie 90

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'20.24"N
Długość geograficzna: 22°31'5.03"E

8.1.2.4 Skrzyżowanie 52

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'54.86"N
Długość geograficzna: 22°31'11.48"E

8.1.2.5 Skrzyżowanie 24

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'46.42"N
Długość geograficzna: 22°30'53.96"E

8.1.2.6 Skrzyżowanie 23

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'33.85"N
Długość geograficzna: 22°30'25.60"E

8.1.2.7 Skrzyżowanie 74

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'19.82"N
Długość geograficzna: 22°30'36.40"E

8.1.2.8 Skrzyżowanie 73

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'22.54"N
Długość geograficzna: 22°30'1.05"E

8.1.2.9 Skrzyżowanie 70

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'16.12"N
Długość geograficzna: 22°29'46.65"E

8.1.2.10 Skrzyżowanie 53

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'5.25"N
Długość geograficzna: 22°29'21.96"E

8.1.2.11 Skrzyżowanie 89

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'0.77"N
Długość geograficzna: 22°29'27.72"E

8.1.2.12 Skrzyżowanie 88

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'0.37"N
Długość geograficzna: 22°29'33.53"E

8.1.2.13 Skrzyżowanie 87

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'0.42"N
Długość geograficzna: 22°29'49.28"E

8.1.2.14 Skrzyżowanie 50

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'53.33"N
Długość geograficzna: 22°28'56.58"E

8.1.2.15 Skrzyżowanie 104

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'38.94"N
Długość geograficzna: 22°28'28.37"E

8.1.3 Pierścień 2

Pierścień 2 złożony jest z 11 skrzyżowań, na każdym z nich zainstalowane zostaną regulatory, kamery, panele, itd., w zależności od potrzeb.

8.1.3.1 Skrzyżowanie 123

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'14.69"N
Długość geograficzna: 22°34'27.04"E

8.1.3.2 Skrzyżowanie 6

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'11.55"N
Długość geograficzna: 22°34'36.30"E

8.1.3.3 Skrzyżowanie 120

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'4.55"N
Długość geograficzna: 22°34'55.50"E

8.1.3.4 Skrzyżowanie 7

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'59.06"N
Długość geograficzna: 22°35'10.64"E

8.1.3.5 Skrzyżowanie 8

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'52.97"N
Długość geograficzna: 22°35'27.53"E

8.1.3.6 Skrzyżowanie 59

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'3.10"N
Długość geograficzna: 22°35'36.79"E

8.1.3.7 Skrzyżowanie 94

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'49.25"N
Długość geograficzna: 22°35'38.06"E

8.1.3.8 Skrzyżowanie 9

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'46.01"N
Długość geograficzna: 22°35'46.80"E

8.1.3.9 Skrzyżowanie 101

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'37.22"N
Długość geograficzna: 22°36'11.05"E

8.1.3.10 Skrzyżowanie 106

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'37.55"N
Długość geograficzna: 22°34'59.36"E

8.1.3.11 Skrzyżowanie 37

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°13'24.43"N
Długość geograficzna: 22°34'31.17"E

8.1.4 Pierścień 3

Pierścień 3 złożony jest z 5 skrzyżowań, na każdym z nich zainstalowane zostaną regulatory, kamery, panele, itd., w zależności od potrzeb.

8.1.4.1 Skrzyżowanie 31

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'4.55"N
Długość geograficzna: 22°35'36.80"E

8.1.4.2 Skrzyżowanie 81

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'2.40"N
Długość geograficzna: 22°35'43.41"E

8.1.4.3 Skrzyżowanie 82

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°15'7.32"N
Długość geograficzna: 22°35'55.46"E

8.1.4.4 Skrzyżowanie 32

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'54.35"N
Długość geograficzna: 22°36'11.77"E

8.1.4.5 Skrzyżowanie 44

Współrzędne skrzyżowania:

Szerokość geograficzna: 51°14'50.22"N
Długość geograficzna: 22°36'36.61"E