

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

DIOGO ORLANDO NUNES DE ALMEIDA

REDES DE ACESSO: Soluções para novos serviços de telecom

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2021

DIOGO ORLANDO NUNES DE ALMEIDA

REDES DE ACESSO: Soluções para novos serviços de telecom

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. MSc. Alexandre Jorge Miziara

CURITIBA
2021

DIOGO ORLANDO NUNES DE ALMEIDA

REDES DE ACESSO: Soluções para novos serviços de telecom

Trabalho de Conclusão do Curso Superior de Tecnologia em Sistemas de Telecomunicações apresentado como requisito para obtenção do título de Tecnólogo em Sistemas de Telecomunicações da Universidade Tecnológica Federal do Paraná (UTFPR).

Data de aprovação: 22/07/2021

Alexandre Jorge Miziara
Mestrado
Universidade Tecnológica Federal do Paraná

Jamea Cristina Batista Silva Franklin
Doutorado
Universidade Tecnológica Federal do Paraná

Kleber Kendy Horikawa Nabas
Doutorado
Universidade Tecnológica Federal do Paraná

- A Folha de Aprovação assinada encontra-se na Secretaria do Programa –

**CURITIBA
2021**

RESUMO

ALMEIDA, Diogo Orlando Nunes de. **Redes de Acesso**: Soluções para novos serviços de telecom. 2021. 215 f. Trabalho de Conclusão de Curso – Curso Superior de Tecnologia em Sistemas de Telecomunicações, Departamento Acadêmico de Eletrônica. Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

Esse trabalho tem como objetivo demonstrar a otimização das redes de acesso do Brasil das tecnologias legadas com as tecnologias novas e como as operadoras estão trabalhando para se adaptar aos novos serviços lançados nessa era como o Whatsapp e a Netflix. As tecnologias que serão estudadas são a ATM, PDH, SDH, XDSL, Frame Relay e Ethernet.

Palavras chave: Multiplexador. Roteador. Switch. Legado. Acesso.

ABSTRACT

ALMEIDA, Diogo Orlando Nunes de. **Access Network:** solutions for telecom new services. 2021. 251 p. Final Course Assignment – Higher education in Telecommunication Systems Technology, Electronic Academic Department - Universidade Tecnológica Federal do Paraná, Curitiba, 2021.

This assignment have as objective demonstrate the Brazilian access network optimizing of legacy technology to new technology and how telecommunication companies are working to adapt the launched new services in this time as Whatsapp and Netflix. The technologies that will be studied are ATM, PDH, SDH, XDSL, Frame Relay and Ethernet.

Keywords: Multiplex. Router. Switch. Legacy. Access.

LISTA DE ILUSTRAÇÕES

Figura 1 - Ilustração do sistema PDH Europeu.	24
Figura 2 - Ilustração do PDH americano.	25
Figura 3 - Ilustração do PDH japonês	26
Figura 4 - Estrutura do sistema SDH.....	28
Figura 5 - Funcionamento do VC.	31
Figura 6 - Funcionamento do VP.....	32
Figura 7 – Pacote Ethernet 802.3.....	34
Figura 8 - Pacote Ethernet.	34
Figura 9 - Sistema DSL.	36
Figura 10 - Espectro do sinal ADSL.	37
Figura 11 - Estrutura do Frame.	40
Figura 12 - Estrutura GPON.....	44
Figura 13 - Estrutura da ONT.....	44
Figura 14 - Topologia.	45
Figura 15 - Esquema DSP.....	48
Figura 16 - Transporte do QOS na rede.....	50
Figura 17 - Configuração do DOT1Q no Cisco.....	55
Figura 18 - Encapsulamento do DOT1Q no Alcatel.	55
Figura 19 - Configurando um <i>customer</i> no Alcatel.	55
Figura 20 - Criando a interface lógica no Alcatel.....	56
Figura 21 - Configurando o QinQ no Cisco.	56
Figura 22 - Configurando o encapsulamento QinQ no Alcatel.	56
Figura 23 - Configurando o customer no Alcatel.	57
Figura 24 - Configurando um QinQ na interface lógica do Alcatel.....	57
Figura 25 - Configurando o SONET no Cisco.	57
Figura 26 - Acessando a configuração da porta no Cisco.....	58
Figura 27 - Configurando o SONET no Alcatel.....	58
Figura 28 - Configurando cliente no Alcatel.	58
Figura 29 - Acessando a porta no Alcatel.	58
Figura 30 - Configurando o E3 no Cisco.	59
Figura 31 - Configurando E1 no Cisco.	59
Figura 32 - Configurando ATM no Cisco.	59
Figura 33 – Configurando X.25 no Cisco.	60
Figura 34 - Configurando túnel no Alcatel.	61
Figura 35 - Configurando uma porta tronco no Cisco.....	61
Figura 36 - Configurando uma porta tronco secundária.....	62
Figura 37 - Ativando a vlan.....	62
Figura 38 - Topologia metro ethernet.	63
Figura 39 - Configurações do OSPF dos roteadores.	63
Figura 40 - Configurações da MPLS dos roteadores.	64
Figura 41 - Configuração do LSP dos roteadores.	65
Figura 42 - Configuração do ldp dos roteadores.	66
Figura 43 - Configurando as pontas do roteadores.....	66
Figura 44 - Criando o túnel.....	67
Figura 45 - Configurando os timeslots.....	67
Figura 46 - Descrição da porta.....	67
Figura 47 - Menu procura equipamentos.	68

Figura 48 - Localizando os equipamentos.....	68
Figura 49 - Multiplexador.....	69
Figura 50 - Localizando facilidades.....	70
Figura 51 - Multiplexador com placa de acesso.....	71
Figura 52 - Ativando uma porta.....	72
Figura 53 - Menu aprovisionando circuito.....	73
Figura 54 - Criando um cliente.....	73
Figura 55 - Criando um serviço.....	74
Figura 56 - Criando um circuito.....	75
Figura 57 - Configurando pontas.....	76
Figura 58 - Localizando o multiplexador.....	76
Figura 59 - Portas configuradas.....	77
Figura 60 - Selecionando a VC.....	78
Figura 61 - Selecionando timeslots.....	78
Figura 62 - Criando a rota.....	79
Figura 63 - Menu procurar circuitos.....	79
Figura 64 - Localizando o circuito.....	80
Figura 65 - Rota do circuito.....	81
Figura 66 - E3 aprovisionado.....	81
Figura 67 - Descrição da porta.....	82
Figura 68 - Tela inicial da Newbridge.....	82
Figura 69 - Menu equipamento nós.....	83
Figura 70 - Filtro de equipamentos da newbridge.....	83
Figura 71 - Multiplexador de acesso newbridge.....	84
Figura 72 - Acessando a placa.....	85
Figura 73 - Acessando a porta e selecionado a DTU.....	85
Figura 74 - Multiplexador de meio.....	86
Figura 75 - Periférico do multiplexador.....	86
Figura 76 - Placa do multiplexador newbridge.....	87
Figura 77 - E1 da placa E3.....	87
Figura 78 - Time Slots do E1.....	88
Figura 79 - Menu criar circuito.....	88
Figura 80 - Gerando rota.....	89
Figura 81 - Tela de configurações gerais do circuito.....	89
Figura 82 - Tela de configurações de dados do circuito.....	90
Figura 83 - Configuração ATM do circuito.....	91
Figura 84 - Configurações da rota do circuito.....	92
Figura 85 - Configuração ISDN do circuito.....	93
Figura 86 - Configurações OAM do circuito.....	94
Figura 87 - Circuito ativado.....	95
Figura 88 - Porta do equipamento Cisco para a rede BPX/IGX.....	96
Figura 89 - Filtrando facilidades.....	96
Figura 90 - Verificando facilidades no BPX.....	97
Figura 91 - Criando PVC no Cisco.....	97
Figura 92 - Verificando placas no IGX.....	98
Figura 93 - Verificando portas no IGX.....	99
Figura 94 - Verificando conexões no IGX.....	99
Figura 95 - Ativando porta no IGX.....	100
Figura 96 - Configurando porta no IGX.....	101

Figura 97 - Criando a conexão no BPX.....	105
Figura 98 - Acessando o servidor Alcatel.....	106
Figura 99 - Procurando caminhos.....	106
Figura 100 - Filtrando o Circuito no SDH.....	107
Figura 101 - Verificando circuitos.....	108
Figura 102 - Verificando a rota.....	108
Figura 103 - Rota criada.....	109
Figura 104 - Mapa gerado.....	110
Figura 105 - Subrede do sistema SDH.....	110
Figura 106 - Multiplexador SDH.....	111
Figura 107 - Placa do SDH.....	112
Figura 108 - Estado das subdivisões do SDH.....	113
Figura 109 - Placa do multiplexador.....	114
Figura 110 - Portas ópticas.....	115
Figura 111 - Alarmes da porta.....	115
Figura 112 - Roteador com porta lag.....	116
Figura 113 - Estado de uma porta lag.....	117
Figura 114 - Tela inicial gerência Nokia AMS.....	118
Figura 115 - Listando um circuito na gerência.....	119
Figura 116 - Aba <i>General</i> continuação.....	120
Figura 117 - Continuação da aba general.....	121
Figura 118 - Aba QOS.....	122
Figura 119 - Aba Details 1.....	124
Figura 120 - Aba Details 2.....	125
Figura 121 - Optical Measurements da ONT.....	126
Figura 122 - Porta Ethernet da ONT.....	127
Figura 123 - Continuação aba General Ethernet.....	127
Figura 124 - Aba QOS do porta Ethernet.....	128
Figura 125 - Porta para o Roteador.....	130
Figura 126 - Aba Ethernet para a porta do roteador.....	131
Figura 127 - Aba Link Agregation.....	132
Figura 128 - Link Aggregation Group 10.....	133
Figura 129 - Configuração de VLAN.....	134
Figura 130 - Procurando SVLAN.....	135
Figura 131 - IHUB 3984.....	135
Figura 132 - VPLS.....	136
Figura 133 - Multiplexador de meio Newbridge.....	137
Figura 134 - Periférico da Newbridge.....	138
Figura 135 - Portas E1 rede Newbridge.....	138
Figura 136 - Time slots da newbridge.....	139
Figura 137 - Menu links da Newbridge.....	139
Figura 138 - Localizando um link.....	140
Figura 139 - Configuração geral do circuito.....	141
Figura 140 - Menu links datacom.....	141
Figura 141 - Localizando link na Datacom.....	142
Figura 142 - Configurando circuito na Datacom.....	143
Figura 143 - Localizando equipamento.....	143
Figura 144 - Configuração do circuito.....	144
Figura 145 - Multiplexador datacom.....	145

Figura 146 - Selecionando o E3 para realizar a cross conexão.	146
Figura 147 - Configuração do circuito terminada.....	147
Figura 148 - Opção equipamentos e nós.	147
Figura 149 - Localizando equipamento.	148
Figura 150 - Multiplexador de meio.....	148
Figura 151 - Periférico newbridge.	149
Figura 152 - Placa E3.....	149
Figura 153 - E1 lógico newbridge dentro de uma E3.	150
Figura 154 - Timeslots.....	150
Figura 155 - Configurando o circuito.	151
Figura 156 - Configurando porta.	152
Figura 157 - Ativando porta.....	152
Figura 158 - Configurando porta lógica.	153
Figura 159 - Localizando cross conexão com o Cisco.	153
Figura 160 - Placa da cross conexão.....	154
Figura 161 - Timeslot da cross conexão.	154
Figura 162 - Localizando porta no Cisco.....	155
Figura 163 - Verificando porta no Alcatel.	156
Figura 164 - Usando a rede metro para ir a outro equipamento.....	157
Figura 165 - Localizando DSLAM.....	157
Figura 166 - Interface U2000.....	158
Figura 167 - DSLAM U2000.....	158
Figura 168 - DSLAM em cascata.	159
Figura 169 - Portas DSL.....	160
Figura 170 - Configurando serviço.....	160
Figura 171 - Configurando PVC.....	161
Figura 172 - Multiplexador ATM newbridge.....	161
Figura 173 - Placa ATM.....	162
Figura 174 - Portas ATM Newbridge.....	162
Figura 175 - Menu para criar a rota ATM.....	163
Figura 176 - Configuração geral circuito ATM.....	163
Figura 177 - Configuração do circuito ATM.....	165
Figura 178 - Configurando tráfego no circuito ATM.....	166
Figura 179 - DSLAM de meio.....	166
Figura 180 - Portas DSLAM.....	167
Figura 181 - Adicionando PVC no DSLAM.....	167
Figura 182 - Tela de configuração de PVC.....	168
Figura 183 - Configurando o PVC.....	169
Figura 184 - Configurando PVC.....	170
Figura 185 - Mapa Estrela X.25/TDM.....	170
Figura 186 - Mux de Acesso X.25.....	171
Figura 187 - Placa PE.....	171
Figura 188 - Placa de recurso.....	172
Figura 189 - Configuração camada de dados X25.....	173
Figura 190 - Configuração camada de rede X.25.....	176
Figura 191 - Tradução de endereços.....	178
Figura 192 - Mux conversor X.25 para PDH.....	179
Figura 193 - Criando uma rota X.25.....	179
Figura 194 - Criação da rota X.25.....	180

Figura 195 – Comandos para configurar velocidade Cisco.....	182
Figura 196 - Configurando velocidade no Alcatel.....	183
Figura 197 - Configurando rota estática Cisco.	183
Figura 198 - Configurando rota estática Alcatel.	184
Figura 199 - BGP no Alcatel.....	185
Figura 200 - BGP no cliente.	186
Figura 201 - Estado da BGP.	187
Figura 202 – Estado da BGP no cliente.	187
Figura 203 - Configurando a BGP no Cisco da operadora.....	189
Figura 204 - Estado da BGP.	189
Figura 205 - Configurando endereçamento IP no Cisco.	190
Figura 206 - Configurando endereçamento IP no Alcatel.....	190
Figura 207 - QOS Alcatel	192
Figura 208 - Escalonador de QOS	193
Figura 209 - Interface com QOS	194
Figura 210 - Estado das DIU's.	196
Figura 211 - Estado das linhas e direcionalidade.....	197
Figura 212 - Sistema de numeração.	198
Figura 213 - Verificando serviços atrelados a linha.....	198
Figura 214 - Configuração de rota.....	199
Figura 215 - Verificação de destino.....	200
Figura 216 - Divisão de tráfego.	200
Figura 217 – Estado das linhas.....	201
Figura 218 - Estado da linha fixa.....	201
Figura 219 - Estado das LTG's.....	202
Figura 220 - Configurações da linha.	203
Figura 221 - Estado da EQN.	203
Figura 222 - Configuração VOIP 1.	205
Figura 223 - Configurando VOIP 2.....	206
Figura 224 - Configurando VOIP 3.....	206
Figura 225 - Configurando VOIP 4.....	208

LISTA DE SIGLAS

ABR	Available Bit Rate
ADSL	Assymetrical Digital Subscriber Line
ADTF	The Allowed-Cell-Rate Decrease Factor
AES	Advanced Encryption System
AIS	Alarm Indicator Signal
ANATEL	Agência Nacional de Telecomunicações
ANF-CMN	Common Information Additional Network Feature
ANI	Access Node Interface
ANSI	American National Standards Institute
AQM	Active Queue Management
ASP	Analogic Signal Processing
ATM	Assynchronous Transfer Mode
ATU	ADSL Transfer Unit
AUG	Administrative Unit Group
BECN	Backward Explicit Congestion Notification Bit
BER	Bit Error Ratio
BERT	Bit Error Ratio Testing
BGP	Border Gateway Protocol
CAC	Connection Admission Control
CBR	Constant Bit Rate
CBS	Committed Burst Size
CCITT Committee	The International Telegraph and Telephone Consultative Committee
CDVT	Cell Delay Variation Tolerance
CIDR	Classless Inter-Domain Routing
CIR	Comitted Information Rate
CLLM	Consolidated Link Layer Management
CLP	Cell Loss Priority
COVID-19	Corona Virus Disease 2019
CPSS	Control Packet Switching System
CSMA/CD	Carrier-sense multiple access with collision detection
CSPF	Constrained Shortest Path First
CVLAN	Customer Virtual Local Area Network
DCE	Data Circuit-Terminating Equipment
DDR	Dial-on-Demand Routing
DDS	Digital Data Service
DHCP	Dynamic Host Configuration Protocol
DIU	Digital Interface Unit
DLCI	Data Link Connection Interface
DLU	Digital Line Unit
DS	Differentiated Services
DSCP	Differentiated Services Code Points
DSL	Digital Subscriber Line.
DSLAM	Digital Subscriber Line Access Multiplexer.
DSP	Digital Signal Processing
DTC	Datacom

DTE	Data Termination Equipament
DTU	Data Termination Unit
EBS	Excess Burst Size
EDD	Ethernet Demarcation Devices
EFCI	Explicit Forward Congestion Indication
ETSI	European Telecommunication Standard Institute
FC	Forward Class
FCES	Flow Control External Segment
FCS	Frame Check Sequence
FEC	Forward Error Correction
FECN	Forward Explicit Congestion Notification Bit
FRTT	Fixed Round Trip Time
FTTB/C	Fibre To The Build/Curb
FTTH	Fibre To The Home
FXO	Foreign Exchange Office
FXS	Foreign Exchange Service
GPON	Gigabit-capable Passive Optical Networks.
HCM	High-performance voice Compression Modules
HDSL	High-bit-rate digital subscriber line
HTC	Highest Two-Way Channel
IBS	Initial Burst Size
ICR	Initial Cell Rate
IDSL	ISDN Digital Subscriber Line
IEEE	Institute of Electrical and Electronics Engineers
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
ILMI	Integrated Local Mangement Interface
IP	Internet Protocol.
ITU	International Telecommunication Union
ISDN	Integrated Services Digital Network
ISO	International organization of Standardization
GEM	Gigabit-capable Passive Optical Network Encapsulation Method
LAN	Local Area Network
LAPB	Link Access Procedures
LAPD	Data Link Layer Protocol
LCN	Logical Channel Number
LLC	Logical Link Control
LMI	Local Management Interface
LOF	Loss of Frame
LOP	Loss of Pointer
LOS	Loss of Signal
LSP	Label Switched Paths
LTG	Line Trunk Group
MAC	Media Access Control Address
MBS	Maximum Burst Size
MCR	Minimun Cell Rate
MDU	Multi-Dwelling Unit
MIR	Minimum Information Rate
MLP	Multilink Procedure

MPLS	Multiprotocol Label Switching
MST	Multiplex Section Termination
NNI	Network-to-Network Interface
NPI	Numbering Plan Identification
NUA	Network User Address
NWB	Newbridge
OAM	Operation, Administration and Maintenance
OC	Optical Carrier
ODN	Passive Optical Distribution Network
OLT	Optical Line Terminator
ONU	Optical Network Unit
ONT	Optical Network Termination
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PABX	Private Automatic Branch Exchange
PCM	Pulse-code modulation
PCR	Peak Cell Rate
PIR	Peak Information Rate
PM	Performance Monitoring
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PSNL	Packet Switch Network Link
PTN	Packet Transport Networks
PVC	Permanent Virtual Circuit
QOE	Quality of Experience
QOS	Quality of Service
RDF	Rate Decrease Factor
RIF	Rate Increase Factor
RPTC	Rede Pública de Telefonía Comutada
RST	Regenerator Section Termination
SAP	Service Access Point
SCR	Sustainable Cell Rate
SDH	Synchronous Digital Hierarchy
SDP	Service Distribution Point
SFD	Start Frame Delimiter
SIP	Session Initiation Protocol
SLP	Single Link Procedures
SMS	Short Message Service
SONET	Synchronous Optical Network
SPI	SDH Physical Interface
SPVC	Switched Permanent Virtual Connection
SR+BS	Single Rate with Burst Size Control
srTCM	Single Rate Three Color Mark
STM	Synchronous Transporte Module
STS	Synchronous Transport Signal
SVC	Switched Virtual Circuit
SVLAN	Stacked Virtual Local Area Network
TBE	Transient Buffer Exposure
TCP	Transport Control Protocol

TDM	Time-division multiplexing
TIM	Trace Interface Mismatch
trTCM	Two Rate Three Color Mark
TUG	Tributary Unit Group
UBR	Unspecified Bit Rate
UNI	User Network Interface
URU	Underlying Resource Unavailable
VBR	Variable Bit Rate
VC	Virtual Container
VCI	Virtual Channel Identifier
VDSL	Very high bit rate digital subscriber line
VLAN	Virtual Local Area Network
VOIP	Voice Over IP.
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPLC	Virtual Path Link Connection
VPLS	Virtual private LAN service
VPN	Virtual Private Network
VPNC	Virtual Path Network Connection
VPRN	Virtual Private Routed Network
VPSC	Virtual Path Sub Network Connection
VPT	Virtual Path Termination
VSVD	Virtual Source Virtual Destination

SUMÁRIO

1 INTRODUÇÃO	17
1.1 TEMA	17
1.2 DELIMITAÇÃO DE ESTUDO	17
1.3 PROBLEMAS E PREMISSAS	18
1.4 OBJETIVOS	20
1.4.1 Geral.....	20
1.4.2 Objetivos específicos.....	21
1.5 JUSTIFICATIVA	21
1.6 PROCEDIMENTOS METODOLOGICOS	21
1.7 ESTRUTURA DO TRABALHO	22
2 FUNDAMENTAÇÃO TEÓRICA	24
2.1 PDH.....	24
2.2 SDH/SONET	26
2.3 ATM.....	30
2.4 ETHERNET	33
2.5 ADSL	35
2.6 PADRÃO V.35.....	37
2.7 X.25.....	38
2.8 FRAME RELAY	39
2.9 INTERNET PROTOCOL (IP).....	41
2.10 FIBRA ÓTICA (GPON).....	43
2.11 PROTOCOLOS DE ROTEAMENTO	45
2.11.1 Rota estática	45
2.11.2 BGP	45
2.11.3 OSPF.....	46
2.12 TECNOLOGIAS DE VOZ	46
2.12.1 PSTN.....	46
2.12.2 ISDN.....	47
2.12.3 DSP	47
2.12.4 FXS/FXO	48
2.12.5 H.323.....	48
2.13 QOS E QOE	49
3 INTEGRANDO E CONFIGURANDO SOLUÇÃO DE DADOS	55
3.1 CONFIGURANDO SALTOS ENTRE ROTEADORES	55
3.1.1 Configurando Dot1Q na rede	55
3.1.2 Configurando QinQ na rede	56
3.1.3 Configurando interface Serial SONET	57
3.1.4 Configurando porta E1/E3	58
3.1.5 Configurando Interface ATM em roteador	59
3.1.6 Configurando Interface X.25 no roteador Cisco	60
3.2 CONFIGURANDO CROSS CONEXÃO ENTRE ROTEADOR E OUTRA GERÊNCIA.....	61
3.2.1 Configurando túnel <i>Metro-Ethernet</i> por dot1q	61
3.2.2 Configurando túnel Metro-Ethernet por MPLS	62
3.2.3 Cross conexão Roteador/Datacom	67
3.2.4 Conexão Roteador e Rede Newbridge.....	81
3.2.5 Conexão Roteador e rede CISCO BPX/IGX.....	95
3.2.6 Cross conexão entre Roteador e rede SDH Alcatel	105

3.2.7 Cross conexão entre Roteador e GPON	116
3.3 CROSS CONEXÃO ENTRE GERÊNCIAS E TECNOLOGIAS DISTINTAS	136
3.3.1 Cross Conexão entre a Rede Newbridge e Rede Datacom	136
3.3.2 Cross conexão rede ATM Cisco Newbridge	151
3.3.3 Cross conexão Metro e DSLAM.	154
3.3.4 Cross Conexão Cisco/ATM/DSLAM	160
3.3.5 Cross conexão X.25 e outra gerência.	170
3.4 SERVIÇOS	180
3.4.1 Configurando a velocidade no roteador	180
3.4.2 Rotas	183
3.4.3 Endereçamento IP	189
3.4.4 Aplicação de QOS	190
4 INTEGRANDO E CONFIGURANDO SOLUÇÃO DE VOZ	195
4.1 DDR VIA NÚMERO CHAVE	195
4.2 CONFIGURAÇÃO DDR POR ROTA	199
4.3 CONFIGURAÇÃO DE NÚMERO FIXO	201
4.4 VOIP	203
5 APRESENTAÇÃO DE DADOS E TRABALHOS FUTUROS	209
6 CONSIDERAÇÕES FINAIS	210
REFERÊNCIAS	211

1 INTRODUÇÃO

1.1 TEMA

Segundo os autores Kurose e Ross (2013, p. 8, 9) a rede de acesso é a rede física que conecta um sistema final ao primeiro roteador (também conhecido como roteador de borda) de um caminho partindo de um sistema final para outro qualquer. Essas podem ser divididas de modo geral em três categorias: acesso doméstico, acesso corporativo e móvel sem fio. Nesse trabalho será abordado o acesso residencial e corporativo no Brasil. A rede sem fio devido à sua complexidade, não será abordada, pois é um assunto que compreende os celulares e rede satélite.

O acesso doméstico tem dois tipos de acesso predominantes que são a linha digital de assinante (DSL) ou a cabo (KUROSE; ROSS, 2013, p.9) e o sistema corporativo e em campus é usado predominantemente o acesso Ethernet (KUROSE; ROSS, 2013, p.12). Seguindo esse raciocínio e o sistema atual brasileiro existem muitos equipamentos gerenciáveis (que podem ser configurados logicamente) como multiplexadores, *Digital Subscriber Line Access Multiplexer* (DSLAM) e *switchs* que são equipamentos passivos entre o acesso e o roteador de borda e esse documento terá foco neles. No caso de equipamentos DSLAM, esses serão mais usados para acesso residencial pois são eles que fornecem a tecnologia DSL porém pode acontecer de ter esse tipo de equipamentos em acesso corporativo.

Já o *backbone* nacional é composto por diversas redes sendo a principal a rede Ethernet, *Internet Protocol* (IP), *Packet Transport Networks* (PTN) e *Synchronous Digital Hierarchy* (SDH), embora existam ainda bancos e empresas que devido limitações de sistema mantêm o *backbone* ATM (*Asynchronous Transfer Mode*) e *Frame-relay* ainda na ativa.

1.2 DELIMITAÇÃO DE ESTUDO

Esse trabalho trata apenas da rede nacional e de projeções de como as operadoras estão se adaptando ao aumento de uso de dados na rede nacional devido ao novo cenário do vírus COVID-19 (*Corona Virus Disease 2019*) e o aumento de pessoas trabalhando em Home Office.

As operadoras que usam a rede legada do antigo sistema Telebrás são abrangidas por esse trabalho e a base de sistema vem da experiência profissional do mesmo que redige esse documento, sendo que esse executa suporte a várias operadoras e tem experiência com atendimento ao *backbone* nacional.

Será abordado também a sobrevida desse sistema legado herdado da Telebrás e demonstrado como um país em desenvolvimento trabalha com a convergência dessa rede para a rede IP e toda a aceleração devido à inserção dos novos serviços como *streaming* e comunicação.

1.3 PROBLEMAS E PREMISSAS

O principal problema que gerou essa pesquisa é a velocidade da internet que o Brasil proporciona ao seu usuário que é 2,75 vezes menor que a média do Estados Unidos, que, conforme quadro 1 é a décima no ranking mundial e 3,94 vezes menor que a média da Coreia do Sul que lidera esse ranking segundo dados do primeiro trimestre de 2017.

Quadro 1 - Velocidade média de internet.

Classificação Global	País/Região	1T. 2017 Mbps Médio	Classificação Global	País/Região	1T. 2017 Mbps Médio
1	Coreia do Sul	28,6	91	Peru	6,2
10	Estados Unidos	18,7	92	Equador	6,2
20	Canadá	16,2	94	Panamá	5,9
57	Uruguai	9,5	99	Colômbia	5,5
60	Chile	9,3	112	Costa Rica	4,1
76	México	7,5	132	Bolívia	2,7
79	Brasil	6,8	144	Venezuela	1,8
90	Argentina	6,3	148	Paraguai	1,4

Fonte: Akamai, 2017.

A informação mais preocupante é sobre a quantidade de usuários que tem uma velocidade acima de 10 Mbps em sua residência o que é o necessário para um bom funcionamento de um serviço *streaming* em alta qualidade. Comparado com os líderes do *ranking* o Brasil tem uma porcentagem bem inferior de residências com internet acima de 10 Mbps.

Quadro 2 - Percentagem de pessoas com mais de 10 Mbps de internet

País/Região	% Acima de 10 Mbps	País/Região	% Acima de 10 Mbps
Coreia do Sul	85	Peru	13
Estados Unidos	67	Panamá	12
Canadá	61	Equador	12
Uruguai	35	Colômbia	7,6
Chile	30	Costa Rica	3,3
México	19	Bolívia	1,1
Brasil	18	Venezuela	0,2
Argentina	16	Paraguai	0,2

Fonte: Akamai, 2017

Com esse problema proposto resta saber se o Brasil está com sua rede preparada para os novos serviços convergentes que estão nascendo no mercado, se a falha está no serviço que é entregue no mercado e como funciona essa rede toda.

Outro problema são os novos serviços que estão aparecendo para competir com os serviços que as operadoras oferecem. Segundo a revista exame por Lucas Agrela (2019) o Brasil em 2019 tinha 120 milhões de usuários que estavam usando o aplicativo para celulares *Whatsapp*. Esse aplicativo pode mandar mensagens sem usar o serviço SMS, fazer ligações sem usar a rede de telefonia pública (RPTC) e fazer vídeo chamadas aumentando bastante o consumo de dados e afetando o lucro das operadoras. Outros serviços que estão vindo são os de *streaming* (armazenamento e transmissão de vídeos) que vieram para competir com o serviço de TV por assinatura das operadoras, sendo a *Netflix* um dos serviços mais populares, o qual tem, conforme dados divulgados pela revista exame por Carolina Riveira (2019), 27 milhões de usuários.

Os impactos desses novos serviços nas operadoras como demonstram os gráficos 1 e 2 ANATEL (2020) estão contribuindo para a queda de assinantes na telefonia e TV por assinatura que desde 2016 demonstram queda.

Gráfico 1 - Quantidade de telefones fixos.

Fonte: ANATEL

Gráfico 2 - Quantidade de TV por assinatura.

Fonte: ANATEL

Algo que incomoda de certo ponto vários estudantes da área é o atraso nas tecnologias de telecomunicações no Brasil. Boa parte das operadoras estão hoje modernizando suas redes, porém usam ainda muitos equipamentos do antigo sistema Telebrás. A rede IP por exemplo foi implementada com um atraso colossal já que muitas empresas não quiseram investir no Brasil e as que investiram acabaram perdendo dinheiro, um pouco devido ao custo para modernização e burocracia.

1.4 OBJETIVOS

1.4.1 Geral

Propor novas soluções em serviços e tecnologias de acesso usando o legado herdado do antigo sistema Telebras e a tecnologia atual das operadoras.

1.4.2 Objetivos específicos

- Demonstrar como funciona a topologia legada hoje no atualmente e rede de acesso nacional (PDH, SDH, ATM, Frame-Relay, DSL e voz).
- Demonstrar como a convergência de rede é importante para o funcionamento da rede legada e a rede moderna.
- Analisar os dados das demonstrações e a evolução da tecnologia.
- Propor novas soluções em serviço e no modelo de negócio da operadora.
- Verificar quais são os novos serviços que estão sendo disponibilizados a operadora e como a rede de acesso está se preparando para tal situação.
- Comparar as velocidades e serviços legados com as novas tecnologias.

1.5 JUSTIFICATIVA

Após o novo cenário internacional que ocorreu no final do ano de 2019 e 2020 devido à crise do corona vírus nota-se como as empresas tiveram que adaptar os seus modelos de negócio e isso gera questões como por exemplo: o Brasil está apto a essa nova realidade com o Backbone e rede de acesso que tem no momento?

Essa questão já era debatida desde o surgimento de serviços que usam a internet como por exemplo: aplicativos de *streaming*, transporte, venda e compra, *internet banking* e outros, mas hoje devido ao trabalho em casa denominado “*Home Office*” a necessidade de banda aumentou de uma forma gigantesca.

1.6 PROCEDIMENTOS METODOLOGICOS

Devido o *backbone* ou núcleo de rede ser o coração de toda a internet seu estudo é altamente relevante para a área de sistemas de telecomunicações como para os demais cursos. Todos usam essa tecnologia diretamente ou indiretamente, exceto se a pessoa viver isoladamente por opção ou pertencer a uma tribo indígena que não teve seu primeiro contato com o mundo.

Cada vez mais a internet está presente na vida humana. Antigamente se existisse uma necessidade de uma pessoa mandar uma informação a outra pessoa seria enviado uma carta que demoraria dias para chegar ao destinatário, hoje com a

internet podemos enviar uma informação em menos de minutos para qualquer lugar do mundo e para qualquer um. O problema é que as pessoas não estão mais satisfeitas em apenas enviar e receber mensagens de texto e sim receber informações audiovisuais que consomem muita banda da conexão que o usuário tem com a internet.

Saber interpretar e ter o conhecimento necessário sobre como funciona a rede nacional é essencial ao curso de Tecnologia em Sistemas de Telecomunicações, inclusive já aconteceu de conhecimento dito como antigo ser usado para criar algo mais aperfeiçoado do que algo dito moderno e a rede brasileira tem muito equipamento legado na rede, principalmente na área agrícola e regiões isoladas. A razão desses equipamentos legados existirem deve-se por má administração e extensão territorial da rede nacional.

O foco desse trabalho é inteiramente feito através de demonstrações e comparações do novo com o antigo como já se percebe ao ler o tópico 1.4.2.

1.7 ESTRUTURA DO TRABALHO

Este trabalho terá a seguinte estrutura:

Capítulo 1 – Introdução: serão apresentados o tema, as delimitações da pesquisa, o problema e a premissa, os objetivos da pesquisa, a justificativa, os procedimentos metodológicos, as indicações para o embasamento teórico, e a estrutura geral do trabalho.

Capítulo 2 – Teoria: Será abordada toda a teoria usada na demonstração prática.

Capítulo 3 – Dados: Será feita a demonstração prática de uma rede de dados.

Capítulo 4 – Voz: Será feita a demonstração prática de um *backbone* legado de voz.

Capítulo 5 – Apresentação e Análise dos Resultados: Tendo como base todas as demonstrações de como funciona alguns sistemas de cada tecnologia será dada a resolução do problema, explicando qual será a tecnologia para a qual as operadoras irão migrar e as que estão sendo usadas e serão descartadas por serem legadas com o tempo.

Capítulo 6 – Considerações finais: será retomada a pergunta de pesquisa e os seus objetivos e apontado como foram solucionados, respondidos, atingidos, por meio do trabalho realizado. Além disto, serão sugeridos trabalhos futuros que

poderiam ser realizados a partir do estudo realizado.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica foi encontrada em livros e normas. O que é específico de uma plataforma foi retirado do menu ajuda do próprio aplicativo. Boa parte das normas consultadas pertencem a International Telecommunication Union (ITU), European Telecommunication Standard Institute (ETSI), American National Standards Institute, ATM Forum Specifications e Institute of Electrical and Electronics Engineers (IEEE). As opiniões de vários especialistas de rede de várias empresas foram analisadas antes de ser feita tal seleção de equipamentos para evitar uma maior quantidade de conteúdo, satélite e telefonia celular não serão abordados.

2.1 PDH

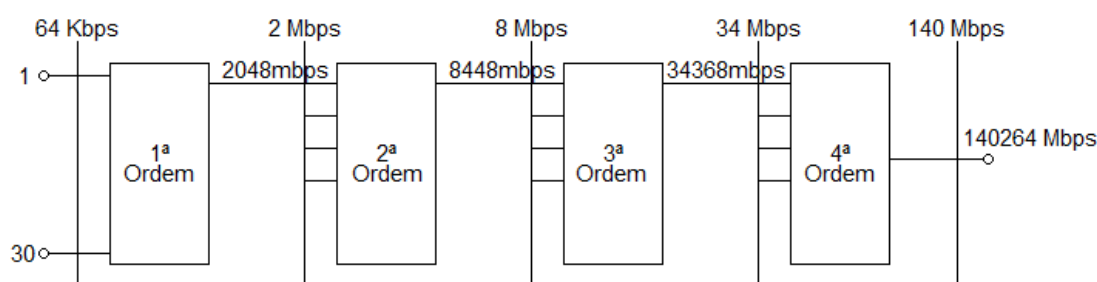
O PDH foi criado em base da modulação por código de pulsos (PCM) que tem a hierarquia, desenvolvida e padronizada na Europa, nos Estados Unidos e no Japão. O padrão de hierarquia PCM europeu, adotado no Brasil, apresenta quatro ordens na sua disposição (NETO; NETO, 2002) conforme figura 1 e no quadro 3.

Quadro 3 - Velocidades das portas PDH europeu.

Padrão Europeu	
E1	2048 kbps
E2	8448 kbps
E3	34368 kbps
E4	140264 kbps

Fonte: NETO e NETO (2002)

Figura 1 - Ilustração do sistema PDH Europeu.

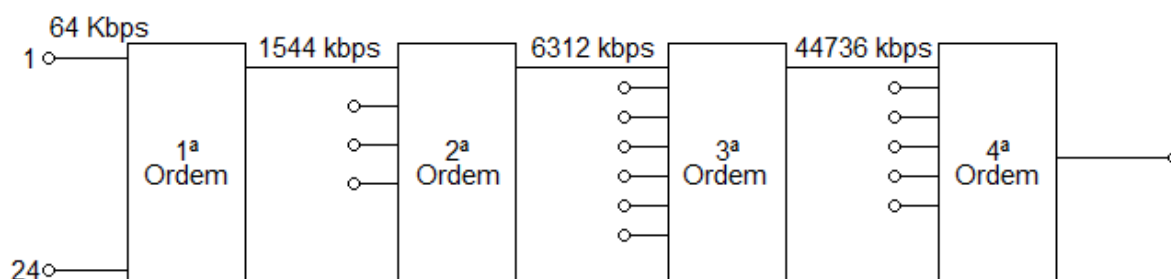


Fonte: NETO e NETO (2002)

A figura 1 demonstra a hierarquia PCM europeia e mostra que existem 30 canais de 64 Kbps na primeira ordem segundo o autor, porém se realizar os cálculos de quantidade de canais pela quantidade de Kbps por canal chega-se no resultado 1920 que é inferior ao valor de 2048. Para justificar isso foi verificado no padrão G.704 que os canais são numerados de 0 a 31 (INTERNATIONAL TELECOMMUNICATION UNION, 1998, p. 29), ou seja, 32 canais, porém o *timeslot* (canal) 0 é usado para a mensagem do estado de sincronização (INTERNATIONAL TELECOMMUNICATION UNION, 1998, p. 14) e o canal 16 pode ser usado para a sinalização. Caso não exista uma necessidade para a sinalização, o canal 16 pode ser usado como um canal de 64 kbit/s do mesmo jeito como um *timeslot* do 1 ao 15 e do 17 ao 31 (INTERNATIONAL TELECOMMUNICATION UNION, 1998, p. 30).

Já o padrão Americano conforme figura 2 e quadro 4 em todas as ordens não tem os valores corretos quando se multiplica pelo número de canais que são 24 no total com capacidade de 64 kbit/s ou pela ordem anterior, isso ocorre conforme a *International Telecommunication Union* (ITU-T) pela sinalização ocorrer de dois métodos alternativos recomendados denominados como sinalização de canal comum (*Common Channel Signalling*) e a sinalização de canal associado (*Channel Associated Signaling*) (INTERNATIONAL TELECOMMUNICATION UNION, 1998, p. 22). Não será explicado em detalhes como são feitas as duas sinalizações devido à complexidade do tema e por não ser aplicado essa teoria nesse trabalho, já que como dito no início desse capítulo o Brasil determinou usar o padrão Europeu.

Figura 2 - Ilustração do PDH americano.



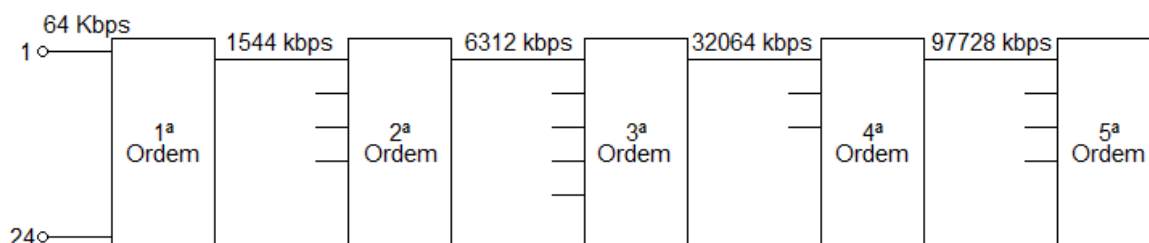
Fonte: NETO, NETO (2002)

Quadro 4 - Velocidade das portas PDH americano.

Padrão Americano	
T1/DS1	1544 kbps
T2/DS2	6312 kbps
T3/DS3	44736 kbps
T4/DS4	274176 kbps

Fonte: NETO, NETO (2002)

O padrão japonês segue inicialmente a mesma ideia do americano, com diferenças nos valores a partir da 3ª ordem. Esse trabalho também não se aprofundará no sistema japonês já que o Brasil decidiu adotar o padrão Europeu.

Figura 3 - Ilustração do PDH japonês

Fonte: NETO, NETO (2002)

Quadro 5 - Velocidade das portas do PDH japonês

Padrão Japonês	
J1	1544 kbps
J2	6312 kbps
J3	32064 kbps
J4	97728 kbps
J5	390912 kbps

Fonte: NETO, NETO (2002)

2.2 SDH/SONET

SDH e o SONET (*Synchronous Optical Network*) definem um padrão para aumentar a confiabilidade da rede, para administração da rede e definir métodos para as multiplexações síncronas dos sinais digitais como DS-1 e DS-3, definir um conjunto de padrões genéricos de equipamentos/operações e arquitetura flexível (BEASLEY; NILKAEW, 2012, p. 136). O SDH está especificado na ETSI (*European Telecommunication Standard Institute*) pelo padrão ETS 300 147 e também na ITU-T

como padrão G.707 e o SONET é um conjunto de normas da ANSI (*American National Standards Institute*).

O SONET pode carregar a hierarquia PDH norte americana que tenha a velocidade 1,5/6/45 Mbps, mais o 2 Mbps (E1 do PDH Europeu). O padrão SDH original determina o transporte de 1,5/2/6/34/45/140 Mbps em uma taxa de transmissão de 155,52 Mbps e está sendo desenvolvido para carregar outros tipos de tráfico, como ATM (*Asynchronous Transfer Mode*) e IP, em taxas que são múltiplos de 155,52 Mbps.

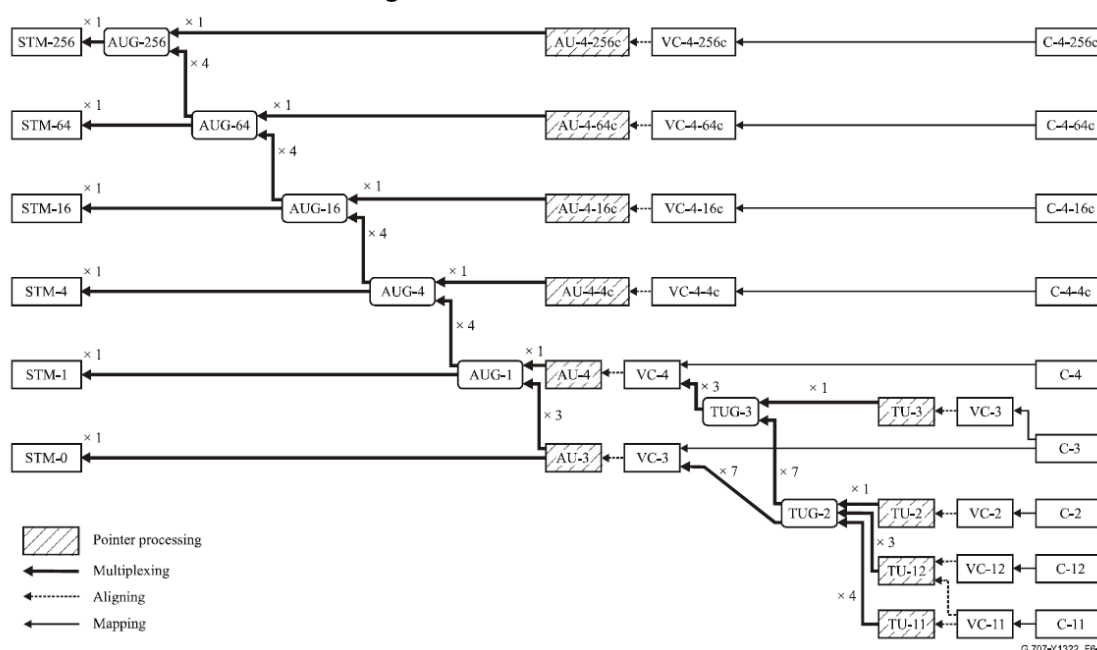
O padrão SDH conforme o padrão G.707 da International Telecommunication Union (2008, p.7) afirma que a relação entre vários elementos de multiplexação é definida pelo quadro 6, ou seja a comunicação é realizada através de contêineres virtuais com outros elementos. A figura 4 mostra a estrutura de multiplexação.

Quadro 6 - Velocidade dos VCs no SDH.

Tipo de VC	Banda de VC	Carga útil do VC
VC-11	1664 kbit/s	1600 Kbit/s
VC-12	2240 kbit/s	2176 kbit/s
VC-2	6848 kbit/s	6784 kbit/s
VC-3	48960 kbit/s	48384 kbit/s
VC-4	150336 kbit/s	149760 kbit/s
VC-4-4c	601344 kbit/s	599040 kbit/s
VC-4-16c	2405376 kbit/s	2396160 kbit/s
VC-4-64c	9621504 kbit/s	9584640 kbit/s
VC-4-256c	38486016 kbit/s	38338560 kbit/s

Fonte: ITU-T (2008, p. 7)

Figura 4 - Estrutura do sistema SDH.



Fonte: ITU-T (2008, p.8)

Conforme o padrão G.780 da International Telecommunication Union (2010, p.12) o STM (módulo de transporte síncrono) é a estrutura da informação usada para suportar a camada de sessão no modelo OSI (*Open System Interconnection*) no SDH. Ele consiste nos dados da informação e os campos de informação da seção de *overhead* (SOH) organizados em uma estrutura de bloco de *frame* que se repete a cada 125 μ s. O STM como base tem 155520 Kbit/s sendo denominado como um STM-1, sendo que o STM-N pode ser definido como $N=4$, $N=16$, $N=64$ e $N=256$ sendo o N um multiplicador que deve ser aplicado ao valor do STM-1. O STM-0 é a representatividade de um grupo de unidade administrativa de nível 3 (AUG-3).

O grupo de unidade administrativa (AUG) também é definido no padrão G.780 da International Telecommunication Union (2010, p. 3) e é uma ou mais unidades administrativas (AU) ocupando fixadas e definidas posições nos dados do STM. No grupo de unidade administrativa 1 (AUG-1) devem ter grupos homogêneos de AU-3 ou AU-4 obrigatoriamente.

A unidade administrativa (AU) é a estrutura de informação a qual provê adaptação entre uma camada de maior ordem e a camada de seção de multiplexação. Ela consiste nos dados da informação (a maior ordem do contêiner virtual) e uma unidade de ponteiro administrativo o qual indica o início dos dados de

um determinado frame (INTERNATIONAL TELECOMUNICATION UNION, 2010, p. 3).

Um virtual contêiner (VC) é a estrutura de informação usada para suportar a camada de conexão de caminhos no SDH e pode ser dividida em baixa e alta ordem, sendo que a de baixa ordem compreende um contêiner apenas e o de alta podem aceitar vários grupos de tributário (INTERNATIONAL TELECOMUNICATION, 2010, p. 13).

A unidade de grupo de tributários (TUG) são uma ou mais unidades de tributários (TU), ocupando de forma homogênea, fixa, posições definidas por um virtual contêiner de alta ordem (INTERNATIONAL TELECOMUNICATION UNION, 2010, p. 13). São divididas entre TUG-2 que consiste de grupos idênticos de TU-11, TU-12 ou TU-2 e TUG-3 que consiste de grupos idênticos de TUG-2 ou uma TU-3.

A unidade de tributário (TU) é uma estrutura que provê adaptação entre a camada de caminho de baixa ordem e o de alta do contêiner virtual (INTERNATIONAL TELECOMUNICATION UNION, 2010, p. 13). E por fim existe o contêiner (C) que é a estrutura da informação que forma a informação da rede síncrona para um contêiner virtual (VC).

No SONET o padrão T1.105 da American National Standards Institute (2001, p.12) define o sinal básico modular como o sinal síncrono de transporte nível 1 (STS-1 *Synchronous Transport Signal level 1*). A contraparte ótica do STS-1 é a portadora ótica de nível 1 (OC-1 *optical carrier*), que é o resultado de uma conversão ótica direta do STS-1 depois do embaralhamento de frames (ANSI). Logo após existem os níveis superiores da portadora ótica (OC) e sinal síncrono de transporte (STS). Os valores desses estão definidos quadro 7.

Quadro 7 - Divisão de velocidade do OC e STS.

Nível OC	Nível STS	Termo SDH	Taxa de transmissão (Mbit/s)
OC-1	STS-1		51,840
OC-3	STS-3	STM-1	155,520
OC-12	STS-12	STM-4	622,080
OC-24	STS-24		1244,160
OC-48	STS-48	STM-16	2488,320
OC-192	STS-192	STM-64	9953,280
OC-768	STS-768	STM-256	39813,12

Fonte: ANSI (2001).

No SONET tem os tributários virtuais que são definidos pela American National Standard Institute (2001, p.13) como uma estrutura designada para transporte e comutação de carga sub STS-1, ou seja, eles fazem parte do STS-1, os valores de cada VT foram definidos no quadro 8 assim como o seu correspondente na rede SDH.

Quadro 8 - Divisão de velocidade do VT.

Nível VT	Termo SDH	Taxa de transmissão
VT1.5	VC-11	1728
VT2	VC-12	2304
VT3		3456
VT6	VC-2	6912

Fonte: ANSI (2001)

2.3 ATM

A rede de transporte ATM é constituída em camadas sendo elas a camada de rede VC (*Virtual Channel*), adaptação VC para VP (*Virtual Path*), a camada de rede VP e a adaptação VP para a camada de transporte (INTERNATIONAL TELECOMMUNICATION UNION, 2003, p.1). A célula do ATM contém 53 octetos consistindo de 5 octetos de cabeçalho e 48 octetos de informação (INTERNATIONAL TELECOMMUNICATION UNION, 2003, p. 3). O cabeçalho consiste em VCI e VPI que são dois identificadores sendo um para canal e outro para o caminho. O VCI é o identificador de uma camada de rede denominada canal virtual (VC) e o VPI é o identificador de camada de caminho denominado caminho virtual (VP).

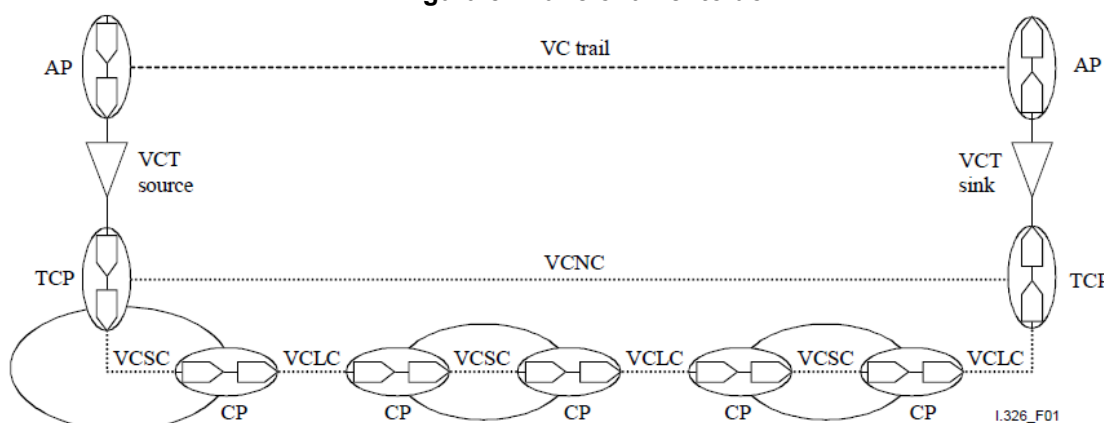
A camada de rede VC provê o transporte da informação em um caminho do canal virtual entre os pontos de acesso que contém um não contínuo fluxo de 48 octetos mais um bit. A característica principal é o fluxo não contínuo da informação adaptada e informação F5 OAM (INTERNATIONAL TELECOMMUNICATION UNION, 2003, p. 4).

Na figura 5 demonstra-se a ação do VC entre dois *access point* (AP) tendo a seguinte função de processamento de transporte e entidades de transporte (INTERNATIONAL TELECOMMUNICATION UNION, 2003, p. 4):

- Caminho de VC (VC trail);

- Terminação do caminho de VC na origem (VCT source): gera o F5 ponto a ponto das células OAM;
- Terminação do caminho de VC no destino (VCT sink): gera o F5 ponto a ponto das células OAM;
- VC conexão de rede (VCNC);
- VC conexão de vínculo (VCLC);
- VC conexão de sub-rede (VCSC);

Figura 5 - Funcionamento do VC.



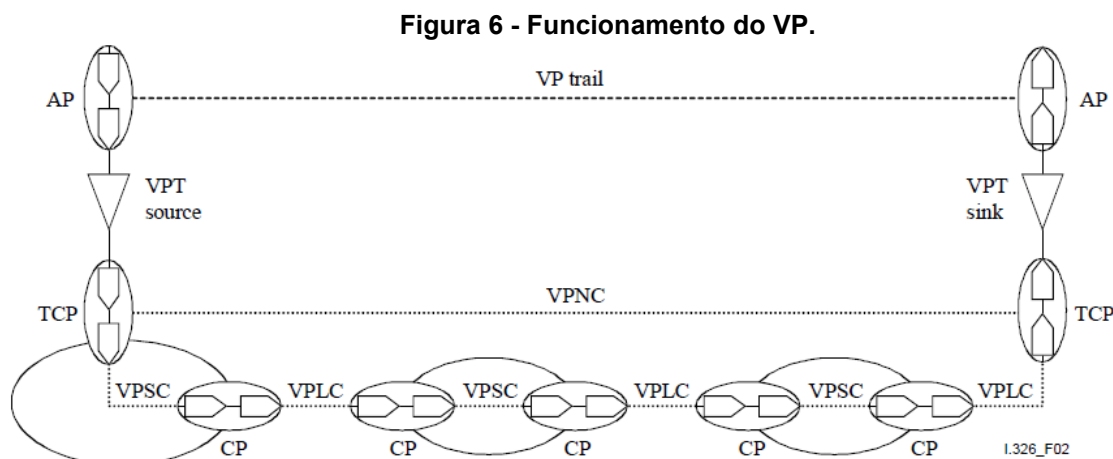
Fonte: International Telecommunication Union (2003)

A camada de rede VP provê o transporte da informação adaptada através de um caminho VP entre os pontos de acesso (AP) que contém um não contínuo fluxo da camada de rede VC mais o identificador (VCI) e o EFCI (indicador explícito de congestionamento a frente) nos campos de cabeçalho. A característica principal é o fluxo não contínuo da informação adaptada e informação F4 OAM (INTERNATIONAL TELECOMMUNICATION UNION, 2003, p.4).

Na figura 6 demonstra a ação do VP entre dois access point (AP) tendo a seguinte função de processamento de transporte e entidades de transporte (INTERNATIONAL TELECOMMUNICATION UNION, 2003, p.5):

- Caminho de VP (VP trail).
- Terminação do caminho de VP na origem (VPT source): gera o F4 ponto a ponto das células OAM.
- Terminação do caminho de VP no destino (VPT sink): gera o F4 ponto a ponto das células OAM.
- VC conexão de rede (VPNC);

- VC conexão de vínculo (VPLC);
- VC conexão de sub-rede (VPSC);



Fonte: International Telecommunication Union (2003)

Em uma rede ATM existem dois tipos de conexão, SVC (Switched Virtual Circuit) e PVC (Permanent Virtual Circuit). O SVC opera como uma chamada de telefone de voz convencional. Um equipamento se comunica com seu switch ATM para requisitar que o switch estabeleça o SVC, o equipamento espera pela rede ATM criar o circuito e por fim o computador remoto deve aceitar o circuito virtual (BAGAD; DHOTRE, 2008, p.55). O PVC ocorre quando um administrador interage com os switches em uma rede ATM para configurar um circuito virtual manual e o mesmo especifica a origem e o destino de um circuito (BAGAD, DHOTRE, 2008, p.56).

A velocidade do ATM é definido pela *ATM Forum Specifications* nas especificações do grupo “*af-phy*” as quais definem as interfaces aceitas e que podem ser compatíveis com a tecnologia ATM. O padrão *af-phy-0017.000* especifica a velocidade de 155 Mbps e 622 Mbps e as interfaces SONET OC-3c, 8B/10B block coded, 4B/5B TAXI, DS-3 e OC-1. O padrão *af-phy-0034.000* define o uso do ATM com E3. O padrão *af-phy-0039.000* oficializa o uso do OC-12 no ATM. O padrão *af-phy-0064.000* define o uso de E1 com o ATM. O padrão *af-phy-0136.000* permite o uso do ATM com OC-12, OC-48 e interfaces Gigabit. Por fim o padrão *af-phy-0144.001* e *af-phy-0133.001* especifica o uso do OC-96, STM-4, STM-16 e STM-64.

As classes de serviço ATM devem ter uma taxa de transmissão desejada para cada tipo de tráfego e deve ser compatível com a classe de serviço apropriada

(MCQUERRY; MCGREW; FOY, 2001, p. 308), sendo elas:

VBR (*Variable Bit Rate*): É uma classe que tem provisões para passar o tráfego em tempo real, como voz e vídeo (incluindo videoconferência) e é adequado para garantir um certo nível de serviço (MCQUERRY, MCGREW; FOY, 2001, p. 308). Pode ser VBR-rt que é usado para conexões que requerem uma relação de tempo fixo entre amostras e VBR-nrt que não é usado em conexões no qual não há um tempo fixo entre amostras, mas que ainda necessita um QOS (*Quality of Service*) garantido (MCQUERRY; MCGREW; FOY, 2001, p. 308).

CBR (*Constant Bit Rate*): Funciona igual ao VBR com a diferença que permite a configuração de uma quantidade de banda, a latência na conexão ponto-a-ponto, e variação de demora para ser especificado durante uma configuração de chamadas (MCQUERRY; MCGREW; FOY, 2001, p. 308).

ABR (*Available Bit Rate*): É designado tendo como tráfego de rajada em mente e é mais adequada para aplicações de dados (MCQUERRY; MCGREW; FOY, 2001, p. 308).

UBR (*Unspecified Bit Rate*): Funciona similarmente ao ABR com a particularidade que não garante a entrega do tráfego de dados (MCQUERRY; MCGREW; FOY, 2001, p. 308).

2.4 ETHERNET

O padrão *Ethernet* é baseado no documento IEEE 802.3 tendo as seguintes sub-divisões:

802.3u: Padrão *Fast Ethernet* com limite de 100 Mb/s.

802.3z: Padrão *Gigabit Ethernet* com limite de 1000 Mb/s.

802.3ae: Padrão 10 *Gigabit Ethernet* com limite de 10 Gb/s.

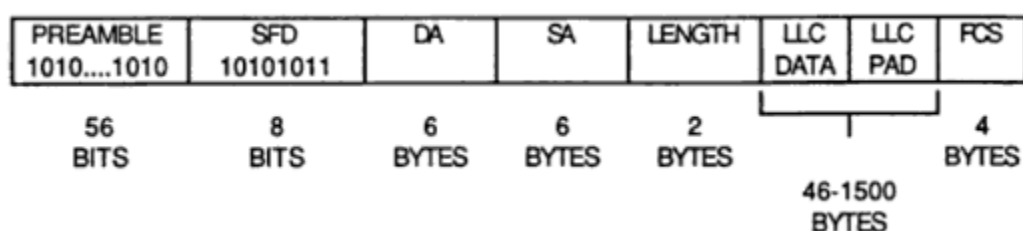
802.3ba: Padrão 40 *Gigabit Ethernet* e 100 *Gigabit Ethernet* com limite de 40 Gb/s e 100Gb/s.

O padrão *Ethernet* IEEE 802.3 reside dentro da camada 1 (Física) e camada 2 (dados) das sete camadas do modelo ISO/OSI (FROEHLICH; KENT, 1995, p.4). Um nó *Ethernet* normalmente é definido pela norma 802.3 IEEE como equipamento terminal de dados (*Data Terminal Equipment* - DTE). O padrão *Ethernet* é construído baseado em pacotes LAN (*Local Area Network*) no protocolo de acesso CSMA/CD (Acesso múltiplo com verificação de portadora com detecção de colisão),

esta é a base que qualquer nó *Ethernet* determina se é permitido transitar sobre o meio compartilhado. A subcamada Controle de Acesso de Meio (MAC) é responsável pela execução do protocolo CSMA/CD (FROEHLICH; KENT, 1995, p.4)

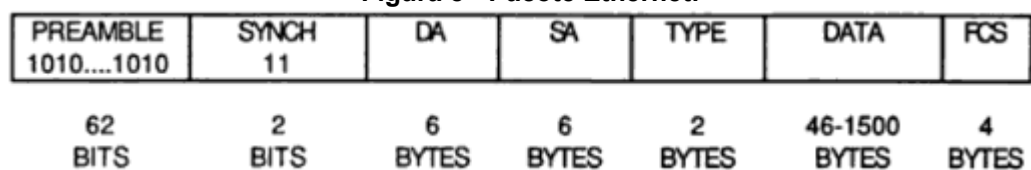
O pacote ethernet/802.3 tem esses frames em sua composição conforme figura 7 (IEEE 802.3) e figura 8 (*Ethernet*), onde o pacote do padrão 802.3 tem os campos preâmbulo, delimitador inicial do frame (SFD, endereço de destino, endereço de origem, tamanho, LLC e campo que verifica a sequência do frame.

Figura 7 – Pacote Ethernet 802.3



Fonte: Froehlich, Kent (1995 p.7)

Figura 8 - Pacote Ethernet.



Fonte: Froehlich, Kent (1995, p.8)

No pacote ethernet o campo preambulo é um campo de 7 octetos que provê uma única frequência (5 mega-hertz (MHz)) no início de cada pacote de rede, o qual permite o receptor “travar” o fluxo de bits de entrada (FROEHLICH; KENT, 1995, p. 7). Isso significa que esse campo serve para realizar o sincronismo entre os dois pontos. O autor (FROEHLICH; KENT, 1995, p. 8) afirma que é usado o codificador/decodificador Manchester para travar o fluxo de bit recebido e permitir a decodificação de dados.

O campo SFD (*Start Frame Delimiter*/Delimitador Inicial do Frame) do 802.3 é definido como um byte com o padrão 1, 0, 1, 0, 1, 0, 1 e 1. O preambulo mais a indicação do início do frame são 64 bits e é de um padrão idêntico, para que uma função MAC idêntica possa negociar os pacotes (FROEHLICH; KENT, 1995, p. 9).

O DA (*Destination Address*/Endereço de destino) é usado pelo MAC recebido para determinar se este pacote recebido é endereçado para este nó em

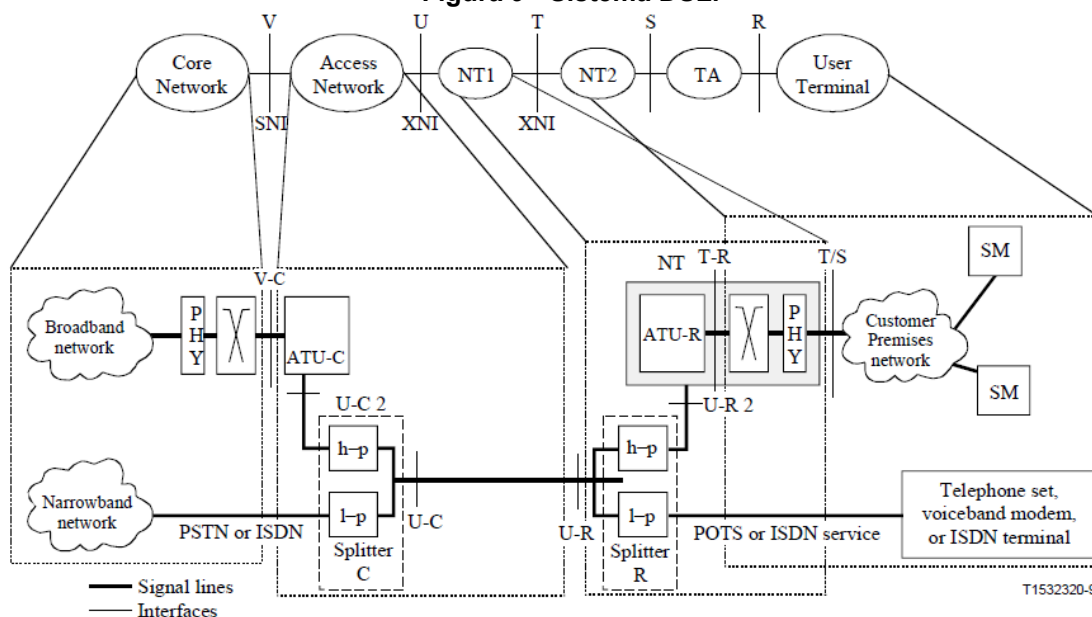
particular (FROEHLICH; KENT, 1995, p. 8), três tipos de endereçamento são aceitos: individual, *multicast* e *broadcast*. O campo SA (*Source Address/Endereço de origem*) é fornecido pelo transmissor do MAC, o qual insere o seu próprio endereço único dentro desse campo como o frame transmitido, indicando que foi a estação originadora (FROEHLICH; KENT, 1995, p. 8).

O campo *length* (tamanho) indica o número de bytes de dados (excluindo blocos de caracteres) que estão somente no campo de dados (excluindo o campo FCS) (FROEHLICH; KENT, 1995, p. 10). O campo data (dados) contém os atuais dados do frame que estão sendo transferidos, e o tamanho é de entre 46 e 1500 bytes. A função LLC é responsável por fragmentar dados em tamanhos de bloco adequados para transmissão sobre a rede (FROEHLICH; KENT, 1995, p. 9). O último campo é o FCS (*Frame Check Sequence/Verificador de sequência de quadros*) é um campo de quatro bytes que contém o verificador cíclico de redundância (CRC) do quadro inteiro (FROEHLICH; KENT, 1995, p.9).

2.5 ADSL

O sistema ADSL (*assymetrical digital subscriber line*) usa a linha telefônica de cobre existente para entregar um serviço de banda larga às casas (PAGANI, 2009, p. 169). Conforme a figura 9, retirada do padrão G.992 ocorre uma interligação entre a rede banda larga (*broadband - internet*) ou banda estreita (*narrowband - telefonia*). Na estação vai ter o filtro passa baixa e filtro passa alta que irá juntar o sinal de voz e de dados em duas frequências diferentes e o ATU-C (ADSL *Transceiver Unit* que fica na central) e no cliente terá o filtro passa alta e passa baixa, um deles vai até o ATU-R (ADSL *Transceiver Terminal* que fica no terminal remoto).

Figura 9 - Sistema DSL.



Fonte: International Telecommunication Union (p. 2, 1999)

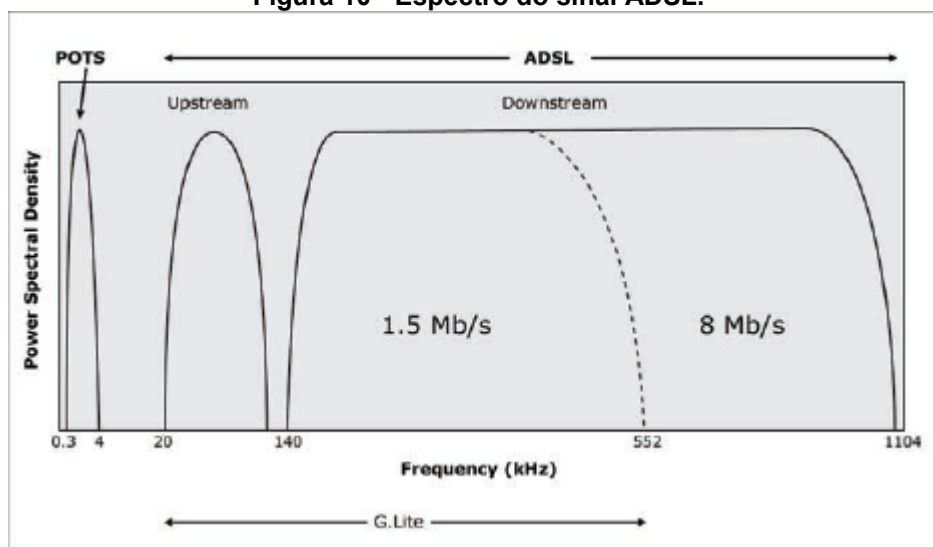
O ADSL faz parte de uma família de tecnologia denominada DSL e todo DSL requer um modem especial nas instalações do usuário, e um multiplexador de acesso DSL (DSLAM) na central da operadora (PAGANI, 2009, p. 150). As velocidades alcançadas por cada tecnologia DSL seguem no quadro 9.

Quadro 9 - Velocidades dos padrões ADSL.

Padrão	Nome	Velocidade Upstream (Mbps)	Velocidade Downstream (Mbps)
ITU-T G.961	IDSL-IDSN	0,160	0,160
ITU-T G.991	HDSL	1,544	1,544
ITU-T G.992.1	ADSL	1	8
ITU-T G.992.4	ADSL2	1	8
ITU-T G.992.4 Annex J	ADSL2	3,5	12
ITU-T G.992.5	ADSL2+	1	24
ITU-T G.992.5 Annex M	ADSL2+	3,5	24
ITU-T G.993.1	VDSL	26 / 12	26 / 52
ITU-T G.993.2	VDSL2	100	100

Fonte: PAGANI (p.150, 2009)

Figura 10 - Espectro do sinal ADSL.



Fonte: Pagani (p.554, 2009)

A figura 10 demonstra o ADSL em sua divisão espectral no par, que funciona de forma analógica, usando a frequência 0,3 kHz a 4 kHz para a linha telefônica ou POTS (*plain old telephone service*), 20 a 140 para *upstream* e 140 a 1104 para *downstream*. O G.Lite, segundo Pagani (2009, p. 555) é o método padrão do desenvolvimento do ADSL sem o uso dos *splitters*, reduzindo de 8 Mb/s para 1,5 Mb/s a velocidade.

2.6 PADRÃO V.35

V.35 é um padrão ITU-T que descreve uma camada de protocolo síncrona física usada para comunicação entre um equipamento de rede de acesso e um pacote de rede e é recomendado para velocidades acima de 48 Kbps. (CHIN, 2004, p.27).

A banda base do sinal deve ser traduzida para a banda 60-104kHz com uma portadora de banda lateral assimétrica suprimida AM de 100 kHz (TUGAL; TUGAL, 1989, p. 121).

As trocas de informação desse circuito são mostradas no quadro 10:

Quadro 10 - Sinalização do V35.

Número	Função
101	Quadro Terra
102	Sinal terra ou retorno comum.

103	Dado transmitido.
104	Dado recebido.
105	Requisitado para enviar.
106	Pronto para enviar.
107	Conjunto de dados pronto.
108	Dados do terminal prontos.
109	Portadora de dados detectado.
113	Tempo de transmissão do elemento de sinal
114	Elemento transmissor de sinal de tempo.
115	Elemento receptor de sinal de tempo.
125	Indicador de Toque

Fonte: Clark, 2003

No caso, a fabricante do modem deve ter no aparelho essas numerações e suas iluminações demonstrando se existe alguma falha.

2.7 X.25

O X.25 é um padrão ITU-T padronizado em 1976 e atualizado em 1996. Aceita a interface física X.21, X.21 bis, série V e X.31 que estarão em um DTE (*Data Terminal Equipment*) e DCE (*Data Circuit-Terminating Equipment*) antes da entrada da placa com suporte a X.25 na gerência selecionada.

Os LAPB (*Link Access Procedures*) são descritos como um elemento da camada de dados e são usados para intercâmbio de dados entre o DCE e o DTE em cima de um ou múltiplos circuitos físicos (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p. 4) sendo sinalizado se um ou múltiplos através dos procedimentos SLP (*Single Link Procedures*) e MLP (*Multilink Procedure*).

O quadro tem o seguinte aspectos:

- Campo *Flag*: São o primeiro e o último Byte e devem iniciar com a sequência de um bit 0 seguidos de 6 bits 1 e um último bit 0 (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p. 5).
- Campo *Address*: Esse campo identifica o receptor pretendido de um quadro de comando e o transmissor de uma resposta (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p.7).
- Campo *Control*: Três tipos são usados sendo o de transferência de

informação numerada (Formato I), a função de supervisão numerada (Formato S) e função de controle inumerada (Formato U) (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p. 10).

- Campo *Information*: Os dados que se deseja trafegar.
- Campo FCS: Campo para fazer a averiguação de CRC.

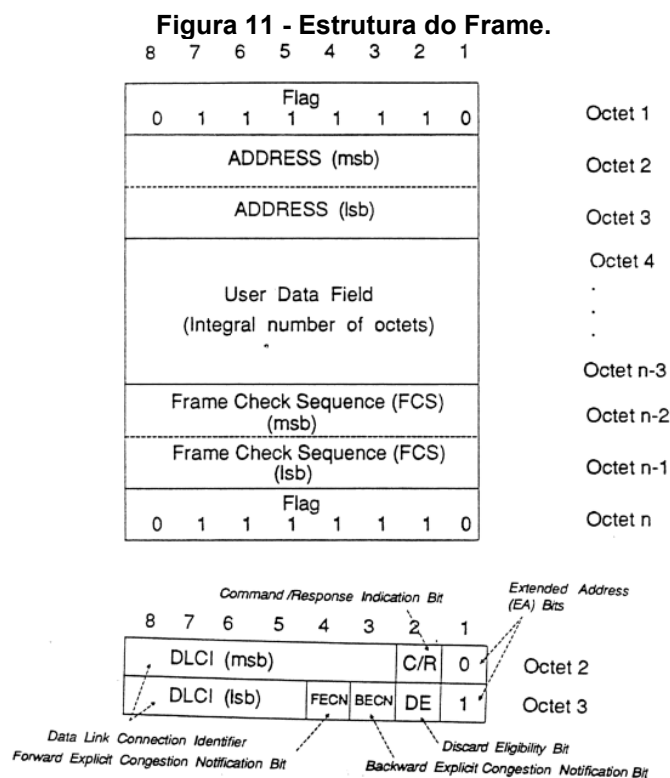
2.8 FRAME RELAY

O Frame relay é uma importante tecnologia na comunicação WAN baseado no protocolo ISDN-LAPD e suporta multiplexação dentro da camada 2. (Swee, 1991, p. 393). A figura 11 ilustra a estrutura do frame, onde:

- *Flags*: Esses são usados para identificar o início e o fim de cada frame (IGI CONSULTING, 1991, p. 14)
- *Address* (Endereços): Esses contêm os seguintes elementos:
 - Data Link Connection Interface (DLCI): Um endereço de 10 bits usado pelos equipamentos da rede frame relay para rotear quadros através da rede. A DLCI não é o endereço de uma origem particular ou destino; ele especifica uma conexão, ou um circuito virtual na rede (IGI CONSULTING, 1991, p. 2 - 14)
 - *Forward Explicit Congestion Notification Bit* (FECN), *Backward Explicit Congestion Notification Bit* (BECN) e *Discard Eligibility Bit* (DE): Estes todos são incluídos no formato de quadro básico para permitir usuários implementarem a função de gerência de congestionamento de rede opcional (IGI CONSULTING, 1991, p. 2 - 16)
 - *The Extended Address bits*: Esses são usados para indicar se o campo endereço irá ser dois, três ou quatro maiores, que são também permitidos pela norma. Endereços estendidos devem permitir DLCI's maiores que 10 bits, fazendo possível o aumento do total de circuitos virtuais em uma rede. (IGI CONSULTING, 1991, p. 2 - 16)
 - C/R: É uma reserva para outros propósitos no qual o formato do quadro foi designado, e é ignorado no frame relay (IGI CONSULTING, 1991, p. 2 - 16)
- *User Data Field* (Campo de dados do usuário): Este campo contém a informação atual que está sendo transmitida por uma das pontas para outra

através da rede frame relay (IGI CONSULTING, 1991, p. 2 - 16)

- *Frame Check Sequence (FCS)*: Este é usado para verificar a integridade do frame, usando a técnica de checagem de redundância cíclica (CRC) (IGI CONSULTING, 1991, p. 2 - 17).



Fonte: IGI Consulting, 1991

Pode ser PVC (*permanent virtual circuit*) que é uma conexão que é disponível todo o tempo através da nuvem *frame relay* de um ponto a outro ponto (MCQUERRY; MCGREW; FOY, 2001, p. 254) ou SVC (*Switched Virtual Circuit*) onde a banda não é disponível quando não é necessária (MCQUERRY; MCGREW; FOY, 2001, p. 254).

Para que o frame relay funcione, outro ponto importante é a necessidade de escolher como vai ocorrer o gerenciamento dessa rede, para isso pode-se determinar se ele vai ocorrer e como:

- LMI (*Local Management Interface*): Provê o usuário com estado e informação de configuração relativa as DLCIs disponível nesta interface (SREETHARAN; SUBRAMANIAM, 2002, p. 50).
- UNI (*User Network Interface*): Define a interface entre equipamentos Frame Relay, por exemplo, uma na interface nas instalações do cliente e outro na

central (SREETHARAN; SUBRAMANIAM, 2002, p. 52).

- NNI (*Network-to-Network Interface*): Define como duas diferentes redes Frame Relay devem comunicar (SREETHARAN; SUBRAMANIAM, 2002, p. 52).

2.9 INTERNET PROTOCOL (IP)

O IP gerencia a transmissão do roteamento de rede do transmissor para o receptor, junto com problemas relacionados da rede e endereços de computador (PYLES; CARREL; TITTEL, 2016, p.2). O protocolo IPv4 usa endereços de 32 bits que chega a ter 3 bilhões de endereços que são usados na Internet pública, porém foi usado a exaustão então o IPv6 foi criado. Já o IPv6 suporta endereços de 128 bits que chega a ter $3,4 * 10^{38}$ endereços públicos.

O IPv4 é um endereço que consiste em 4 *bytes*, onde cada *byte* tem 8 bits e um bit tem 2 valores possíveis sendo 1 e 0. O intervalo de um byte tem o intervalo de valores decimais possíveis de 0 a 255. No IPv4 existe a máscara de subrede, que define a quantidade de IP que uma rede pode ter, sendo que o primeiro endereço dessa faixa é o endereço de rede e o último é o broadcast que é um endereço que envia um pacote de dados para todos os IP's daquela faixa. A máscara de subrede é definida como a sequência de bits em 1 da esquerda para a direita até a sequência 0 que vai até o final do endereço, sendo o 1 a rede e 0 para os endereços referentes aos computadores e endereços especiais. O exemplo abaixo demonstra uma máscara de rede, um endereço especial de rede e um endereço qualquer.

11111111.11111111.11111111.00000000 = 255.255.255.0

11000000.10101000.00110100.00000000 = 192.168.52.0

11000000.10101000.00110100.01100100 = 192.168.52.100

Se usar a operação “e” lógico entre uma máscara de rede e um endereço de rede o resultado será o endereço de rede. Se usar o operador “condicional” ou “implicação” entre a máscara de subrede e o endereço IP existirá o endereço de *broadcast*. Tanto o endereço de rede como o endereço de *broadcast* são endereços reservados. O endereço de rede identifica um grupo de IPs que pertencem a tal rede que compreende ele até o endereço de *broadcast*. O endereço de *broadcast* é

usado para enviar um pacote em todos os endereços da rede.

Outra notação existente para a combinação de endereço de rede é a CIDR (*Classless Inter-Domain Routing in IPV4*) que ignora a tradicional classe A, B e C designações para os endereços IPv4 e insere o laço de ID de rede-computador onde ele quer, do jeito que simplifique o roteamento através dos espaços de endereços IPs resultantes (PYLES; CARREL; TITTEL, 2016, p.61). Essa notação funciona contando a quantidade de bits 1 na máscara de rede junto com uma barra (\) antes do resultante após o endereço de rede. Exemplo:

11111111.11111111.11111111.00000000 = 255.255.255.0

11000000.10101000.00110100.00000000 = 192.168.52.0

Notação CIDR: 192.168.52.0/24

As classes IPv4 nomeadas A, B e C não são mais usadas e foram substituídas pela notação CIDR, e as operadoras não as usam.

O IPv6 é um endereço de 128 bits sendo expressado em hexadecimal, sendo divididos em 8 blocos pelo símbolo dois pontos (:), podendo ser chamado também de palavras, de quatro caracteres cada, dividido por dois pontos tendo 32 valores hexadecimal sendo determinados de 0 a F, A equivale ao 10, B equivale ao 11 e assim sucessivamente.

Em endereços IPv6 os prefixos de rede são escritos do mesmo modo que no IPv4, utilizando a notação CIDR (ipv6.br). Uma diferença é o uso do símbolo de dois pontos duas vezes seguidas (::) que pode ser usado uma única vez para evitar ambiguidades com o fim de ocultar muitos zeros seguidos. Exemplo:

Endereço completo: 2001:db8:800e:50:0000:0000:0000:20

Endereço simplificado: 2001:db8:800e:50::20

Endereço de rede: 2001:db8:800e:50::/64

Como verificado no exemplo, o endereço de rede também pode ser abreviado usando o símbolo dois pontos duas vezes (::). No IPv6 não existe mais o endereço *broadcast*, porém surgem nativamente os endereços “*anycast*” e “*multicast*”. As definições de “*Anycast*” identifica um conjunto de interfaces e ocorre quando um pacote encaminhado a um endereço *anycast* é entregue à interface

pertencente a este conjunto mais próximo da origem (ipv6.br). “*Multicast*” também identifica um conjunto de interface. Entretanto, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. O endereço “*Anycast*” é usado para balanceamento e redundância e pode ser usado qualquer endereço IPv6 (desde que não seja reservado) e o “*Multicast*” no momento está sendo como um substituto do *broadcast* para descoberta de vizinhança através da faixa de endereço ff00::/8.

2.10 FIBRA ÓTICA (GPON)

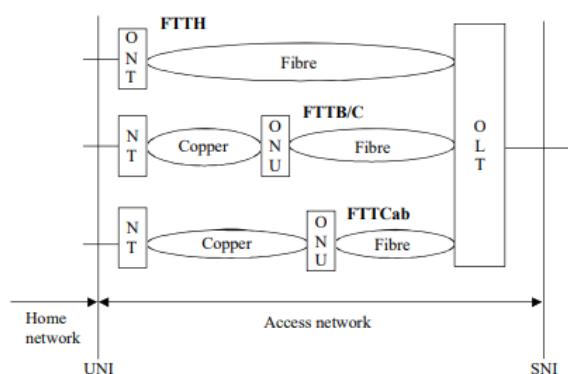
A rede GPON é reconhecida pelo padrão ITU-T G.984 e padrões que estão conectados a ela, sistemas GPON são caracterizados, geralmente, por um sistema de terminação de linha ótica (OLT) e uma unidade de rede ótica (ONU) ou uma terminação de rede ótica (ONT) com uma rede de distribuição ótica passiva (ODN) interconectando eles (INTERNATIONAL TELECOMMUNICATION UNION, 2008, p. 1).

A figura 12 demonstra estrutura da rede GPON e as possibilidades para o acesso:

- O acesso FTTH (*Fibre To The Home*) tem como objetivo prover os serviços de banda assimétricos, simétricos e POTS e ISDN, sendo que esses dois últimos devem habilitados para receber o serviço de telefonia (INTERNATIONAL TELECOMMUNICATION UNION, 2008, p. 5).
- O acesso FTTB/C (*Fibre To The Build/Curb*) pode ser apenas FTTB ou FTTC, o FTTB pode ter um MDU (*Multi-Dwelling Unit*) na topologia, caso isso ocorra o uso ficará semelhante ao FTTH. Caso não ele se tornará um FTTB para negócios que será usado para serviços simétricos, serviços de linha privada e se a rede tiver capacidade POTS e ISDN. O FTTC terá a mesma capacidade do FTTH com a inclusão de se tornar um *backhaul* DSL.
- O FTTCab tem a mesma função que o FTTC.

O termo UNI do GPON tem a mesma definição do Frame-Relay com a diferença que a conexão é realizada entre equipamentos GPON e esse será identificado apenas para o cliente. O SNI (Service Node Interface) é a outra ponta, ou seja, é a interface do provedor.

Figura 12 - Estrutura GPON



Fonte: INTERNATIONAL TELECOMUNICATION UNION, 2008, p.4

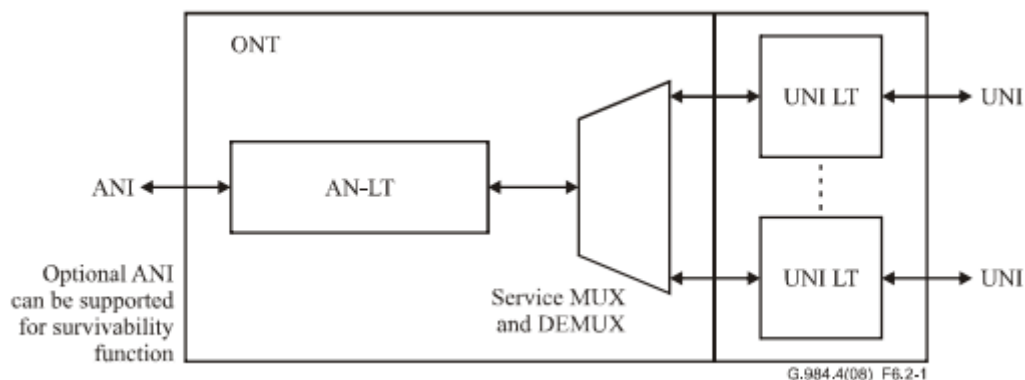
Como uma tecnologia moderna, esse equipamento tem a velocidade maior ou igual a 1.2 Gbit/s, podendo ter a combinação de 1.2 Gbit/s para upload e 2.4 Gbit/s para download ou 2.4 Gbit/s para ambos (INTERNATIONAL TELECOMUNICATION UNION, 2008, p. 7).

A distância máxima logicamente falando é de 60 km, porém a parte física pode ser de até 10 km ou 20 km. É assumido que estes 10 km é a distância máxima para atingir 1,2 Gbit/s ou acima. (INTERNATIONAL TELECOMUNICATION UNION, 2008, p. 7).

Pode ser usado um *Splitter* para dividir o sinal, podendo ser divididos para mais de 64 para a tecnologia atual, de qualquer jeito, antecipando a evolução continua dos módulos ópticos pode passar dos 128. (INTERNATIONAL TELECOMUNICATION UNION, 2008, p. 7).

No caso trabalhado o acesso será feito FTTH onde a ONT trabalhará da forma ilustrada na figura 13, onde a ONT receberá dados do OLT através da UNI e de lá enviará para a ANI (Access Node Interface).

Figura 13 - Estrutura da ONT



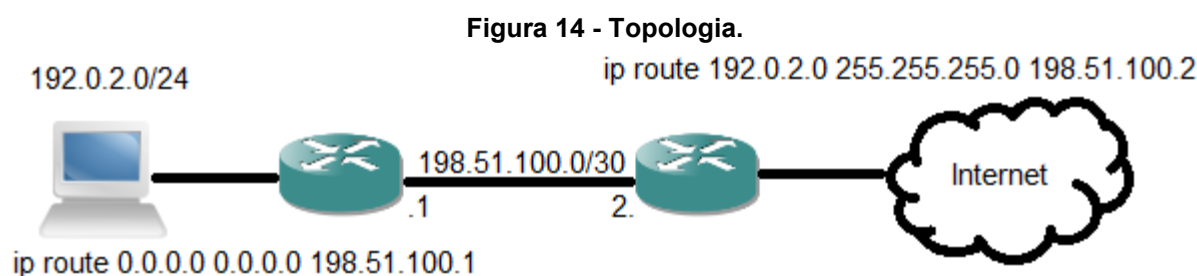
Fonte: INTERNATIONAL TELECOMUNICATION UNION, 2008, p. 11

2.11 PROTOCOLOS DE ROTEAMENTO

As rotas definem o caminho que os pacotes irão percorrer através da rede, conforme os endereços IP.

2.11.1 Rota estática

As rotas estáticas são configuradas manualmente no roteador. Elas não reagem a interrupções de rede, a única exceção é quando a rota estática especifica a interface de saída, se a interface cair, a rota estática é removida da tabela de roteamento (BRUNO; KIM, 2003, p.268). É a rota de mais simples implementação, com normalmente uma linha de código no roteador para realizar a configuração.



Fonte: Autoria Própria

No roteador Cisco por exemplo será usado o comando “*ip route* (rota destino) (máscara de subrede destino) (ip da porta destino)” para definir uma rota estática. Existe também a rota padrão (rota *default*) que sempre terá como parâmetros a rota destino 0.0.0.0 e máscara de subrede destino 0.0.0.0 a qual o roteador irá enviar os pacotes que não estão definidos na tabela de roteamento.

2.11.2 BGP

O protocolo BGP (*Border Gateway Protocol*) tem como função primária prover e trocar informações de acessibilidade de rede entre domínios ou sistemas autônomos (AS) (BRUNO; KIM, 2003, p. 348). Esse protocolo de roteamento é bem complexo de implementação e é usado para muitas aplicações, aqui será aplicado

em rede VPN (*Virtual Private Network*) que é um meio de conectar localizações corporativas quando garantias de banda não são requeridas para suportar tráfego crítico e como um backup acessível para circuitos dedicados (p. 180), ou seja para conectar duas redes corporativas através da *internet* sem que ninguém da *internet* acesse essa rede ou que quem está dentro dessa rede não saia para *internet* através desse link. Uma VPN pode ser várias redes corporativas comunicando entre si ou várias redes corporativas conversando com uma rede concentradora de serviços, mesmo sendo uma rede de longa distância existe um trecho de rede de acesso nessas topologias e nesse documento será tratado apenas esse trecho.

2.11.3 OSPF

O protocolo OSPF é definido como um protocolo de roteamento de estado de link que usa o algoritmo *Dijkstra* de primeiro caminho mais curto (*shortest-path first* – SPF) para calcular os caminhos para o destino (BRUNO; KIM, 2003, p.325). Esse algoritmo é muito usado para solucionar problemas com grafos e na área da ciência da computação em geral. Ele passa por todos os nós de um conjunto finito sendo que cada caminho de passagem receba um valor peso.

O OSPF é dividido por áreas onde cada roteador OSPF em determinada área mantém um banco de dados idêntico descrevendo a topologia da área (BRUNO; KIM, 2003, p.325), e esse conceito mostra que quanto maior a quantidade de equipamentos em uma área, maior é o banco de dados de um roteador. Esse banco de dados ocupa um espaço na memória no equipamento e seu tamanho influencia na velocidade de pesquisa de determinado destino.

Esse protocolo terá aqui como principal uso a implementação de uma metro-ethernet, embora seu uso em conjunto com os demais protocolos de roteamento seja muito abrangente, tanto em redes locais como redes de longa distância.

2.12 TECNOLOGIAS DE VOZ

2.12.1 PSTN

A rede PSTN, segundo Goleniewski (2002, p.111), basicamente inclui telefones, fax e comutadores de circuito que estabelece conexões contínuas, mas

temporárias. É uma rede paralela à rede de computadores onde pode se passar ligações de números telefônicos, normalmente cada telefone é composto por uma quantidade de números decimais tendo os primeiros dígitos a identificação do local ao qual o número pertence e os últimos que são o identificador do usuário.

2.12.2 ISDN

O ISDN, segundo Lee (1997, p. 3), é a habilidade para passar linhas de telefone múltiplas dentro de uma linha sozinha, e por fazer em um formato digital, abrindo a porta para aplicações de dados largos no domínio das chamadas de voz de telefone.

O uso do ISDN se faz necessário quando precisa de um serviço especial como 0800, 0900, 4000, *centrex*, dados e vídeo.

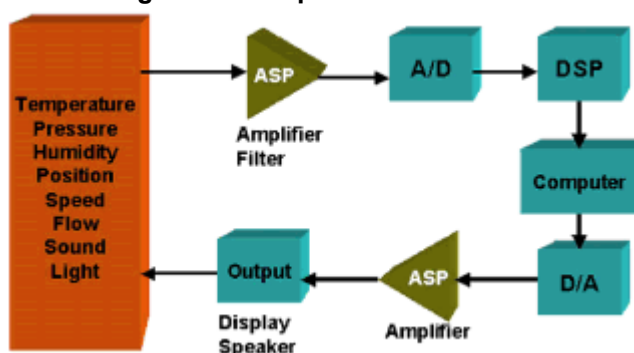
2.12.3 DSP

Essa tecnologia é uma que pode processar desde dados analógicos a temperatura até a voz, que segundo Oshana (2012, p. 1) é o método de processar sinais e dados em ordem para realçar, modificar ou analisar estes sinais para determinar um conteúdo de informação específico. Com essa tecnologia é possível que em um roteador trafegue dados analógicos e possa gerar comunicação entre dois sistemas que usem essa tecnologia.

Nesse documento essa tecnologia irá ser usada para a implementação do VOIP no equipamento Cisco através da tecnologia CUCM (*Cisco Unified Communications Manager*).

Na figura 15 é mostrado o esquema do DSP aonde entra um dado analógico no equipamento ASP que é um filtro amplificador analógico, vai a um conversor analógico digital, chega a um DSP, entra em um computador, que envia o sinal em um conversor digital analógico, entra no amplificador e por fim saí em um dispositivo de saída.

Figura 15 - Esquema DSP



Fonte: Oshana (2012, p. 4)

Outro ponto que é importante ressaltar é que segundo Oshana (2012, p.17) é que o DSP é um sistema normalmente qualificado como um sistema de tempo real rígido, ou seja não tem atrasos o que é ótimo para a implementação do VOIP.

2.12.4 FXS/FXO

Uma interface FXS (*Foreign Exchange Service*), conforme Ellis, Pursell e Rahman (2003, p. 23), é usado para conectar um telefone analógico, máquina de fax, modem ou qualquer outro dispositivo que deve ser conectado em uma linha de telefone. Já a interface FXO (*Foreign Exchange Office*), conforme Ellis, Pursell e Rahman (2003, p. 23), é usado para conectar um sistema de comutação provendo serviços e supervisão, sendo o oposto do FXS.

Essa tecnologia serve para conectar à rede estrangeira como a PSTN com a IP e é usado no VOIP e até no meio de transmissão de operadoras para clientes específicos e que necessitam do serviço, embora o uso no meio de transmissão está ficando sucateado e é usado apenas para clientes antigos que tem exigência contratual.

2.12.5 H.323

O padrão H.323 é um padrão de comunicação produzido pela ITU-T, iniciado no final de 1996 e mira a área emergente de comunicação multimídia sobre LANs (BEKAKOS, GRAVVANIS, ARABNIA, 2006, p. 58). Ele provê funcionalidade de gerência de conferência em áudio e vídeo usando a funcionalidade de sinalização de chamada H.225 e H.245 (BEKAKOS, GRAVVANIS, ARABNIA, 2006, p. 59). Os

protocolos H.225 e H.245 proveem configuração de chamada e transferência de conexão de chamada em tempo real para suportar conferência multiponto de pequena escala (BEKAKOS, GRAVVANIS, ARABNIA, 2006, p. 59).

Essa tecnologia na prática é usada em combinação com outras tecnologias de voz como por exemplo o DSP em roteadores da Cisco, gerando a conversão necessária da rede IP para a sinalização de voz. Isto será visto na prática no tópico 4.4.

O protocolo SIP será responsável para definir como estabelece, realiza manutenção e conclui a sessão de internet incluindo conferências multimídias (BEKAKOS, GRAVVANIS, ARABNIA, 2006, p. 59) e será usado para executar a comunicação com a rede IP.

2.13 QOS E QOE

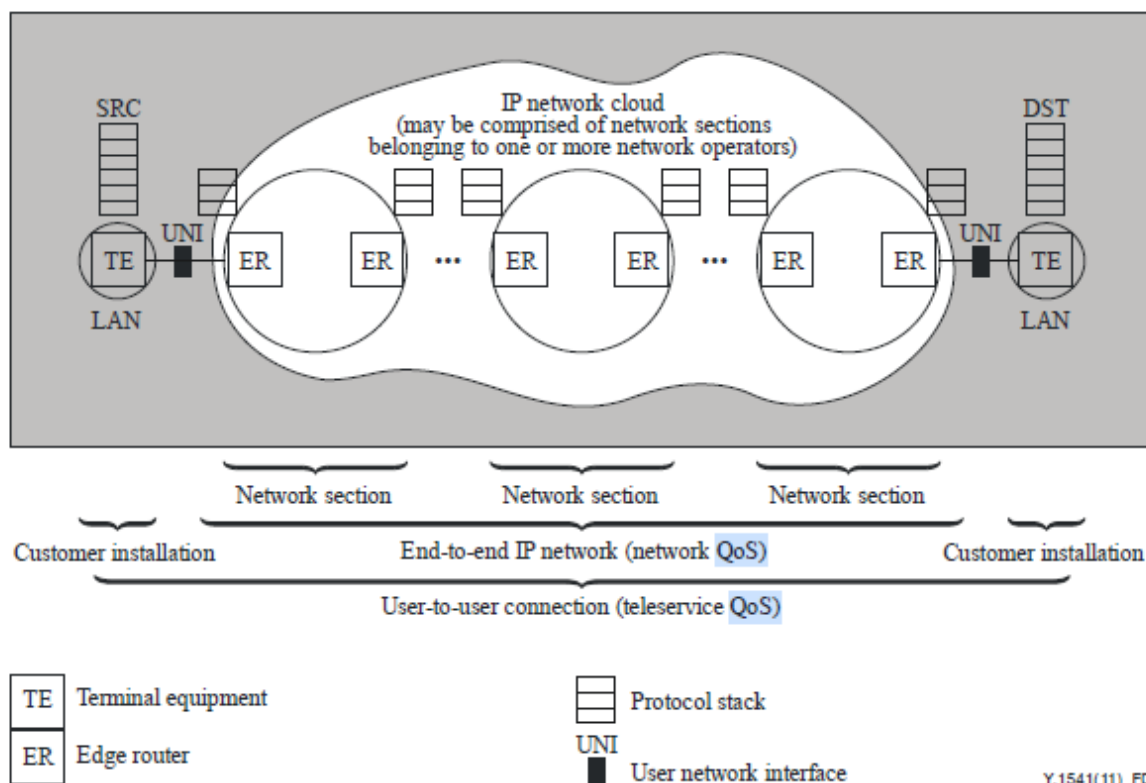
QOS (Quality of Service) é o coletivo efeito das performances de serviço, a qual define o grau de satisfação do usuário de um serviço (INTERNATIONAL TELECOMMUNICATION UNION, 2016, p. 18). A ITU-T (2016, p.18) determina como aspectos que devem ser levados em consideração na medição da QOS:

- A performance da operabilidade do serviço;
- A performance da acessibilidade do serviço;
- A performance da capacidade de retenção do serviço;
- A performance da integridade de serviço;
- Outros fatores específicos de cada serviço.

Normalmente a operadora cria perfis de QOS em algumas tecnologias, a ITU-T(2016, p.17) determina esse perfil com o objetivo de incluir um número de parâmetros de QOS. Este perfil será sempre conectado a uma sessão de QOS que segundo a ITU-T(2016, p. 18) é o período entre a abertura e o fechamento de uma conexão cuja as características são determinadas pelo perfil.

Para a tecnologia IP o funcionamento ocorre na camada de rede conforme mostrado na figura 16, o pacote sai de uma interface UNI já encapsulada e vai até outra conectando dois clientes, o pacote no meio de rede passa por vários roteadores de backbone com o QOS imbutido.

Figura 16 - Transporte do QoS na rede



NOTE – Customer Installation equipment (shaded area) is for illustrative purposes only.

Fonte: INTERNATIONAL TELECOMMUNICATION UNION (2011, p.8)

O quadro 11 determina como funciona as 5 classes de QoS, considerando o seu IPTD (IP Packet Transfer Delay) que determina o valor de atraso que cada classe tolera, sendo que em caso de longas distâncias ou comunicação satélite os objetivos de IPTD nas classes 0 e 2 não serão alcançáveis (INTERNATIONAL TELECOMMUNICATION UNION, 2011, p. 11). O quadro mostra as especificações de IPDV (IP Packet Delay Variation) que é a variação de atraso do pacote IP entre 2 pontos (INTERNATIONAL TELECOMMUNICATION UNION, 2011, p. 9, tabela 1, observação 2) sendo este um valor dependente da capacidade dos links de inter redes (INTERNATIONAL TELECOMMUNICATION UNION, 2011, p. 9, tabela 1, observação 3).

O quadro ainda demonstra os dados referentes ao IPLR (IP packet Loss Ratio) que cada classe permite onde a performance desse parâmetro pode ser estimada por inverter a probabilidade de sucesso na transferência de pacote através “n” seções de rede (INTERNATIONAL TELECOMMUNICATION UNION, 2011, p. 15),

sendo “n” um número inteiro qualquer de seções de rede.

O último parâmetro mostrado pelo quadro para as classes é referente ao IPER (IP packet Error Ratio) onde a performance pode ser estimada através da inversão de probabilidade de transferência de pacotes livres de erros através de “n” seções de rede (INTERNATIONAL TELECOMUNICATION UNION, 2011, p.15). A letra U em alguns parâmetros no quadro significa não especificado (unspecified) e quando isso ocorre a ITU-T (2011, p.9, tabela 1, notas gerais) determina que não há objetivo para esse parâmetro e qualquer objetivo padrão pode ser ignorado.

Quadro 11 - Classes 1 à 5 de QOS

Parametro de performance de rede	Natureza do objetivo de performance de rede	Classes QOS					
		Classe 0	Classe 1	Classe 2	Classe 3	Classe 4	Não especificada classe 5
IPTD	Limite superior da média IPTD	100 ms	400 ms	100 ms	400 ms	1 s	U
IPDV	Limite superior de $1 - 10^{-3}$ do quantil de IPTD menos o mínimo IPTD	50 ms	50 ms	U	U	U	U
IPLR	Limite Superior na probabilidade da perda de pacote	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	U
IPER	Limite superior	1×10^{-4}					U

Fonte: INTERNATIONAL TELECOMUNICATION UNION, 2011, p. 9

O Quadro 12 mostra as aplicações das classes.

Quadro 12 - Aplicações de classes QOS

Classe QOS	Aplicação (exemplos)	Mecanismos de nós	Técnicas de rede
0	Tempo real, jitter sensível, Alta Interatividade (VOIP, VTC)	Fila separada com serviços preferenciais e limpeza de trafego	Roteamento e distância restrita
1	Tempo real, jitter sensível, Alta Interatividade (VOIP, VTC)		Menos roteamento e distância restrita
2	Transação de dados e alta interatividade (Sinalização)	Fila separada, prioridade na perda	Roteamento e distância restrita
3	Transação de dados, interativo		Menos roteamento e distância restrita
4	Somente baixa perda (transações curtas, dados em massa e transmissão de vídeo)	Fila longa, prioridade na perda	Qualquer rota/caminho

5	Aplicações tradicionais de redes IP padrão	Fila separada (a menor prioridade)	Qualquer rota/caminho
---	--	------------------------------------	-----------------------

Fonte: INTERNATIONAL TELECOMUNICATION UNION, 2011, p. 12

O quadro 13 determina as classes 6 e 7 que são determinadas como classes provisórias, que diferente do quadro 11 tem o parâmetro IPRR (IP packet reordering rating) que trata a reordenação de pacotes se necessário.

A diferença entre as classes 1, 2, 3, 4 e 5 e as classes 6 e 7 é que os valores de todos os objetivos são provisórios e eles necessitam não serem encontrados pelas redes até eles serem revisados, baseado na experiência operacional real (INTERNATIONAL TELECOMUNICATION UNION, 2011, p. 13).

Quadro 13 - Classe 6 e 7

Parametro de performance de rede	Natureza do objetivo de performance de rede	Classes QOS	
		Classe 6	Classe 7
IPTD	Limite superior da média IPTD	100 ms	400 ms
IPDV	Limite superior de 1 - 10^{-5} do quantil de IPTD menos o minimo IPTD	50 ms	
IPLR	Limite Superior na probabilidade da perda de pacote	1×10^{-5}	
IPER	Limite superior	1×10^{-6}	
IPRR	Limite superior	1×10^{-6}	

Fonte: INTERNATIONAL TELECOMUNICATION UNION, 2011, p.13

A IETF (Internet Engineering Task Force) usa o “Diffserv” que pode ser correspondida pelo padrão ITU-T conforme quadro 14.

Quadro 14 - Diffserv e Classe IP QOS

Diffserv PHB associada	Classe IP QOS	Observações
Padrão (BE)	Não especificada QOS de classe 5	Um serviço IP legado quando operado em uma rede carregada levemente pode alcançar um bom nível de QOS IP.
AF	Classes QOS 2, 3, 4	O objetivo do IPLR somente aplica-se para os pacotes IP nos níveis de prioridade mais altos de cada classe AF. O IPTD se aplica em todos os pacotes.
EF	Classes QOS 0 e 1	

Fonte: INTERNATIONAL TELECOMUNICATION UNION, 2011, p. 33 (adaptado)

A IETF usa o DSCP (Differentiated Services Code Points) para definir QOS e muitas fabricantes americanas preferem por usar esse padrão. O quadro 15 mostra os códigos CSP e suas utilizações, o SR+BS (Single Rate with Burst Size control) é um mecanismo de política que provê um controle de taxa única com tamanho de rajada (BARBIARZ, HO CHAN, BAKER, 2006, p. 20. O AQM (Active Queue Management) descarta pacotes antes de a fila ficar cheia permitindo que os roteadores controlem quando e como os pacotes serão descartados (Braden, et. al., 1998, p.4). O DS (Differentiated Services) também é chamado de DiffServ é o que define os serviços diferenciados em uma rede de dados.

O quadro 15 também demonstra se o DSCP é condicionado ao DS de borda usando marcador de duas taxas e três cores (nomeada de trTCM – *Two Rate Three Color Mark*) ou de uma única taxa e três cores (nomeada de srTCM – *Single Rate Three Color Mark*). O trTCM mede um fluxo de pacotes IP e marca os pacotes baseados em duas taxas, PIR e CIR, e deles associa um tamanho de rajada que pode ser identificado por verde, amarelo ou vermelho (Heinanen, Guerin, 1999, p. 1). O srTCM mede um fluxo de pacotes IP e marca os pacotes baseados em duas taxas, CIR, CBS (Committed Burst Size) e EBS (Excess Burst Size) e deles associa um tamanho de rajada que pode ser identificado por verde, amarelo ou vermelho (Heinanen, Guerin, 1999, p. 1).

Quadro 15 - Classe de serviço e DSCP

Classe de serviço	DSCP	Condicionado ao DS de borda	Fila	AQM
Controle de rede	CS6	Rota e controle.	Taxa	Sim
Telefonia	EF	Política usando SR+BS	Prioridade	Não
Sinalização	CS5	Política usando SR+BS	Taxa	Não
Conferência Multimídia	AF41 AF42 AF43	Usando marcador duas taxas e três cores.	Taxa	Sim por DSCP
Interatividade em tempo real	CS4	Política usando SR+BS	Taxa	Não
Transmissão Multimídia	AF31 AF32 AF33	Usando marcador duas taxas e três cores.	Taxa	Sim por DSCP
Broadcast Video	CS3	Política usando SR+BS	Taxa	Não
Dados de baixa latência	AF21 AF22 AF23	Usando marcador de taxa única e três cores.	Taxa	Sim por DSCP
OAM	CS2	Política usando SR+BS	Taxa	Sim

Dados de alta transferência	AF11 AF12 AF13	Usando marcador duas taxas e três cores.	Taxa	Sim por DSCP
Padrão	DF	Não Aplicável	Taxa	Sim
Dados de baixa prioridade	CS1	Não Aplicável	Taxa	Sim

Fonte: BARBIARZ, HO CHAN, BAKER, 2006, p. 19. (adaptado)

A definição de QOE é a aceitabilidade no geral de uma aplicação ou serviço percebida subjetivamente pelo o usuário final (INTERNATIONAL TELECOMMUNICATION UNION, 2015, p.3) e para realizar tal avaliação deve ser através de testes subjetivos com métricas, assim como a pontuação de opinião média (MOS) (INTERNATIONAL TELECOMMUNICATION UNION, 2015, p.4).

As medições podem ser feitas através de escala nominal (identificando igualdade), ordinal (identificando mais ou menos), intervalo (identificando igualdade de intervalos de diferença) e relação (identificando igualdade de relações) (INTERNATIONAL TELECOMMUNICATION UNION, 2015, p. 6).

O método de apresentação usado pode ser de ajustes ou constância, a modalidade de teste pode ser passivo (ouvindo ou vendo), ativo (falando ou movendo) ou interativo (conversação) e o julgamento pode ser realizado depois de algum estímulo ou de forma continua durante o estímulo (INTERNATIONAL TELECOMMUNICATION UNION, 2015, p. 7). Os serviços visados a atingir são o de áudio, vídeo e dados e nesse trabalho será abordado através da QOS nos serviços contratados pelo cliente.

3 INTEGRANDO E CONFIGURANDO SOLUÇÃO DE DADOS

Nesse tópico será abordado toda a configuração e simulação de uma rede virtual.

3.1 CONFIGURANDO SALTOS ENTRE ROTEADORES

3.1.1 Configurando Dot1Q na rede

Para criar a VLAN dot1q foi necessário lançar os seguintes comandos nos equipamentos do fabricante cisco:

Figura 17 - Configuração do DOT1Q no Cisco.

```
32#conf t
Enter configuration commands, one per line. End with CNTL/Z.
32(config)#config
32(config)#inter
32(config)#interface Gi4/6.1240
32(config-subif)#encapsulation dot1q 17541
```

Fonte: Aatoria Própria.

Já para fabricante Nokia foi configurado a interface física no equipamento com dot1q:

Figura 18 - Encapsulamento do DOT1Q no Alcatel.

```
*A:01# configure port 4/2/3
*A:01>config>port# ethernet
*A:01>config>port>ethernet# encap-type dot1q
```

Fonte: Aatoria Própria.

Logo após foi criado um “customer”, se não houver nenhum já criado no roteador, que tem a intenção de agrupar todos os circuitos que tem um mesmo parâmetro.

Figura 19 - Configurando um customer no Alcatel.

```
*A:01# configure service customer 2 create
*A:01>config>service>cust# description "teste";
```

Fonte: Aatoria Própria

Criar um serviço para poder configurar o IP, QOS, BGP entre outros. Os valores possíveis para serviço IP é o “IES” que normalmente será usado para

conexões IP e “VPRN” para serviços a qual será usada para conexões VPN que será explicado mais adiante. Nesse caso irá ser simulado um serviço IES:

Figura 20 - Criando a interface lógica no Alcatel.

```
*A:01# configure service ies 921001054 customer 2 create
*A:01>config>service>ies$ interface "A000" create
*A:01>config>service>ies>if$ sap 4/2/3:0111 create
*A:01>config>service>ies$ no shutdown
```

Fonte: Autoria Própria

Ao criar o serviço há a necessidade de criar uma interface lógica, pois existem serviços como o VPN que obrigatoriamente haverá uma ou mais interfaces lógicas, nessa interface lógica cria-se o ponto de acesso de serviço (*service access point* - SAP) a qual será a interface física e sua respectiva VLAN, nesse caso a VLAN 0111.

3.1.2 Configurando QinQ na rede

No equipamento cisco é apenas entrar na interface lógica e dentro da caixa definir o encapsulamento QinQ com duas dot1q, sendo uma primária (SVLAN) e a segunda secundária (CVLAN), deixando claro que a interface lógica pode ter números diferentes do configurado na SVLAN e CVLAN.

Figura 21 - Configurando o QinQ no Cisco.

```
32#conf t
Enter configuration commands, one per line. End with CNTL/Z.
32(config)#int Gi4/1.28160111
32(config-subif)#encapsulation dot1q 2816 second-dot1q 0111
```

Fonte: Autoria Própria

No equipamento Nokia deve-se entrar na interface física e alterar o encapsulamento para QinQ.

Figura 22 - Configurando o encapsulamento QinQ no Alcatel.

```
*A:01# configure port 4/1/2
*A:01>config>port# ethernet
*A:01>config>port>ethernet# encap-type qinq
```

Fonte: Autoria Própria

Logo após, deve-se criar um *customer* ou usar um já existente:

Figura 23 - Configurando o customer no Alcatel.

```
*A:01# configure service customer 2 create
*A:01>config>service>cust# description "teste";
```

Fonte: Autoria Própria

Ao executar tal procedimento, deve-se configurar um serviço para realizar as configurações necessárias como IP e QOS e vincular a interface lógica ao serviço para que por fim haja a possibilidade de inserir o ponto de acesso do serviço (*service access point* – SAP) que é composto da interface física com a CVLAN e a SVLAN.

Figura 24 - Configurando um Qinq na interface lógica do Alcatel.

```
*A:01# configure service ies 921001054 customer 2 create
*A:01>config>service>ies$ interface "A000" create
*A:01>config>service>ies>if# sap 4/1/2:0111.15 create
```

Fonte: Autoria Própria

3.1.3 Configurando interface Serial SONET

Na tecnologia criada pela Cisco deve-se configurar a controladora para reconhecer aquela porta serial emulada, então nesse caso primeiramente se entra na controladora “SONET”. Ao entrar dentro da caixa da “SONET” acessa-se a caixa da “TUG-3” informando o “AU-4” e a “TUG-3”, por fim configura-se a “TUG-2”, “E1”, o “*channel-group*” que é o canal do que irá se referir determinado conjunto indicado no parâmetro “*timeslots*”.

Figura 25 - Configurando o SONET no Cisco.

```
32#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
32(config)#controller sonet 3/1/0
32(config-controller)#au-4 1 tug-3 3
32(config-ctrlr-tug3)#tug-2 3 e1 1 channel-group 13 timeslots 13-20
32(config-ctrlr-tug3)#
```

Fonte: Autoria Própria

No exemplo acima existe a configuração do “SONET” 3/1/0, “au-4” 1, “tug-3” 3, “tug-2” 3, “e1” 1 e “*channel-group*” 13, criando a serial com essa forma: “Serial 3/1/0.1/3/3/1:13”. Para fazer configurações como inserir IP, perfil de QOS, protocolos específicos, entre outro tem que entrar dentro da interface indicando sua serial conforme abaixo:

Figura 26 - Acessando a configuração da porta no Cisco.

```
32#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
32(config)#interface Serial 3/1/0.1/3/3/1:13
```

Fonte: Autoria Própria

Na tecnologia Nokia deve-se acessar a placa através do comando “*configure port*”, logo após sinalizar-se o “E1” e o “*channel-group*” que representará o grupo de *timeslots*. Dentro dessa caixa pode-se configurar a quantidade de “*timeslots*” e alguns protocolos referente à camada 2 do modelo OSI.

Figura 27 - Configurando o SONET no Alcatel.

```
*A:01# configure port 6/2/1
*A:01>config>port# tdm e1 1.2.3 channel-group 1
*A:01>config>port>tdm>e1>channel-group#
```

Fonte: Autoria Própria

Deve-se criar um “*customer*” caso já não exista, que pode ser usado para agrupar serviços por semelhança, nesse caso pode-se colocar uma descrição.

Figura 28 - Configurando cliente no Alcatel.

```
*A:01# configure service customer 2 create
*A:01>config>service>cust# description "teste",
```

Fonte: Autoria Própria

Com o “*customer*” criado, pode-se criar um serviço para vincular a ele, após criar o serviço, existe a possibilidade de criar a interface lógica para conseguir vincular o ponto de acesso de serviço (*service access point* - SAP). Dentro dessa caixa pode-se configurar as políticas de QOS e dentro da interface lógica IP, DHCP, VPLS entre outros.

Figura 29 - Acessando a porta no Alcatel.

```
*A:01# configure service ies 921000353 customer 2 create
*A:01>config>service>ies$ interface "AAA000" create
*A:01>config>service>ies>if$ sap 6/2/1.1.2.3.1 create
```

Fonte: Autoria Própria

3.1.4 Configurando porta E1/E3

Para realizar a configuração de uma porta E3 no fabricante cisco, deve-se emular a placa E3 e depois gerar o E1 para poder configurar a comunicação como o

IP, QOS, encapsulamento entre outros.

Figura 30 - Configurando o E3 no Cisco.

```
11#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
11(config)#controller e3 7/1/0
11(config-controller)#E1 1 channel-group 1 timeslots 1-2
11(config-controller)#
```

Fonte: Autoria Própria

No E1 na mesma fabricante, se emula apenas o E1:

Figura 31 - Configurando E1 no Cisco.

```
05(config)#controller E1 1/1
05(config-controller)#channel-group 1 timeslots 1-2
05(config-controller)#
```

Fonte: Autoria Própria

3.1.5 Configurando Interface ATM em roteador

Para configurar a interface ATM o roteador o mesmo deve ter uma placa que suporte tal tecnologia, nesse tópico será simulado um roteador da fabricante Cisco com uma placa dessa já instalada.

Conforme figura 32 usa-se o comando “*configure terminal*” para entrar no modo de configuração e logo em seguida digita-se o comando “interface ATM8/0/0.41408” para entrar na interface e lançar os comandos. Aqui é importante ter em mente que 41408 pode ser um número aleatório e que pode não ter nenhum padrão, mas por conveniência aqui foi usado o mesmo número do PVC que será configurado na próxima linha.

Figura 32 - Configurando ATM no Cisco.

```
700#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
700(config)#interface ATM8/0/0.41408
700(config-subif)#pvc 41/408
700(config-if-atm-vc)#
```

Fonte: Autoria Própria

O PVC nesse caso terá como parâmetros 41 e 408, sendo 41 o VP e 408 o VC, o VP (*virtual path*) e o VC (como já explicado no tópico 2.3.) um identificará a rota e outro o canal.

3.1.6 Configurando Interface X.25 no roteador Cisco.

A configuração do X.25 em um roteador Cisco deve-se entrar no modo de configuração através do comando “configure terminal” e acessar a caixa de configuração referente a porta que tenha suporte ao protocolo X.25.

O comando “description” é opcional, mas em uma operadora é importante para identificação e não se deve configurar IP a essa porta. O encapsulamento nessa porta deve ser x25 e deve usar o comando “encapsulation x25”, já o comando “load-interval” é para o roteador computar as estatísticas médias para os últimos segundos da carga de dados (Stringfield, White, Mckee, 2007, p. 169), o padrão desse comando é 5 minutos (300 segundos), mas para roteadores da operadora é comumente usado 30 segundos para gerar as estatísticas para testes e verificação de erro.

O comando “x25 address” determina um endereço para a porta, no caso exemplificado na figura 33 foi usado o endereço 3000005, outro comando utilizado é o “x25 htc” que determina o HTC (highest two-way channel) que conjuntamente com LTC (lowest two-way channel) determinam a faixa de canais lógicos que serão designados para canais lógicos de duas mãos para chamadas virtuais (INTERNATIONAL TELECOMUNICATION UNION, 1996, p. 120).

O comando “x25 use-source-address” indica que a porta usará o endereço de origem para ligações encaminhadas. O comando “serial restart-delay” determina o atraso ao reiniciar a porta em segundos e o comando “no dce-terminal-timing-enable” impede que a fase de troca de dados em linhas de dados com alta velocidade atravesse longas distâncias (Boney, 2005, p. 422).

Figura 33 – Configurando X.25 no Cisco.

```
325#sh run int Serial4/0/4
Building configuration...

Current configuration : 268 bytes
!
interface Serial4/0/4
 description LINK_X25
 no ip address
 encapsulation x25
 load-interval 30
 x25 address 3000005
 x25 htc 600
 x25 use-source-address
 serial restart-delay 0
 no dce-terminal-timing-enable
end
```

Fonte: Autoria Própria.

3.2 CONFIGURANDO CROSS CONEXÃO ENTRE ROTEADOR E OUTRA GERÊNCIA

Nesse tópico é tratado o acesso do cliente, já que normalmente o roteador não vai estar ao lado da empresa ou casa do cliente e usar uma porta de 1 Gb/s para atender um cliente de 512 Kb/s é muito caro sendo mais fácil colocar um multiplexador ou um *switch* que é mais barato e melhor para a operadora.

3.2.1 Configurando túnel *Metro-Ethernet* por dot1q

Para configurar o túnel *ethernet* no fabricante Nokia é necessário criar um serviço chamado de “*epipe*”. Nesse serviço coleta-se as duas portas com VLAN para realizar a comunicação entre elas.

Figura 34 - Configurando túnel no Alcatel.

```
B:1011# configure service epipe 96011 customer 3 create
*B:1011>config>service>epipe$ sap 4/2/16:3030 create
*B:1011>config>service>epipe$ sap 10/2/3:3030 create
```

Fonte: Autoria Própria

Para configurar o túnel em um *switch* Cisco deve-se entrar nas duas interfaces e sinalizar que as duas pertencem a mesma VLAN.

Figura 35 - Configurando uma porta tronco no Cisco.

```
01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
01(config)#interface Gi1/2
01(config-if)#switchport
01(config-if)#switchport trunk encapsulation dot1q
01(config-if)#switchport trunk allowed vlan 4
01(config-if)#switchport mode trunk
```

Fonte: Autoria Própria

Nota-se que em ambas as portas deve-se indicar o encapsulamento dot1q para a VLAN, gerar as permissões para a operação de uma ou mais VLAN's na porta (para isso deve-se usar o comando “*switchport trunk allowed vlan add*”, para mais que uma, ou colocar todas as VLAN's comando “*switchport trunk allowed vlan*” com vírgula ou traço (“-”) para determinar intervalos) e indicar modo *trunk* se for meio de rede. Caso seja acesso deve-se indicar o modo “*access*”, lembrando que no modo “*access*” só pode ser inserida uma única VLAN.

Figura 36 - Configurando uma porta tronco secundária.

```

01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
01(config)#interface Gi1/3
01(config-if)#switchport
01(config-if)#switchport trunk encapsulation dot1q
01(config-if)#switchport trunk allowed vlan 4
01(config-if)#switchport mode trunk

```

Fonte: Autoria Própria

Após essas configurações é necessário entrar na caixa da VLAN e depois sair apenas para ativá-la, caso contrário não poderá consultar suas informações podendo interferir no funcionamento.

Figura 37 - Ativando a vlan.

```

01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
01(config)#vlan 4
01(config-vlan)#exit

```

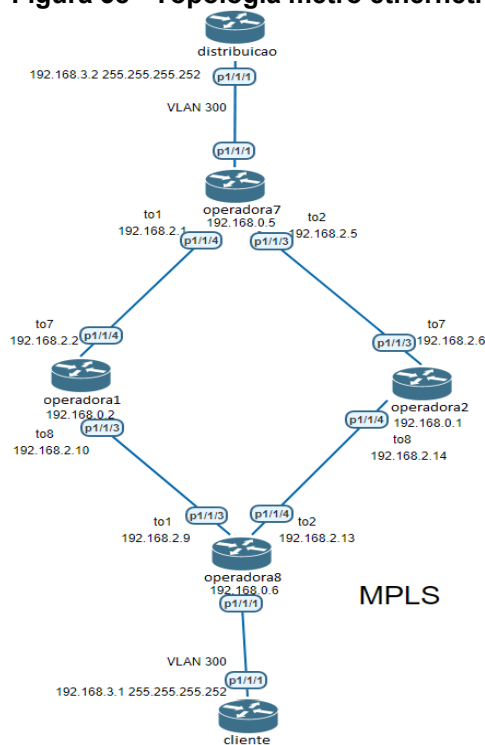
Fonte: Autoria Própria

3.2.2 Configurando túnel Metro-Ethernet por MPLS

Outra forma bastante utilizada para fazer a conexão na rede metro é através da rede MPLS entre o equipamento que distribui os IP's e o cliente. Esse tipo de configuração é realizada quando existe um anel de *switchs* de camada 3 e necessita garantir redundância caso exista uma falha em um ponto de rede.

A figura 38 mostra a topologia anel, que ocorre entre os roteadores operadora1, operadora2, operadora7 e operadora8, para ter a opção de redundância e economia em codificação, evitando que todo cliente tenha um *epipe* para cada roteador da rede, será gerado um túnel pelos dois caminhos entre operadora7 e operadora8 através de um SDP em roteadores Nokia.

Figura 38 - Topologia metro ethernet.



Fonte: Autoria Própria

No anel, cuja configuração é demonstrada na figura 39, todos os equipamentos estarão com OSPF habilitado, sendo que esses *switchs* operam em camada 3 embora não sejam seus objetivos, dentro do OSPF terá as interfaces que participarão daquela área. No caso trabalhado será a interface dos vizinhos e uma interface lógica (interface “system”) que será o identificador daquele equipamento, obrigatoriamente um endereço /32.

Figura 39 - Configurações do OSPF dos roteadores.

```
A:operadora7# admin display-config | match ospf context all
#-----
ospf
 traffic-engineering
 area 0.0.0.56
 interface "system"
 no shutdown
 exit
 interface "to1"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 interface "to2"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 exit

A:operadora1# admin display-config | match ospf context all
#-----
ospf
 traffic-engineering
 area 0.0.0.56
 interface "system"
 no shutdown
 exit
 interface "to7"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 interface "to8"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 exit

A:operadora2# admin display-config | match ospf context all
#-----
ospf
 traffic-engineering
 area 0.0.0.56
 interface "system"
 no shutdown
 exit
 interface "to7"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 interface "to8"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 exit

A:operadora8# admin display-config | match ospf context all
#-----
ospf
 traffic-engineering
 area 0.0.0.56
 interface "system"
 no shutdown
 exit
 interface "to1"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 interface "to2"
 interface-type point-to-point
 mtu 9000
 no shutdown
 exit
 exit
```

Fonte: Autoria Própria

Dentro da caixa “router” (comando “*configure router*”) pode ser configurado o MPLS. Nessa caixa, a princípio terá o tempo de atualização com o comando “*resignal-timer*” sendo 30, a interface lógica system e as interfaces “to7” e “to8” que são acopladas pelas portas físicas. Dentro da interface “to7” e “to8” tem sua direcionalidade podendo ser “HORARIO” ou “ANTIHORARIO”, ou seja, caso um equipamento falhe ou a fibra se rompa terá outro caminho a seguir no anel. O “*admin-group*” HORARIO e ANTIHORARIO ficarão dentro do comando “*configure router if-attribute*”.

Figura 40 - Configurações da MPLS dos roteadores.

```

A:operadora8# admin display-config | match mpls context all
#-----
mpls
  resignal-timer 30
  interface "system"
    no shutdown
  exit
  interface "to1"
    admin-group "HORARIO"
    no shutdown
  exit
  interface "to2"
    admin-group "ANTIHORARIO"
    no shutdown
  exit

A:operadora1# admin display-config | match mpls context all
#-----
mpls
  resignal-timer 30
  interface "system"
    no shutdown
  exit
  interface "to7"
    admin-group "HORARIO"
    no shutdown
  exit
  interface "to8"
    admin-group "ANTIHORARIO"
    no shutdown
  exit

A:operadora2# admin display-config | match mpls context all
#-----
mpls
  resignal-timer 30
  interface "system"
    no shutdown
  exit
  interface "to7"
    admin-group "ANTIHORARIO"
    no shutdown
  exit
  interface "to8"
    admin-group "HORARIO"
    no shutdown
  exit

A:operadora7# admin display-config | match mpls context all
#-----
mpls
  resignal-timer 30
  interface "system"
    no shutdown
  exit
  interface "to1"
    admin-group "ANTIHORARIO"
    no shutdown
  exit
  interface "to2"
    admin-group "HORARIO"
    no shutdown
  exit
  
```

Fonte: Autoria Própria

Na figura 40 tem-se o exemplo da configuração de um roteador, e como fica a configuração para com seus vizinhos. A configuração para ser realizada deve ser feita na caixa *router* (comando “*configure router*”). Aqui deve-se configurar os caminhos “HORARIO” e “ANTIHORARIO” através do comando “*path*” e os lsp para os vizinhos com a linha “*to*” com IP do roteador destino, linha “*from*” com o IP do roteador origem, ou seja, o roteador no qual está sendo feita as configurações. A seleção de rota vai ser por CSPF, conforme sinalizado em todos os lsp’s, o roteamento deve ser rápido por isso do comando “*fast-reroute facility*” e o tempo de reconexão daquele lsp. Dentro do lsp ainda existe a rota primária e secundária (*primary* e *secondary*), as duas serão adaptativas e se adaptarão conforme a disponibilidade da rede, sendo que a secundária ficará aguardando a primária cair através da linha de comando “*standby*”, as linhas “*include*” e “*exclude*” demonstrarão qual roteador vai, no caso estudado “HORÁRIO” e “ANTIHORARIO”, mas poderia

ser “ESQUERDO” ou “DIREITO” ou qualquer nomenclatura de fácil entendimento, desde que sempre se cumpra a lógica direcional.

Figura 41 - Configuração do LSP dos roteadores.

```

operadora8# admin display-config | match mpls context all
#-----
mpls
  path "ANTIHORARIO"
  no shutdown
  exit
  path "HORARIO"
  no shutdown
  exit
  lsp "torouter1"
  to 192.168.0.2
  from 192.168.0.6
  cspf
  fast-reroute facility
  exit
  retry-timer 10
  primary "HORARIO"
  adaptive
  include "HORARIO"
  exclude "ANTIHORARIO"
  exit
  secondary "ANTIHORARIO"
  standby
  adaptive
  include "ANTIHORARIO"
  exclude "HORARIO"
  exit
  no shutdown
  exit
  lsp "torouter2"
  to 192.168.0.1
  from 192.168.0.6
  cspf
  fast-reroute facility
  exit
  retry-timer 10
  primary "ANTIHORARIO"
  adaptive
  include "ANTIHORARIO"
  exclude "HORARIO"
  exit
  secondary "HORARIO"
  standby
  adaptive
  include "HORARIO"
  exclude "ANTIHORARIO"
  exit
  no shutdown
  exit
  no shutdown
  
```

Fonte: Autoria Própria

Na figura 42 aparece o exemplo da configuração feita para um roteador. Para o funcionamento é necessário a configuração em todos. Na caixa “*configure router ldp*” serão configuradas as interfaces que serão pertencentes ao ldp através do comando “*interface-parameters*” no caso as interfaces lógicas “to1” e “to2” que são acasaladas com portas físicas, dentro da caixa “*targeted-session*” são configurados os vizinhos. Por exemplo o endereço do “router2” é 192.168.0.1, então será gerado o *peer* para esse IP com o tunelamento (*tunneling*) com lsp “torouter2” e assim sucessivamente para os demais vizinhos e roteadores.

Figura 42 - Configuração do ldp dos roteadores.

```
A:operadora8# admin display-config | match ldp context all
#-----
ldp
  interface-parameters
    interface "to1"
    exit
    interface "to2"
    exit
  exit
  targeted-session
    peer 192.168.0.1
      tunneling
        lsp "torouter2"
      exit
    exit
  peer 192.168.0.2
    tunneling
      lsp "torouter1"
    exit
  exit
  peer 192.168.0.5
    tunneling
      lsp "torouter7"
    exit
  exit
exit
no shutdown
```

Fonte: Autoria Própria

Como a premissa é criar um túnel entre os roteadores operadora 8 e operadora 7 será criado um serviço “SDP”, como ilustrado na figura 43, através da linha de comando “*configure service sdp 2 customer 1 create*” (após criado serviço pode-se utilizar o comando “*configure service sdp 2*”) nomeado de 2, com o comando “*description*” é gerada uma descrição, o “*far-end*” será o IP /32 (*interface system*) do equipamento da outra ponta, sendo nesse caso a comunicação entre o roteador “operadora7” de IP 192.168.0.5 e “operadora8” de IP 192.168.0.6. Como a comunicação é feita MPLS usa-se o comando “*ldp*” com *keep-alive* em “*shutdown*” evitar gastar processamento desnecessário.

Figura 43 - Configurando as pontas do roteadores.

<pre>A:operadora8>config>service>sdp# info #----- description "router8torouter7" far-end 192.168.0.5 ldp keep-alive shutdown exit no shutdown</pre>	<pre>A:operadora7>config>service>sdp# info #----- description "router07torouter08" far-end 192.168.0.6 ldp keep-alive shutdown exit no shutdown</pre>
--	--

Fonte: Autoria Própria

Após realizadas as configurações será criado um serviço denominado *epipe* igualmente ilustrado na figura 44, que vai interligar a interface dot1q 1/1/1:300 com o túnel 2:300, gerando economia de mão de obra, já que não haverá a necessidade de criar vários dot1q em todos os roteadores da rede, através do túnel consegue-se agrupar todos os clientes sem nem ter que acessar o roteador “operadora1” e

“operadora2”.

Figura 44 - Criando o túnel.

```
A:operadora8>config>service>epipe# info
-----
sap 1/1/1:300 create
exit
spoke-sdp 2:300 create
no shutdown
exit
no shutdown

A:operadora7>config>service>epipe# info
-----
sap 1/1/1:300 create
exit
spoke-sdp 2:300 create
no shutdown
exit
no shutdown
```

Fonte: Autoria Própria

3.2.3 Cross conexão Roteador/Datacom

Para começar a criação deve-se entrar no *channel-group* da interface serial/E1/E3 e definir quantos *timeslots*, nesse caso foi definido o *timeslot* 11 e 12 conforme ilustrado na figura 45.

Figura 45 - Configurando os timeslots.

```
*A:01# configure port 6/2/1
*A:01>config>port# tdm e1 1.3.1
*A:01>config>port>tdm>e1# channel-group 11
*A:01>config>port>tdm>e1>channel-group$ timeslots 11-12
```

Fonte: Autoria Própria

Para saber quais equipamentos se interligam, pode-se verificar de duas maneiras: primeiramente pela porta do roteador usando o comando “*show port*” com a porta serial sem o “*tdm*”, “*e1*” e “*channel-group*”, o campo “*description*” mostrará a qual equipamento ele se liga, normalmente com o nome do multiplexador, *slot*, posição da STM e fabricante. A figura 46 ilustra isso.

Figura 46 - Descrição da porta.

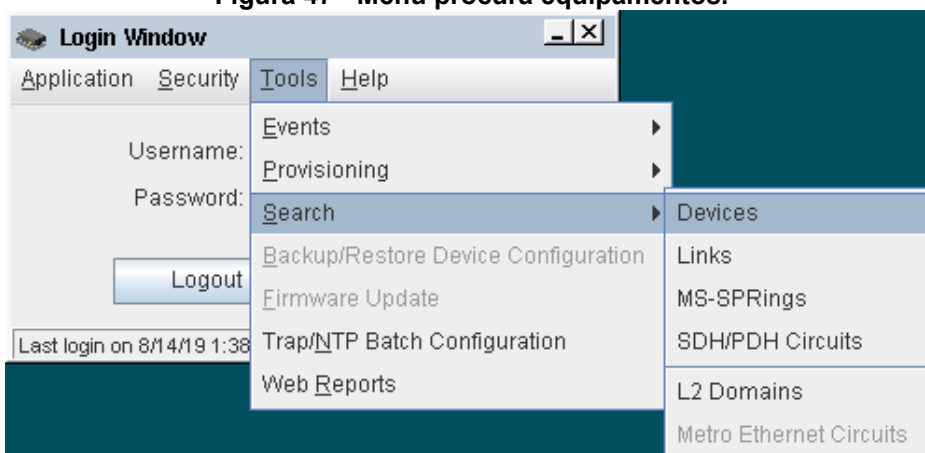
```
*A:01# show port 6/2/1
=====
SONET/SDH Interface
=====
Description      : teste mux1 SLOT 10 STM 6 DTC
```

Fonte: Autoria Própria

A figura 47 mostra a interface gráfica de uma gerência Datacom. Usando a gerência da gráfica da fabricante Datacom pode-se localizar o equipamento, sendo que normalmente a rede multiplexada está em alguma gerência gráfica. Para localizar o equipamento da porta, pode-se entrar no menu “*Tools*”, opção “*Search*” e

logo após “Devices”.

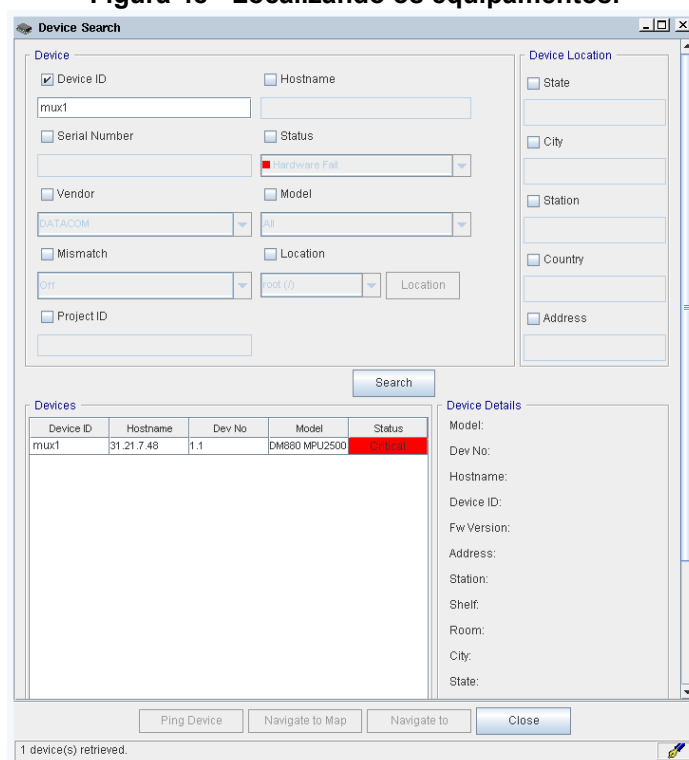
Figura 47 - Menu procura equipamentos.



Fonte: Autoria Própria

Na figura 48 terá uma janela com vários critérios de busca. Nesse caso deve ser marcada a caixa “Device ID” e no campo abaixo que irá ser habilitado, digita-se o nome do multiplexador “mux1” e clica-se em “Search”. Percebe-se que um equipamento aparece no quadro “Devices”.

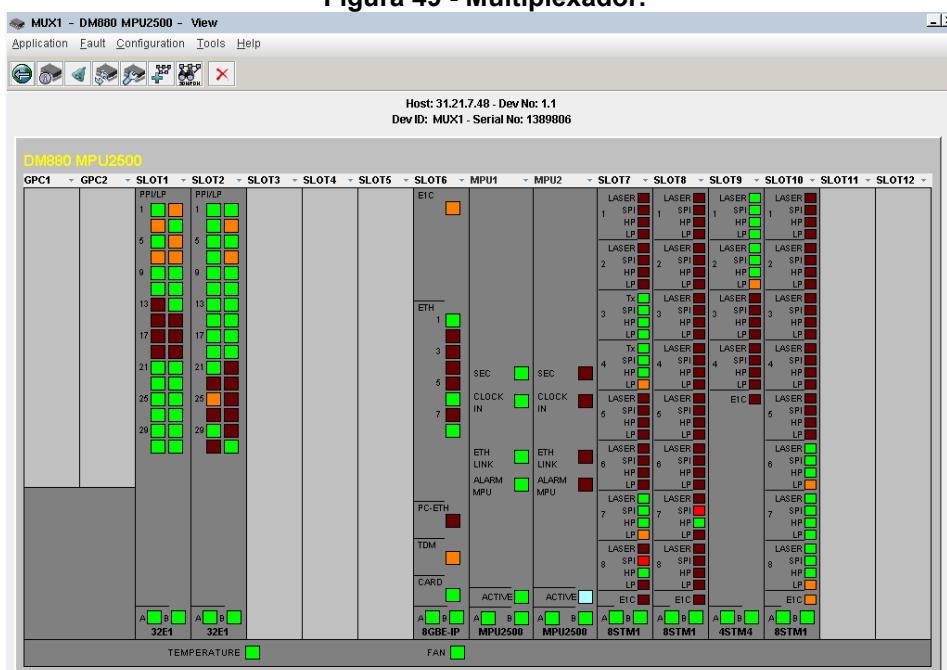
Figura 48 - Localizando os equipamentos.



Fonte: Autoria Própria

Ao clicar duas vezes no equipamento abrirá o multiplexador DM8800 conforme ilustrado na figura 49, nesse existem 12 *slots* para placas diversas e 4 para a administração e serviços. Nesses *slots* com placas diversas contém a placa 32E1 que contém 32 E1's, placa 8GBE-IP que faz a conversão da tecnologia *Ethernet* para PDH e STM, placa 8STM1 que contém 8 portas STM's e placa 4STM1 que contém 4 portas STM's. Nesse caso a porta serial conforme a descrição vista anteriormente está diretamente conectada a porta STM encontrada no slot 10, porta 6.

Figura 49 - Multiplexador.



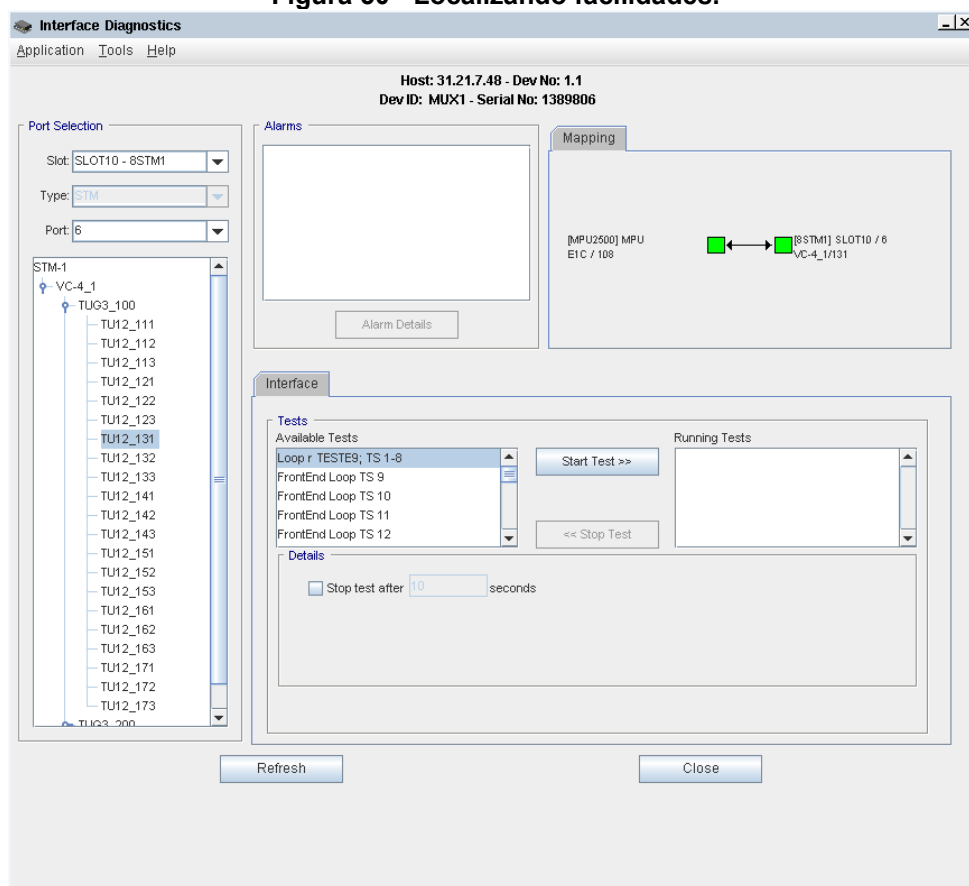
Fonte: Autoria Própria

Ao clicar com o botão direito na porta STM 6 ao lado do parâmetro SPI, abrirá algumas opções, ao selecionar a opção "*Interface Diagnostic*" abrirá uma tela, vide figura 50, a qual pode-se escolher a VC, TUG-3 e TU12 assim como realizar testes. A parte de testes será explicada mais a frente. Na porta serial dentro do roteador foi gerada a facilidade 6/2/1.1.3.1.11 com os *timeslots* 11 e 12, a 6/2/1 e a conexão física, a 1.3.1 será a junção entre a TUG-3 e a TU12, ou seja, será TUG-3 100. Esta centena representa o primeiro dígito na serial e TU-12 131 (1.3.1) que representa o numeral inteiro. Ao selecionar a TU12 abrirá na caixa "*Available Tests*" a distribuição de "*timeslots*" usados e vagos, na primeira linha dessa caixa haverá uma linha com o conteúdo "*Loop r TESTE9; TS 1-8*", o "*TS 1-8*" afirma que os

“*timeslots*” de 1 a 8 já estão utilizados para dados para um serviço ou cliente nomeado como “TESTE9” e que não utiliza-se para aprovisionar o serviço a não ser que se apaguem esses dados, o que não será feito nesse momento.

A segunda linha terá escrita a seguinte frase: “*FrontEnd Loop TS9*”, indicando que o *timeslot* 9 está livre para uso, o *timeslot* 10, 11, 12 aparentam estar livres também, o *timeslot* 13 embora não apareça na figura também está livre. Como a contagem de *timeslot* na Datacom começa no 0 até 31 e no Alcatel é de 1 a 32, deve-se corresponder os *timeslots* conforme as duas tecnologias, como no exemplo foi aprovisionado os *timeslots* 11 e 12 no roteador Alcatel, na Datacom será acrescentado 1 transformando em *timeslots* 12 e 13.

Figura 50 - Localizando facilidades.

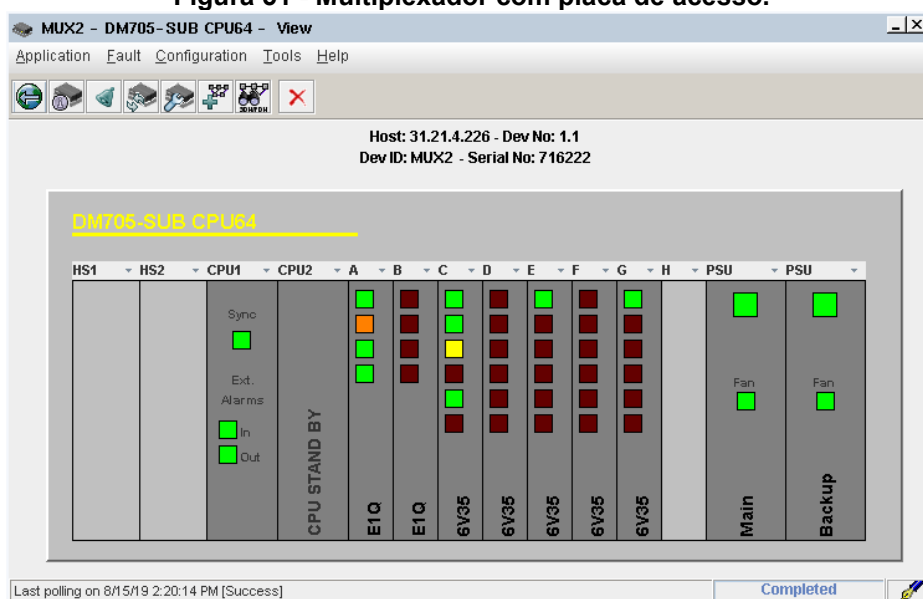


Fonte: Autoria Própria

Após a análise, se os *timeslots* estão ocupados, garante-se que há a possibilidade de gerar uma rota fechando um circuito entre roteador/switch de camada 3 da operadora e roteador do cliente. Logo após, como mostrado na figura 44, deve-se procurar o multiplexador de acesso que irá se conectar a operadora ao

cliente, nesse caso mux2 que está sendo ilustrado na figura 51, nesse mux2 deve-se habilitar a porta de acesso desse cliente, nota-se também que esse equipamento com 6 placas de controle/serviço e 8 placas para acesso, sendo que tem 2 placas E1 que servem para fazer a intercomunicação entre dois multiplexadores normalmente e 5 placas V35 que modulam o sinal ao *modem*/EDD.

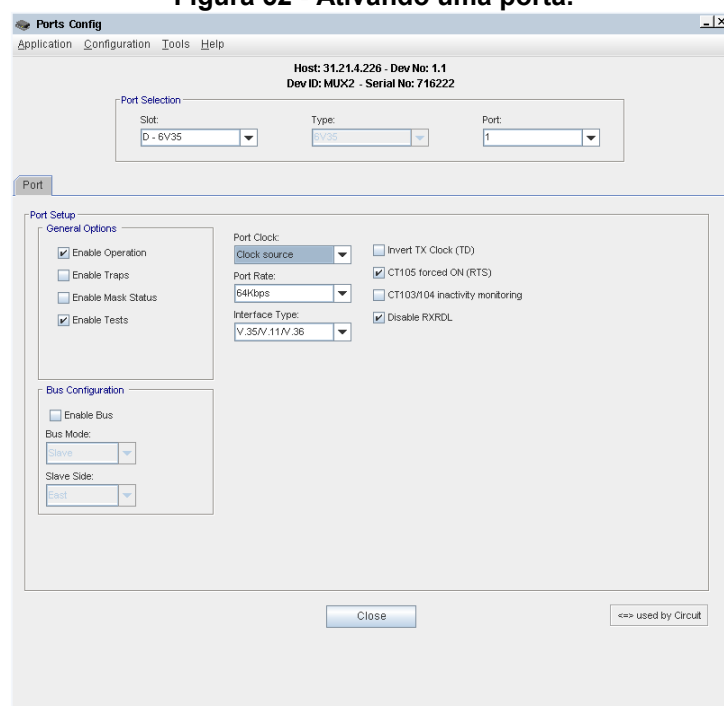
Figura 51 - Multiplexador com placa de acesso.



Fonte: Autoria Própria

Para proceder com o procedimento para habilitar a porta é obrigatório escolher o menu “*Configuration*” e depois “*Device Configuration*”, ao realizar tal ação a janela ilustrada na figura 52 se abrirá e nela deve-se escolher o slot e porta que se deve habilitar. Será usado como exemplo o slot D e porta 1. Ao se selecionar tem que escolher a opção “*Enable Operation*” para habilitar a porta, as demais opções desta janela serão tratadas na parte de testes. Ao fechar a janela, será questionado o que se deve fazer, para salvar na memória mas não no arquivo de configuração (arquivo de boot) para que perca as configurações na próxima vez que o equipamento seja reiniciado, escolha “*Activate*”, para salvar na memória e no arquivo de configuração, escolha “*Activate/Save Config*”, para não salvar escolha “*Discard Changes*” e para voltar ao equipamento e fazer mais alguma alteração escolha “*Cancel*”.

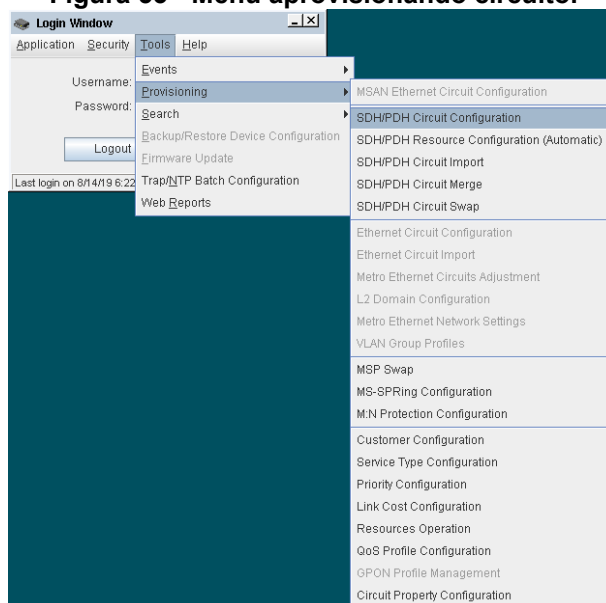
Figura 52 - Ativando uma porta.



Fonte: Autoria Própria

Com a porta de comunicação com o cliente configurada e “*timeslots*” da porta canalizada para o roteador livres ocorrerá a configuração. Para realizar tal passo é necessário escolher algumas opções no menu principal, ilustrado na figura 53. As opções usadas em ordem de aparecimento serão encontradas na aba “*Tools*”, na opção “*Provisioning*”, dentro de “*Provisioning*” seleciona-se “*Customer Configuration*” para configurar as informações de determinado cliente criando a opção de agrupamento de circuito por cliente, “*Service Type Configuration*” tem a funcionalidade de agrupar serviços específicos e tem a funcionalidade de gerar QOS para limitar velocidade. Vale lembrar que aqui o limitador de velocidade vai ser a quantia de *timeslot* e normalmente o QOS vai ser aplicado nos equipamentos de camada 3 caso necessário. Por fim a opção “*SDH/PDH Circuit Configuration*” que gera a rota na rede para a passagem de dados a qual é conhecida como circuito.

Figura 53 - Menu aprovisionando circuito.



Fonte: Autoria Própria

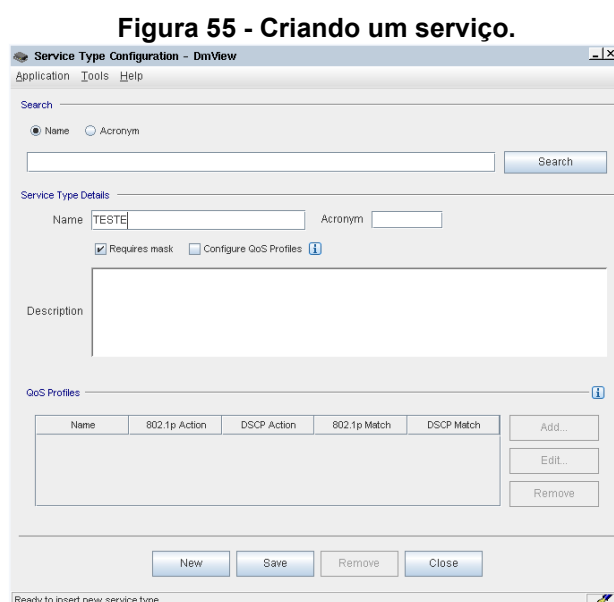
Para criar um circuito deve-se ter ao menos um “*Customer*” e um “*Service*” para proceder com a configuração. Ao entrar na opção “*Customer Configuration*” abrirá uma tela, ilustrada na figura 54, com apenas o campo “*Search by name*” habilitado e os botões “*new*” que será responsável pela criação do “*Customer*”, “*remove*” que removerá o “*Customer*” e “*close*” que fecha a janela. Ao selecionar “*new*” para iniciar a configuração, os demais campos são habilitados, sendo que os únicos que são obrigatórios de preenchimento são os campos “*Name*” e “*Priority*”. Após isso deve-se pressionar o botão *save*.

Figura 54 - Criando um cliente.

The screenshot shows the 'Customer Configuration' window. At the top, there is a search field labeled 'Search by name' and a 'Search' button. Below this is the 'Customer Details' section, which contains several input fields: Name (filled with 'TESTE'), Priority (dropdown menu set to '1 (Higher)'), Address, City, State, Area code, Telephone, Country, Email, Contact, and Notes (a text area). At the bottom of the window, there are four buttons: 'New', 'Remove', 'Save', and 'Close'.

Fonte: Autoria Própria

Para criar o circuito também é necessário ter ao menos um serviço configurado que pode ser feito na opção “*Service Type Configuration*”, essa opção gera a janela ilustrada na figura 55. Nesta janela existe o campo “*search*” que é apenas usado para pesquisa, o botão “*New*” que cria um novo serviço, “*Remove*” que deleta um serviço e “*Close*” para fechar. Para criar um novo serviço os únicos campos obrigatórios são “*Name*” e “*Acronym*”, campos como QOS não é configurado aqui na camada de transporte. Após esses procedimentos é necessário acionar o botão “*save*”.



Fonte: Autoria Própria

Após ter ao menos um “*Customer*” e um “*Service Type*”, pode-se criar um novo circuito selecionando a opção “*SDH/PDH Circuit Configuration*”, abrindo a janela ilustrada na figura 56, preenchendo o campo “*Name*”, “*Customer*” e “*Service Type*”. Os demais campos não são obrigatórios e deve se verificar qual é o padrão adotado pela operadora em questão.

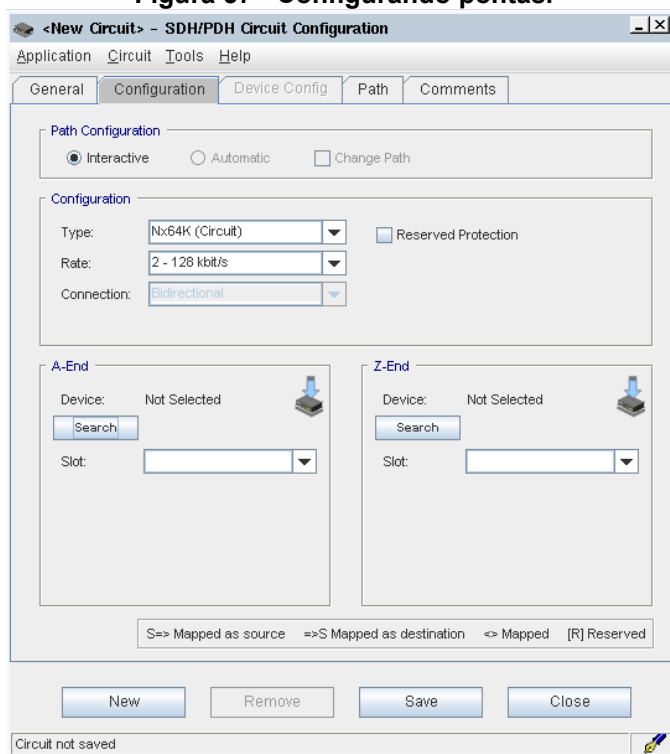
Figura 56 - Criando um circuito.

The screenshot shows a software window titled "<New Circuit> - SDH/PDH Circuit Configuration". The window has a menu bar with "Application", "Circuit", "Tools", and "Help". Below the menu bar are five tabs: "General", "Configuration", "Device Config", "Path", and "Comments". The "General" tab is selected. The "Identification" section contains four fields: "Mask" (a dropdown menu), "Name" (a text box containing "TESTE 4" and an "Edit" button), "Customer" (a dropdown menu containing "TESTE"), and "Service Type" (a dropdown menu containing "TESTE"). The "Management" section contains two fields: "Level" (a dropdown menu containing "Commissioned") and "Priority" (a dropdown menu containing "1 (Higher)"). Below these is a "History" section, which is currently empty. At the bottom of the window are four buttons: "New", "Remove", "Save", and "Close". A status bar at the bottom left of the window displays the text "Circuit not saved".

Fonte: Autoria Própria

Na aba “*configuration*”, vide figura 57, deve-se escolher um tipo de configuração. Aqui será usado o “Nx64K” que é uma quantidade N de canais 64 Kbit/s para trafegar os dados, e também será usado o “Rate” 2 que nesse caso compreende a 128 Kbit/s, porém se o cliente trafegar por outra velocidade múltipla de 64 Kbit/s e que fique abaixo de 2048 Kbit/s. Agora irá ser configurado o E1 e o E3 para fazer a comunicação entre multiplexadores, depois indo em “*Device Config*” e configurando conforme o padrão da operadora que difere entre uma e outra. Procedendo com a configuração do “Nx64K”, deve se escolher o “*A-End*” e o “*Z-End*”, para isso seleciona-se “*Search*” no quadro “*A-End*” e abrirá a tela para procurar o equipamento.

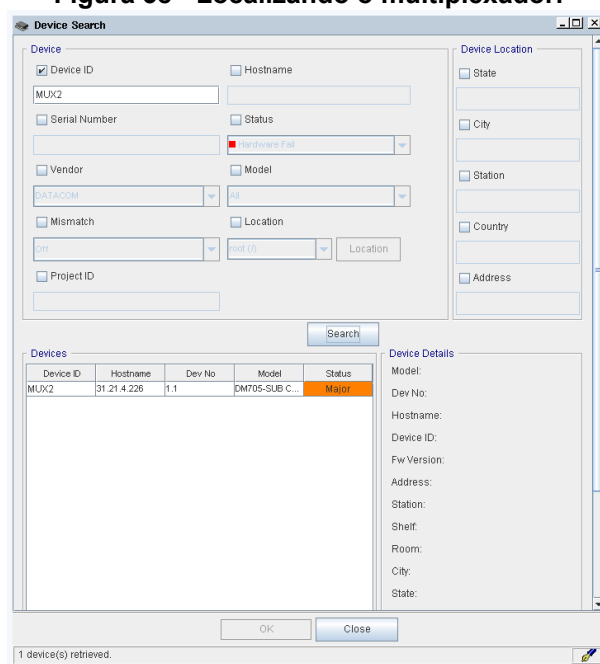
Figura 57 - Configurando pontas.



Fonte: Autoria Própria

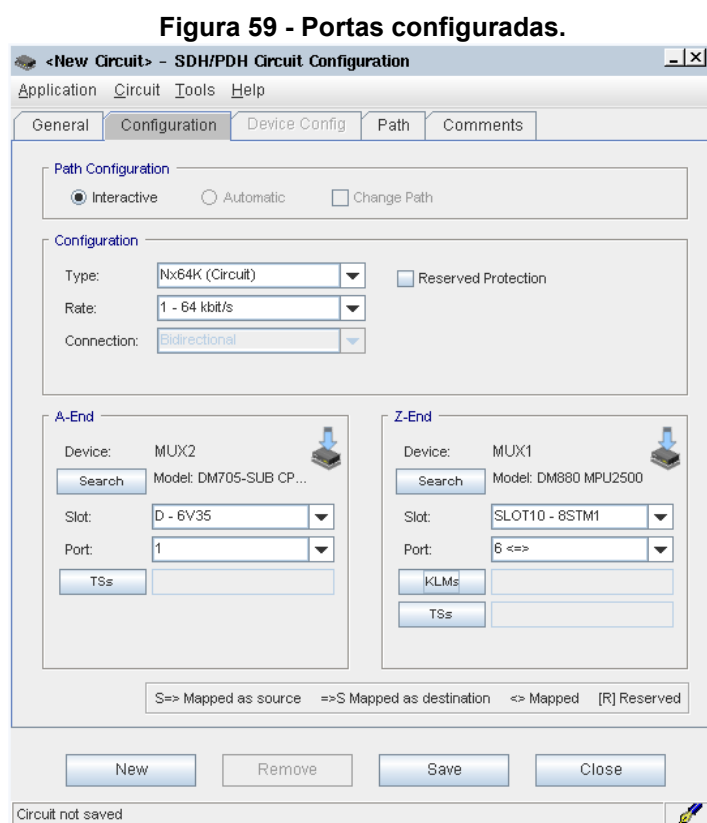
Na tela ilustrada na figura 58 deve ter o nome do multiplexador que está conectado à placa de acesso, ao digitar tem que clicar em “Search” e selecionar o multiplexador no quadro “Devices”.

Figura 58 - Localizando o multiplexador.



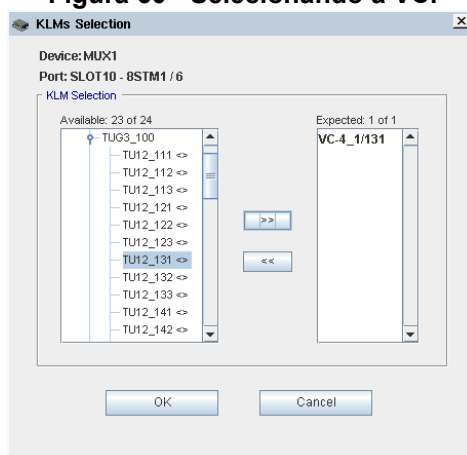
Fonte: Autoria Própria

Após isso, existe a necessidade de fazer o mesmo para o “Z-End”. Após realizar esse passo, é necessário selecionar o *slot* e porta como no exemplo foi usado no “MUX2” que provê o acesso *Slot* D, porta 1 e “MUX1” Slot 10, porta 6. Agora é importante selecionar o “KLM” que vai ser o E1 que interliga o roteador com o multiplexador, para isso haverá a obrigação de selecionar o botão “KLM”. A figura 59 ilustra a configuração sem o KLM.



Conforme foi selecionado no roteador o E1 na posição 1.3.1 no multiplexador deverá ter o mesmo 1.3.1 no TU12 para que haja a comunicação. A figura 60 mostra a seleção do TU12 131 que é 1.3.1 sem os pontos.

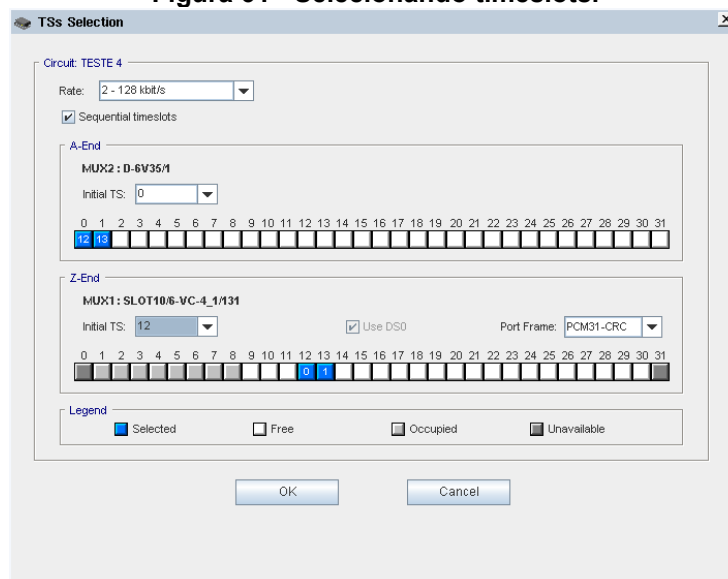
Figura 60 - Selecionando a VC.



Fonte: Autoria Própria

Logo após, é possível selecionar os “*timeslots*” sempre acasalando os números do roteador que como a interligação foi realizado com o roteador da Nokia deve-se subtrair 1 dos “*timeslots*” para que a comunicação seja realizada corretamente. No caso exemplificado foi selecionado o conjunto de *timeslot* 11-12 e aqui deve ser selecionado o 12-13. Se por algum motivo os “*timeslots*” estejam cinzas, como ocorre na figura 61, onde o conjunto de *timeslot* 1-8 do “Z-End” está neste estado é provável que exista algo aprovisionado.

Figura 61 - Selecionando timeslots.

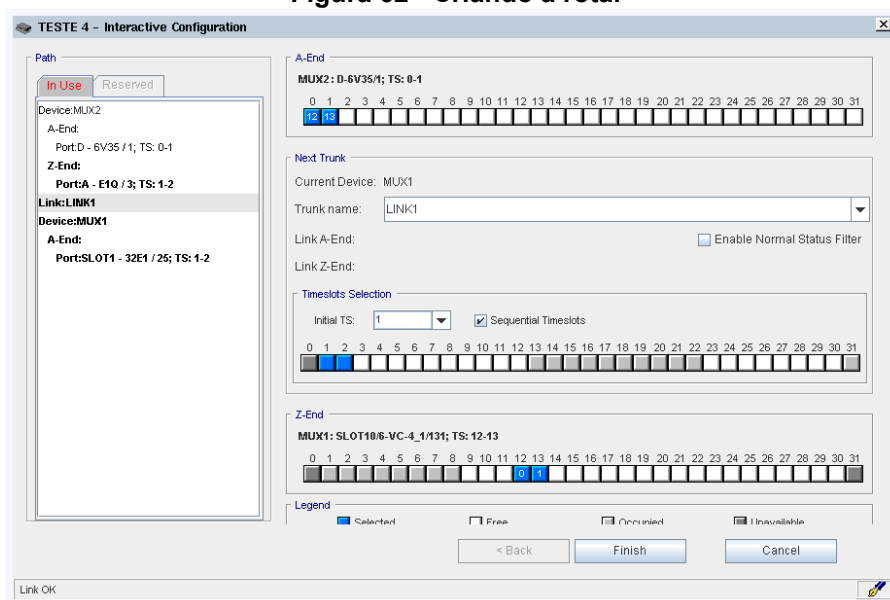


Fonte: Autoria Própria

Após confirmar os “*timeslots*” e salvar as configurações tem que gerar uma rota entre os multiplexadores. Nesse caso tem que ir selecionando os *links* E1 até

chegar no destino, ao chegar no destino o botão “*Finish*” vai habilitar igualmente mostrado na figura 62.

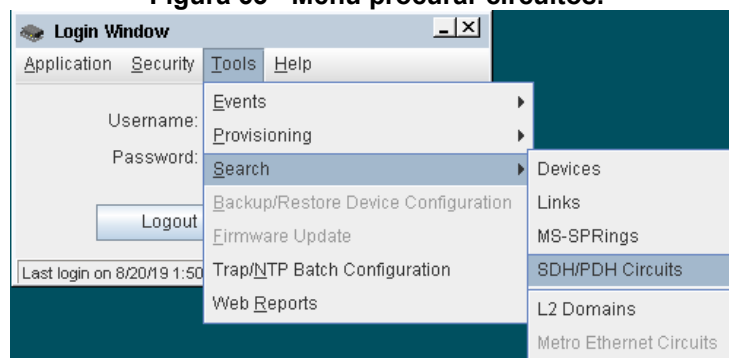
Figura 62 - Criando a rota.



Fonte: Autoria Própria

Para localizar no sistema o que foi criado deve-se selecionar as opções “*Tools*”, “*Search*” e “*SDH/PDH Circuits*” conforme ilustrado na Figura 63.

Figura 63 - Menu procurar circuitos.

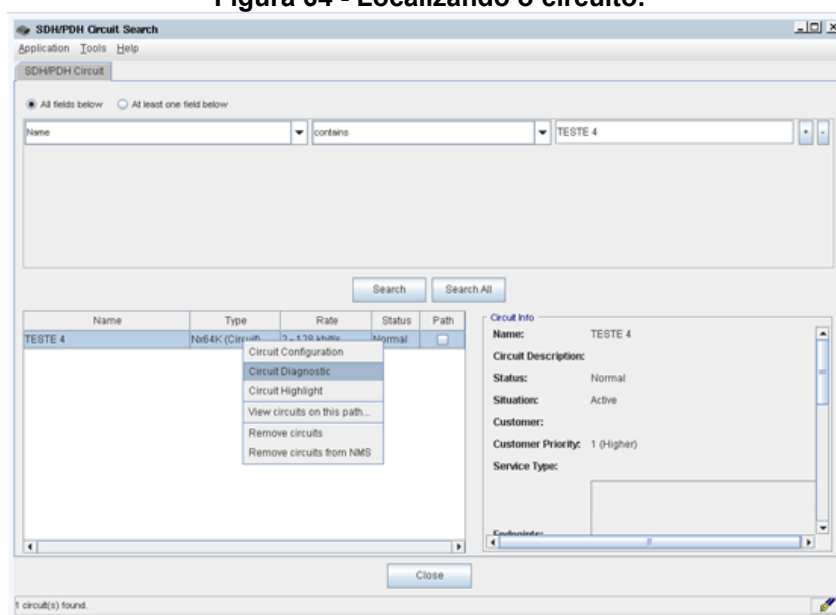


Fonte: Autoria Própria

Na janela que se abre haverá vários filtros conforme demonstrado na figura 64, a qual pode-se filtrar por nome, tipo, nível de alarme, sobre se a busca é igual, contém ou não contém a cadeia de caractere entre outros. Nesse caso foi escolhido o filtro por nome o qual contém o nome que foi configurado inicialmente, após selecionar “*Search*”, aparece no quadro inferior o que foi criado. Ao abrir o menu

flutuante terá a opção “*Circuit Diagnostics*” para verificar possíveis falhas e alarmes, “*Circuit Configuration*” para realizar configurações, “*Circuit Highlight*” que demonstra no mapa os saltos que o circuito realiza e não será utilizado, a opção “*View circuits on this path...*” que altera os filtros de busca para circuitos que estejam trafegando um E1 sendo que essa opção não é usada por não ser prática e por fim “*Remove circuits*” que serve para remover o circuito criado.

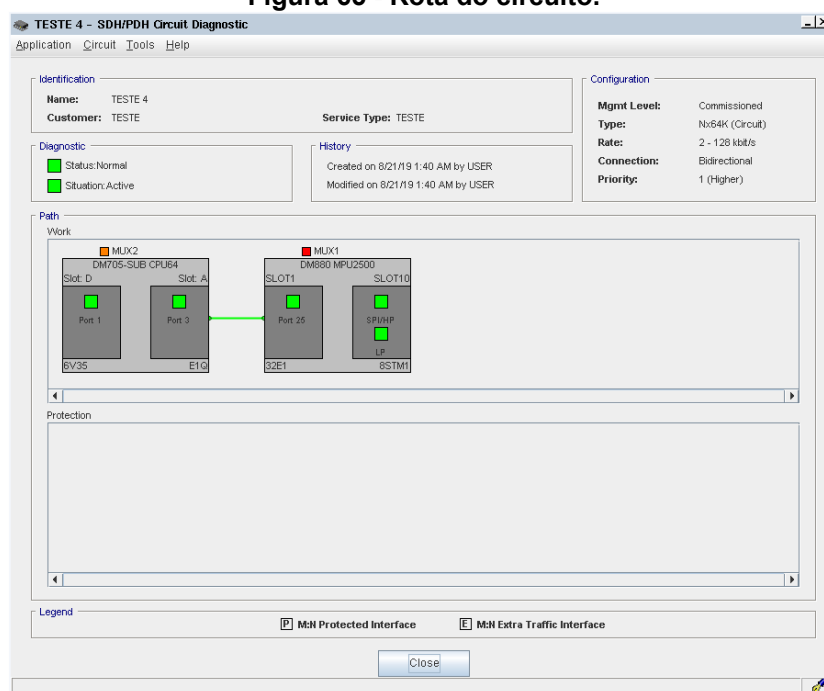
Figura 64 - Localizando o circuito.



Fonte: Autoria Própria

Ao entrar na opção “*Circuit Diagnostics*” haverá a opção de ver a rota do cliente e se algo na rota está alarmado, quanto mais multiplexadores for configurado no meio da rota mais saltos aparecerão e mais pontos de falhas existirão. A figura 65 ilustra isso.

Figura 65 - Rota do circuito.



Fonte: Autoria Própria

3.2.4 Conexão Roteador e Rede Newbridge

Para iniciar esse tipo de configuração foi necessário aprovisionar no roteador uma porta E3 para realizar a conexão com a gerência multiplexada conforme comandos da figura 66.

Figura 66 - E3 aprovisionado.

```
11#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
11(config)#controller E3 7/1/0
11(config-controller)#E1 1 channel-group 1 timeslots 1-2
```

Fonte: Autoria Própria

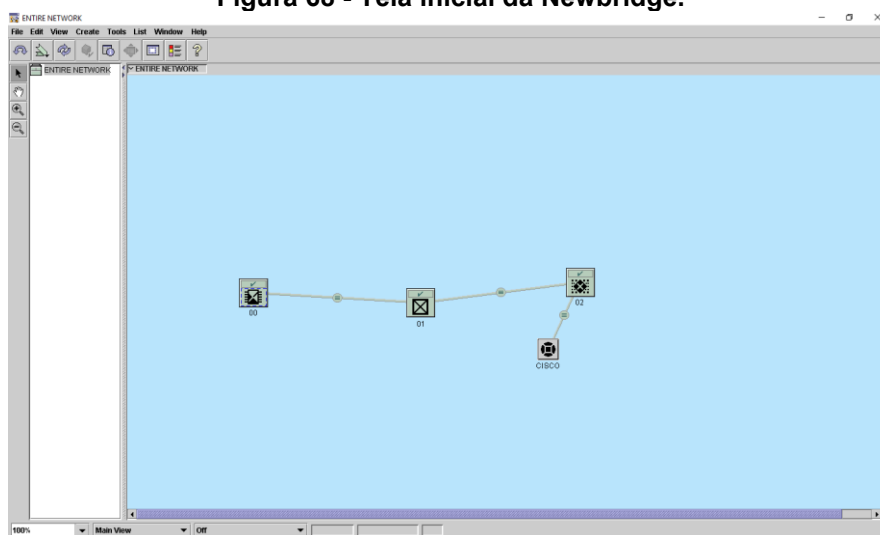
Para localizar as facilidades na outra gerência a operadora colocará a informação dentro da controladora como uma descrição. Para isso pode-se usar o comando “*show controller (placa) (facilidade)*”. O resultado do comando é ilustrado na figura 67.

Figura 67 - Descrição da porta.

```
11#show controller E3 7/1/0
E3 7/1/0 is up.
CE3 H/w Version : 4.2.1, CE3 ROM Version : 1.1, CE3 F/w Version : 1.2.1
Applique type is Channelized E3
Description: Interconexco com a NWB - 2AP3/12/1
```

Fonte: Autoria Própria

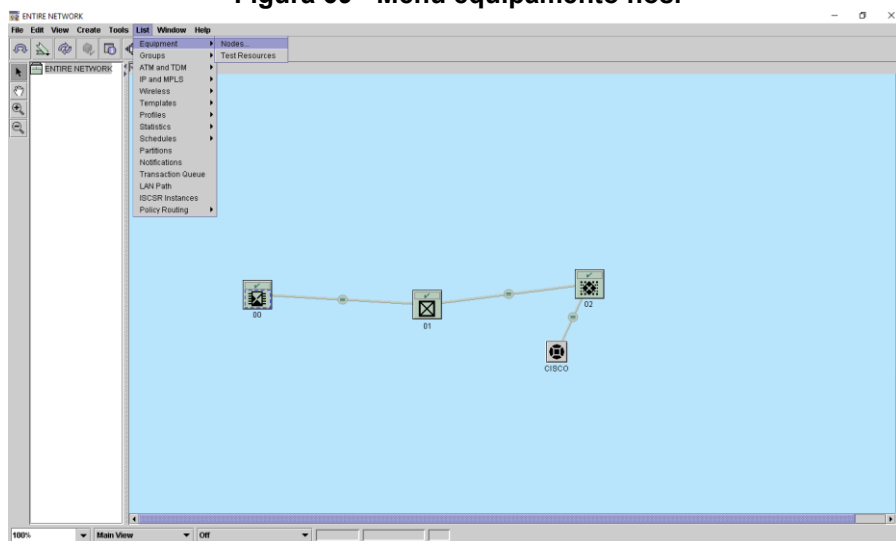
Desta vez será utilizada a gerência Newbridge que atualmente está com a patente da Nokia e serve para administrar os equipamentos da linha *mainstreet*, porém outras gerências como a datacom tem disponibilidade dessa placa em seus multiplexadores. A gerência tem a interface demonstrada na figura 68.

Figura 68 - Tela inicial da Newbridge.

Fonte: Autoria Própria

Normalmente existe muitos multiplexadores em uma rede nível operadora, o ideal então é conseguir filtrar os equipamentos desejados para realizar o provisionamento, nesse caso acessando o menu "List", opção "equipment" e depois opção "Nodes...". A figura 69 demonstra as opções selecionadas.

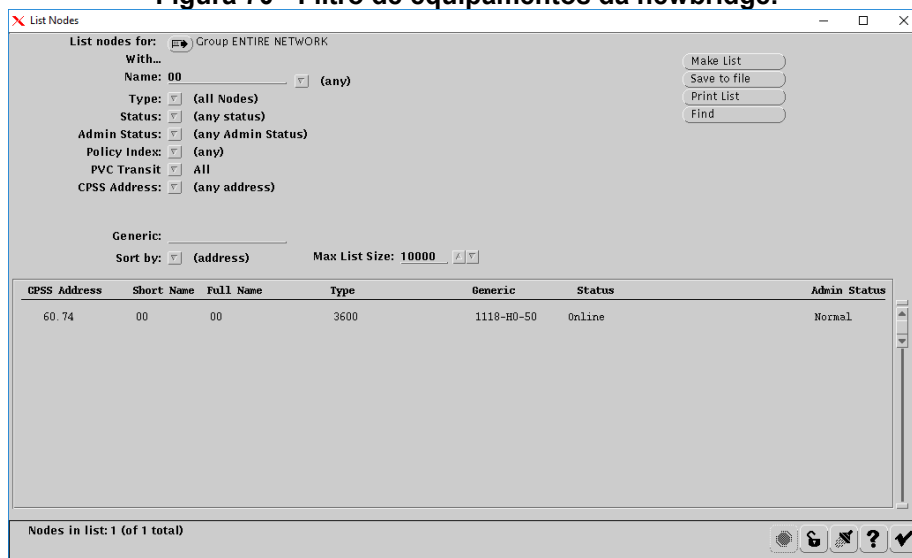
Figura 69 - Menu equipamento nós.



Fonte: Autoria Própria

A Newbridge possibilita o filtro por nome, tipo, estado do *link*, bloqueado ou não para provisionamento, configuração de tráfego e CPSS entre outros. Normalmente será passado o nome do equipamento para o técnico responsável pelo provisionamento das pontas pelo engenheiro de tráfego ou gestor técnico da região, nesse caso a ponta onde será configurado o IP do cliente e seu serviço vai ser no roteador Cisco que estará conectado ao multiplexador 02, e o acesso será provido pelo multiplexador 00. Então ambos serão localizados, independente da ordem. Nesse caso será o multiplexador 00. A figura 70 ilustra a interface de busca de equipamento da rede Newbridge.

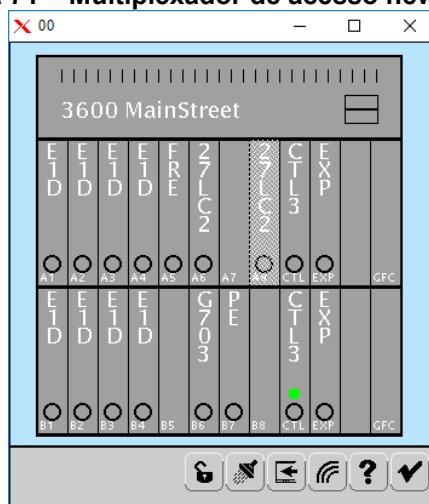
Figura 70 - Filtro de equipamentos da newbridge.



Fonte: Autoria Própria

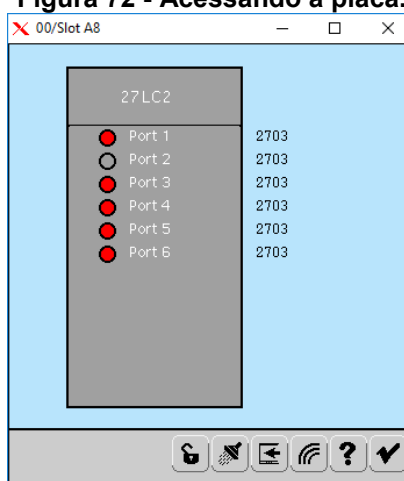
Ao localizar o multiplexador e abrir a janela referente ao mesmo ela mostrará a quantidade de placas, conforme ilustrado na figura 71. Dentro do multiplexador de acesso “00” tem-se 16 slots de placas e 6 para controle, as placas E1 fazem entroncamento entre multiplexador e placas 27LC, G703 e PE fazem acesso, as placas V35 e 28LC que não estão aqui fazem acesso também, a placa FRE é uma placa de recurso para *Frame Relay*. Nesse caso será usado como facilidade de provisionamento o slot A8 porta 2 DTU A. Para isso é necessário seleccionar a placa A8 no multiplexador.

Figura 71 – Multiplexador de acesso newbridge.



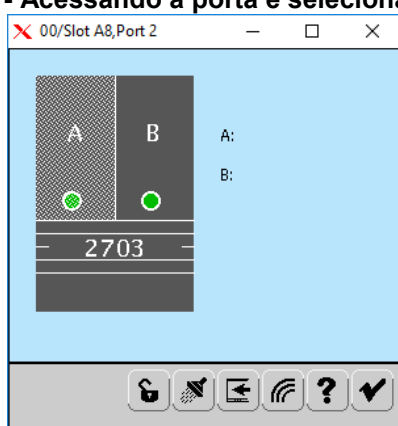
Fonte: Autoria Própria

Ao abrir a placa aparecerão portas, cuja quantidade poderá variar conforme o modelo da placa. A figura 72 mostra uma placa 27LC com 6 portas, as portas em vermelho não têm uma DTU configurada e é necessário a inserção da DTU fisicamente na estação, para proceder com a configuração deve-se entrar na porta 2 para acessar a DTU.

Figura 72 - Acessando a placa.

Fonte: Autoria Própria

Ao acessar a DTU, conforme figura 73, deve-se apertar no botão “lock” cuja aparência é de um cadeado para evitar que essa tela seja substituída na hora de abrir o outro multiplexador, já que para realizar o aprovisionamento essa tela deve estar aberta.

Figura 73 - Acessando a porta e selecionado a DTU.

Fonte: Autoria Própria

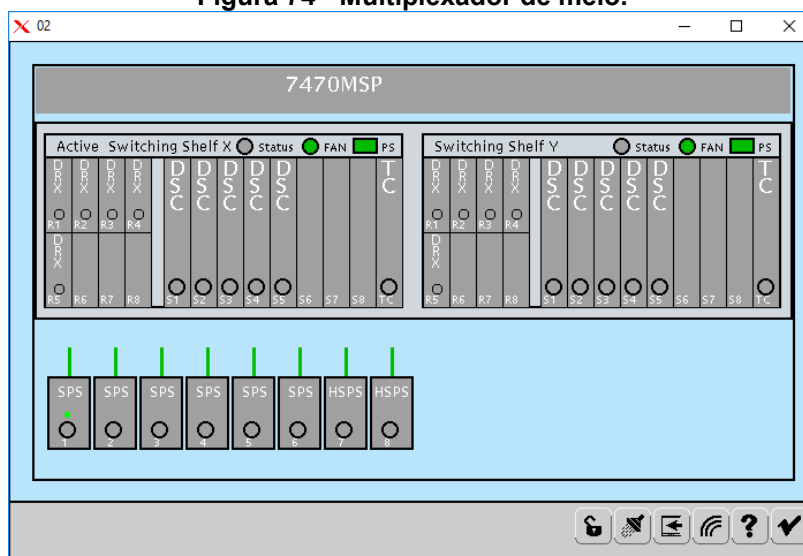
Nesse momento deve-se procurar o multiplexador 02 que faz a interface com o roteador Cisco. Esse multiplexador é do modelo 7470 MSP que é mais robusto e raramente é usado para prover acesso. Normalmente ele serve apenas para meio de transporte, como observado na figura 74, e tem placas DRX e DSC que tem a funcionalidade de executar a multiplexação dos dados entre duas portas sendo que a DRX faz a parte de recepção e a DSC a parte de transmissão, as placas “TC” são usadas para controle.

Os SPS e HSPS são periféricos que estão anexados ao multiplexador tendo

12 slots de transmissão para placas o modelo SPS e o modelo HSPS 8 slots, sendo este último para placas de alta capacidade como placas STM4.

Conforme a descrição verificada na figura 66, a *cross* conexão entre o roteador e o multiplexador é realizada no periférico 3, *slot* 12 e porta 1.

Figura 74 - Multiplexador de meio.



Fonte: Autoria Própria

No periférico 3 (SPS 3), cuja figura 75 ilustra tal periférico, haverá as placas sendo que as placas no *slot* HX e HY são de controle, e as E1 e E3 serão normalmente usadas para transporte. Nesse caso a conexão entre o Cisco e *Newbridge* está sendo realizada através de uma placa E3 localizada no *slot* 12, para proceder com o provisionamento tem que selecionar a placa desse *slot*.

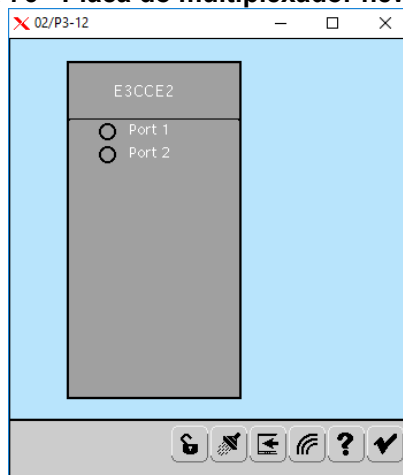
Figura 75 - Periférico do multiplexador.



Fonte: Autoria Própria

Nesse modelo de placa E3 haverá 2 portas vide figura 76, conforme demonstrado na descrição da controladora do Cisco a porta a ser selecionada é a 1.

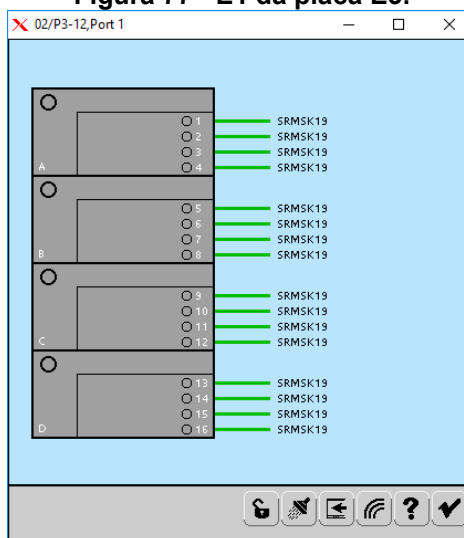
Figura 76 - Placa do multiplexador newbridge.



Fonte: Autoria Própria

A placa E3 é composta por 4 E2 que tem 4 E1 gerando no total 16 E1, conforme figura 66 desses 16 foi selecionado o E1 na posição 1, então conforme ilustrado na figura 77 deve ser selecionado a posição 1 também.

Figura 77 - E1 da placa E3.

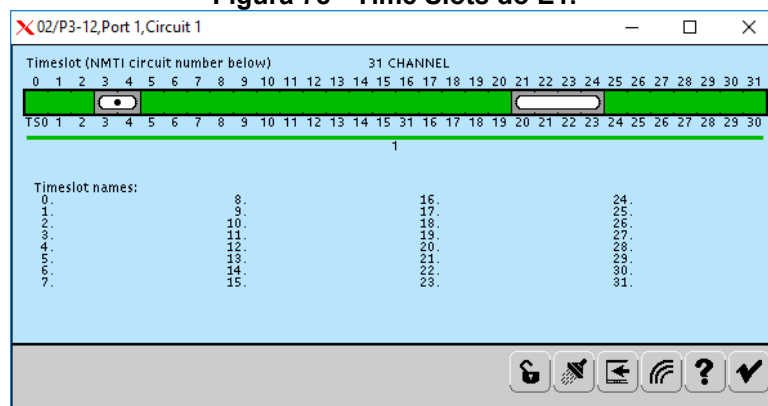


Fonte: Autoria Própria

Nesse ponto deve-se clicar no botão “lock” que aparenta ser um cadeado e está no canto inferior direito demonstrado na figura 78 para evitar que essa tela seja substituída. Aqui tem os 32 “timeslots” para serem selecionados no momento do provisionamento sendo que o *timeslot* 1 e 2 serão selecionados, os *timeslots* em

verde estão disponíveis, os demais estão sendo usados.

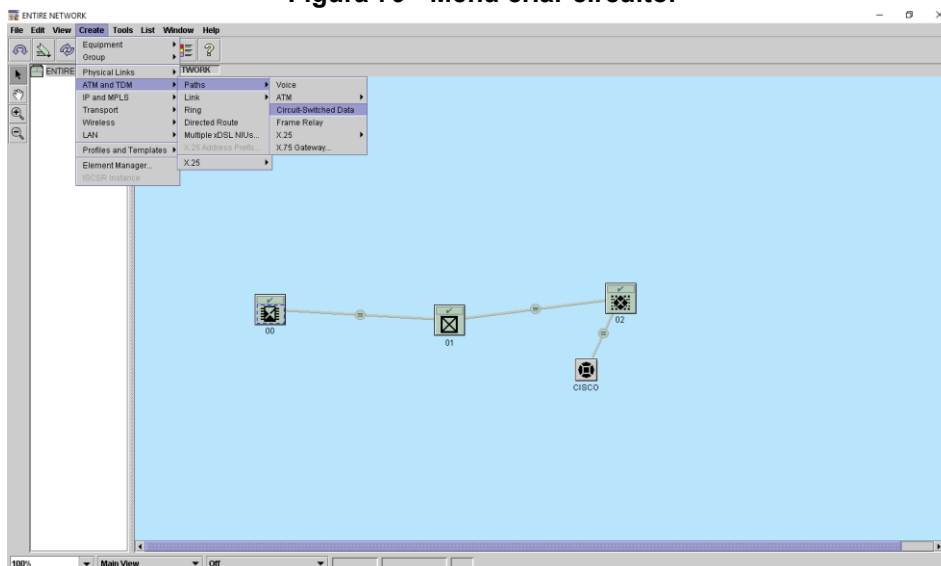
Figura 78 - Time Slots do E1.



Fonte: Autoria Própria

Para gerar a rota, deve-se selecionar a opção “Create”, “ATM and TDM”, “Paths” e “Circuit-Switched Data”. Existem outras tecnologias que podem ser provisionadas aqui como ATM e X.25 que não serão vistas nesse momento, porém estão ilustradas na figura 79.

Figura 79 - Menu criar circuito.

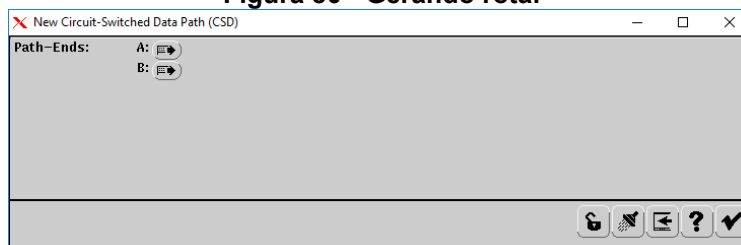


Fonte: Autoria Própria

Na tela que se abre não há como digitar nada, apenas haverá dois botões para poder indicar as pontas. Deve-se voltar ao multiplexador de acesso conforme passos ilustrados anteriormente até chegar no resultado da figura 73. Nesse ponto deve-se clicar na porta A da DTU e clicar logo em seguida no botão ao lado de “A:”

ilustrado na imagem 80 para determinar a ponta A. Para seleccionar a ponta B tem que se seguir os passos até alcançar o resultado da imagem 78 e seleccionar o *timeslot* 1 e logo depois seleccionar o botão ao lado de B: da imagem 80.

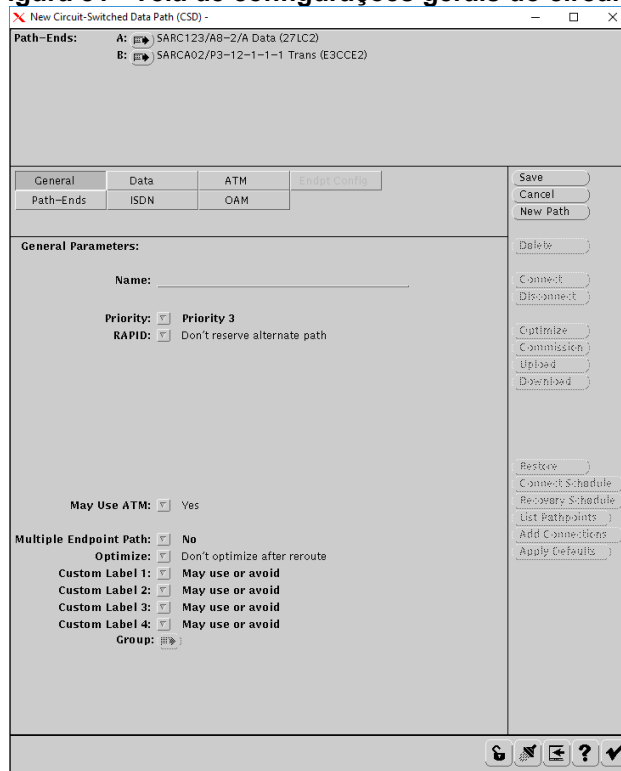
Figura 80 - Gerando rota.



Fonte: Autoria Própria

Após isso a tela se expandirá automaticamente mostrando um grande leque de opções conforme ilustrado na figura 81, sendo “Name:” o nome da rota, “*priority*” que é usada para a classificação de circuitos e agrupamentos, “*Multiple End Point Path*” que gera um link multiponto e os “*label*” que servem para gerar divisões em links multipontos. Não há a necessidade de gerar *links* multipontos devido ser uma conexão entre roteador e cliente nesse momento.

Figura 81 - Tela de configurações gerais do circuito.



Fonte: Autoria Própria

A figura 82 mostra a janela resultante ao clicar no botão “Data” e nela existem várias opções, sendo elas:

Subrate: Dividido em “*Don’t use subrate multiplexing*” usado para circuitos com taxa de dados superiores 56Kbps/s e “*Use subrate multiplexing*” para inferiores.

Rate adaptation: Pode ser selecionada o padrão I.460, DDS e HCM. Recomenda-se para esse tipo de uso o padrão I.460.

Interface Speed: Velocidade de tráfego.

Transport Bandwidth: Tamanho do *timeslot* em Kbp/s.

Figura 82 - Tela de configurações de dados do circuito.



Fonte: Autoria Própria

Ao selecionar o botão “ATM” têm-se as seguintes opções conforme figura 83.

Must Use VPC Link: Passarão vários VP’s no caminho. Nesse exemplo vai passar apenas uma que pertence ao cliente então será decidido colocar não.

VC Application: Tem como opção a conexão PVC, SPVC ou pode usar SPVC (*May use SPVC*). Sendo PVC um caminho fixo e SPVC um caminho que pode ser roteador em caso de queda por outro caminho disponível. É importante frisar que o SPVC ocorra e todos os multiplexadores devem ter suporte para essa ocorrência.

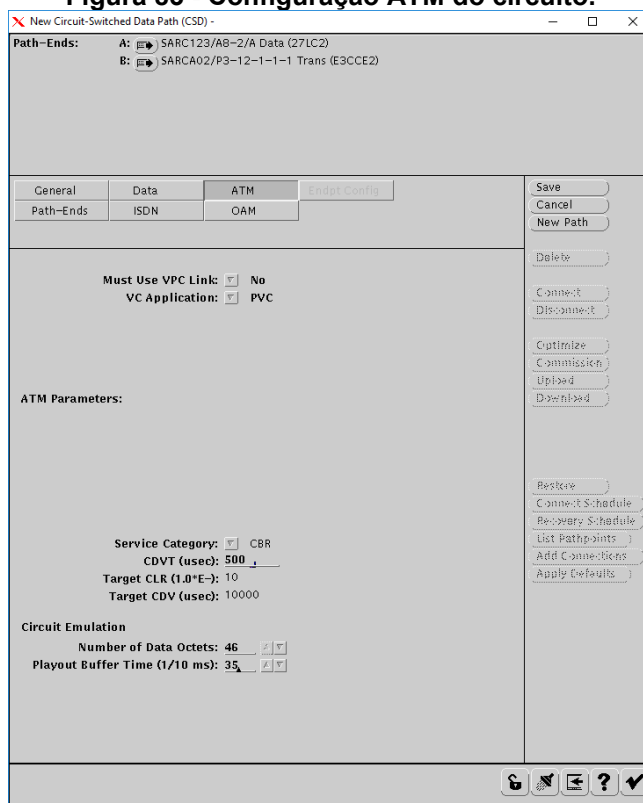
Service Category: Divididos em CBR, rt-VBR, nrt-VBR e UBR, conforme já explicado no tópico 2.3.

CDVT (usec): “*Cell Delay Variation Tolerance*” conforme tópico 3.2.5.

Number of Data Octets: Uma célula ATM tem por padrão 48 octetos de dados, mas aqui pode-se personalizar com mais ou menos, lembrando que caso tenha menos que 48 menor é a perda que ocorre no meio de transmissão caso tenha falha. Caso maior que 48 pode ocorrer problemas devido a *overhead*.

Playout Buffer Time (1/10 ms): Esse valor define o tempo que uma célula pode ficar aguardando na fila antes do descarte.

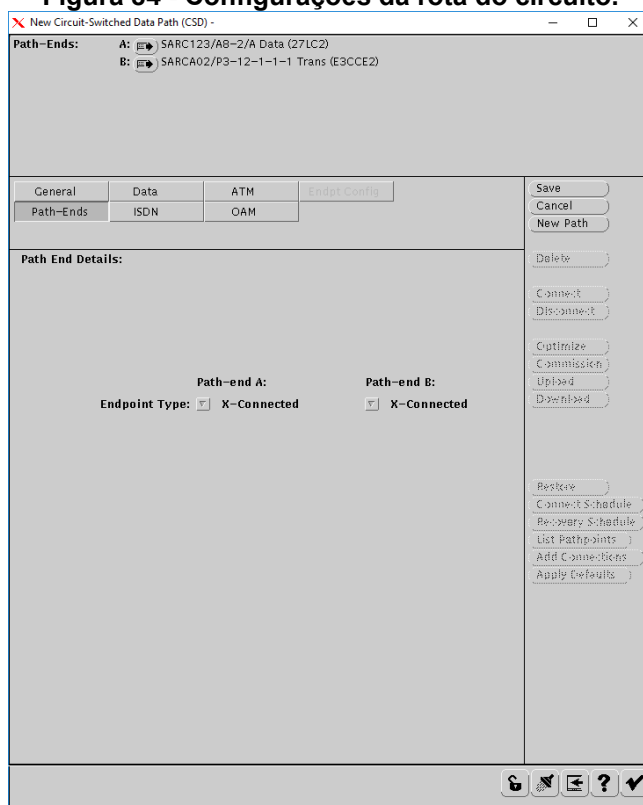
Figura 83 - Configuração ATM do circuito.



Fonte: Autoria Própria

No botão “*Path-Ends*” existem as duas pontas A e B conforme ilustrado na figura 84, aqui será selecionado se haverá *cross* conexão ou não. A opção “*X-Connected*” demonstra que haverá e a opção “*Non X-Connected*” não haverá *cross* conexão.

Figura 84 - Configurações da rota do circuito.



Fonte: Autoria Própria

Ao selecionar o botão ISDN se configura a tecnologia de voz ISDN, na opção “*primary path*” demonstrada na figura 85 existe tais parâmetros:

Must avoid ISDN: Usará apenas para tráfego entre as facilidades.

Use ISDN only if necessary: Onde o ISDN será usado apenas se necessário, se não houver nada trafegando no meio o ISDN irá trafegar.

May use ISDN: O ISDN irá trafegar em conjunto com os dados entre as facilidades, porém com pouca prioridade.

Must use only ISDN: A linha é reservada para a tecnologia ISDN.

Caso as 3 últimas opções sejam escolhidas, a opção “*Calling Line ID verification*” habilita onde se tem a opção de deixar ativo ou não. Aqui as ligações que trafegam por essa rede terão uma identificação.

Figura 85 - Configuração ISDN do circuito.



Fonte: Autoria Própria

Ao selecionar o botão OAM pode-se escolher as seguintes opções para o parâmetro “OAM Cell Flow”:

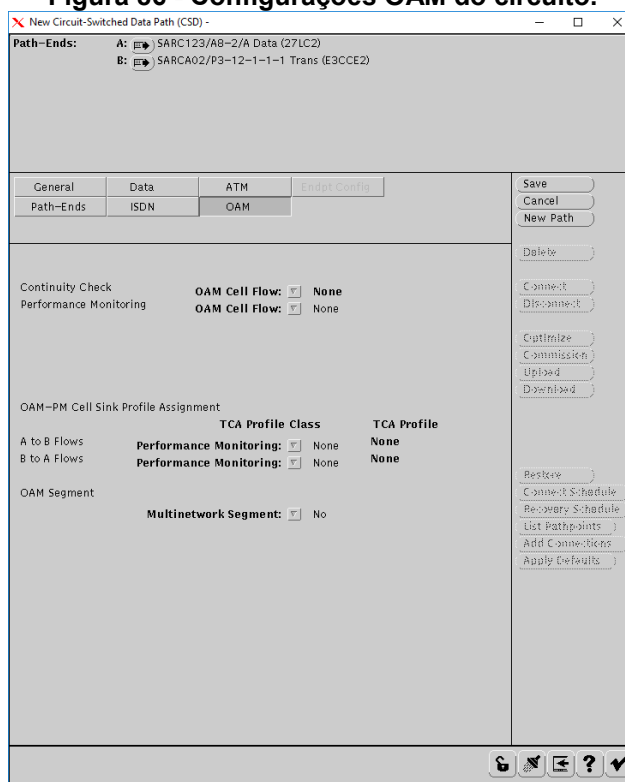
None: Desativa a verificação da continuidade de células.

A to B: Ativa a verificação da continuidade de células de A para B.

B to A: Ativa a verificação da continuidade de células de B para A.

Bidirectional: Ativa a verificação da continuidade de células em ambas as pontas.

Figura 86 - Configurações OAM do circuito.



Fonte: Autoria Própria

Após a realização de todas as configurações, deve-se escolher a opção *save* seguida de *connect*. No campo Status que está no canto superior esquerdo da figura 87, mostrará o estado atual do circuito que pode ser:

Connected: Conectado sem nenhum alarme na rede.

Connected (down): Circuito com alguma falha na rede.

Waiting for resources: Circuito com algum recurso indisponível na rede, durante os testes, sempre ocorreu após um multiplexador ficar indisponível ou apenas haver um E1 lotado no meio de comunicação, não existindo outro caminho para o circuito seguir

Waiting for repairs: Quando um recurso é colocado em reparo por algum motivo.

Interrupted via NMTI: Circuito interrompido via linha, normalmente quando há alguma alteração de política de tráfego no circuito quando ele está em funcionamento.

Under maintenance: Quando um loop é colocado no meio da rede ou BERT.

Disconnected requested: Está entrando em estado de “*Disconnected*”.

Reroute requested: Circuito sendo otimizado.

Ready for connect: Circuito desconectado manualmente.

Figura 87 - Circuito ativado.

Config Circuit-Switched Data Path (CSD) - TESTE 04

Path-Ends: A: SARCA123/AB-2/A Data (27LC2) P 1196-5136135
B: SARCA02/P3-12-1-1-1 Trans (E3CCEZ)

Status: Connected

OAM-CC Status: Not Configured
OAM-PM Status: Not Configured

Path Call ID: 3637005

General | Data | ATM | Endpt Config

Path-Ends | ISDN | OAM

Save
Cancel
New Path

General Parameters:

Name: TESTE 04

Priority: Priority 3

RAPID: Don't reserve alternate path

May Use ATM: Yes

Multiple Endpoint Path: No

Optimize: Don't optimize after reroute

Custom Label 1: May use or avoid

Custom Label 2: May use or avoid

Custom Label 3: May use or avoid

Custom Label 4: May use or avoid

Group:

Delete
Connect
Disconnect
Optimize
Commission
Upload
Download
Restore
Connect Schedule
Recovery Schedule
List Pathpoints
Add Connections
Apply Defaults

Fonte: Autoria Própria

3.2.5 Conexão Roteador e rede CISCO BPX/IGX

Para que haja a conexão de uma rede moderna com uma rede ATM que é legada e ainda utilizada existe a necessidade de gerar a *cross* conexão, nessa parte haverá a explicação da conexão de um multiplexador ATM BPX/IGX a um roteador Cisco. Conforme figura 88 normalmente na hora da criação da porta existe uma descrição de qual é a porta e equipamento de destino no roteador Cisco, nesse caso é o BPX ME500 porta física 2.6, infelizmente na rede BPX não há como colocar uma descrição.

Figura 88 – Porta do equipamento Cisco para a rede BPX/IGX.

```
#sh int ATM5/0/1
ATM5/0/1 is up, line protocol is up
Hardware is SPA-2XOC3-ATM, address is 001a.e336.9cc0 (bia 001a.e336.9cc0)
Description:BPX_ME500_2.6
MTU 4470 bytes, sub MTU 4470, Bw 149760 Kbit, DLY 80 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive not supported
Encapsulation(s): AAL5
4095 maximum active VCs, 29 current VCCs
VC idle disconnect time: 300 seconds
0 carrier transitions
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 4w4d
Input queue: 0/75/0/12 (size/max/drops/flushes); Total output drops: 21861
Queueing strategy: fifo
Output queue: 0/40 (size/max)
30 second input rate 6000 bits/sec, 15 packets/sec
30 second output rate 265000 bits/sec, 271 packets/sec
80480462 packets input, 7973472912 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
10465162 input errors, 10465162 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1611824843 packets output, 217261009776 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Fonte: Autoria Própria

O primeiro passo é ver se a facilidade que se quer inserir o circuito está disponível ou sem uso, será selecionado para exemplo a pvc 201/94 e o padrão selecionado pela operadora é deixar VPI 201 oculto no nome, ou seja a porta será X.94. Nesse exemplo a porta é AT5/0/1, ao lançar o comando “*show interface description*”, conforme ilustrado na imagem 85, filtrará tudo o que há na porta. Na figura 89 é verificado que a porta AT5/0/1.94 está disponível.

Figura 89 - Filtrando facilidades.

```
303#show interface description | include AT5/0/1
AT5/0/1                up                up                BPX_ME500_2.6
AT5/0/1.51            up                up
AT5/0/1.64            up                up
AT5/0/1.67            up                up
AT5/0/1.73            down             down
AT5/0/1.80            up                up
AT5/0/1.83            up                up
AT5/0/1.86            up                up
AT5/0/1.105           up                up
AT5/0/1.125           up                up
AT5/0/1.132           up                up
AT5/0/1.141           down             down
AT5/0/1.156           deleted          down
AT5/0/1.171           down             down
AT5/0/1.174           admin down      down
AT5/0/1.175           up                up
AT5/0/1.187           up                up
AT5/0/1.198           deleted          down
AT5/0/1.209           up                up
AT5/0/1.224           up                up
AT5/0/1.233           up                up
```

Fonte: Autoria Própria

No BPX, diferente da rede Datacom e Newbridge que há interface gráfica, será tudo por linha de comando, o primeiro comando usado é o “*dspscons*” que demonstra as conexões entre ponta A e ponta B na rede BPX/IGX assim como demonstrado na figura 90. Esse comando será usado para confirmar se a VPI/VCI está sendo usada na interface 2.6 que se interliga com a porta ATM 5/0/1 do roteador. Aqui pode-se ver que começa com a facilidade 2.6.201.95 se conectando com o equipamento V400, não tendo uma conexão com a facilidade 2.6.201.94 que

será configurada.

Figura 90 - Verificando facilidades no BPX.

```

500      TN      User:2      BPX 8620  9.3.51  Nov. 12 2019 07:00 G-03
FROM
2.6.201.94 Remote Remote State Type Route
NodeName Channel          Avoid COS O
2.6.201.95 V400 14.6.16 ok atxfst 0 L
2.6.201.96 N400 8.26.16 ok atxfst 0 L
2.6.201.100 N401 9.6.16 ok atxfst 0 L
2.6.201.105 N500 13.4.201.233 ok nrt-vbr 0 L
2.6.201.118 E500 3.3.201.118 ok abrst 0 L
2.6.201.125 N500 13.4.201.264 ok nrt-vbr 0 L
2.6.201.126 N500 1.5.201.126 ok nrt-vbr 0 R
2.6.201.130 N500 12.1.201.322 ok nrt-vbr 0 R
2.6.201.132 N500 13.4.201.113 ok nrt-vbr 0 L
2.6.201.144 N500 1.5.201.178 ok nrt-vbr 0 L
2.6.201.145 E400 10.8.16 ok atxfst 0 L
2.6.201.147 N401 9.2.16 ok atxfst 0 L
2.6.201.148 E400 16.48.16 ok atxfst 0 L
This Command: dspcons 2.6.201.94
Continue direction - Next/Quit? (n/q) █
MAJOR ALARM

```

Fonte: Autoria Própria

Para configurar no cisco essa conexão basta entrar no “*configure terminal*” e entrar na caixa da interface desejada, não necessariamente sendo ATM5/0/1.94, se quiser colocar a VCI junto ou usar uma formula matemática para gerar o número após o ponto também pode, o importante é que seja bem documentado para o filtro. Dentro da caixa interface pode-se configurar IP, VRF, QOS e o que for necessário, depois disso tem que se criar o PVC que receberá como parâmetro o VPI/VCI, dentro dessa caixa será configurado o encapsulamento atm desejado e configurações pertinentes ao ATM. Todos os passos foram ilustrados para melhor entendimento na figura 91.

Figura 91 - Criando PVC no Cisco.

```

#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface ATM5/0/1.94
(config-subif)#pvc 201/94
(config-if-atm-vc)#encapsulation aal5snap

```

Fonte: Autoria Própria

Para gerar a conexão deve-se encontrar um outro equipamento, foi usado o equipamento V400 no exemplo e após isso lançado o comando *dspscds* para verificar as placas disponíveis, tendo 2 placas OC3 da tecnologia SONET, 5 placas E1 e 4 placas V35 conforme demonstrado na figura 92, a conexão aqui gerada será para uma placa V35 que provê acesso ao cliente, as placas E1 e SONET são usadas para conexão de BPX e IGX ou outras gerências.

Figura 92 - Verificando placas no IGX.

```

V400          Vi          User:2          IGX 8420          9.3.51          Nov. 14 2019 02:37 G-03

FrontCard    BackCard
Type Rev     Type Rev     Status
1  NPM  EPS                AD Standby
2  NPM  EPS                AD Active
3  UXM  BDT  OC3            AD Active
4  UXM  BDT  OC3            AD Active
5  UFM  AWW  E1B            AD Active
6  UXM  BFT  OC3            AC Active
7  UFMU ASN  V35            AD Active
8  UFMU BWH  V35            AD Active-T

FrontCard    BackCard
Type Rev     Type Rev     Status
9  UFMU AUN  V35            AD Active
10 Empty universal backplane
11 Empty universal backplane
12 Empty universal backplane
13 UFM  AXW  E1B            AE Active
14 UFM  AXW  E1B            AE Active-T
15 UFM  AXW  E1B            AE Active
16 UFM  AXW  E1B            AE Active

Last Command: dspcds

Next Command: █

Virtual Terminal          MAJOR ALARM

```

Fonte: Autoria Própria

Nesse caso foi selecionado a placa 7, que é uma placa V35 com capacidade para 12 portas conforme lançado o comando “*dspport*” com o número da placa como parâmetro conforme a figura 93. Existe as seguintes colunas aqui:

- *Port*: É o número da porta física.
- *Line*: Porta lógica, usado para placas E1.
- *Port ID*: Serve para agrupamentos, esse parâmetro não será usado nesse material.
- *Speed*: Velocidade da porta.
- *Interface*: Nesse caso sempre será V.35, com a diferença de ser DTE e DCE. Segundo a ITU-T padrão V.24 uma ponta terá que ser obrigatoriamente DTE e outra DCE.
- *State*: Poderá ser *Failed*, *Active* e *Inactive*, sendo que quando *Failed* apresenta alguma falha, *Active* está alinhado sem falha e *Inactive* desativada manualmente.
- *Protocol*: Terá como opções Cisco LMI, *Annex A UNI*, *Annex D UNI*, *Annex A NNI* or *Annex D NNI*, sendo todos protocolos *Frame Relay*.

Figura 93 - Verificando portas no IGX.

```

V400 VT User:2 IGX 8420 9.3.51 Nov. 14 2019 02:49 G-03
Port configuration for UFMU 7
Port Line ID Speed Interface State Protocol
1 1 0 256 Kbps V35 (DTE) FAILED Annex D UNI
2 2 0 2048 Kbps V35 (DTE) ACTIVE None
3 3 0 512 Kbps V35 (DTE) FAILED Annex D UNI
4 4 0 2048 Kbps V35 (DTE) FAILED Annex D UNI
5 5 0 2048 Kbps V35 (DTE) FAILED Annex D UNI
6 6 0 2048 Kbps V35 (DTE) INACTIVE Annex D UNI
7 7 0 512 Kbps V35 (DTE) FAILED Annex D UNI
8 8 0 2048 Kbps V35 (DTE) ACTIVE None
9 9 0 1024 Kbps V35 (DTE) FAILED Annex D UNI
10 10 0 1024 Kbps V35 (DTE) FAILED Annex D UNI
11 11 0 1024 Kbps V35 (DTE) FAILED Annex D UNI
12 12 0 512 Kbps V35 (DTE) FAILED Annex D UNI
Last Command: dspport 7

Next Command: █
Virtual Terminal MAJOR ALARM

```

Fonte: Autoria Própria

Ao verificar as portas, existe uma inativa que é a da posição 6. A princípio essa porta será utilizada para exemplificar sendo a ponta B do exemplo.

Figura 94 - Verificando conexões no IGX.

```

V400 VT User:2 IGX 8420 9.3.51 █
From Remote Remote State Type Compress Code COS
7.6 NodeName Channel
7.11.16 ME500 2.6.201.168 ok atfx 0
8.9.100 E400 10.12.103 ok fst 0
8.10.541 E400 11.12.238 ok fst 0
8.12.100 N500 12.8.41.826 ok atfx 0
9.2.19 E501 14.3.251.102 Failed atfxfst 0
9.8.16 E400 7.10.28 ok fst 0
13.8.21 P400 6.2.100 Failed fst 0
13.8.999 E400 10.4.165 Failed fst 0
13.20.16 N500 12.8.41.105 ok atfx 0
13.156.16 C400 9.2.100 Down fst 0
13.156.999 ME500 2.6.99.999 ok atfst 0
13.160.16 V400 4.2.10.133 ok atfx 0
14.4.16 ME500 2.6.201.94 ok atfxfst 0
This Command: dspcons 7.6

Continue direction - Next/Quit? (n/q)
█ █

```

Fonte: Autoria Própria

Após lançar o comando que demonstra as conexões (*dspscons*), ilustrado na figura 94, é verificado que a porta localizada no *slot 7* e posição 6 não tem nenhuma conexão garantindo o seu uso. Após isso deve-se deixar a porta como ativa (*Active*), então seleciona-se o comando *upport* conjuntamente com o *slot* e porta, a figura 95 exemplifica seu uso.

Figura 95 - Ativando porta no IGX.

```

V400          VT          User:2          IGX 8420 9.3.51 Nov. 15 2019 00:49 G-03
Port:         7.6          [ACTIVE ]
Interface:    V35          DTE          Configured Clock: 2048 Kbps
Clocking:     Normal      Measured Rx Clock: 0 Kbps
Neighbor IP   Add: 0.0.0.0 Neighbor IIndex: 0
Port ID       0           Min Flags / Frames 1
Port Queue Depth 65535 OAM Pkt Threshold 3 pkts
ECN Queue Threshold 65535 T391 Link Intg Timer 10 sec
DE Threshold 100 %      N391 Full Status Poll 6 cycl
Signalling Protocol Annex D UNI EFCI Mapping Enabled No
Asynchronous Status Yes CLLM Enabled/Tx Timer No/ 0 msec
T392 Polling Verif Timer 15 IDE to DE Mapping Yes
N392 Error Threshold 3 Interface Control Template
N393 Monitored Events Count 4 Lead RTS DTR
Communicate Priority No State ON ON
Advertise Intf Info Disable
Last Command: upport 7.6
Next Command:

```

Fonte: Autoria Própria

Após isso pode-se configurar a forma conforme desejado, usando o comando “*cnfport*” junto com o *slot* e porta que receberá como parâmetros adicionais obrigatórios:

- *Port type*: Pode ser DTE ou DCE, lembrando que duas pontas não podem ser iguais.
- *Port speed*: Velocidade da porta, alcançando até 2048 Kbps.
- *Clock type*: Normal ou *looped*, sendo que esse loop não será usado devido às topologias aqui trabalhadas.
- *Port ID*: Serve para agrupamentos, esse parâmetro não será usado nesse material.
- *Maximum transmit queue depth*: Esse parâmetro define a profundidade máxima da fila para a transmissão.
- *Port ECN queue threshold*: É o limite da fila que a porta pode ter de FECN ou BECN.
- *DE threshold*: É o limite de frames elegíveis para descarte que a porta pode guardar.
- *Signalling Protocol*: Pode ser selecionado como C para Cisco, A para padrão ITU e D para padrão ANSI.
- *NNI Status*: Se o padrão vai ser NNI ou UNI.
- *Asynchronous Status*: Habilita o envio de uma mensagem de tempos em tempos para verificar se o PVC falhou ou caiu.
- *Polling Verification Timer*: Para os padrões UNI é o tempo que começa a contar após o não recebimento do frame de informação de estado.
- *Error Threshold*: Limite de erros tolerado.

- *Monitored Events Count*: Contador de eventos monitorados como queda e restabelecimento da porta.
- *OAM Threshold*: Limite de pacotes OAM.
- *Enable EFCI to BECN mapping*: Ativa o mapeamento de “*Explicit Forward Congestion Indication threshold*” da rede ATM para “*Backward Explicit Congestion Notification*” da rede *Frame Relay*.
- *Foresight over port* (CLLM): Freeman (2005, p. 335) afirma que CLLM (*Consolidated Link Layer Management*) é uma mensagem gerada para rede como forma de prover o BECN (*Backward Explicit Congestion Notification*). O *Foresight* é um mecanismo de controle de tráfego implementado pela Cisco (CASTELLI, 2002, p. 392). Conforme os autores esse protocolo controla o congestionamento de tráfego com *Foresight* que é usado apenas em equipamentos Cisco e pode ser ativado se tiver apenas equipamentos Cisco com suporte a essa tecnologia.
- *Map IDE to DE at Egress*: Mapeia o campo IDE (*Indicator Discard Eligibility*) que é um indicador de descarte recebido por ele ser um equipamento DTE para o campo DE (*Discard Eligibility*) do *Frame Relay*.
- *Min Number of Flags between Frames*: O mínimo de *flags* que podem existir entre os quadros.
- *Advertise Interface Information*: Indica se o equipamento deve-se comunicar a porta com a ILMI (*Integrated Local Management Interface*).

Essa complexa configuração é exemplificada na figura 96.

Figura 96 - Configurando porta no IGX.

```

V400          Vi          User:2          IGX 8420  9.3.51          Nov. 15 2019 01:53 G-03
Port:         7.6          [ACTIVE ]
Interface:    V35          DTE          Configured clock: 256 kbps
Clocking:     Normal
Neighbor IP  Add: 0.0.0.0 Neighbor IfIndex: 0
Port ID      0           Min Flags / Frames 1
Port Queue Depth 65535 OAM Pkt Threshold 3 pkts
ECN Queue Threshold 65535 T391 Link Intg Timer 10 sec
DE Threshold 100 %      N391 Full Status Poll 6 cyl
Signalling Protocol Annex D UNI EFCI Mapping Enabled No
Asynchronous Status Yes CLLM Enabled/Tx Timer No/ 0 msec
T392 Polling Verif Timer 15 IDE to DE Mapping Yes
N392 Error Threshold 3 Interface Control Template
N393 Monitored Events Count 4 Lead RTS DTR
Communicate Priority No State ON ON
                          Advertise Intf Info Disable

Last Command: cnfport 7.6 DTE 256 NORMAL 0 65535 65535 100 d N Y 15 3 4 3 N N Y
I N
Next Command: █
Virtual Terminal MAJOR ALARM

```

Fonte: Autoria Própria

Para gerar a conexão foi retornado ao equipamento “ME500” e ali será usado o comando “*cnfport*” tendo como parâmetros:

- Porta: A porta selecionada no equipamento local, no caso estudado será a porta 2.6.201.94.
- Equipamento Remoto: O equipamento remoto a qual a conexão será realizada, que nesse caso é o equipamento V400.
- Porta Remota com DLCI: A porta remota deverá ter uma DLCI conforme tópico 2.7 nos casos de acesso via V35, no exemplo foi inserido “7.6.16”, sendo 16 a DLCI.
- Tipo de encapsulamento ou classe: Aqui pode-se se selecionar vários parâmetros como:
 - *Constant Bit Rate (CBR)*: Já abordado no tópico 2.3;
 - *Variable Bit Rate (rt-Vbr/nrt-Vbr)*: Conforme abordado no tópico 2.3;
 - *ATM-to-Frame Relay interworking connection (ATFR)*: Conexão transparente na rede ATM por VBR entre conexões *Frame Relay*, com parâmetros reduzidos em frente do ATFT/ATFTFST;
 - *ATM-to-Frame Relay interworking with Foresight connection (ATFST)*: Ocorre como ATFR contendo o algoritmo *Foresight* em uma conexão ATM ABR;
 - *Available Bit Rate according to ATM Forum standards (ABRSTD)*: Abordado no tópico 2.3. como ABR;
 - *Available Bit Rate with Foresight (ABRFST)*: A mesma definição que o ABRSTD, porém com o algoritmo *Foresight* rodando se habilitada na porta;
 - *Frame Relay-to-ATM transparent Service Interworking (ATFT)*: Parâmetro usado para quando as duas pontas sejam *Frame Relay*, passando de forma transparente pela rede ATM como vbr;
 - *Frame Relay-to-ATM transparent Service Interworking with Foresight (ATFTFST)*: O mesmo que ATFT mas com o algoritmo *Foresight* e ATM como ABR;
 - *Frame Relay-to-ATM translational Service Interworking (ATFX)*: Parâmetro usado quando uma das pontas é ATM, sendo traduzido no meio ATM como vbr;
 - *Frame Relay-to-ATM translational Service Interworking with Foresight*

(ATFXFST): Mesmo que o ATFX porém com o algoritmo *Foresight* ativo sendo traduzido no meio ATM como ABR;

- *Unspecified Bit Rate* (UBR): Conforme tópico 2.3.
- PCR(0+1) (*Peak Cell Rate*): Esta é a taxa máxima na qual um usuário é permitido injetar dados na rede (KASERA, 2006, p. 132).
- % Utilização: Porcentagem de utilização de banda, pode ser ultrapassada se houver banda.
- MCR (*Minimum Cell Rate*): Esta é a taxa negociada entre os sistemas finais e a rede, qual a taxa de célula enviada pelos sistemas finais na conexão ABR necessita nunca ser menor que o MCR (MISHRA, 2010, p. 73).
- CDVT(0+1) (*Cell Delay Variation Tolerance*): Representa o limite superior na variação de atraso das células (KASERA, 2006, p. 134).
- VSVD (*Virtual Source Virtual Destination*): Opção que permite para dividir uma conexão ABR em segmentos ABR controlados separadamente (KOTA; PAVALAN; LEPPANEN, 2004, p. 239). Configuração para satélite.
- FBTC (*AAL Frame-Based Traffic Control*): Se esta opção é permitida, supõe-se que a conexão leva os quadros AAL5. O termo quadro significa o AAL5PDU. As pilhas AAL5 contêm a informação para indicar o início e final de frame. O FBTC permite o descarte de pacote anterior (EPD) em tudo através dos troncos para uma conexão específica (CISCO SYSTEM INC., 2018).
- FCES (*Flow Control External Segment*): Esta opção permite que o BXM forneça a informação de congestionamento ao Produtos não-Cisco usando uma interface padrão. O FCES estende o controle de fluxo ABR ao segmento externo (CISCO SYSTEM INC., 2018).
- *Default extended parameters*: Deixa diversos valores em padrão.
- SCR (*Sustainable Cell Rate*): Este é o limite superior da taxa média das células conforme a conexão ATM (MISHRA, 2010, p. 73)
- MBS (*Maximum Burst Size*): É o número máximo de células que pode ser transmitido no pico de taxa de célula (MISHRA, 2010, p. 73).
- *Policing*: É a definição da política de tráfego variando conforme o tipo de conexão.
- *VC Qdepth*: É a profundidade da fila de VC (*Virtual Circuit*).

- *CLP Setting*: Pode ativar as configurações referentes a CLP (*Cell Loss Priority*) que é um campo usado para designar dois níveis de prioridade para uma célula, os bits sinalizados com 0 tem uma maior prioridade a células com 1 (KASERA, 2006, p. 96).
- *CLP Hi (Cell Loss Priority High)*(em % do valor de VC *Qdeph*t): Quando o limite aqui definido é excedido o nó irá descartar células com CLP = 1 até que o número de células da fila caia abaixo do nível especificado por CLP Lo/EPD.
- *CLP Lo/EPD (Cell Loss Priority Low/Early Packet Discard)*(em % do valor de VC *Qdeph*t): Quando o número de células na fila cai para baixo do nível definido aqui o nó para de descartar células com CLP=1.
- *EFCI (Explicit Forward Congestion Indication)* (em % do valor de VC *Qdeph*t): Este mecanismo o bit de congestionamento no cabeçalho ATM é colocado em 1 para indicar um congestionamento na rede (KASERA, 2006, p. 167).
- *ICR (Initial Cell Rate)*: Limite superior na taxa de transmissão de origem, imposta no início e depois de um período parado (KASERA, 2006, p. 308).
- *ADTF (The Allowed-Cell-Rate Decrease Factor)*: Tempo permitido entre a transmissão de células RM para a frente, antes da origem é requisitado para diminuir a taxa de transmissão para ICR (KASERA, 2006, p. 308).
- *Trm*: Limite superior de tempo entre células RM a frente de uma origem ativa (KASERA, 2006, p. 308).
- *RIF (Rate increase Factor)*: Controla a quantidade que a taxa de transmissão de célula pode aumentar após o recebimento de uma célula RM (KASERA, 2006, p. 163).
- *RDF (Rate Decrease Factor)*: Controla o decremento na taxa de transmissão de célula (KASERA, 2006, p. 163).
- *Nrm*: É o número máximo de células que uma origem pode enviar para cada Célula RM a frente (KASERA, 2006, p. 163).
- *FRTT (Fixed Round Trip Time)*: A soma dos delays fixos e de propagação da origem para o destino (KASERA, 2006, p. 163).
- *TBE (Transient Buffer Exposure)*: O número de células negociadas que a rede gostaria de limitar a origem de enviar durante os períodos iniciais, antes do retorno da primeira célula RM (KASERA, 2006, p. 163).

- IBS (*Initial Burst Size*): Tamanho de intermitência inicial (equivalente ao *Frame Relay Cmax*) (KASERA, 2006, p. 163).
- *Trunk cell routing restrict*: Restringe o tronco de realizar a rota de células.

A figura 97 exemplifica o uso do comando, lembrando que o parâmetro asterisco (*) é considerado como o padrão estabelecido pelo equipamento.

Figura 97 - Criando a conexão no BPX.

```
ME500      TN      User:2      BPX 8620  9.3.51      Nov. 15 2019 02:05 G-03
```

From	Remote NodeName	Remote Channel	State	Type	Route Avoid	COS	Q
2.6.201.94	V400	7.6.16	ok	atxfst	0	L	
2.6.201.95	N400	8.26.16	ok	atxfst	0	L	
2.6.201.100	N401	9.6.16	ok	atxfst	0	L	
2.6.201.105	N500	13.4.201.233	ok	nrt-vbr	0	L	
2.6.201.118	E500	3.3.201.118	ok	abrstd			
2.6.201.125	N500	13.4.201.264	ok	nrt-vbr	0	L	
2.6.201.126	N500	1.5.201.126	ok	nrt-vbr	0	R	
2.6.201.130	N500	12.1.201.322	ok	nrt-vbr	0	R	
2.6.201.132	N500	13.4.201.113	ok	nrt-vbr	0	L	
2.6.201.144	N500	1.5.201.178	ok	nrt-vbr	0	L	
2.6.201.145	E400	10.8.16	ok	atxfst	0	L	
2.6.201.147	N401	9.2.16	ok	atxfst	0	L	
2.6.201.148	E400	16.48.16	ok	atxfst	0	L	

```
Last Command: addcon 2.6.201.94 CTAJV400 7.6.16 ATXFST * * * * * Disable * * *
* * * * *
Next Command: █
```

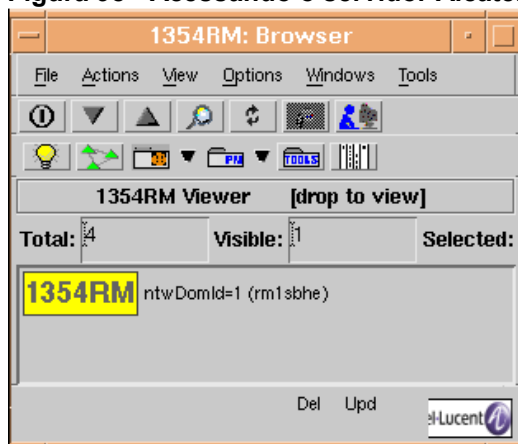
MAJOR ALARM

Fonte: Autoria Própria

3.2.6 Cross conexão entre Roteador e rede SDH Alcatel

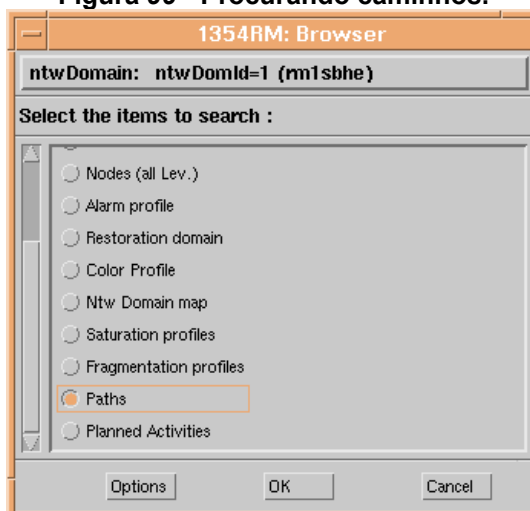
O trecho SDH é mais usado para transmissão do que acesso devido a velocidade de tráfego que normalmente será superior a 155 Mbps, devido a esse motivo será mostrado de forma bem sucinta a informação referente a esse tipo de gerência. Será usado nesse material a gerência da Alcatel, mas a mesma lógica é implementada em outras gerências como Huawei, Bosch, Siemens, NEC entre outras...

A figura 98 ilustra a tela inicial para acesso ao servidor *1354RM viewer* usado para acesso ao sistema SDH Alcatel.

Figura 98 - Acessando o servidor Alcatel.

Fonte: Autoria Própria

Ao acessar o servidor 1354RM para consulta deve-se clicar duas vezes no 1354RM da figura 99 para que se abra o leque de opções abaixo:

Figura 99 - Procurando caminhos.

Fonte: Autoria Própria

Nesse ponto existirá várias consultas que poderão ser realizadas, nesse caso será usado o circuito denominado teste para a busca. Para fazer tal busca use-se a opção *Paths*. Logo após a figura abaixo se apresentará:

Figura 100 - Filtrando o Circuito no SDH.

The screenshot shows a dialog box titled "DEFINE QUERY FOR Path, pathSdh, pathWdm, pathSC". It has several tabs: "Specific", "Status", "Alarms", "PH", "Mdm", "NAD", "Routing", "CP Restoration", "Miscellaneous", "Virtual Concatenation", and "Ethernet". The "Specific" tab is active. The dialog contains the following fields and values:

Field	Value
User Label	Contains TESTE
Transport Network	SDH
Service Type	PDH
Path Type	Bidirectional
Service Rate	2Mb-LO
Transport Rate	TU12
Protection	None
Allocation Rule	User
Implement Rule	User
Path Group	
Definition Time	

At the bottom of the dialog, there are three buttons: "Apply", "Cancel", and "OK".

Fonte: Autoria Própria

Pode-se gerar várias formas de busca nessa opção, algo importante a frisar é que uma gerência típica SDH poderá ter placas de outras tecnologias para existir a convergência de rede. Nesse ponto foi selecionado a busca por nome do circuito através da opção "User Label", selecionando o filtro "Contains" e escrevendo o nome do circuito, nesses casos será "TESTE".

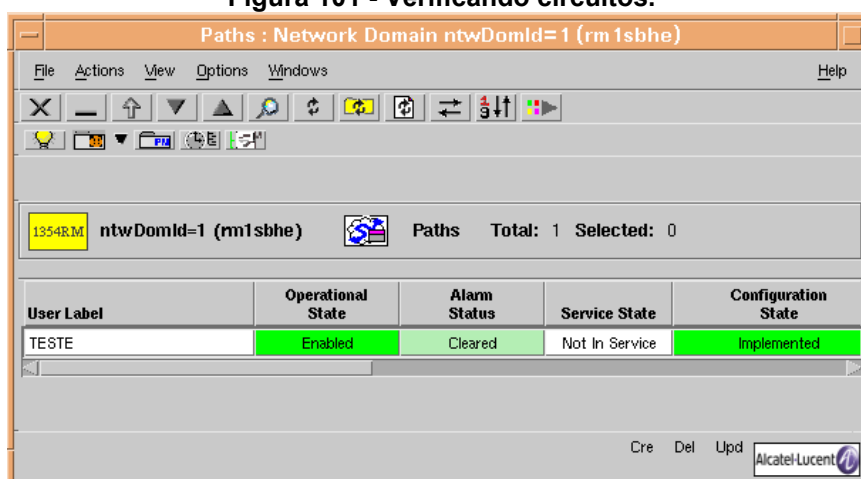
Ao realizar a busca aparecerá o resultado desejado conforme ilustrado na figura 101, tendo os campos a seguir:

- *Operational State (Enable/Disable)*: Demonstra se o circuito foi desativado na gerência.
- *Alarm Status (undefined/Warning/Minor/Major/Critical/Pending/Cleared)*: Se estiver "cleared" estará alinhado, se estiver com outro estado terá problemas no meio de transmissão.
- *Service State (In Service/Not In Service)*: Pode ser configurado se o circuito estará em serviço ou não, sendo a última usado para testes.
- *Configuration State*: Pode ser referir as seguintes opções:
 - *Defined*: O caminho foi definido, porém não há dados trafegando, pode ser usado por outro circuito o caminho nesse período.
 - *Allocated*: O caminho foi alocado, sendo que não há como alocar outro circuito nesse caminho.
 - *Implemented*: O circuito foi implementado e se não houver alarmes no

meio estará operacional. Nesse estado os alarmes são apresentados no campo “Alarm Status”.

- *Comissioned*: O circuito foi implementado e se não houver alarmes no meio estará operacional. Nesse estado os alarmes ficam ocultos.
- *Partially implent*: A implementação foi concluída até uma parte e está faltando configurações.

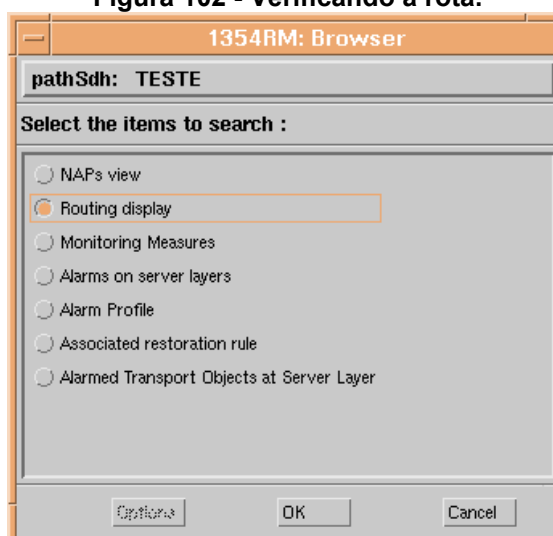
Figura 101 - Verificando circuitos.



Fonte: Autoria Própria

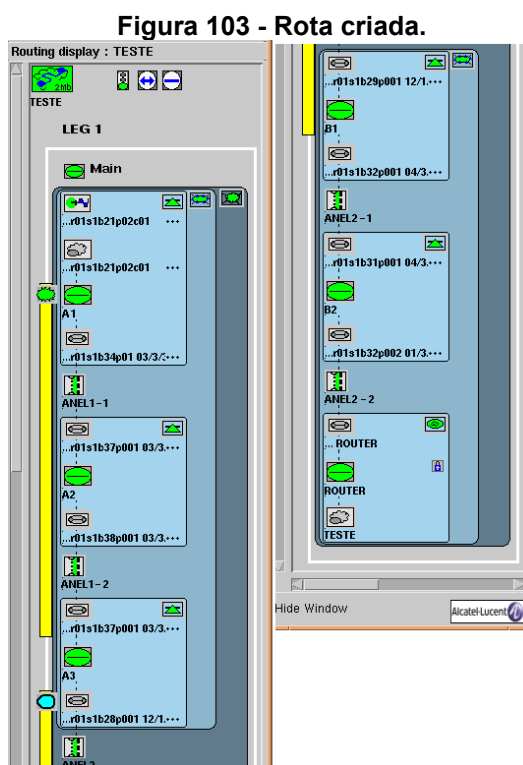
Ao clicar duas vezes no circuito da figura 101 aparecerão as opções da figura 102, para consultar a rota desse cliente é importante escolher “Routing display”.

Figura 102 - Verificando a rota.



Fonte: Autoria Própria

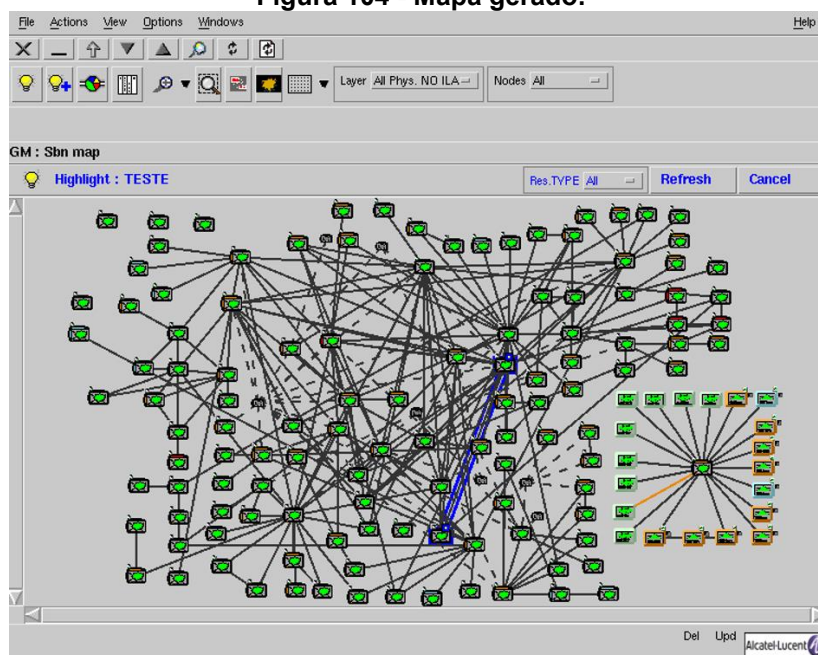
A figura 103 aparece cortada para melhora na visualização, mas apresenta os saltos que tem nos anéis apresentando o equipamento A1, A2 e A3 no anel 1 e B1 e B2 no anel 2. Em cada porta terá uma identificação rXXsXbXXpXXX sendo X um numeral qualquer, o “r” representa o rack, “s” a prateleira ou *subrack*, o “b” a placa e o “p” a porta.



Fonte: Autoria Própria

A figura 104 demonstra o que ocorre quando se gera um “*Highlight*” no circuito, primeiramente serão mostrados vários retângulos verdes, sendo que cada um representa um anel distinto, o circuito estudado tem dois anéis, o 1 e o 2 por isso que o caminho destacado em azul demonstra dois anéis de ligando.

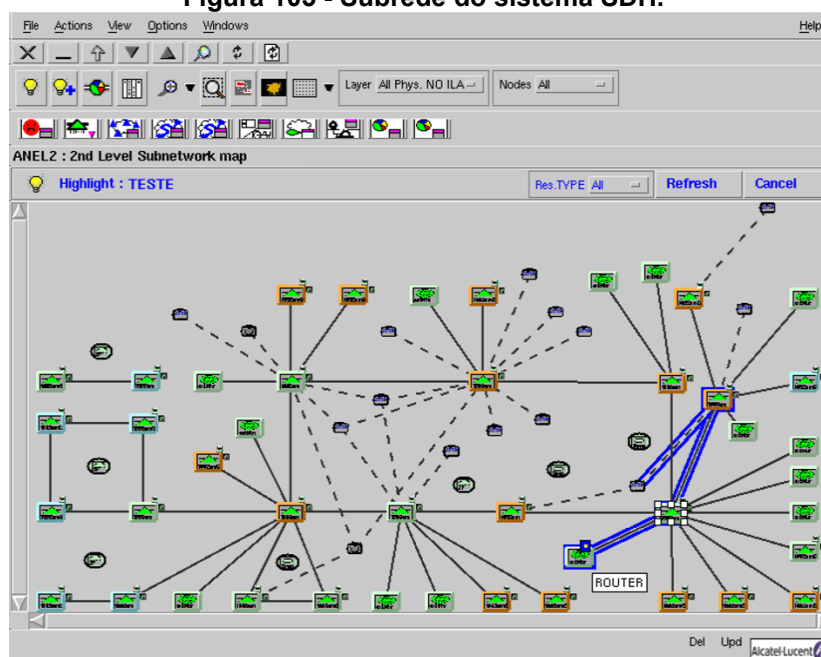
Figura 104 - Mapa gerado.



Fonte: Autoria Própria

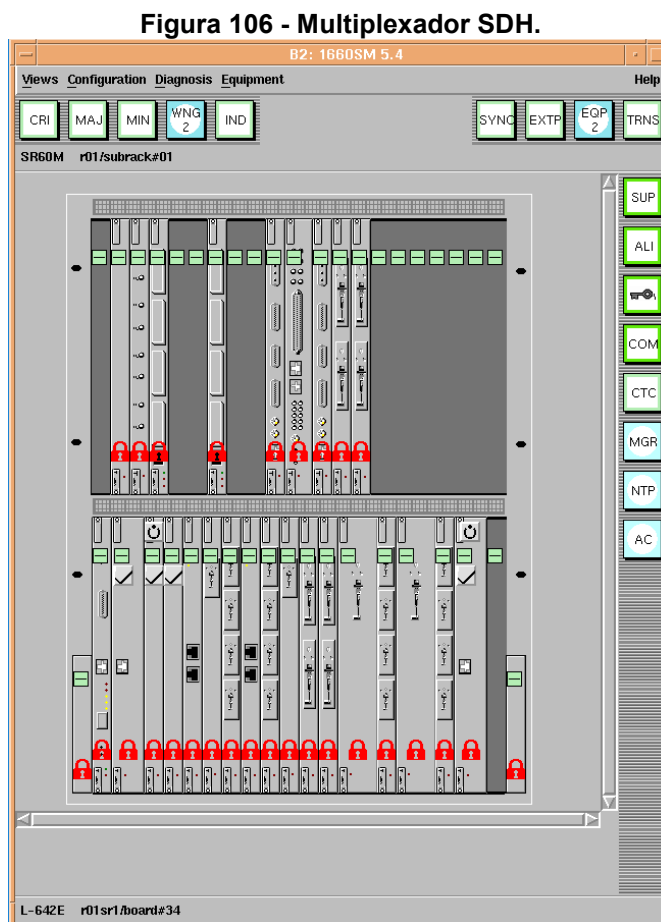
No anel 2 tem o roteador (*ROUTER*) que não é gerenciável pela gerência pois não é um multiplexador SDH e multiplexador B1 e B2, aqui será selecionado o equipamento mais próximo do roteador que é o multiplexador B2 conforme visto na figura 105. Caso exista um alarme a linha que interliga dois equipamentos ficará laranja ao invés da coloração preta.

Figura 105 - Subrede do sistema SDH.



Fonte: Autoria Própria

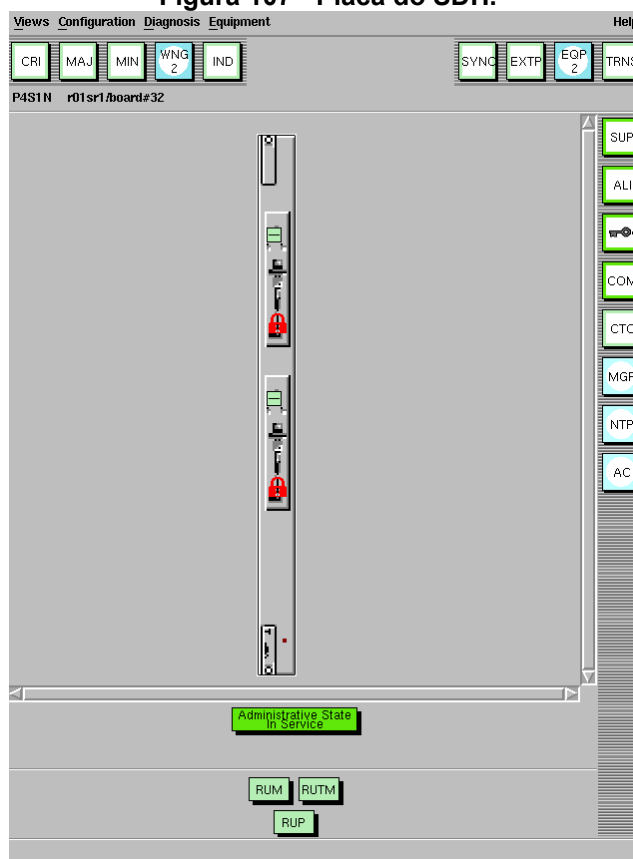
Ao selecionar o equipamento é mostrado o *rack*, *subrack* e as diversas placas do equipamento. Nesse exemplo foi selecionado a placa 32 que está localizado na fileira de baixo da figura 106 a qual demonstra na parte inferior, caso o usuário passe o mouse em cima das placas, a numeração da placa sendo ilustrado a placa 34 na figura (*board#34*).



Fonte: Autoria Própria

Essa placa que está sendo ilustrada através da figura 107 contém duas fibras óticas para verificar os alarmes caso exista deve-se selecionar a porta que é indicada junto com o cadeado vermelho. No exemplo da figura 107 existem duas portas. No caso exemplificado será usado a porta 2 que é a de baixo.

Figura 107 - Placa do SDH.



Fonte: Autoria Própria

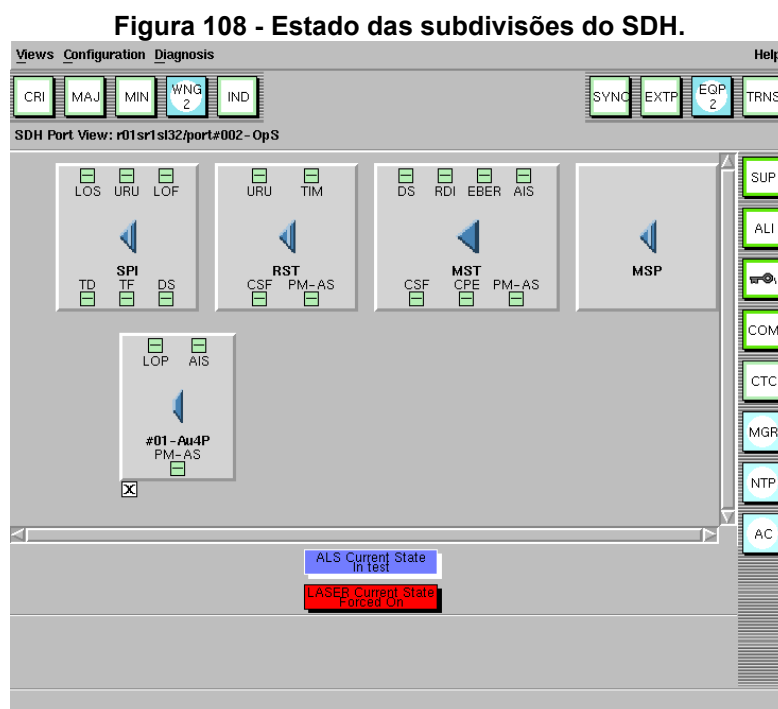
Na figura 108 existem os alarmes que uma porta pode ter, caso esteja com um sinal de subtração (-) e verde ela estará sem alarmes, caso o sinal seja de adição (+) e laranja, significa que há um alarme. Como a imagem 101 demonstra que não há alarmes, pois, a linha que interliga o roteador ao multiplexador está na coloração preta determina-se que há apenas o sinal de subtração (-) verde. Os alarmes nesse trecho da rede SDH pode partir do:

- SPI (*SDH Physical Interface*): Interface física.
- RST (*Regenerator Section Termination*): Gerador de sinal.
- MST (*Multiplex Section Termination*): Multiplexador do sinal.
- Au4P (*Au-4 Pointer*): Ponteiro Au-4.

Sendo os principais:

- LOS (*Loss of Signal*): Perda de sinal.
- LOF (*Loss of frame*): Perda de quadros.
- AIS (*Alarm Indicator Signal*): Sinal de indicador de alarme.
- LOP (*Loss of Pointer*): Perda de ponteiro.
- URU (*Underlying Resource Unavailable*)

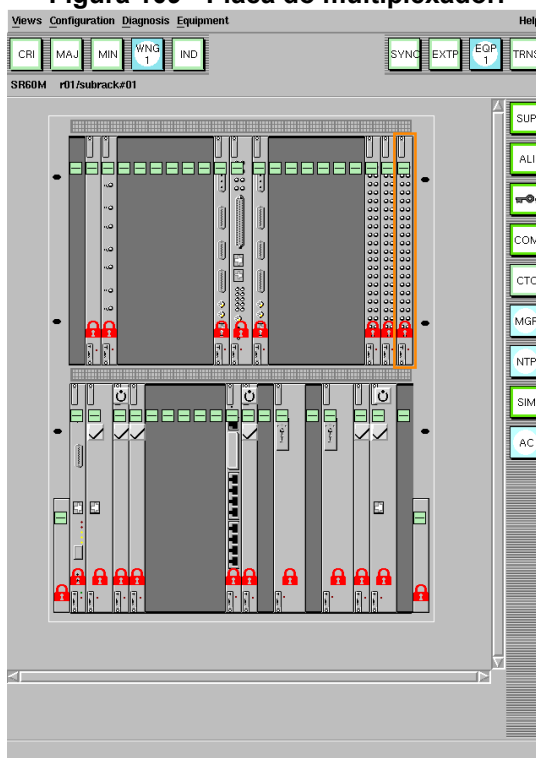
- TIM (*Trace Interface Mismatch*)



Fonte: Autoria Própria

Já a figura 109 demonstra o multiplexador de acesso pois a configuração no meio de transmissão segue o mesmo padrão do que explicado no multiplexador que se liga ao roteador. Para encontrar o multiplexador de acesso, deve-se voltar ao mapa da figura 105 e ir para a outra ponta através de um anel similar ao representado na figura 104, nesta imagem será encontrado um equipamento interligado por uma única linha que será o multiplexador de acesso do cliente.

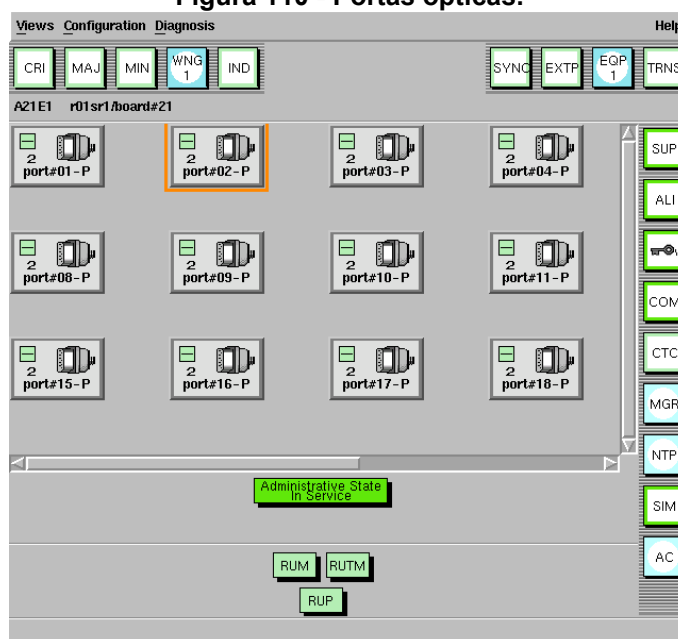
A figura 109 segue a mesma lógica explicada na figura 107, se for seguido o acesso é concedido ao cliente através da placa 21 que já está destacada na imagem de exemplo.

Figura 109 - Placa do multiplexador.

Fonte: Autoria Própria

Dentro dessa placa existem 21 portas disponíveis conforme ilustrado pela figura 110 que é interligado em um cabo coaxial que irá ao cliente. Selecionando a porta pode-se ver os alarmes existentes. No exemplo aqui trabalhado será usado a porta 2.

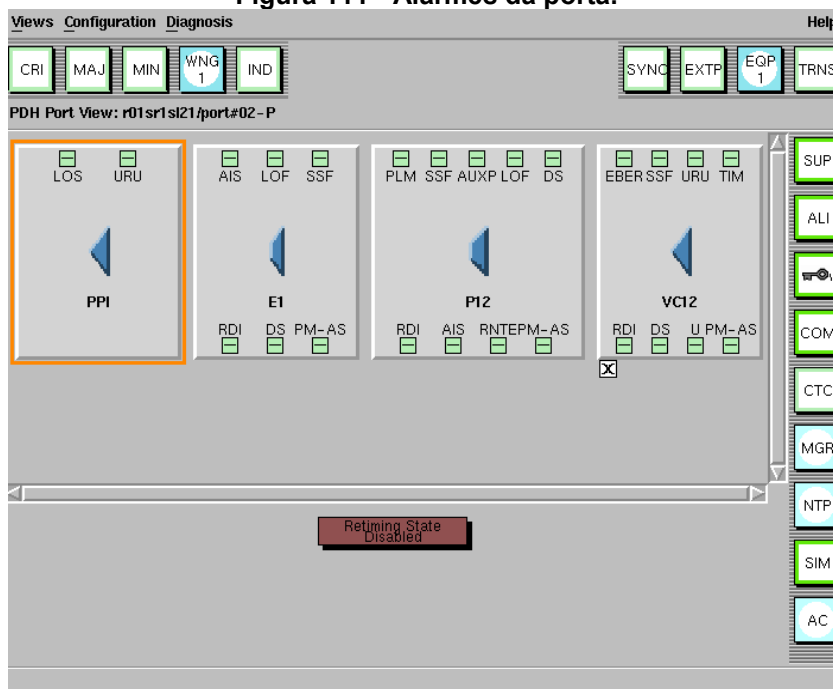
Figura 110 - Portas ópticas.



Fonte: Autoria Própria

A figura 111 demonstra a conversão do VC12 para o E1 que normalmente será entregue ao cliente, os alarmes principais já foram explicados anteriormente e se mantém a mesma explicação.

Figura 111 - Alarmes da porta.



Fonte: Autoria Própria.

3.2.7 Cross conexão entre Roteador e GPON

Nesse tópico será explicado como será feita a conexão de fibra óptica GPON entre roteador até o cliente. Na figura 112 existe o exemplo de um cliente com fibra óptica conectado a uma porta “lag”, com um qinq que é necessário nesse tipo de conexão. Nem toda a porta “lag” vai para a rede GPON necessariamente e a porta “lag” é uma porta lógica que indica o agrupamento com balanceamento em 2 portas físicas.

Figura 112 - Roteador com porta lag

```
*A:A01# admin display-config | match 200 context all
#-----
service
  ies 200 customer 1 create
    description "200"
    interface "2" create
      description "By DFID# = 23 (200)"
      address 10.10.10.10/30
      icmp
        no mask-reply
        no redirects
        no unreachable
      exit
    ip-mtu 1500
    sap lag-2:3984.1918 create
    exit
  urpf-check
    ignore-default
  exit
service-name "200"
```

Fonte: Autoria Própria

A porta “lag” descrita na figura 113 tem duas portas físicas agrupadas e alinhadas cujo seus nomes são 7/2/2 e 8/2/1. O encapsulamento no campo “encap type” é “qinq” o que será necessário para determinar a rota e o acesso do cliente no meio GPON.

No campo “*description*” é o que determina o próximo equipamento que essas duas portas estão conectando, afinal nela estará a descrição da porta. No exemplo foi usado a nomenclatura A2 para definir o equipamento, mas pode ter informações mais completas para saber qual equipamento está conectado na rede ou usar um sistema secundário que desenhe topologias para descobrir qual é o próximo equipamento interligado a essa porta.

Figura 113 - Estado de uma porta lag.

```
*A:A01# show lag 2 detail
```

LAG Details									
Description	: A2								

Details									
Lag-id	: 2								
Adm	: up								
Thres. Exceeded Cnt	: 16								
Thres. Last Cleared	: 04/22/2021 15:21:59								
Dynamic Cost	: false								
Configured Address	:								
Hardware Address	:								
Hold-time Down	: 0.0 sec								
Per-Link-Hash	: disabled								
Include-Egr-Hash-Cfg	: disabled								
Per FP Ing queuing	: disabled								
Per FP SAP Instance	: disabled								
Access Bandwidth	: N/A								
Access Available BW	: 0								
Access Booked BW	: 0								
LACP	: enabled								
LACP Transmit Intvl	: fast								
Selection Criteria	: highest-count								
MUX control	: coupled								
Subgrp hold time	: 0.0 sec								
Subgrp selected	: 1								
Subgrp count	: 1								
System id	:								
Admin Key	:								
Prtr System Id	:								
Prtr Oper Key	:								
Standby Signaling	: lacp								
Port weight speed	: 0 gbps								
weight Threshold	: 0								
Mode	: access								
Opr	: up								
Port Threshold	: 0								
Threshold Action	: down								
Encap Type	: qinq								
Lag-IFindex	: 1342177282								
Adapt Qos (access)	: link								
Port Type	: standard								
Forced	: -								
Per FP Egr Queuing	: disabled								
Access Booking Factor	: 100								
Mode	: active								
LACP xmit stdby	: enabled								
Slave-to-partner	: disabled								
Remaining time	: 0.0 sec								
Subgrp candidate	: -								
System Priority	:								
Oper Key	:								
Prtr System Priority	:								
Number/weight Up	: 2								
Threshold Action	: down								

Port-id	Adm	Act/Stdby	Opr	Primary	Sub-group	Forced	Prio		
7/2/2	up	active	up	yes	1	-	10000		
8/2/1	up	active	up		1		10000		

Port-id	Role	Exp	Def	Dist	col	Syn	Aggr	Timeout	Activity
7/2/2	actor	No	No	Yes	Yes	Yes	Yes	Yes	Yes
7/2/2	partner	No	No	Yes	Yes	Yes	Yes	Yes	No
8/2/1	actor	No	No	Yes	Yes	Yes	Yes	Yes	Yes
8/2/1	partner	No	No	Yes	Yes	Yes	Yes	Yes	No

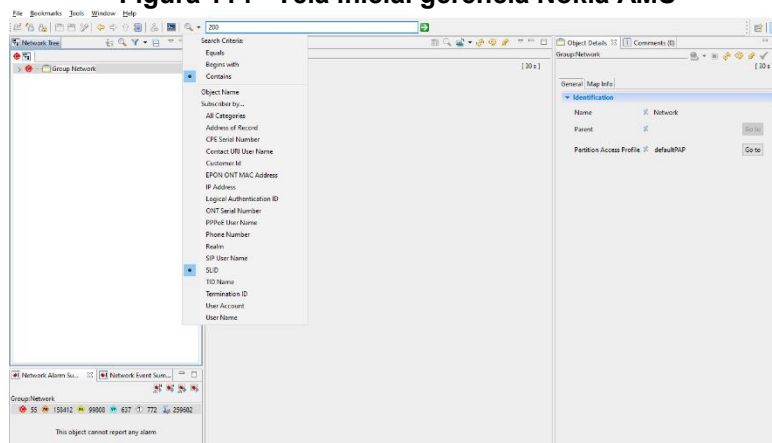
Fonte: Autoria Própria.

A figura 114 exemplifica a tela inicial da gerência GPON Nokia AMS que será usada de exemplo para implementação de um circuito com GPON, lembrando que existe a gerência da Huawei e de outras empresas, mas nesse trabalho será abordado apenas essa tecnologia.

Para realizar a busca pode-se clicar na lupa no menu superior e escolher a opção "SLID" e após "Contains", lembrando que é obrigatório escolher a opção "SLID" primeiro para habilitar o campo "Contains". Logo após na barra superior ao lado da lupa haverá um campo onde será realizado a busca do circuito, na figura 112 foi escrito o circuito simulado 200 nesse campo.

As buscas podem ser feitas por "object name" e por procura pela porta manualmente ou até pelo serial da ONT que está configurado no multiplexador.

Figura 114 - Tela inicial gerência Nokia AMS



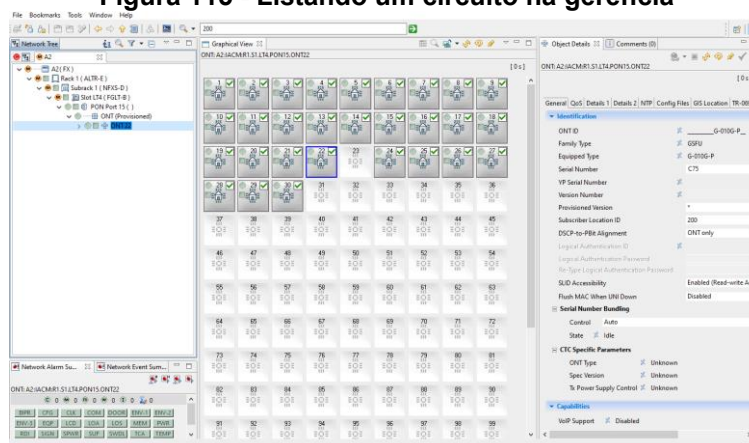
Fonte: Autoria Própria

A figura 115 mostra um circuito sendo listado na ferramenta, temos na árvore à esquerda o equipamento A2, rack 1, *subrack* 1, *slot* LT4, porta PON 15 e a ONT 22. No menu “*general*”, deve-se sempre se atentar se o campo “serial number” está com o serial da ONT física se isso não ocorrer gerará indisponibilidade no circuito. O campo “*Provisioned Version*” ficará com o asterisco (*) garantindo que a OLT receberá a versão mais atualizada do sistema. O campo “*Subscribed Location ID*” seria a identificação do circuito, podendo ser usada ou não e é importante para a busca e documentação.

O campo “SLID Accessibility” terá três opções sendo a que está configurado que seria para leitura e escrita usando HTTP ou *Telnet*, só leitura ou desabilitado. O campo “*Flush MAC When UNI Down*” pode estar ativado ou desativado e controla a liberação do endereço MAC caso o equipamento no cliente caia. A opção “*Control*” dentro do grupo “*Serial Number Bundling*” pode ser *auto*, *manual* ou *disable*, isto será usado quando o campo *Serial Number* não esteja sendo pego automaticamente (*auto*) e será necessário digitar manualmente (*manual*), a não ser que exista uma necessidade específica não é interessante selecionar a opção desativado (*disable*).

Quando não há como alterar um campo existe algum bloqueio no serviço que não foi implementado no sistema ou o OLT não tem suporte, esse não serão abordados aqui, pois o serviço que deve ser entregue ao cliente é o GPON transparente.

Figura 115 - Listando um circuito na gerência



Fonte: Autoria Própria

A figura 116 demonstra a continuação da aba general da figura 115 a qual não coube por restrição do sistema. Na caixa *Rates* existe a velocidade para OLT, nesse caso só terá “Nominal Line Rate” e a velocidade de 1,25 Gbps devido a OLT ter apenas essa configuração, existe a opção de multiponto mas não será usado aqui.

A caixa *States* tem a opção *Administrative State* que bloqueia a porta administrativamente através da opção “*Locked*” ou libera o acesso através da opção “*Unlocked*” e pode ser usado para bloqueio financeiro ou problemas que o cliente tenha. O campo estado operacional (*Operational State*) demonstra se o equipamento está alinhado e o campo data de última mudança (*Last Change Date*) mostra última queda do circuito e pode ser usado para detectar intermitências.

O campo *Rogue ONT Disabling Decision* determina se a ONT que se encontra no cliente, subestação ou poste pode desativar a comunicação automaticamente (*Auto*), proibir a desativação manual (*Manually Disable*) ou permitir a desativação manualmente (*Manually Enable*). O campo *Current Reporting State* mostrará se existirá alarmes na ONT, o campo *Ranged* demonstra se o equipamento OLT está na estação do multiplexador ou se o equipamento OLT está em outro local e o campo *Estimated Distance to OLT* é a distância que está o equipamento da estação do multiplexador óptico aproximadamente. O campo de detecção de loop pode deixar sem controle (*No Control*), ativado (*Enable*) ou desativado (*Disable*), o ideal deixar sem controle e deixar que o local defina isso.

A caixa *Software* mostra as opções referentes a atualizações e versões da OLT, pode deixar como automático ou como desativado, mas é extremamente recomendado que deixe em automático, exceto se alguma coisa impeça a

atualização que o cliente use da versão anterior e isso deve ser visto contratualmente.

Figura 116 - Aba General continuação

The screenshot displays the 'General' configuration page for an ONT. At the top, 'IP Host Support' is set to 'Disabled'. The 'Rates' section shows 'Planned (Up)' as 'Nominal Line Rate' and 'Actual (Up)' as '1.25 Gb/s'. The 'States' section includes 'Administrative State' (Unlocked), 'Operational State' (Up), 'Last Change Date' (Yesterday at 15h36min52s BRT), 'Rogue ONT Disabling Decision' (Auto), 'Current Reporting State' (No Defect), 'Ranged' (Yes), and 'Estimated Distance to OLT' (1,7 km). The 'Loop Detection on ONT LAN Ports' section has 'State' set to 'No Control' and 'Automatic Shutdown' set to 'Enabled'. The 'Software' section shows 'Active Software' (3FE45655AOCK76 (R05.06.01 No VoIP)), 'Passive Software' (3FE45655AOCK88 (R05.07.01 No VoIP)), 'Planned Software' (AUTO (use OLT for auto download)), and 'Downloaded Software' (AUTO (use OLT for auto download)). A 'Download Status' field is also present.

Fonte: Autoria Própria

A figura 117 demonstra a continuação das figuras 116 e 115 e é a última figura referente a aba *general*. Na janela *Version (from ONT SW Version Control)* tem a versão do software do ONT planejada (Planned Software) e descarregada (Downloaded Software) e tem um campo para um software variante planejado (Planned Variant) que é usado para fins de atualização de software da ONT, mas não é recomendável mexer nesse campo sem autorização da fabricante.

A janela *Alarms* tem o campo que determina o menor alarme que a porta irá demonstrar visualmente ao administrador de rede (*Minimum Alarm Reporting Security*), sendo interessante deixar o padrão para pegar todos os alarmes, mas se for importante para algum caso específico tem as opções “Indeterminate”, “Warning”, “Minor”, “Major”, “Critical” ou “No Alarms” sendo que se for bloqueado o “Critical”, os alarmes inferiores como *Major*, *Minor*, *Warning* e *Indeterminate* serão bloqueados juntos.

A janela *Additional Information* é o local onde se pode colocar as informações referentes ao cliente ou nada se for desejado, nesse caso no campo *Description (Part 1)* tem a informação 200 que seria referente ao cliente especificado. Na janela *Profiles* tem a configuração de perfil XDSL (*GPON XDSL*

DPBO Profile) caso o cliente passe por um trecho DSL, como não é o caso aqui exemplificado e normalmente a operadora não fará esse tipo de configuração devido a tecnologia DSL ser legada, mas caso um dia necessite pode-se colocar a configuração XDSL.

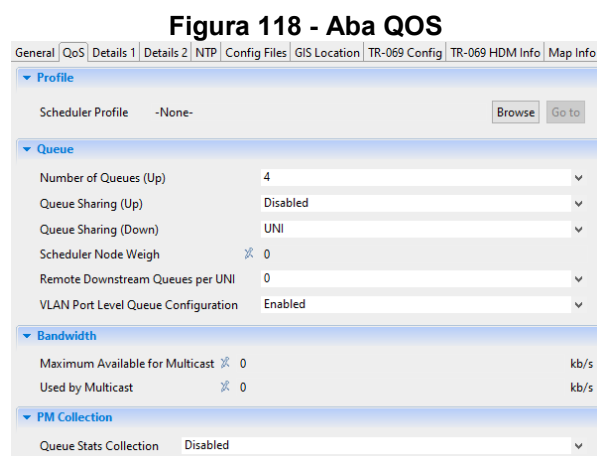


Fonte: Autoria Própria

Na aba QOS retratada na figura 118 haverá a janela *Profile* que é responsável pelo perfil na opção *Scheduler Profile*, clicando em *Browse* terá os perfis configurados pela operadora no OLT, normalmente esse tipo de configuração será feita na VLAN e não aqui e isso será explicado mais para frente nesse mesmo capítulo.

Na janela “*Queue*” se configura as filas, no campo “*Number of Queues*” a quantidade de filas que pode passar por essa QOS, normalmente QOS é configurado na VLAN, mas pode-se escolher entre 4 ou 8 filas. A opção “*Queue Sharing(up)*” determina se existirá filas compartilhadas para upload podendo ser ativada essa opção (*enable*) ou não ativada (*disable*), a opção “*Queue Sharing(Down)*” determinara se haverá fila compartilhada para *download*, nesse caso existe como deixar a rede GPON se encarregar disso com a opção ONT ou o cliente com a opção UNI. A opção *Remote Downstream Queues per UNI* determina as filas que cada UNI terá, como só haverá uma UNI (um cliente) essa opção será 0 no exemplo e a única opção importante nessa janela é *VLAN Port Level Queue Configuration* que deve estar ativada para o tráfego de VLAN (*enable*).

A janela *bandwidth* é usada para OLT *multicast* o que não será usada no exemplo, mas limita a velocidade de banda nesse tipo de topologia e por fim temos a janela *PM Collection* que coleta estatísticas dessas filas, pode ser ativada (*Enabled*) na opção *Queue Stats Collection*, mas aqui no exemplo não será ativada, pois como já afirmado anteriormente, isso será configurado na VLAN.



Fonte: Autoria Própria

A figura 119 tem alguns detalhes sobre a ONT como o abastecimento de bateria, nesse caso essa ONT não terá abastecimento reserva de bateria (*Battery Backup*) por isso dessa opção estar em *No*, logo não terá um perfil de abastecimento de energia (*Power Shed Profile*), se tiver pode entrar na opção *Browse* e escolher uma predeterminada pela operadora. A informação referente ao estado de abastecimento de energia (*Power Shedding Status*) será apenas vinda da ONT (*Reported from ONT*) e como não tem bateria reserva então não haverá uma classe vinculada que gerencie quando o abastecimento de energia reserva estará ligado (*Power Shiedding Active On*).

A janela *Policing* representa como ficará as políticas de filas de QOS, a OLT será configurada para ficar que o QOS não interfira na velocidade deixando isso para a VLAN, o modo da política de upstream (*Upstream Policing Mode*) será determinada pelo Local para OLT (*Local at OLT*), nesse caso pode ser configurado do remoto para a ONT (*Remote at ONT*) sendo que a próxima opção (*ONT TC Policing Mode*) terá a mesma perspectiva. Como as informações vem do local então no exemplo as filas de prioridade (*Priority Queue*) ficaram quantificadas como 72, os contêineres de transmissão (*Transmission Containers*) ficaram com 9 e a quantidade de tarefas de tráfego (*Traffic Schedulers*) ficaram com 9 também.

O FEC (*Forward Error Correction*) habilita o suporte a atenuação ODN em uma série de atenuações com transmissores e receptores de baixa performance (INTERNATIONAL TELECOMUNICATION UNION, 2019, p.23) e pode ser habilitado (*enable*) na janela *Traffic* na opção *FEC Upstream Indicator*. Na opção *Ethernet Port-to-Port Traffic* será habilitado quando a OLT tiver suporte e ter alguma

necessidade, nesse caso não há suporte para isso.

A janela taxa de limitação por UNI (*Rate Limiting per UNI*) tem as opções de DHCP e ARP para evitar congestionamento desses pacotes na OLT, nesse caso foi limitado 10 para upload de cada um desses pacotes.

Na janela segurança existe a opção de encriptação AES (*Advanced Encryption Standard*) que é um algoritmo que trata entrada e saída de uma sequência de 128 bits cada que é nomeada algumas vezes como blocos e o número de bits que eles contêm são chamados de tamanho tendo uma cifra de 128, 192 e 256 (INTERNATIONAL TELECOMUNICATION UNION, 2002, p.13), é importante deixar habilitado (*Enabled*) para aumentar a segurança no tráfego de dados.

A janela *RF Video (Cambridge ONT)* determina quais rádios frequências para vídeos será usado e terá as opções de filtro passa alta e passa baixa (*Pass Low and High Band*), passar filtro passa baixa de 431 MHz (*Pass Only Low Band 1 431 MHz*), passar filtro passa baixa de 639 MHz (*Pass Only Low Band 2 639 MHz*) e não passar filtro nenhum para vídeo (*Pass Nothing*), essa opção depende do contrato com cliente.

A janela de *Debug* serve para depurações e é usado para testes com o endereço IP do cliente (*Client IP Address*) e não será tratado nesse documento a parte de testes.

A janela VLAN demonstra o modo onde a ONU se comunicará com a VLAN (*ONU VLAN Connectivity Mode*) aqui deve ser deixado na opção *1:MP Map Filtering* devido a conexão ser realizada para apenas um cliente, mas se for multiponto pode ser selecionado *N:P Bridge Filtering* ou *N:MP Bridge Filtering* e isso deve ser verificado com o pessoal de engenharia de rede da empresa para ter a opção mais rentável. Pode-se nessa janela escolher aonde será feita a tradução da CVLAN, (*C-VLAN Translation*), caso haja mudança na topologia o melhor é configurar para a ONT fazer isso, senão pode ser deixado para a OLT fazer isso.

Figura 119 - Aba Details 1

The screenshot shows the following configuration details:

- Battery/Power Shedding:** Battery Backup: No; Power Shed Profile: -None-; Power Shedding Status: Reported from ONT; Power Shedding Active on: No Class.
- Policing:** Upstream Policing Mode: Local at OLT; ONT TC Policing Mode: Local at OLT; Priority Queues: 72; Transmission Containers: 9; Traffic Schedulers: 9.
- Traffic:** FEC Upstream Indicator: Enabled; Ethernet Port-to-Port Traffic: Blocked.
- Rate Limiting per UNI:** DHCP (Up): 10 packet/s; ARP (Up): 10 packet/s.
- Security:** AES Encryption: Enabled.
- RF Video (Cambridge ONT):** Programmable Filter: Pass Low and High Band.
- Debug:** Client IP Address: 0.0.0.0.
- VLAN:** ONU VLAN Connectivity Mode: 1:MP Map Filtering; C-VLAN Translation: Remote (ONT).

Fonte: Autoria Própria

A Figura 120 demonstra a aba *details 2*, nessa aba as informações referente janelas *Self Test*, *Physical Parameters*, *ONT Data Storage* e *Remote Inventory* estão ocultas devido não haver informações alteráveis nelas, são apenas informações se está tendo teste, quantidade de placas (que nesse caso é apenas uma), a última vez que houve dados armazenados na ONT e dados de inventário.

A janela *Optical Measurements* tem a opção *Collection State* que serve para determinar se a ONT irá coletar medidas ópticas e colocar em uma nova opção na árvore determinada *optical monitor* (essa opção só aparece na árvore após colapsar e expandir a ONT na gerência). Já o *Optical Signal Level (Rx)* é a medida do sinal óptico entre ONT e OLT.

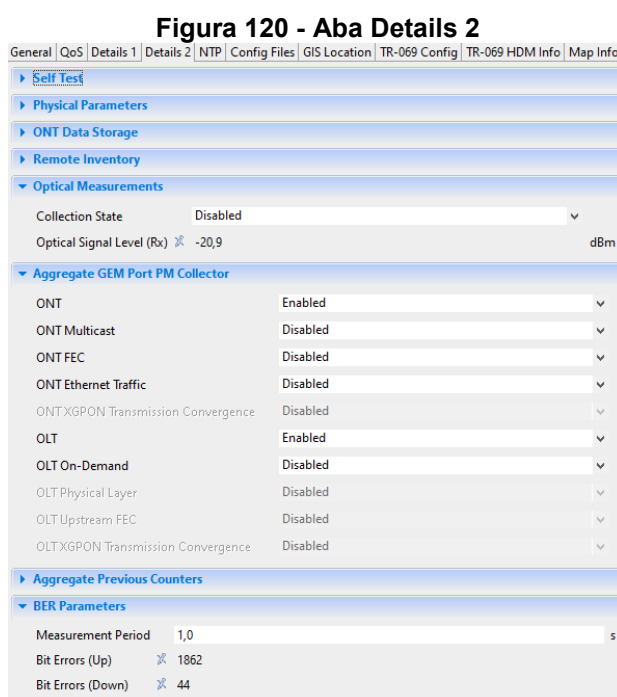
A janela *Agregate GEM Port PM Collector* sendo GEM (*Gigabit-capable Passive Optical Network Encapsulation Method*) embutido na sessão PON (*Passive Optical Network*) e é independente dos tipos de UNI sendo esse um tipo de encapsulamento em quadros (INTERNATIONAL TELECOMUNICATION UNION, 2008, p. 11) e PM (*performance monitoring*) como a tradução literal já afirma é o monitoramento de performance da fibra.

As opções na janela são ONT onde se habilita ou desabilita (*enable/disable*) o teste de performance em tempo real na ONT, ONT multicast, ONT FEC, ONT

Forward Traffic, OLT e OLT On-Demand.

Na janela *BER parameters* sendo BER (*Bit Error Rate*) é a taxa de erro de bit que está tendo na ONT, podendo alterar o tempo de atualização em *Measurement Period* e os erros serão demonstrados nos campos *Bit Errors (Up)* e *Bit Errors (Down)* para upload e download consecutivamente.

As abas *NTP*, *Config Files*, *Gis Location*, *TR-069 Config*, *TR-069 HDM Info* e *Map Info* não interferem no funcionamento da ONT e não serão tratados nesse documento.

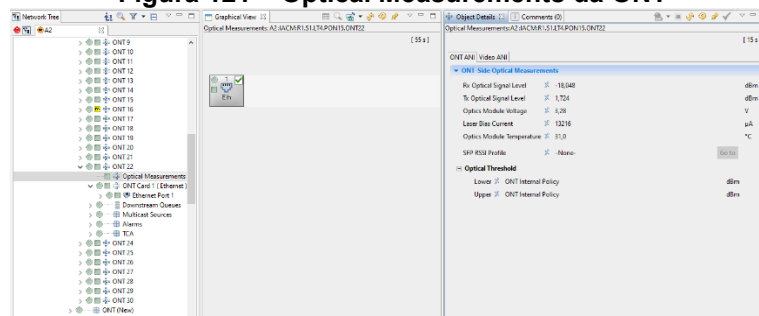


Fonte: Autoria Própria

A figura 121 demonstra as opções quando se clica na opção *optical measurements* detectado na árvore à esquerda, essas opções aparecem a direita e são divididos em *ONT ANI* e *Video ANI*, aqui será tratado o ONT ANI apenas devido a parte de vídeo não ser tratada nesse documento.

Na aba ONT ANI temos as medições para a porta de acesso ao equipamento do cliente sendo elas *Rx Optical Signal Level*, *Tx Optical Signal Level*, *Optics Module Voltage*, *Laser Bias Current* e *Optics module Temperature* de importante ao estudo, todos esses valores serão passados pela operadora devido a distância, projeto e qualidade da fibra e significam consecutivamente o sinal ótico de recepção, o sinal ótico de transmissão, a voltagem do módulo ótico, a atual polarização do laser e a temperatura do módulo ótico.

Figura 121 – Optical Measurements da ONT



Fonte: Autoria Própria

A figura 122 demonstra a porta *ethernet* da ONT, na janela parâmetros no lado direito pode-se colocar o nome do cliente no campo *Customer ID*, no campo *Label* pode-se colocar uma etiqueta para agrupar as portas de um cliente e o campo *Data Class Power Shedding* pode determinar se o abastecimento elétrico seguirá o padrão determinado pelo sistema ou não.

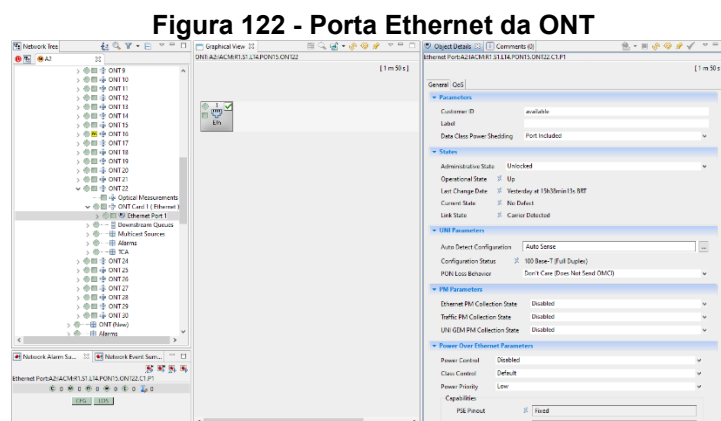
A janela *States* é responsável pelo funcionamento da porta, o campo *Administrative State* determina algum bloqueio administrativo seja por falta de pagamento, problemas administrativos do cliente, equívoco ou para evitar que alguém conecte um cabo e acesse a rede sem pagar, a porta pode ficar bloqueada (*locked*) e desbloqueada (*unlocked*). O campo *Operational State* demonstra o alinhamento da porta, o campo *Last Change Data* mostra a última queda na porta com a data e hora, o campo *Current State* demonstra se existe defeito ou não na porta e o *Link State* que demonstra a existência de portadora do sinal ou não.

O campo *UNI Parameters* tem a opção *Auto Detected Configuration* que escolhe o padrão que essa porta ethernet receberá como o *Auto Sense* que é a configuração automática da porta ou velocidade da porta com a sua tecnologia e se funciona no modo *Half-Duplex* ou *Full-Duplex*. O campo *Configuration Status* mostra o modo que a porta *ethernet* decidiu operar, no caso exemplificado ficou *100 Base-T(Full Duplex)*, lembrando que se a configuração diferir com o equipamento do cliente pode gerar perda de pacotes e até inoperância.

A Janela *PM Parameters* temos as opções *Ethernet PM Collection State*, *Traffic PM Collection State* e *UNI GEM PM Collection State*, ao habilitar qualquer uma dessas opções a porta será monitorada e para acessar os resultados deve-se clicar com o botão direito do mouse em cima do *Ethernet Port 1* localizado na árvore a direita escolher *Show*, dentro dessa opção *PM Counters* e por fim *Object*

Monitoring View.

A janela *Power Over Ethernet Parameters* terá configurações de energia a qual normalmente não se mexe, porém aqui temos a opção *Power Control*, *Class Control* e *Power Priority* que será usado conforme configurado pela operadora.

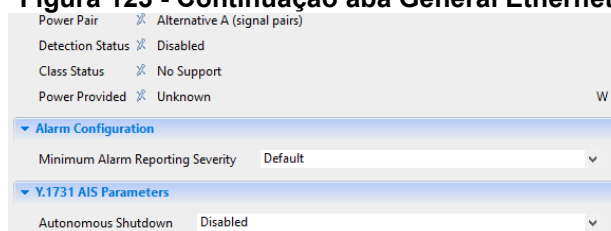


Fonte: Autoria Própria

Na figura 122 é apresentado a continuação da janela *Power Over Ethernet Parameters* e a janela *Alarm Configuration* que apresenta a opção *Minimum Alarm Reporting Severity* tem a mesma função apresentada na figura 117, mas não para a ONT e sim para a porta Ethernet.

A janela *Y.1731 AIS Parameters* tem uma única opção que é *Autonomous Shutdown* que desligará a porta no primeiro sinal de alarme e pode ser útil em ocasiões de reparos e testes.

Figura 123 - Continuação aba General Ethernet



Fonte: Autoria Própria

A figura 124 mostra a aba QOS que tem a janela QOS parameters e nela contém informações interessantes como o *CAC profile* sendo *CAC (Connection Admission Control)* que são níveis de prioridade que determinam se chamadas ou sessões recebidas pode ser admitida dependendo da criticidade do serviço e a disponibilidade de uma potencial redução de recursos de rede (INTERNATIONAL

TELECOMUNICATION UNION, 2006, p. 2). Normalmente a operadora cria alguns perfis para vídeo, voz e dados, nesse caso será transmitido apenas dados.

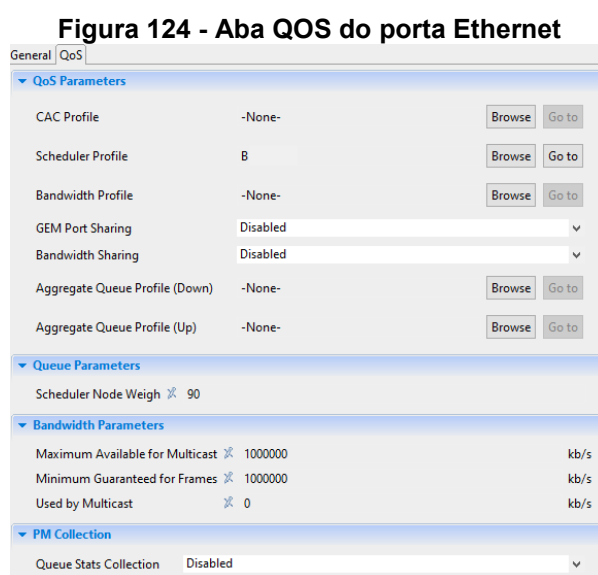
A opção *Scheduler Profile* tem o perfil de tarefas e prioridade na tratativa de pacotes, aqui foi criado um perfil B apenas para exemplificar, clicando em *go to* pode-se verificar as regras aplicadas.

A opção *Bandwidth Profile* pode-se controlar a quantidade de banda que passará para esse circuito, nesse caso foi deixado transparente.

As opções *GEM Port Sharing* e *Bandwidth Port Sharing* seria definido caso a ONT tivesse mais de uma porta ethernet e representa o compartilhamento de banda e de quadros entre elas, nesse caso deixar em desativado (disable) ou ativado (enable) não faria diferença.

As opções *Aggregate Queue Profile (Down)* e *Agregate Queue Profile (Up)* determina as filas dessa porta, como nesse exemplo as filas de QOS são determinadas pela VLAN e essa opção não tem muita serventia, mas caso a operadora deseje usar aqui será selecionado a prioridade de pacotes.

Na janela *Bandwidth Parameters* terá para visualização os valores referentes a velocidade, como os parametros *Maximum Available for Multicast* (O máximo disponível por multicast), *Minimum Guaranteed for Frames* (O mínimo garantido para os quadros) e *Used by Multicast* (Usado por Multicast). A última janela fica para o *PM Collection* já abordado anteriormente.



Fonte: Autoria Própria

A figura 125 mostra a configuração de uma das portas que se comunicam

com o roteador, lembrando que nesse caso para garantir a redundância foi colocado duas portas, mas o que for mostrado aqui será válido para a outra porta Ethernet. Pode se perceber vendo a árvore a esquerda que não se está mais na ONT, mas sim na porta Ethernet localizado no rack 1, sub rack 1, *slot* NTA, porta 6, na porta que está fazendo redundância estará no *slot* NTB, garantindo redundância de placa.

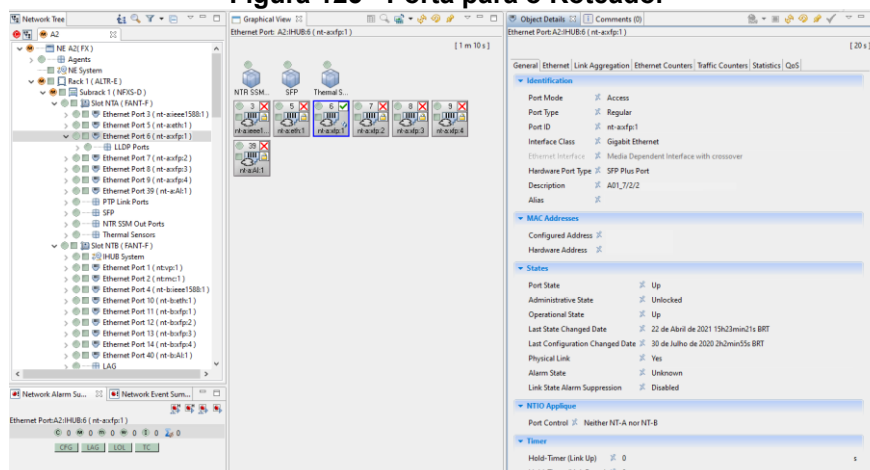
No menu a direita temos as seguintes informações na aba *General* onde tem-se na janela *Identification* a informação que o modo de porta (*Port Mode*) está configurado para acesso (*access*), sendo um tipo de porta (*Port Type*) regular, tendo um identificação de porta (port ID) padrão pelo equipamento, classe de interface (*Interface Class*) determinado como *Gigabit Ethernet*, com um tipo hardware (*Hardware port type*) determinada com *SFP Plus Port*, na descrição (*description*) foi colocada o nome do roteador com a porta na outra ponta e o apelido (*Alias*) deixado em branco.

A janela *MAC address* (endereço de MAC) tem o endereço de MAC do equipamento, por se tratar de um simulador esse equipamento não recebeu nenhum endereço, mas normalmente existirá um endereço no campo *Configured Address* que mostra o endereço configurado e o *Hardware Address*, normalmente ambos os campos terão o mesmo valor.

Na janela *State* terá os valores de alinhamento (*Port State/Operational State*) que deverão ambos estar no estado alinhado (*up*), se há algum bloqueio administrativo (*Administrative State*) usado nesse tipo de porta para evitar deixar a porta exposta quando não usada, as últimas datas referentes a última mudança de estado e configuração (*Last State Changed Date/Last Configuration Changed Date*), configuração se existe algum cabo físico conectado (*Physical Link*), se existe algum alarme (*Alarm State*) e por fim se os alarmes não foram suprimidos (*Link State Alarm Suppression*).

O que não foi citado nesse trecho é que não tem uma relevância muito alta para a interconexão.

Figura 125 - Porta para o Roteador



Fonte: Autoria Própria

Na figura 126 tem as informações referentes a aba *Ethernet* e nela contém a janela *Encapsulation* onde mostra as configurações de encapsulamento para interconexão como é demonstrado que essa porta aceita o encapsulamento de VLAN na opção *Encapsulation Type*, sendo do tipo *0x8100* no campo *802.1Q Ethertype* e não tendo nível de *VLAN Ethertype*.

A janela *Auto-Negotiation* contém a informação que a auto negociação da porta (*Auto-Negotiation*) está desativada (*disable*), o modo de negociação configurado e operacional (*Configured Duplex Mode/Operational Duplex Mode*) está em Full Duplex e a velocidade configurada e operacional (*Configured Speed/Operational Speed*) está em 10000 Mb/s.

As janelas *Egress Rate Limiting*, *Loopback* e *Thresholds*, tem respectivamente informações referente a limitação da porta, se está com algum teste rodando e se a porta está com taxa de erro de CRC e utilização.

Figura 126 - Aba Ethernet para a porta do roteador

General	Ethernet	Link Aggregation	Ethernet Counters	Traffic Counters	Statistics	QoS
Encapsulation						
Encapsulation Type	✖	802.1Q				
802.1Q Ethertype	✖	0x8100				
VLAN Level EtherType	✖	No				
Auto-Negotiation						
Auto-Negotiation Mode	✖	Disabled				
Configured Duplex Mode	✖	Full Duplex				
Operational Duplex Mode	✖	Full Duplex				
Configured Speed	✖	10000				Mb/s
Operational Speed	✖	10000				Mb/s
Egress Rate Limiting						
Maximum Rate	✖	No Limit				kb/s
Burst Size	✖	No Limit				kB
Loopback						
Mode	✖	None				
VLAN ID	✖	0				
Thresholds						
Used Input Bandwidth	✖	Disabled				%
Used Output Bandwidth	✖	Disabled				%
Receive CRC/Align Errors	✖	Disabled				%
Transmit CRC/Align Errors	✖	Disabled				%
Transmit Collisions	✖	Disabled				%
Number of Occurrences in Last 8h	✖	32				

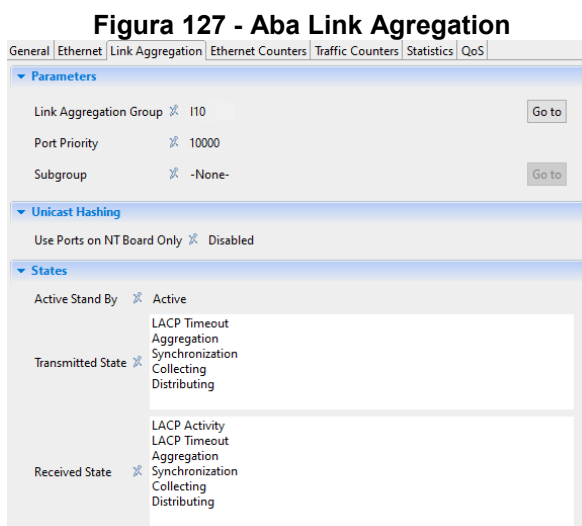
Fonte: Autoria Própria

A figura 127 demonstra a configuração de agregação de porta que nada mais é do que o agrupamento das duas portas vinda do roteador. Na janela *Parameters* existe o parâmetro mais importante visto aqui que é o apelido da agregação de porta, a figura 128 será a resposta ao clicar em *go to*. A *Port Priority* demonstra a prioridade dessa porta e o *Subgroup* demonstra se essa porta pertence a um subgrupo.

A janela *Unicast Hashing* tem a opção *Use Ports on NT Board Only* de desativar as placas LT e deixa apenas as placas NT ativas, caso esse equipamento fizesse interconexão de backbone essa opção seria bem útil, mas nesse caso ele tem que usar as placas LT para conectar as ONT's aos clientes, pois ele é um equipamento de acesso.

A janela *Status* demonstra o estado do agregação do link sendo *Active Stand by* demonstrando que a interface está ativa (Active). E as opções referente ao Transmitted State e Received State são sobre o que a porta está transmitindo e recebendo respectivamente.

As abas Ethernet Counters, Traffic Counters, Statistics e QOS são usadas para testes e terão informações de utilização e erros na porta, QOS não é aplicada nessa porta.

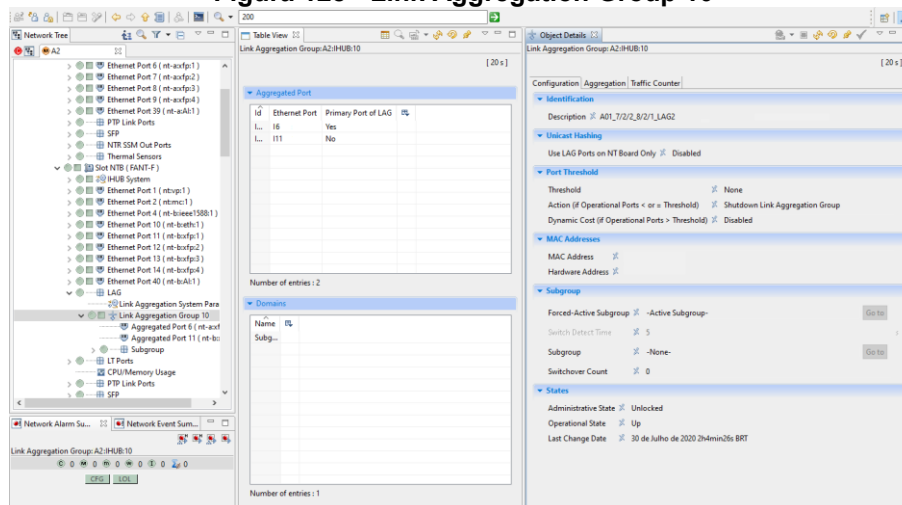


Fonte: Autoria Própria

A figura 128 demonstra a configuração da agregação de porta, na árvore à esquerda percebe-se que a emulação dessa porta virtual está sendo feita pelo *Slot* NTB em um serviço dentro de uma LAG, dentro dessa LAG terá o *Link Aggregation Group 10* e dentro dela existe a *Aggregated Port 6 (nt-a:xfp:1)* e *Aggregated Port 11 (nt-b:xfp:1)* onde ambos estão cortados na figura porém é esse o nome completo, nt-a e nt-b são os *slots*, xfp:1 a identificação da porta. A identificação da porta fica ao lado do *Ethernet Port #* entre parênteses (ex: *Ethernet Port 6 (nt-a:xfp-1)*), ou seja, as duas portas dentro do *Link Aggregation Group 10* são as portas que estão conversando com o roteador.

Na aba *Configuration* na janela *Identification* tem o campo *Description* onde normalmente a operadora vai colocar as informações sobre a outra ponta. Não será discutido as demais opções da agregação de porta devido essas informações serem suficiente para a implementação da VLAN.

Figura 128 - Link Aggregation Group 10



Fonte: Autoria Própria

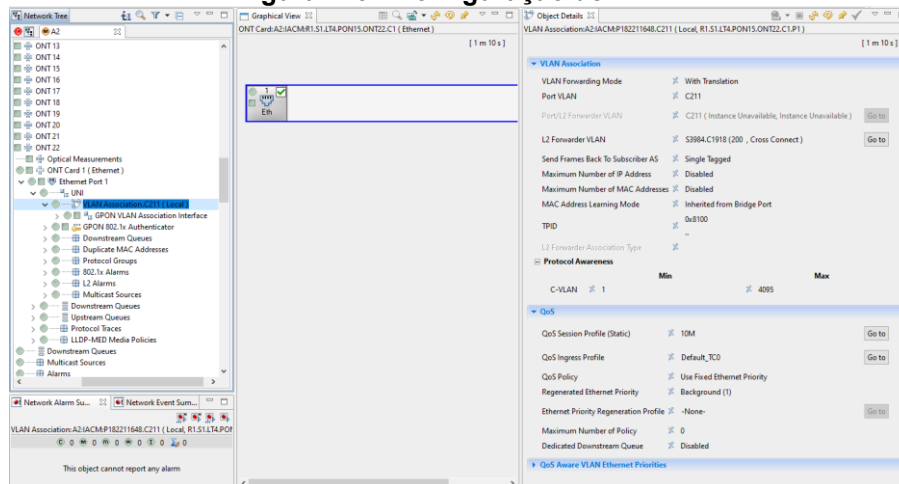
Voltando a ONT do cliente conforme figura 129, a parte mais importante para a comunicação entre cliente e operadora que são as configurações de VLAN, para iniciar essa configuração deve-se ver se já não há uma VLAN cadastrada na porta e para isso na árvore à esquerda existe a necessidade dentro da Ethernet Port 1, escolher UNI e dentro dela terá a VLAN associada que nesse caso será a CVLAN 211 que está configurado no roteador (*VLAN Association.C211 (Local)*).

As informações importantes para a VLAN ficam na janela a direita denominado *VLAN Association* as quais são *VLAN Forwarding Mode* determinando que haverá uma tradução de CVLAN, a Port VLAN que determinará a CVLAN 211 para o cliente, *L2 Forwarder VLAN* que será a SVLAN e CVLAN enviada por *cross conexão* ao roteador que pode ser alterada clicando em *Go To* e realizará a tradução da CVLAN 1918 para 211, a opção *Send Frames Back To Subscriber AS* que terá uma etiqueta somente, *Maximum Number of IP Address* que determina o número máximo de IPs que essa pode receber e que normalmente será irrestrito devido o roteador tratar disso, o *Maximum Number of MAC Adress* que nesse caso ficou desativado e o *MAC Address Learning Mode* que será herdado da porta de acesso.

A janela QOS terá o perfil de QOS dessa porta e limitará a velocidade do cliente, caso o roteador já não esteja fazendo essa função, aqui pode ser configurado a velocidade. Nesse caso o roteador não tem perfil de QOS nele e aqui foi inserido na opção QOS Session Profile (Static) uma perfil nomeado 10 M que representa apenas 10 Mbps de banda, caso haja necessidade de um perfil diferente

deve-se clicar em *Go To* sendo que esse procedimento também vale para a opção *QoS Ingress Profile* que cuidará das filas de prioridades.

Figura 129 - Configuração de VLAN



Fonte: Autoria Própria

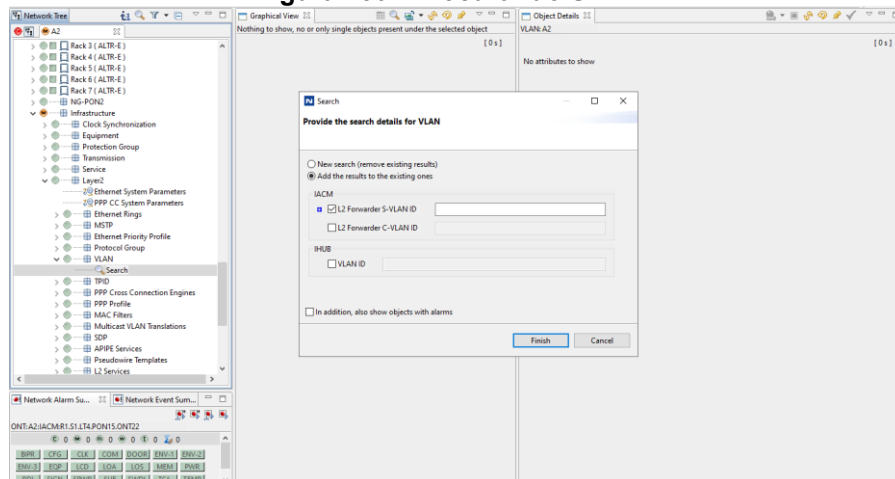
Como CVLAN é apenas para identificar a porta de um cliente e a SVLAN é a rota que vários clientes irão passar, deve-se verificar se a SVLAN está configurada com a Link Aggregation Group 10 (LAG 10) conforme figura 128. Para isso os multiplexadores da Nokia têm essas configurações separadas das portas, placas, sub racks e racks, na árvore localizada a esquerda na figura 130 que é denominado *Infraestructure*, nela terá vários serviços que não são configurados diretamente nas portas como perfis de QOS, VOIP, serviços de camada 2 e 3, entre outros.

Dentro de *Infraestructure* é necessário verificar se a SVLAN está configurada corretamente ou configura-la, para que isso seja possível deve-se escolher a opção *Layer 2* e *VLAN* respectivamente dentro da árvore. Ao clicar em *Search* dentro de *VLAN*, pode-se procurar o a VLAN desejada podendo iniciar a pesquisa limpando o filtro existente na opção *New Search (removing existing results)* ou incluir mais resultados sobre aqueles já mostrados com a opção *Add the results to the existing ones*.

Aqui será importante a procura da SVLAN dentro de IACM e em IHUB, a busca pelo IACM deve ser realizada se houver a necessidade de procurar se existe uma CVLAN onde deve-se marcar os campos *L2 Forwarded S-VLAN ID* e *L2 Forwarded C-VLAN ID* e preenche-los com a SVLAN e CVLAN respectivamente e escolher *Finish*, caso só haja a importância de procurar apenas SVLAN, fica sem necessidade de marcar o CVLAN. O IHUB é o que será buscado no exemplo e

apenas tem a SVLAN para ser buscada, ao digitar no campo VLAN ID a SVLAN deve-se escolher *Finish*.

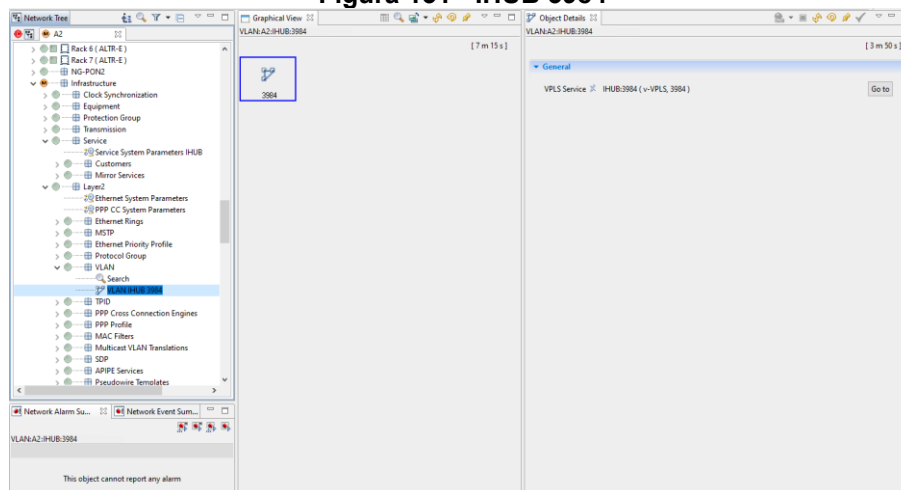
Figura 130 - Procurando SVLAN



Fonte: Autoria Própria

Ao localizar o IHUB conforme mostrado na figura 131, que aparecerá na árvore à esquerda, existirá no menu direito uma VPLS vinculada a ele e ao clicar em *Go To* irá para a VPLS.

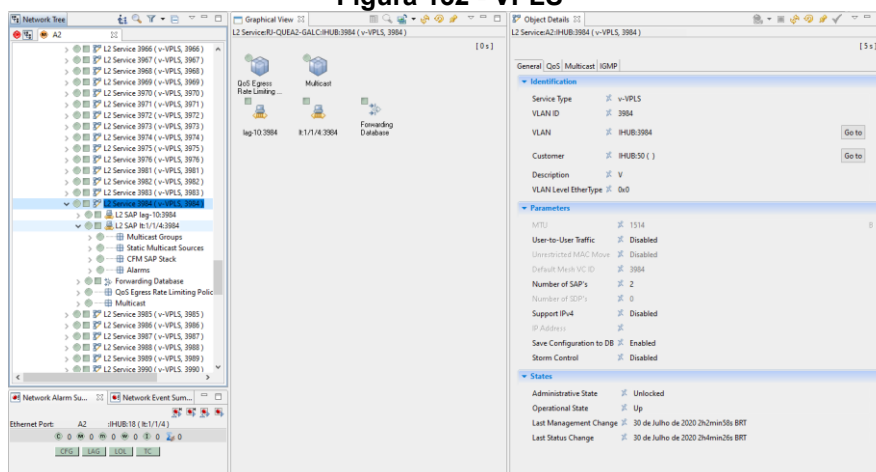
Figura 131 - IHUB 3984



Fonte: Autoria Própria

Na VPLS terá a interconexão entre a lag-10:3984 e a It:1/1/4:3984 que é a placa onde estão as ONT's dos clientes que poderão ter acesso a essa SVLAN, gerando assim a cross conexão entre o cliente e sua CVLAN e o roteador conforme ilustrado árvore à esquerda na figura 132.

Figura 132 - VPLS



Fonte: Autoria Própria

3.3 CROSS CONEXÃO ENTRE GERÊNCIAS E TECNOLOGIAS DISTINTAS

A *cross* conexão entre duas redes é muito utilizada pelas empresas de telecomunicações para estender a comunicação até clientes mais distantes e que precisam de comunicação e não podem ser atendidas via rádio ou via satélite.

Por exemplo, uma grande corporação precisa criar uma rede WAN para sua empresa atendendo todas as filiais de sua empresa e aciona a operadora para contratar o serviço, porém existe uma filial isolada em uma região do país onde a operadora não tem como contratar um link de outra operadora e vai precisar colocar a estrutura dela nesse local. Quando isso ocorre a operadora acaba pegando algum equipamento legado de algum lugar e fazendo uma pequena estação ali para evitar comprar novos equipamentos.

Quando ocorre a criação de uma nova estação é possível que o equipamento enviado para lá pode não ser do mesmo fabricante da estrutura mais próxima, nesse caso a *cross* conexão é realizada.

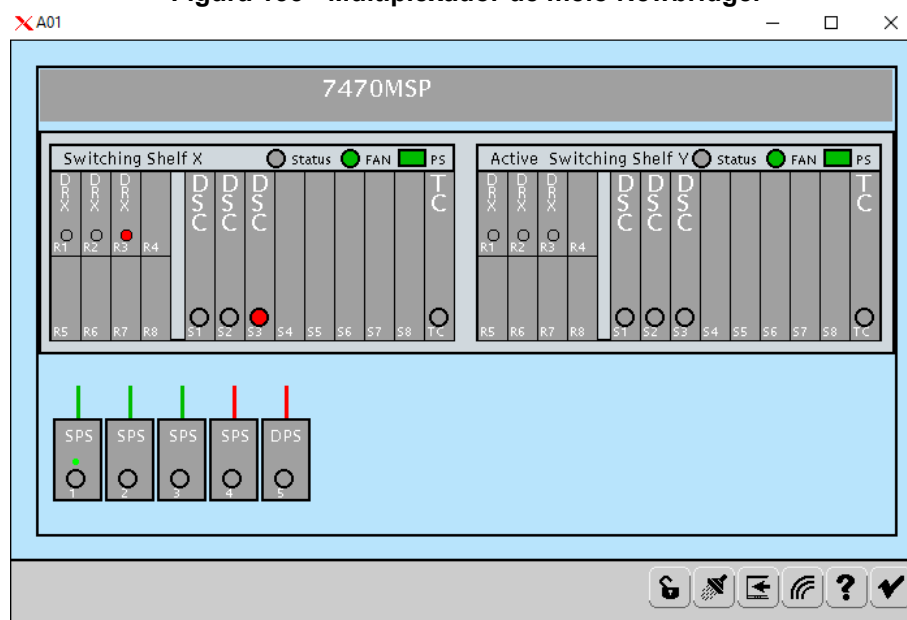
3.3.1 Cross Conexão entre a Rede Newbridge e Rede Datacom

Normalmente quando há a necessidade de aprovisionar um circuito, a operadora passa as facilidades para realizar as configurações, nesse caso foi pego informações pré-determinadas com finalidade didática, e por isso foi escolhido o equipamento “A01” na rede Nokia Newbridge.

Esse equipamento tem 5 periféricos, conforme ilustrado na figura 133, sendo

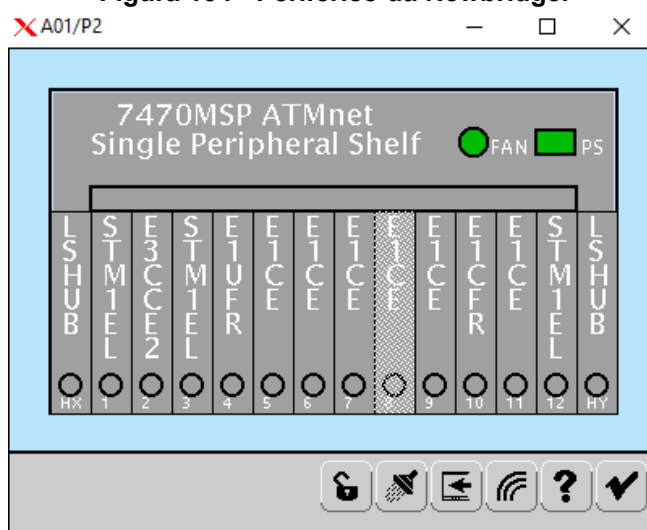
2 periféricos alarmados e conseqüentemente inoperantes, tendo eles uma linha vermelha acima, aqui foi selecionado o periférico 2. Lembrando que os periféricos são o conjunto de retângulos indicados por SPS e DPS.

Figura 133 - Multiplexador de meio Newbridge.



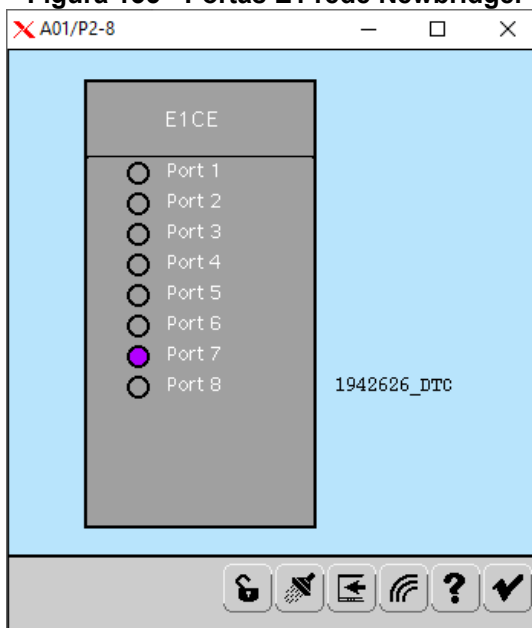
Fonte: Autoria Própria

A figura 134 demonstra que existem 12 placas e 2 placas controladoras (indicadas por LSHUB na posição HX e HY), aqui existem 3 placas STM1EL, uma placa E3CCE2 com 2 portas, 6 placas E1CE determinísticas com 8 portas e uma placa E1CFR estatística com 4 portas. Aqui será selecionado a placa que está no slot 8.

Figura 134 - Periférico da Newbridge.

Fonte: Autoria Própria

Conforme anteriormente explicado existem 8 portas na placa E1CE demonstrado na figura 135, sendo a porta 8 a selecionada ao lado da qual está escrito “1942626_DTC”. DTC nesse caso é o acrônimo de Datacom e o numeral ali escrito é a identificação do laço (*link*), porém isso varia de operadora para operadora sendo que pode ter outras informações aqui, como nome do equipamento, porta e *slot* remoto.

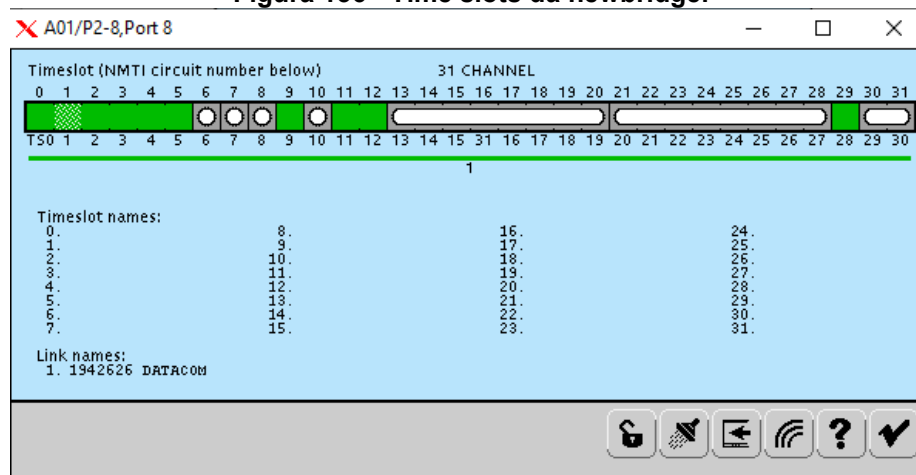
Figura 135 - Portas E1 rede Newbridge.

Fonte: Autoria Própria

Na figura 136 existem os “*timeslots*”, sendo que os que estão em verde

ainda não foram usados, nesse caso serão usados 2 “*timeslots*”, ou seja 128 Kb/s. Serão selecionados os “*timeslots*” 1 e 2.

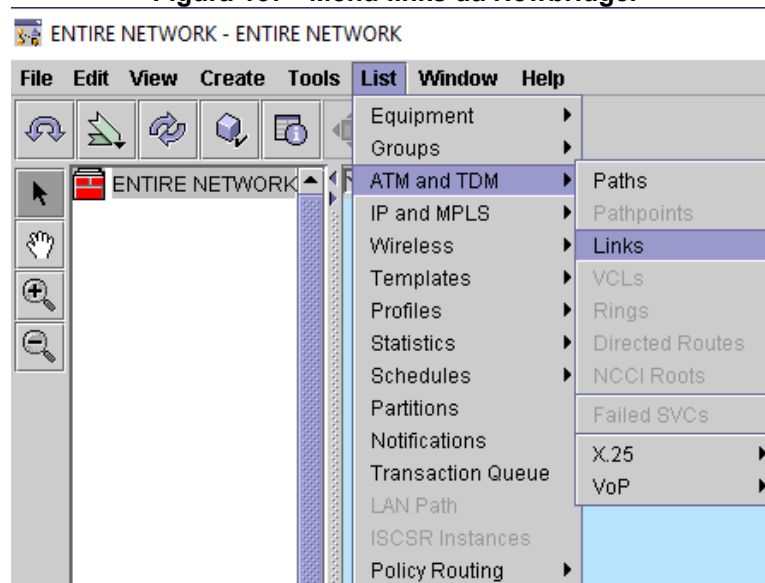
Figura 136 - Time slots da newbridge.



Fonte: Autoria Própria

Caso seja passado o número do *link* ao invés do equipamento, é só selecionar a opção “*List*”, “*ATM and TDM*” e “*Links*” conforme ilustrado na figura 137 e digitar o número do *link* na tela que se abrirá conforme exemplificado na figura 138.

Figura 137 - Menu links da Newbridge.

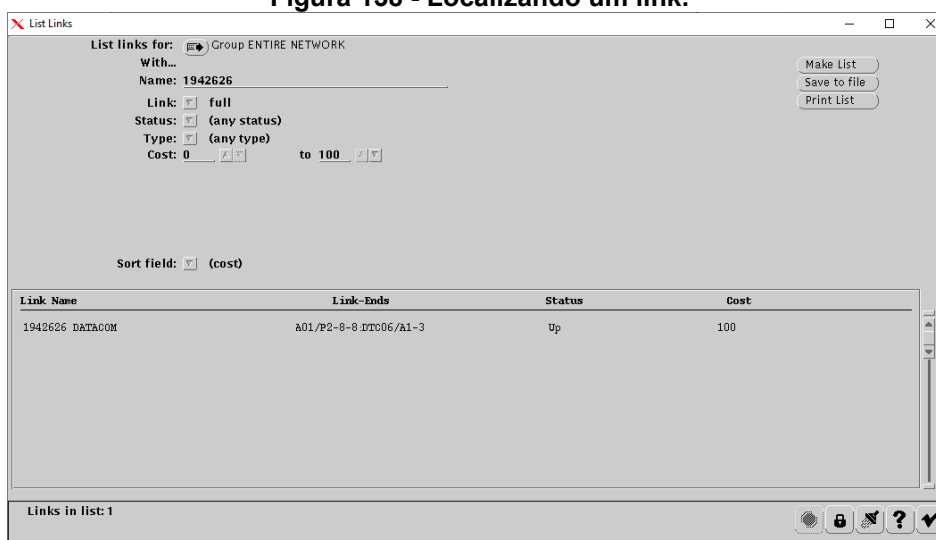


Fonte: Autoria Própria

Algo importante de se frisar é que a coluna “*Link-Ends*” ilustrada na figura 138 tem as pontas A e B separadas por dois pontos, sendo que a ponta A é o nome

do equipamento aqui exemplificado e a ponta B um equipamento fictício chamado de “DTC06” que é a representação do equipamento Datacom. A operadora pode colocar o mesmo nome do equipamento Datacom nesse caso fictício.

Figura 138 - Localizando um link.

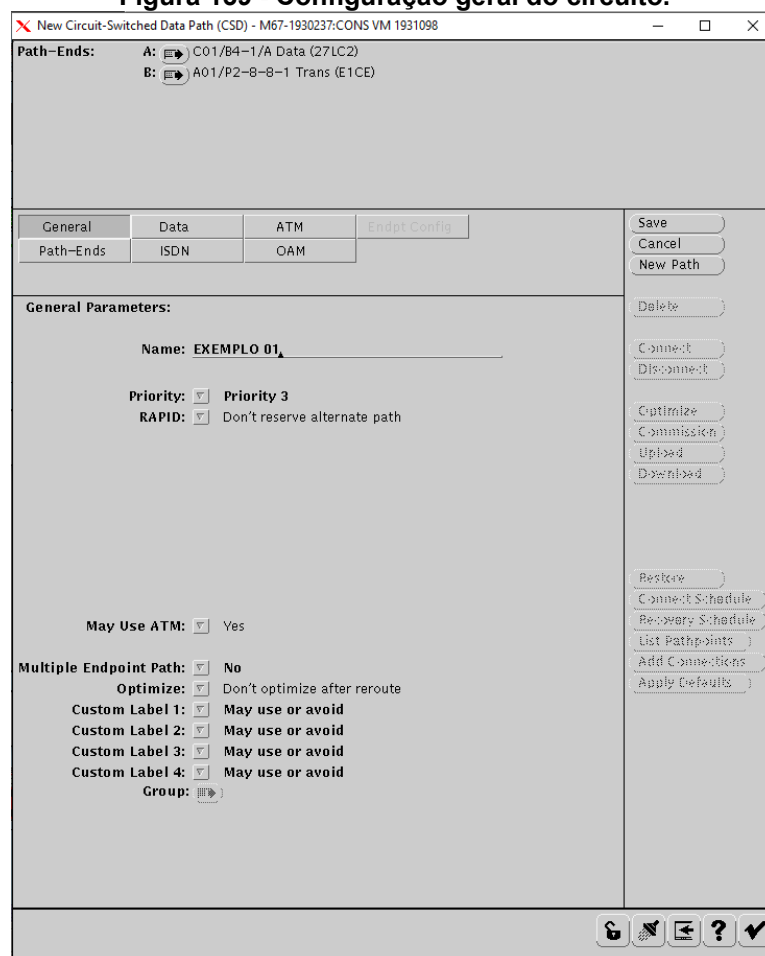


Fonte: Autoria Própria

Não será reexplicado como se configura o circuito na rede *Newbridge*, afinal a única alteração que existe é que o “*timeslot*” ao invés de ser casado com o roteador, vai ter que casar com o multiplexador da rede Datacom. O tópico 3.2.4. trará mais informações.

A figura 139 demonstra a configuração entre a porta do cliente e a gerência Datacom, mas nada impede que ao invés de ser a porta do cliente na ponta A seja um roteador da operadora.

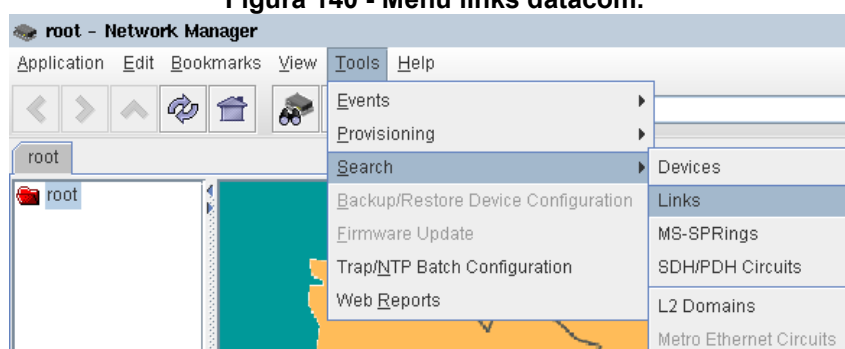
Figura 139 - Configuração geral do circuito.



Fonte: Autoria Própria

Agora na rede Datacom pode-se localizar a porta que se comunicará com a rede Newbridge através do laço (*link*) ou equipamento caso tenha na *Newbridge* as facilidades do equipamento no fictício. Aqui será usada a busca por laço primeiramente e para isso deve-se escolher a opção “Tools”, “Search” e “Links” conforme figura 140.

Figura 140 - Menu links datacom.



Fonte: Autoria Própria

Ao escolher *Links* a tela ilustrada na figura 141 aparecerá e será necessário que a opção “*name*” esteja habilitada. Com ela habilitada digita-se a designação (nome) do *link* que identificará a interligação dos equipamentos de ambas as pontas. Na coluna “*A-End*” tem um equipamento fictício que representa o equipamento real na rede *Newbridge*, pode ocorrer de a operadora querer colocar o mesmo nome do equipamento fictício do real, porém nesse caso isso não ocorreu. Na coluna “*Z-end*” tem o equipamento “MUX-01” que faz a comunicação com a *Newbridge*, já indicando que a placa está no *slot* A porta 1.

Figura 141 - Localizando link na Datacom.

Name	A-End	Z-End	Type	Status	Situation	Cost
1942626 NMB	NMB_D: 1 - CUSTOM-E1 / 2	MUX-01: A - E1Q / 1	E1	Active	Active	0

Fonte: Autoria Própria

Aqui, a parte de configuração foi diretamente para o que interessa, pulando passos já explicados no tópico 3.2.2. sobre o meio de rede. Na tela de configuração será selecionado no quadro “*Z-end*” a opção “*Search*” conforme demonstrado na figura 142.

Figura 142 - Configurando circuito na Datacom.

The screenshot shows the 'New Circuit' configuration window. The 'Configuration' tab is active. Under 'Path Configuration', 'Interactive' is selected. In the 'Configuration' section, 'Type' is 'Nx64K (Circuit)', 'Rate' is '2 - 128 kbit/s', and 'Connection' is 'Bidirectional'. The 'A-End' section shows 'Device: MUX-05', 'Model: DM705-SUB CP...', 'Slot: C - 6V35', and 'Port: 1'. The 'Z-End' section shows 'Device: Not Selected' and an empty 'Slot' field. A legend at the bottom indicates mapping symbols: 'S=> Mapped as source', '=>S Mapped as destination', '<=> Mapped', and '[R] Reserved'. Buttons for 'New', 'Remove', 'Save', and 'Close' are at the bottom.

Fonte: Autoria Própria

Já que o Link que faz a *cross* conexão é o equipamento “MUX-01” deve-se procurá-lo e indicar ao sistema conforme realizado na figura 143.

Figura 143 - Localizando equipamento.

The screenshot shows the 'Device Search' window. Search criteria include 'Device ID' (MUX-01), 'Vendor' (DATAKOM), and 'Model' (DM705-SUB C...). The search results table is as follows:

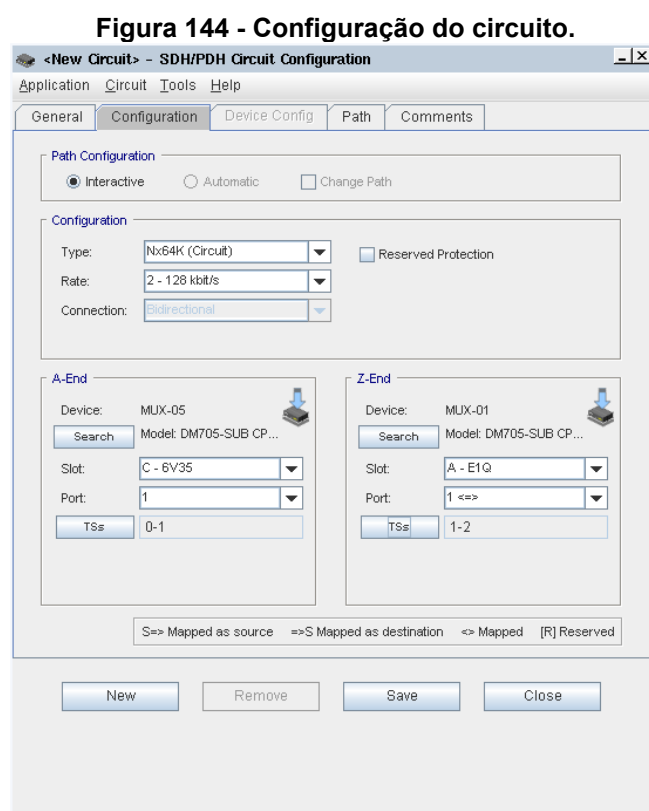
Device ID	Hostname	Dev No	Model	Status
MUX-01	31.21.7.62	1.1	DM705-SUB C...	Normal

The 'Device Details' section on the right is currently empty. Buttons for 'Ping Device', 'Navigate to Map', 'Navigate to', and 'Close' are at the bottom. A status bar at the bottom left indicates '1 device(s) retrieved.'

Fonte: Autoria Própria

Após isso deve-se escolher o “slot” e a “porta” que conforme o caso estudado é “A” e “1”. No botão “TSs” será selecionado os “timeslots” aqui para efetuar o casamento e existir comunicação têm que ser selecionados os mesmos “timeslots” em ambas as pontas que ocorrem a comunicação conforme figura 144. Após isso está concluída a configuração.

Neste ponto é deixado claro que a ponta A pode ser tanto um roteador da operadora ou o cliente, a gerência não distingue o que está fora dela. A comunicação só não existirá se o casamento entre os *timeslots* não seja realizado corretamente.

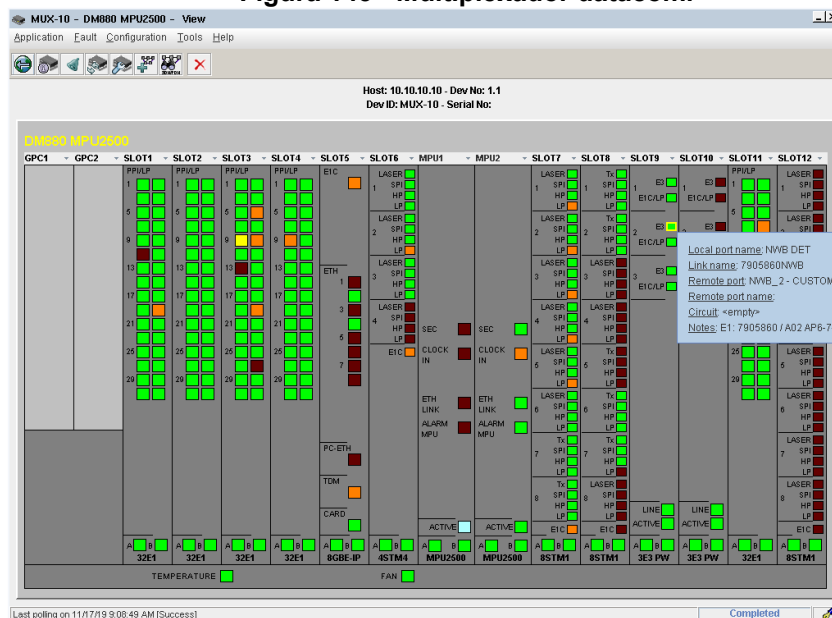


Fonte: Autoria Própria

A partir desse ponto será verificada a *cross* conexão entre E3, começando pela Datacom. O equipamento exemplificado é o “MUX-10” que tem 12 *slots*, que tem 5 placas 32E1, 1 placa 8GBE-IP, 1 placa 4STM4, 2 placas 8STM1 e 2 placas 3E3 que está sendo exemplificado na figura 145, no caso estudado será selecionado o *slot* 9 e a porta 2. Ao deixar o mouse encima da porta aparece informações pertinentes a ela, no campo “*Local port name*” a informação “NWB DET” afirmando

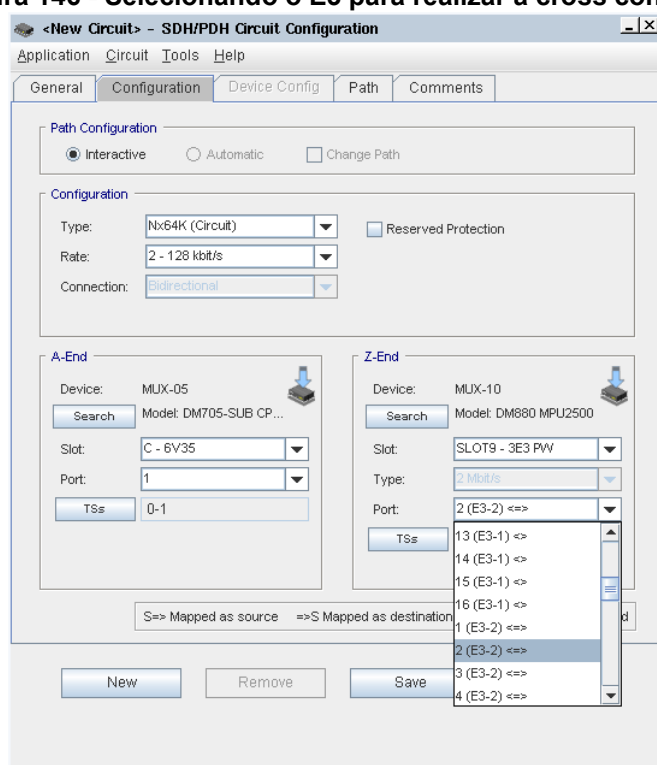
que a porta é determinística, no campo “*Link name*” o nome do laço (“*link*”), no campo “*Remote port:*” o nome do equipamento fictício e no campo “*Notes:*” o número do *link* e o nome do equipamento com suas facilidades.

Figura 145 - Multiplexador datacom.



Fonte: Autoria Própria

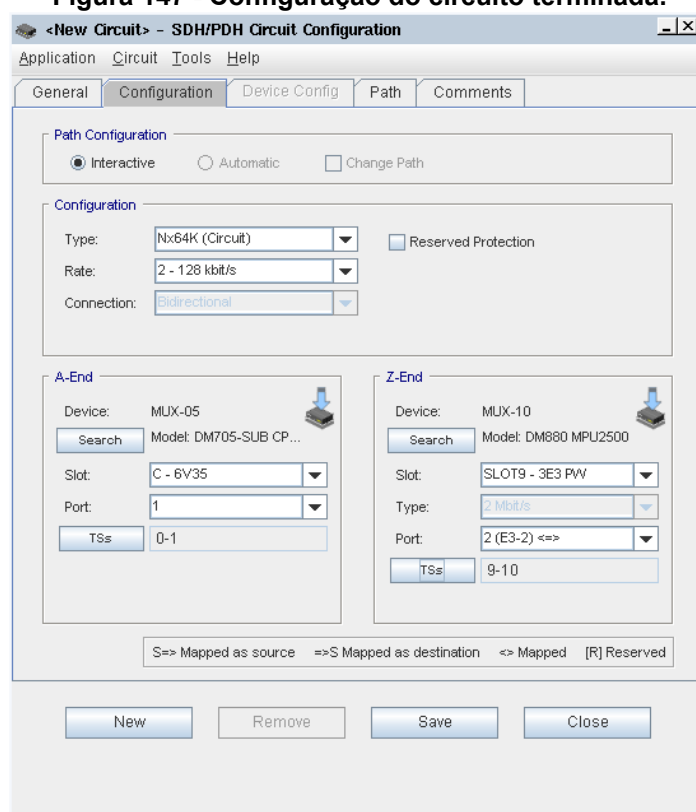
Ao criar o circuito é verificada uma alteração. O campo “*Port:*” não demonstra o número da porta, mas sim a posição lógica do E1 tendo entre parênteses a porta física E3 a qual posição pertence. A figura 146 demonstra o menu flutuante com os E1’s. Nesse exemplo será escolhida a posição lógica 2 e porta física 2.

Figura 146 - Selecionando o E3 para realizar a cross conexão.

Fonte: Autoria Própria

Ao escolher os “*timeslots*”, foi selecionado o 9 e 10 para acasalar com os que serão configurados na *newbridge* conforme figura 147.

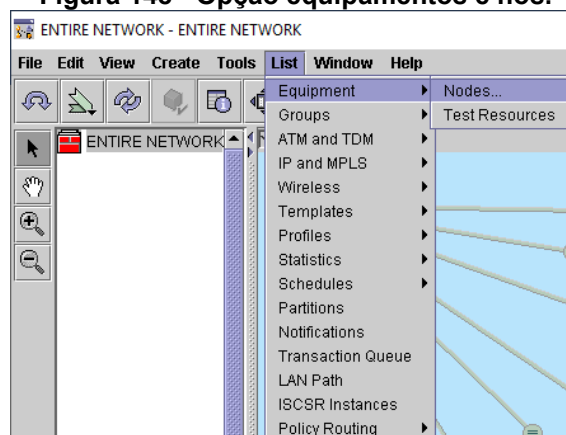
Figura 147 - Configuração do circuito terminada.



Fonte: Autoria Própria

Já na rede Newbridge pode-se procurar por laço (“link”) ou por equipamento. Nesse caso será procurado por equipamento. Para que isso seja possível, deve-se escolher a opção “List”, “Equipment” e “Nodes” conforme demonstrado na figura 148.

Figura 148 - Opção equipamentos e nós.



Fonte: Autoria Própria

Ao selecionar essa opção a janela ilustrada na figura 149 irá se abrir e com isso pode-se no campo “Name:” digitar o nome do equipamento e selecionar “Make

list", ao clicar duas vezes no equipamento o mesmo aparecerá.

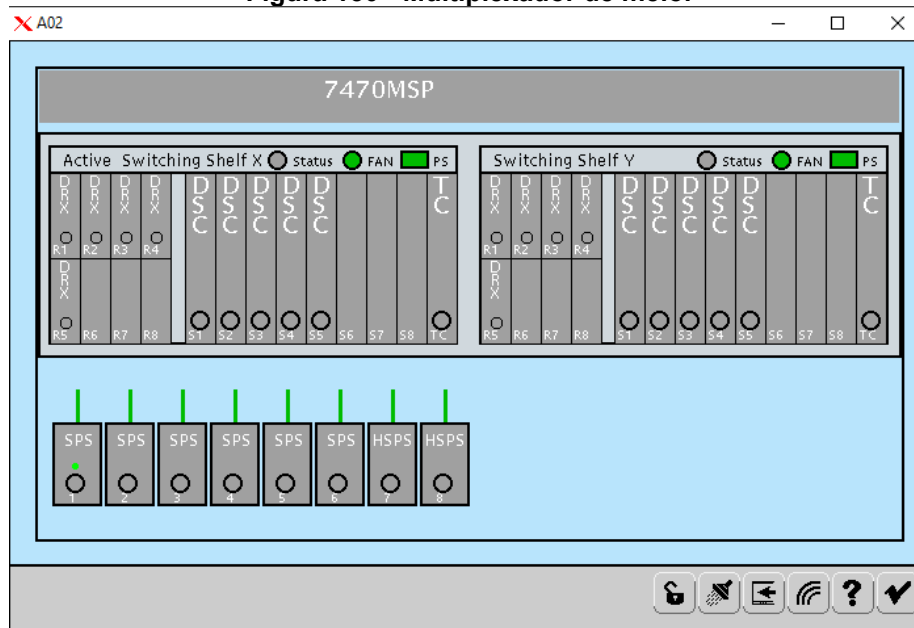
Figura 149 - Localizando equipamento.



Fonte: Autoria Própria

O equipamento “A02” tem 8 placas de recursos, a qual pode ser observada na figura 150, sendo dois para placas de alta velocidade e 6 para placas comuns. Aqui será selecionado o periférico 6 como já visto na Datacom.

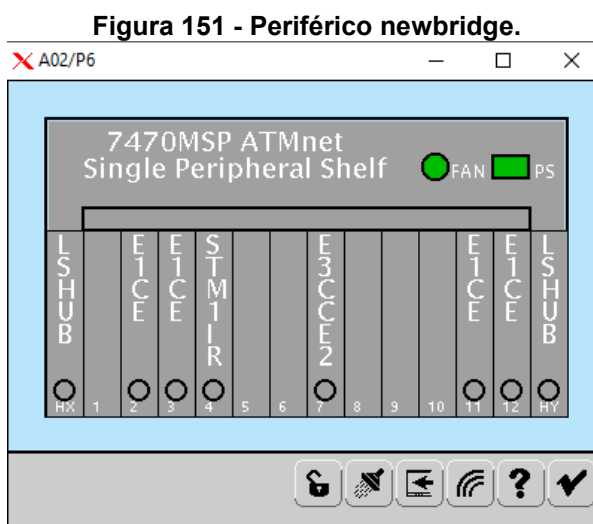
Figura 150 - Multiplexador de meio.



Fonte: Autoria Própria

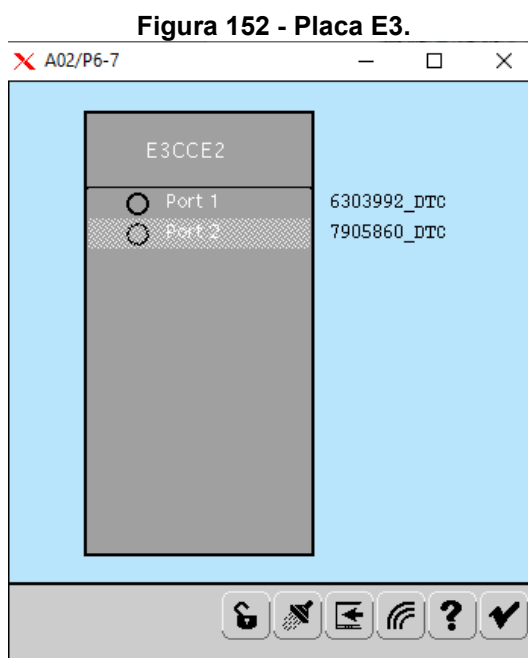
Dentro do periférico existem 6 *slots* vazios, 4 placas E1, 1 placa STM e 1 placa E3, como pode ser verificado na figura 151, então será selecionado o *slot* 7

seguinto o exemplo.



Fonte: Autoria Própria

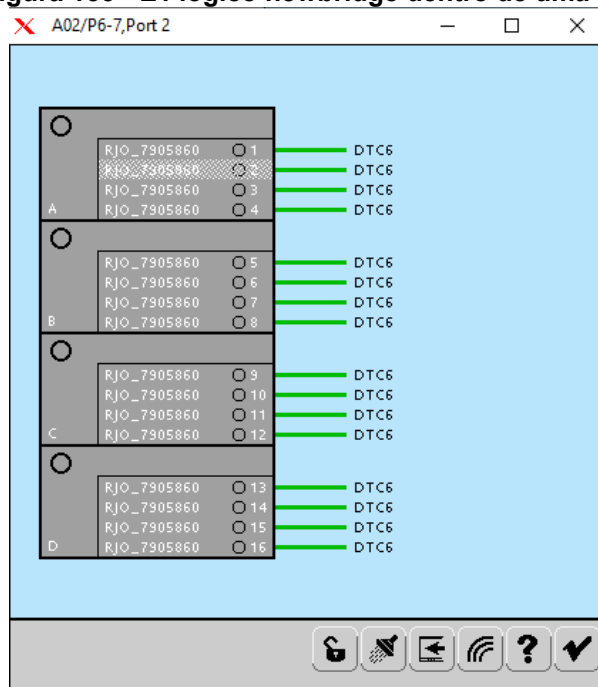
Essa placa também tem 2 portas, vide figura 152, ambas indo para a Datacom, conforme a facilidade vista na Datacom será selecionada a porta 2.



Fonte: Autoria Própria

Após todos esses passos, deve-se escolher o E1 lógico igual ao que foi selecionado na Datacom. Como na Datacom foi escolhido o E1 de número 2, aqui também será selecionado o mesmo.

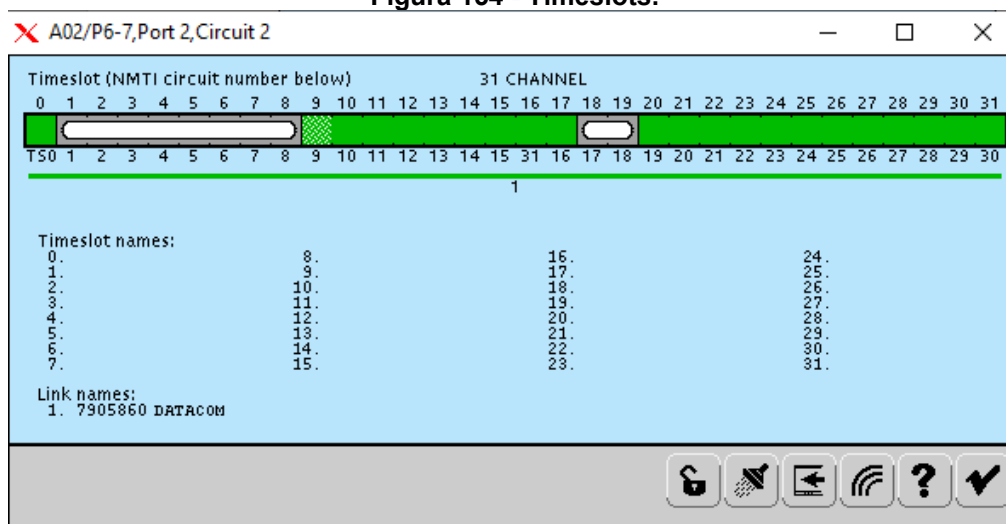
Figura 153 - E1 lógico newbridge dentro de uma E3.



Fonte: Autoria Própria

Por fim será selecionado os “timeslots” na janela demonstrada na figura 154. No caso estudado será escolhido o intervalo 9 e 10 para que haja o casamento de facilidades e a comunicação ocorra de forma ininterrupta.

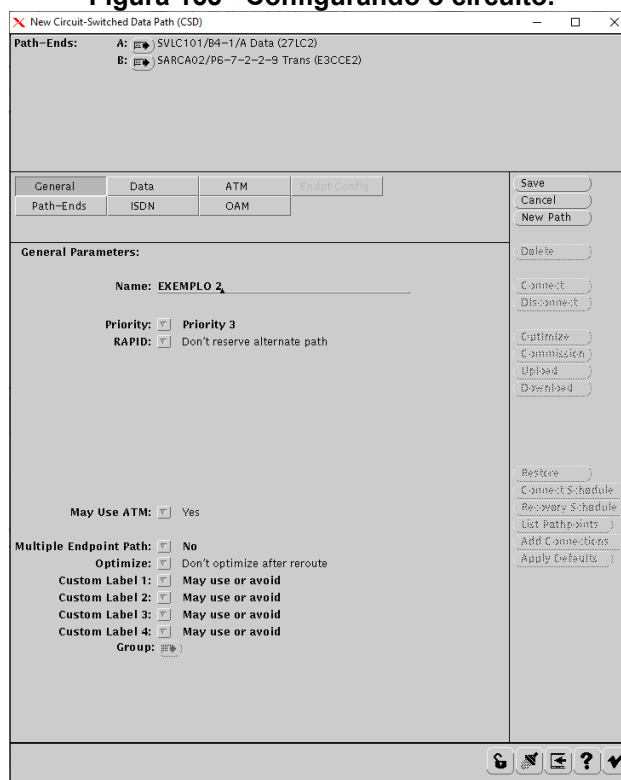
Figura 154 - Timeslots.



Fonte: Autoria Própria

Após encontrar o “timeslot” é só proceder com a configuração conforme o tópico 3.2.3. A figura 155 ilustra a configuração entre uma placa de acesso e a gerência Datacom.

Figura 155 - Configurando o circuito.



Fonte: Autoria Própria

3.3.2 Cross conexão rede ATM Cisco Newbridge

Nessa *cross* a conexão das facilidades poderão ser passadas via terceiros pois na rede ATM da Cisco não têm campo de descrição para localizar as facilidades, na *Newbridge* será mostrado como localizar as facilidades do BPX e IGX.

Para realizar a conexão entre essas duas gerências será suposto que a facilidade que se comunica com a *Newbridge* é o slot 14, porta 5 com a faixa de *timeslots* de 1 a 4. Ao ter essas informações e sabendo que o slot 14 tem uma placa E1, será necessário criar uma porta lógica para encapsular as informações dos *timeslots* e da porta física.

Para criar a porta lógica usa-se o comando “*addport*” junto com a placa e a porta lógica, sendo porta lógica um numeral qualquer que não seja repetido para aquela placa, após digita-se a porta física com o intervalo de *timeslots*. O comando é ilustrado na figura 156.

Figura 156 - Configurando porta.

```

V400          VT          User:2          IGX 8420 9.3.51 Nov. 20 2019 04:35 G-03
Port configuration for UFM 14

```

From	Line	Chan	Speed	Interface	State	Protocol
4	5	1-4	256 Kbps	E1B	INACTIVE	None
6	8	28-31	256 Kbps	E1B	FAILED	Annex D UNI
8	2	25-26	128 Kbps	E1B	FAILED	Annex D UNI
12	2	7-8	128 Kbps	E1B	FAILED	Annex D UNI
16	2	15-16	128 Kbps	E1B	FAILED	Annex D UNI
17	2	17-18	128 Kbps	E1B	FAILED	Annex D UNI
23	8	7-10	256 Kbps	E1B	FAILED	Annex D UNI
24	7	2-3	128 Kbps	E1B	FAILED	Annex D UNI
26	7	6-7	128 Kbps	E1B	FAILED	Annex D UNI
27	8	14-15	128 Kbps	E1B	FAILED	Annex D UNI
33	8	1-2	128 Kbps	E1B	FAILED	Annex D UNI
34	7	12	64 Kbps	E1B	FAILED	Annex D UNI

```

Last Command: addport 14.4 5.1-4

Next Command: █
Virtual Terminal          MAJOR ALARM

```

Fonte: Autoria Própria

Logo após essas configurações, deve-se ativar a porta com o comando “*upport*” e a facilidade da porta lógica conforme demonstrado na figura 157.

Figura 157 - Ativando porta.

```

V400          VT          User:2          IGX 8420 9.3.51 Nov. 20 2019 04:35 G-03
Port:          14.4          [ACTIVE ]
Interface:     E1B          Configured Clock: 256 Kbps
Clocking:     None          Measured Rx Clock: None
Neighbor IP Add: 0.0.0.0    Neighbor IfIndex: 0
Port ID       -             Min Flags / Frames      1
Port Queue Depth 65535      OAM Pkt Threshold       3 pkts
ECN Queue Threshold 65535    T391 Link Intg Timer    10 sec
DE Threshold   100 %        N391 Full Status Poll   6 cyl
Signalling Protocol None      EFCI Mapping Enabled    No
Asynchronous Status No       CLLM Enabled/Tx Timer   No/ 0 msec
T392 Polling Verif Timer 15      IDE to DE Mapping       Yes
N392 Error Threshold 3        Channel Speed           64
N393 Monitored Events Count 4      Line Number             5
Communicate Priority No       Channel Range           1-4
Advertise Intf Info Disable

```

```

Last Command: upport 14.4

Next Command: █
Virtual Terminal          MAJOR ALARM

```

Fonte: Autoria Própria

E configurar a porta para uso com o comando “*cnfport*”. No caso do exemplo foi selecionada a configuração “Annex D” demonstrado na figura 158. Depois disso deve-se criar a conexão com a outra ponta, mais detalhes no capítulo 4.2.4.

Figura 158 - Configurando porta lógica.

```

V400      VT      User:2      IGX 8420  9.3.51      Nov. 20 2019 02:47 G-03
Port:      14.4      [ACTIVE ]
Interface:  E1B      Configured Clock:  256 kbps
Clocking:   None     Measured Rx Clock: None
Neighbor IP Add: 0.0.0.0  Neighbor IfIndex: 0
Port ID     -        Min Flags / Frames  1
Port Queue Depth  65535  OAM Pkt Threshold  3 pkts
ECN Queue Threshold  65535  T391 Link Intg Timer  10 sec
DE Threshold  100 %  N391 Full Status Poll  6 cyl
Signalling Protocol Annex D UNI  EFCI Mapping Enabled  No
Asynchronous Status  No     CLLM Enabled/Tx Timer  No/ 0 msec
T392 Polling Verif Timer  15    IDE to DE Mapping     Yes
N392 Error Threshold  3     Channel Speed         64
N393 Monitored Events Count  4     Line Number           5
Communicate Priority  No     Channel Range         1-4
                                       Advertise Intf Info  Disable
-----
Last Command: cnfport 14.4 65535 65535 100 d N N 15 3 4 3 N N Y 1 N

Next Command: █

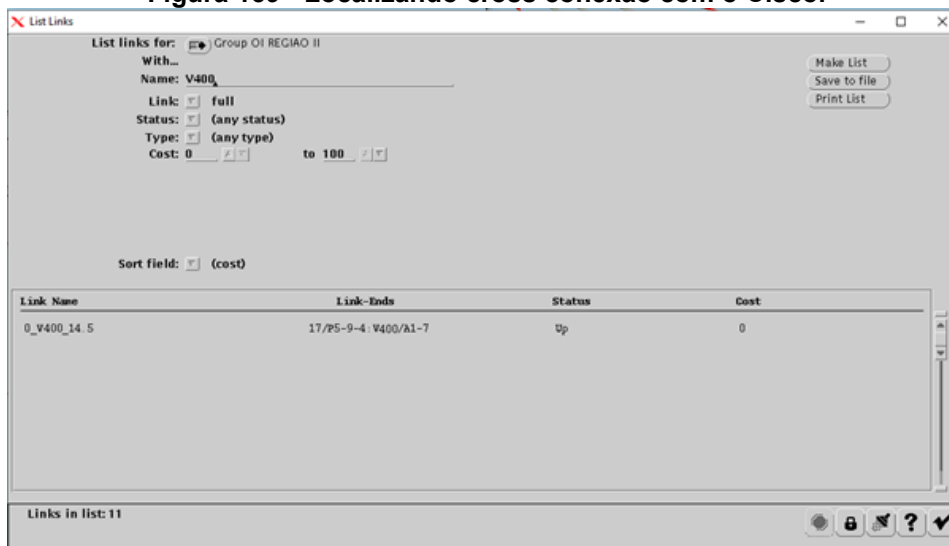
Virtual Terminal MAJOR ALARM

```

Fonte: Autoria Própria

Caso não tenha a facilidade, o ideal é ir à outra gerência e procurar a interface. Como se quer um equipamento na rede *Newbridge* que faça comunicação com o equipamento V400 da rede ATM cisco, em *list links* foi localizado o *link* que faz a comunicação como demonstrado na figura 159. Mais detalhes serão apresentados no capítulo 3.3.1.

Figura 159 - Localizando cross conexão com o Cisco.

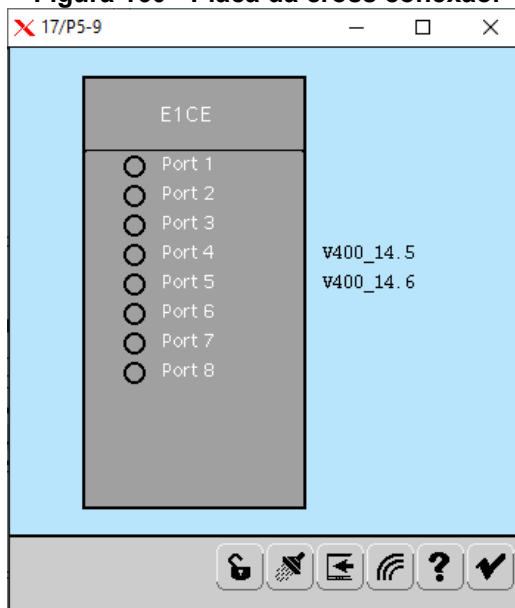


Fonte: Autoria Própria

Foi encontrado o laço (*link*) que faz a conexão entre a rede *Newbridge* e na porta 14.5. do equipamento V400 da rede ATM cisco no equipamento 10.017 periférico 5, *slot* 9 e porta 4. A figura 160 mostra o *slot* 9 da placa E1CE a qual afirma a existência de um laço com a porta 14.6 na porta 5 que não lista na figura acima, isso se deve a essas descrições não serem atribuídas ao laço (*link*), mas sim

à porta.

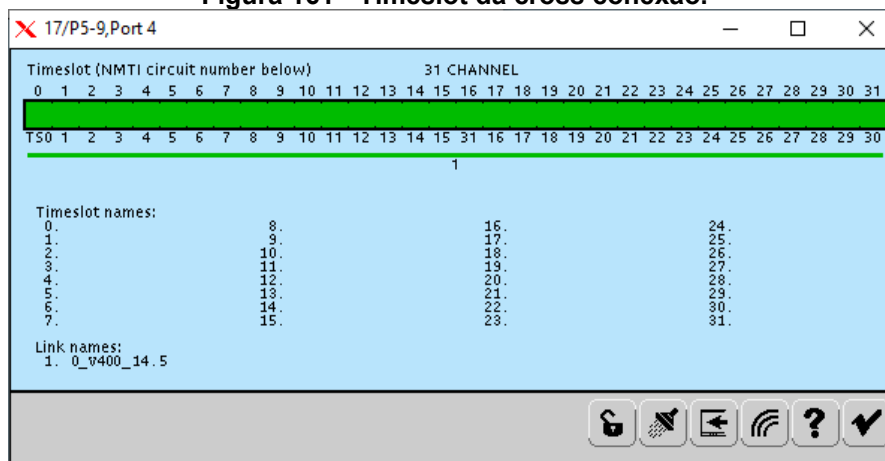
Figura 160 - Placa da cross conexão.



Fonte: Autoria Própria

Dentro do *slot*, pode-se selecionar o *timeslot* e fazer a conexão com outra gerência conforme já explicado no capítulo 3.2.3. A figura 161 demonstra os *timeslots* do equipamento 17, periférico 5, *slot* 9 e porta 4.

Figura 161 - Timeslot da cross conexão.



Fonte: Autoria Própria

3.3.3 Cross conexão Metro e DSLAM.

Nesse capítulo será abordada a *cross* conexão entre DSLAM e a rede *Metroethernet*. É importante lembrar que o DSLAM sempre terá que ter um roteador

trabalhando em conjunto para poder ter um endereço IP válido na internet e não será usado como meio de comunicação entre duas gerências.

A figura 162 mostra dois comandos sendo lançados, o comando “*show interface description | i 193*” que aparece abreviado e realiza uma busca em todas as portas por descrição. A operadora normalmente colocará o nome cliente, um ID ou até o nome do outro equipamento na descrição da interface, outra forma pode ser por um sistema autônomo que mostra a porta que está sendo configurada, a resposta do comando é a porta com um QinQ, já explicado no tópico 3.1.2. O segundo comando é o “*show interface*”. Esse comando é realizado para coletar o próximo equipamento (salto) da topologia, no “*description*” do resultado mostra A1 gi 4/2/13, nesse caso o equipamento é A1 e porta gi 4/2/13.

Figura 162 - Localizando porta no Cisco.

```
C1#sh int desc | i 193
Gi7/0/0.39711134          up          up          193
C1#sh int gi7/0/0
GigabitEthernet7/0/0 is up, line protocol is up
Hardware is GiEther SPA, address is 001e.f741.1440 (bia 001e.f741.1440)
Description: A1 gi 4/2/13;
MTU 1500 bytes, Bw 1000000 kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set
Keepalive not supported
Full Duplex, 1000Mbps, link type is force-up, media type is SX
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 27w6d
Input queue: 0/75/14373094/380158 (size/max/drops/flushes); Total output drops: 95246783
Queueing strategy: Class-based queueing
Output queue: 0/40 (size/max)
30 second input rate 971000 bits/sec, 442 packets/sec
30 second output rate 1296000 bits/sec, 261 packets/sec
47614438112 packets input, 11100753928834 bytes, 0 no buffer
Received 141414714 broadcasts (52394258 IP multicasts)
0 runts, 0 giants, 3064 throttles
1416837 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 247375877 multicast, 0 pause input
71748507227 packets output, 7941892379786 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Fonte: Autoria Própria

Ao realizar o acesso ao equipamento A1, é descoberto que o mesmo é um equipamento da Nokia o que é bastante comum essa convergência entre fabricantes distintos. A figura 163 demonstrou que a porta física é 4/2/13 e também foi considerado que a interface lógica estava com os números de SVLAN e CVLAN igual ao real, então foi usado o comando “*admin display-config | match 4/2/13:3971 context all*”, sendo 3971 a SVLAN do túnel. Uma outra abordagem possível pode ser por descrição usando o comando “*admin display-config | match (ID/nome do cliente) context all*”, mas isso varia de operadora e a primeira forma é a mais correta. A resposta do comando foi o número da *epipe* conforme explicado o funcionamento no tópico 3.2.2.

Uma informação interessante é que houve nesse salto uma alteração de SVLAN, que de 3971 virou 30972, ou seja, durante os saltos a SVLAN pode ser

traduzida para outra.

Ao usar o número da *epipe* (30972) no comando “*show service id 30972 base*”, demonstrará se o túnel está operante e qual é o IP do próximo salto na linha “*sdp:3019:30972 S(200.223.230.190) ...*”, sendo ele o IP 200.223.230.190, pode-se conectar ao próximo equipamento (salto) através desse IP.

Figura 163 - Verificando porta no Alcatel.

```
*A:A1# admin display-config | match 4/2/13:3971 context all
#-----
service
  epipe 30972 customer 112 create
  sap 4/2/13:3971 create
  description "Port 1/2/1 - Vlan 1971"
*A:A1# show service id 30972 base
=====
Service Basic Information
=====
Service Id       : 30972          vpn Id       : 0
Service Type    : Epipe
Name            : (Not Specified)
Description     : 193

Customer Id     : 112
Last Status Change: 01/16/2020 20:54:29
Last Mgmt Change : 10/07/2019 05:03:33
Admin State     : Up
VTU             : 1522
VC Switching   : False
SAP Count       : 1
Per Svc Hashing : Disabled
Force QTag Fwd : Disabled
Creation Origin  : manual
Oper State      : Up
SDP Bind Count  : 1

=====
Service Access & Destination Points
=====
Identifier                                     Type      AdmMTU  OprMTU  Adm  Opr
-----
sap:4/2/13:3971                               q-tag    1564    1564    Up   Up
sdp:3019:30972 S(200.223.230.190)           Spok     1522    1522    Up   Up
=====
```

Fonte: Autoria Própria

Na figura 164 foi considerado que o *epipe* é igual nas duas pontas, o que facilitaria o trabalho, mas pode ocorrer de não ser. Caso isso ocorra pode ser por convenção colocada uma descrição e usado o comando “*admin display-config | include “ID/nome do cliente” context all*” ou através da SVLAN que será igual nas duas pontas para que o túnel exista, usando o comando “*admin display-config | include 30972 context all*” e logo após “*show service sdp-using (spoke-sdp)*” nesse caso a *spoke-sdp* é “3012:30972”.

Aqui se destaca a tradução de SVLAN que ocorre novamente de 30972 para 1971, a qual será entregue ao próximo salto. A CVLAN permanece a mesma do início, ou seja, 1341. O “*” que surgiu indica que toda CVLAN será passada para a outra gerência e já é um indício que haverá *cross* conexão com a rede DSLAM.

Figura 164 - Usando a rede metro para ir a outro equipamento.

```

B:A2 # show service id 30972 base
=====
Service Basic Information
=====
Service Id       : 30972          vpn Id          : 0
Service Type    : Epipe
Name            : (Not Specified)
Description     : 1931943

Customer Id     : 112
Last Status Change: 01/16/2020 20:54:29
Last Mgmt Change : 03/18/2019 08:21:56
Admin State     : Up              oper State      : Up
MTU             : 1522
Vc Switching   : False
SAP Count      : 1              SDP Bind Count : 1
Per Svc Hashing : Disabled
Force QTag Fwd : Disabled

-----
Service Access & Destination Points
-----
Identifier                               Type      AdmMTU  OprMTU  Adm  opr
-----
sap:4/2/2:1971.*                         qinq     1564    1564    up   up
sdp:3012:30972 s(200.223.230.125)       Spok     1522    1522    up   up
=====

```

Fonte: Autoria Própria

Ao usar o comando “*show port 4/2/2*” como mostrado na figura 165 terá o campo *description* com o nome do equipamento e a tecnologia, ou a operadora pode ter algum sistema que indique que a porta do roteador vai para esse equipamento.

Figura 165 - Localizando DSLAM.

```

B: A02# show port 4/2/2
=====
Ethernet Interface
=====
Description      : M1-Huawei

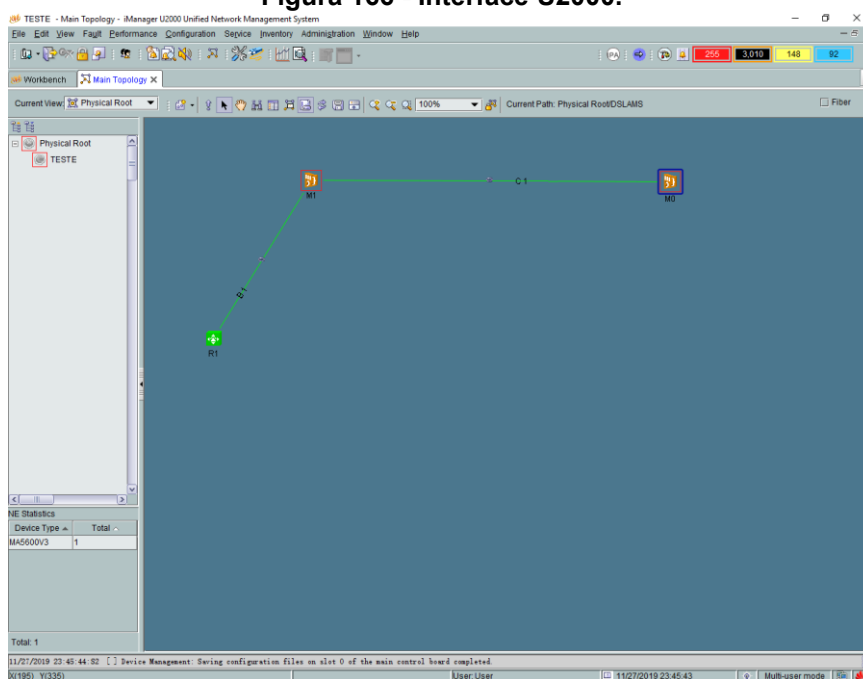
```

Fonte: Autoria Própria

Ao acessar a gerência U2000 no exemplo da figura 166 existem os equipamentos R1, M1 e M0 sendo R1 um equipamento fictício, M1 e M0 equipamentos DSLAM. O cenário aqui é que M0 entrega para o cliente M1 é um DSLAM de cascata, então a primeira configuração necessária é em M1.

O exemplo é bem simplificado já que num ambiente real a quantidade de equipamentos é gigantesca. Na figura 166, ao lado esquerdo terá uma estrutura escrito “*Physical Root*” e dentro do escopo dela “*TESTE*”, normalmente ao invés de “*TESTE*” terá os estados do país e vários agrupamentos dentro dessa estrutura.

Figura 166 - Interface U2000.

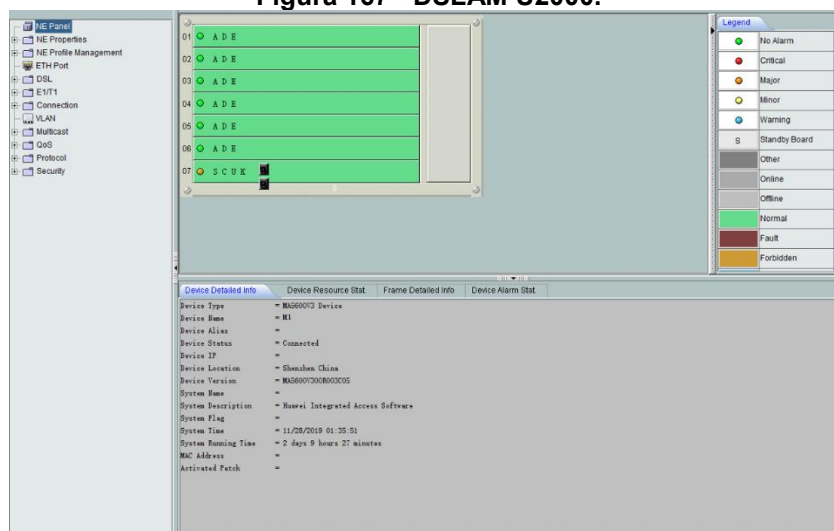


Fonte: Autoria Própria

Normalmente cada multiplexador desse, terá uma placa ou duas para a tecnologia *ethernet* e as demais para a tecnologia ADSL. A placa SCUK é uma placa com duas interfaces *ethernet* e as placas ADE suportam até 64 portas, como será configurada uma cascata então será configurado a placa *ethernet* com 2 portas.

A figura 167 demonstra um multiplexador com 7 placas, sendo 6 para serem usadas para clientes através da placa ADE e uma com portas Ethernet para o envio das informações a um roteador ou outro DSLAM.

Figura 167 - DSLAM U2000.



Fonte: Autoria Própria

A figura 168 ilustra duas interfaces *GigabitEthernet* que estão dentro da placa SCUK, uma indo ao roteador R1 e outra indo para o multiplexador M1. Aqui deve-se criar a SVLAN 1971 em ambas as portas, para criar basta clicar com o botão direito do mouse e escolher “*add VLAN...*” e digitar a SVLAN. Se fosse entregue ao cliente só seria necessário criar a SVLAN na porta que se comunica com R1.

Figura 168 - DSLAM em cascata.

The screenshot shows a network management interface with a left sidebar containing various configuration categories like NE Plans, NE Properties, ETH Port, DSL, E/F/T1, Connection, VLAN, Multicast, QoS, Protocol, and Security. The main window displays the 'Ethernet Port' configuration table and a 'VLAN ID' table below it.

Status	Name	Alias	Port Type	Working Mode	Port Rate (Mbps)	Type of Connected Cable	Default VLAN ID (1-4095)
Activated	Frame 0/Slot 7/Port 0	R1	GE Optical Port	Full Duplex	1000	--	--
Activated	Frame 0/Slot 7/Port 1	M1	GE Optical Port	Full Duplex	1000	--	--

VLAN ID	Name	Alias	Type	Attribute	Super VLAN ID
1	VLANID_1		MUX VLAN	Common	--
12	VLANID_12		Standard VLAN	Common	--
1971	VLANID_1971		Smart VLAN	Stacking	--
2106	VLANID_2106		Smart VLAN	Stacking	--
2222	VLANID_2222		Smart VLAN	Stacking	--
2223	VLANID_2223		Smart VLAN	Stacking	--
2334	VLANID_2334		Smart VLAN	Stacking	--
2335	VLANID_2335		Smart VLAN	Stacking	--
2336	VLANID_2336		Smart VLAN	Stacking	--
2337	VLANID_2337		Smart VLAN	Stacking	--
2423	VLANID_2423		Smart VLAN	Stacking	--
2565	VLANID_2565		Smart VLAN	Stacking	--
3502	VLANID_3502		Smart VLAN	Stacking	--
3514	VLANID_3514		Smart VLAN	Stacking	--

Fonte: Autoria Própria

Criada a SVLAN nas portas necessárias, basta ir até o outro multiplexador (caso o cliente ficasse no mesmo multiplexador não seria necessário) e escolher a placa e porta ADSL para realizar a configuração conforme demonstrado na figura 169.

Figura 169 - Portas DSL.

Status	Name	Alias	Line Profile	Alarm Profile	Extended Profile	Port Type	Latest Activated Time
Activated	Frame 0/Slot 6/Port 0	1931341	4000	DEFVAL		ADSL2+	--
Activated	Frame 0/Slot 6/Port 1	1930614	8000	DEFVAL		ADSL2+	--
Activated	Frame 0/Slot 6/Port 2	1962150	4000	DEFVAL		ADSL2+	--
Activated	Frame 0/Slot 6/Port 3	1931470	4000	DEFVAL		ADSL2+	--
Activated	Frame 0/Slot 6/Port 4	1937417	15M_ASSI	DEFVAL	EXT_op5_op5	ADSL2+	--
Activating	Frame 0/Slot 6/Port 5	LIVRE	4000	DEFVAL	EXT_1_1	ADSL2+	--
Activated	Frame 0/Slot 6/Port 6	1936728	4000	DEFVAL		ADSL2+	--
Activating	Frame 0/Slot 6/Port 7	LIVRE	4000	DEFVAL	EXT_op5_op5	ADSL2+	--
Activated	Frame 0/Slot 6/Port 8	1930803	15M_ASSI	DEFVAL		ADSL2+	--
Deactiva	Frame 0/Slot 6/Port 9	1930859	3000	DEFVAL		ADSL2+	--
Activating	Frame 0/Slot 6/Port...	LIVRE	4000	DEFVAL		ADSL2+	--
Activated	Frame 0/Slot 6/Port...	1937899	15M_ASSI	DEFVAL	EXT_op5_op5	ADSL2+	--
Activated	Frame 0/Slot 6/Port...	1937254	15M_ASSI	DEFVAL	EXT_op5_op5	ADSL2+	--

No. 0, Total: 64, Selected: 0 Updated at: 11/28/2019 02:16:04

Fonte: Autoria Própria

Nesse ponto pode-se clicar duas vezes na configuração existente e alterar as VLANS ou clicar com o botão direito do mouse e selecionar “add...” e digitar as VLANS, lembrando que “VLAN ID” é a SVLAN e “Inner VLAN” é a CVLAN.

Figura 170 - Configurando serviço.

Service Type	Service Para	Upstream Traffic Profile	Downstream Traffic Profile	VLAN ID	Inner VLAN ID	Max. Learnable MAC Addresses
Single	--	ubrPcr_102400K	ubrPcr_102400K	1971	1134	255
Single	--	ubrPcr_102400K	ubrPcr_102400K	3514	353	255

No. 0, Total: 2, Selected: 0, Update at: 11/28/2019 02:44:04

Fonte: Autoria Própria

3.3.4 Cross Conexão Cisco/ATM/DSLAM

Para que a *cross* conexão exista haverá a necessidade de aprovisionar uma interface ATM no roteador Cisco, passando pela rede Newbridge e chegando a DSLAM.

No roteador foi criada uma interface. Para criar basta entrar na interface (comando “interface ATM 7/1/0.50”), gerar o PVC e colocar o encapsulamento desejado conforme figura 171.

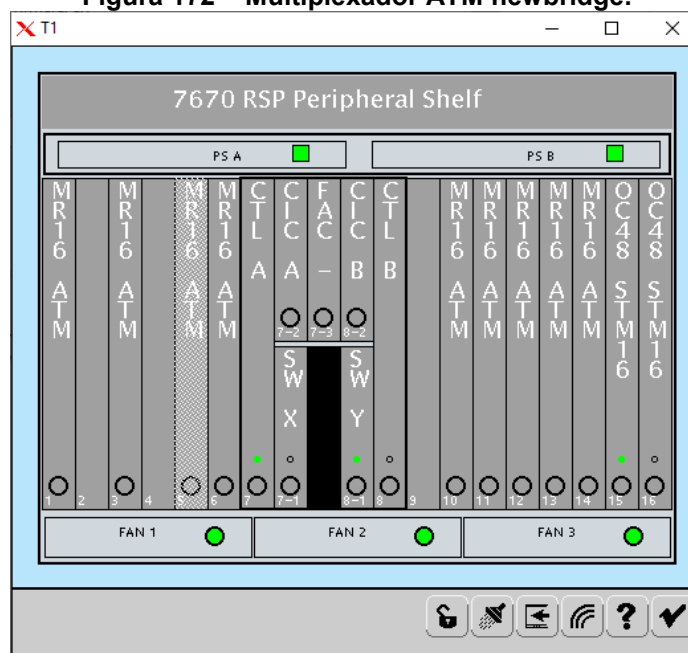
Figura 171 - Configurando PVC.

```
01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
01(config)#interface ATM 7/1/0.50
01(config-subif)#pvc 0/50
01(config-if-atm-vc)#encapsulation aal5snap
```

Fonte: Autoria Própria

Na rede Newbridge basta selecionar o equipamento desejado, no exemplo demonstrado na figura 172 foi selecionado o equipamento T1 e a placa 5.

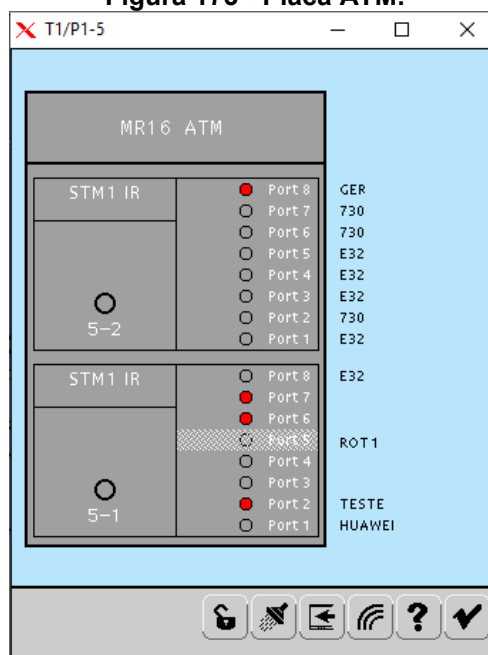
Figura 172 – Multiplexador ATM newbridge.



Fonte: Autoria Própria

Dentro da placa tem duas subdivisões lógicas STM sendo 2 e 1. Foi selecionado no exemplo da figura 173 a placa STM 1 porta 5 que vai para o roteador Cisco.

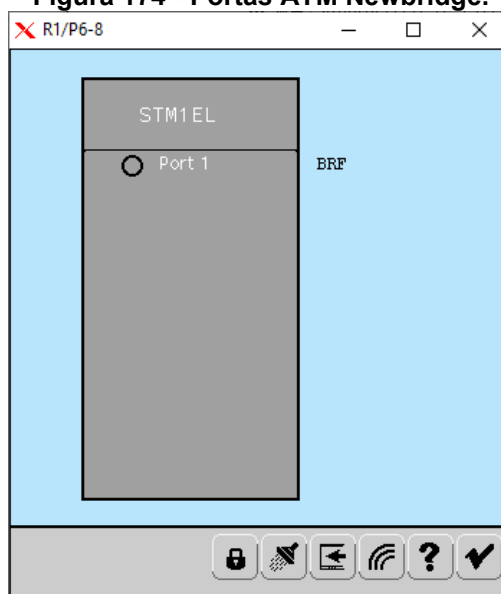
Figura 173 - Placa ATM.



Fonte: Autoria Própria

Na outra ponta foi selecionado o equipamento que tem uma porta física que vai para a DSLAM conforme mostrado na figura 174.

Figura 174 - Portas ATM Newbridge.

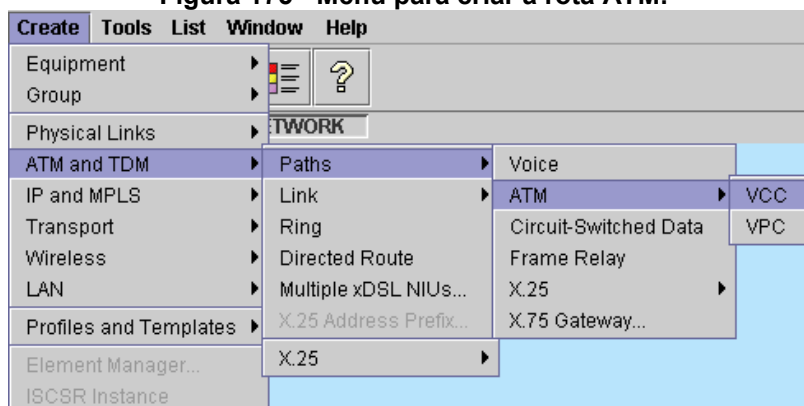


Fonte: Autoria Própria

Para criar a rota deve-se escolher as opções “create, ATM and TDM, paths, ATM e VCC” que são demonstradas na figura 175, pois será criada uma rota ATM com VPC que será o túnel de comunicação onde todos os clientes irão passar e o

VPC, que é a identificação do cliente nesse túnel.

Figura 175 - Menu para criar a rota ATM.



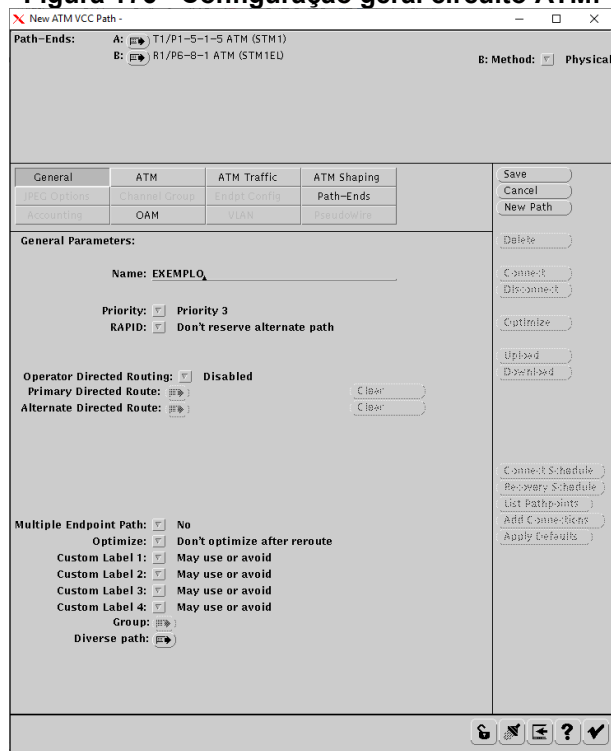
Fonte: Autoria Própria

A figura 176 segue o que está escrito no tópico 3.2.4 com algumas diferenças:

Operator Directed Routing: A rota será configurada pelo operador.

Diverse Path: Caminho diferente caso o principal vir a cair.

Figura 176 - Configuração geral circuito ATM.



Fonte: Autoria Própria

Na figura 177 existem as informações da janela ATM cuja informações

refere-se a cross conexão ATM, sendo elas:

- *VPI (Virtual path Identifier)*: É o caminho entre o equipamento A (*Endpoint A*) e o equipamento B (*Endpoint B*), não sendo necessário serem iguais entre ambas as pontas, porém precisam ter o mesmo que o configurado no roteador e na DSLAM, no exemplo o roteador tinha o pvc 0/50 então VPI será 0 e na DSLAM terá configurado no exemplo o numeral 112 sendo necessário apontar nesse campo.
- *VCI (Virtual channel identifier)*: É o canal virtual entre o equipamento A (*Endpoint A*) e o equipamento B (*Endpoint B*), não sendo necessário serem os mesmos em ambas as pontas, porém deve-se ter o mesmo configurado no roteador e na DSLAM, no exemplo o roteador tinha o pvc 0/50 então o VCI deve-se ser configurado 50 e no DSLAM será usado o VCI 300 no exemplo sendo necessário configura-lo nesse ponto.
- *VC Application*: Tem como opção a conexão PVC, SPVC ou pode usar SPVC (*May use SPVC*). Sendo PVC um caminho fixo e SPVC um caminho que pode ser roteador em caso de queda por outro caminho disponível, lembrando para que o SPVC ocorra todos os mux devem ter suporte para essa ocorrência.
- *Connection Type*: Pode ser selecionado as opções:
 - *Point to point – asymmetrical*: Velocidade de upload e download diferentes.
 - *Point to Point – symmetrical*: Velocidade de upload e download iguais.
 - *Multipoint*: Multiponto.
- *Service Category*: Pode ser selecionado as opções UBR, ABR, CBR, VBR-rt e VBR-nrt que já foram explicadas no tópico 2.3.
- *Alarm Surveillance*: Mantém uma vigilância ativa de alarmes. Nesse exemplo ficará desativado pois esse recurso custa muito do processamento dos multiplexadores.
- *Must use VPC Link*: Se passará vários VP's no caminho, nesse exemplo vai passar apenas uma que pertence ao cliente, então será decidido colocar não.
- *May Use PSNL*: Patenteado por Farid et al. (2006), o PSNL (*Packet Switch Network Link*) é uma abstração da rede MPLS (*Multi-Protocol Label Switch*) em infraestrutura de rede multisserviços, no exemplo trabalhado.
- *MIR (Minimum Information Rate)*: É usado pelo algoritmo de gerência de banda otimizada para representar a menor taxa de informação quando a rede

está congestionada (OPPENHEIMER, 2001).

- PIR (*Peak Information Rate*): É a banda de pico que a conexão pode usar durante rajadas de dados quando atingem o excesso de banda disponível e sem congestionamento na conexão de rede (OPPENHEIMER, 2001).

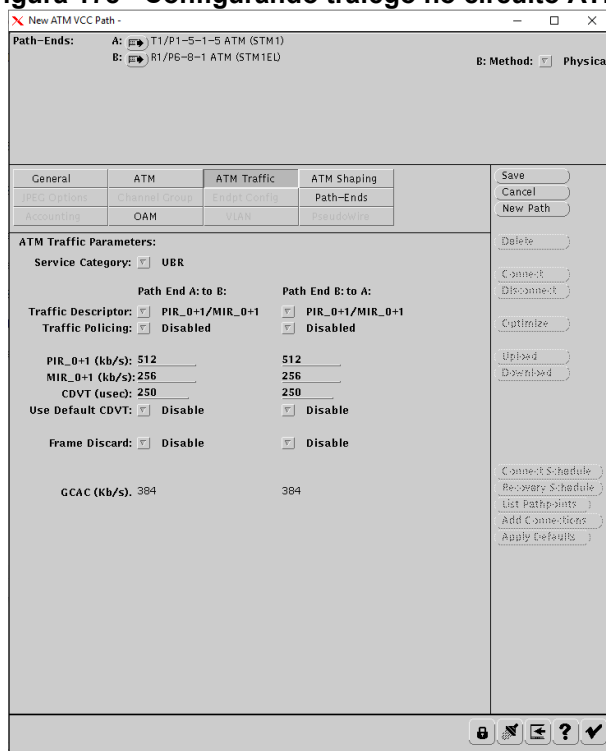
Figura 177 - Configuração do circuito ATM.

The screenshot shows the 'New ATM VCC Path' configuration window. At the top, it displays 'Path-Ends' with endpoints A: T1/P1-S-1-5 ATM (STM1) and B: R1/P6-B-1 ATM (STM1ED), and 'B: Method: Physical'. Below this is a tabbed interface with 'General', 'ATM', 'ATM Traffic', and 'ATM Shaping' tabs. The 'General' tab is active, showing fields for 'Endpoint A' (Vpi: 0, Vci: 50) and 'Endpoint B' (Vpi: 112, Vci: 300). There are also checkboxes for 'Special Study Endpoint A' (Disable), 'Endpoint B' (Disable), 'VC Application' (PVC), 'Connection Type' (Point to Point - asymmetrical), 'Service Category' (UBR), 'Alarm Surveillance' (Disable), 'Must Use VPC Link' (No), and 'May Use PSNL' (No). At the bottom, there are fields for 'Minimum Info Rate (MIR) (kb/s): 256' and 'Peak Info Rate (PIR) (kb/s): 512'. A sidebar on the right contains buttons for 'Save', 'Cancel', 'New Path', 'Delete', 'Connect', 'Disconnect', 'Optimize', 'Upload', 'Download', 'Connect Schedule', 'Recovery Schedule', 'List Path-points', 'Add Connections', and 'Apply Defaults'.

Fonte: Autoria Própria

Na figura 178 terá as informações da aba “*ATM traffic*” existem várias configurações repetidas aos da aba “*ATM*”, o que difere é a configuração do CDVT (*Cell Delay Variation Tolerance*) que define a tolerância no atraso do envio de células. O campo “*Traffic Descriptor*” só tem a opção “*PIR_0+1/MIR_0+1*” e o campo “*traffic policing*” pode ser selecionado “*Disabled*” ou “*Discard*” sendo a última usada para descartar as células em caso de congestionamento. Por fim, os campos “*Use Default CDVT*” e “*Frame Discard*” ficam em *default* (padrão) no exemplo, no primeiro caso ocorre devido estar explícito o valor do CDVT e o segundo define se haverá caso de descarte de quadros caso haja congestionamento. Realizadas tais configurações as demais abas ficam com seus valores padrões.

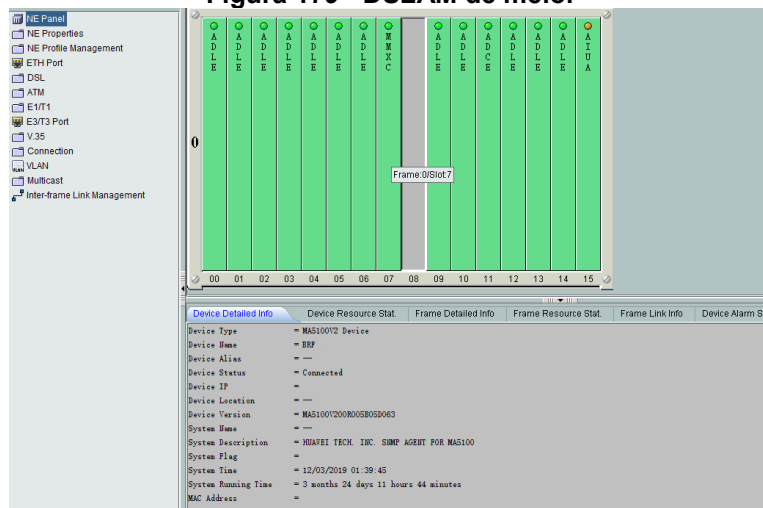
Figura 178 - Configurando tráfego no circuito ATM.



Fonte: Autoria Própria

Ao entrar no DSLAM, conforme figura 179, existirá a placa 07 e 15 que serão de tecnologia ATM, as demais placas serão ADSL.

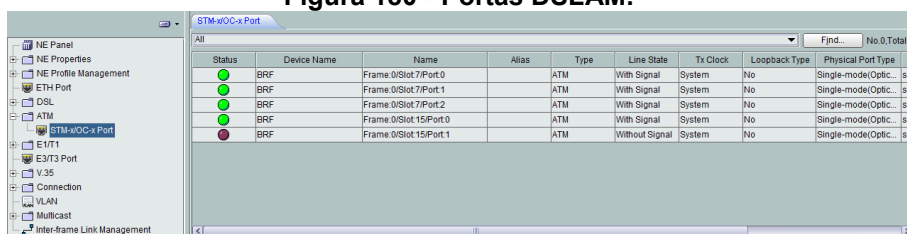
Figura 179 - DSLAM de meio.



Fonte: Autoria Própria

Pode-se filtrar usando o menu à esquerda as portas com tecnologia ATM, tendo uma que irá para a rede *Newbridge* e as demais para DSLAM's de cascata.

Figura 180 - Portas DSLAM.

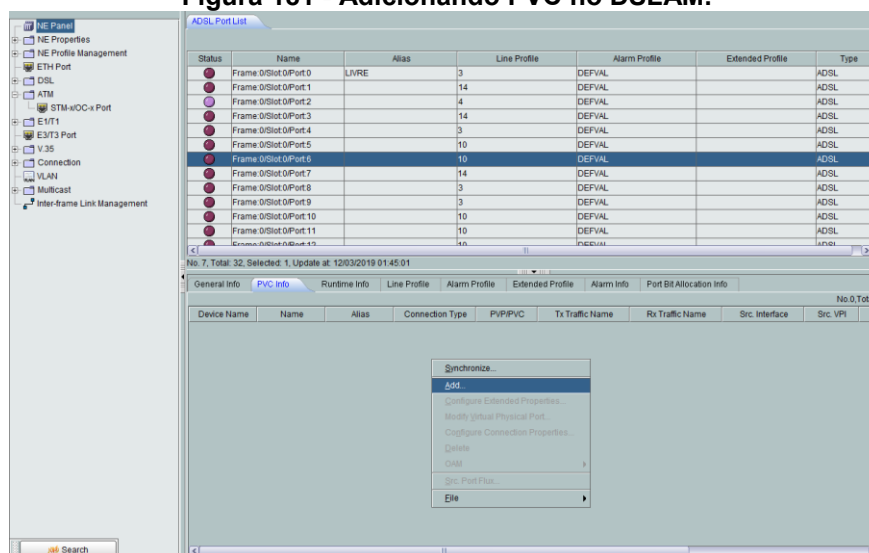


Status	Device Name	Name	Alias	Type	Line State	Tx Clock	Loopback Type	Physical Port Type
●	BRF	Frame 0/Slot 7/Port 0		ATM	With Signal	System	No	Single-mode/Optic...
●	BRF	Frame 0/Slot 7/Port 1		ATM	With Signal	System	No	Single-mode/Optic...
●	BRF	Frame 0/Slot 7/Port 2		ATM	With Signal	System	No	Single-mode/Optic...
●	BRF	Frame 0/Slot 7/Port 0		ATM	With Signal	System	No	Single-mode/Optic...
●	BRF	Frame 0/Slot 15/Port 1		ATM	Without Signal	System	No	Single-mode/Optic...

Fonte: Autoria Própria

Conforme figura 181, foi acessada pelo painel (NE *panel*) a placa 0 que é uma placa com portas DSL, nesse caso será simulado uma conexão *Newbridge* com a porta DSL, para isso foi necessário acessar a aba *PVC Info*, clicar com o botão direito do mouse e selecionar “*Add...*”.

Figura 181 - Adicionando PVC no DSLAM.



Status	Name	Alias	Line Profile	Alarm Profile	Extended Profile	Type
●	Frame 0/Slot 0/Port 0	LIVRE	3	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 1		14	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 2		14	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 3		14	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 4		3	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 5		10	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 6		10	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 7		14	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 8		3	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 9		3	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 10		10	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 11		10	DEFVAL		ADSL
●	Frame 0/Slot 0/Port 13		10	DEFVAL		ADSL

Device Name	Name	Alias	Connection Type	PvPPVC	Tx Traffic Name	Rx Traffic Name	Src. interface	Src. VPI	Sr
Synchronize... Add... Configure Extended Properties... Modify Virtual Physical Port... Configure Connection Properties... Delete... GDM... Src. Port Flap... File...									

Fonte: Autoria Própria

A figura 182 mostra a tela onde se configura a conexão entre a porta que faz a conexão da porta DSL com a rede *Newbridge*. O quadro “*Src. Interface*” demonstra a interface de origem da conexão. Nesse caso o “*frame*” será 0 pois só existe um DSLAM na prateleira, se tivesse mais deveria ser selecionado o DSLAM desejado, a placa será 0 e a porta será 6. No quadro “*Dest. Interface*” será configurada a facilidade da *Newbridge* que no exemplo estudado estará na prateleira 0, slot 7 e porta 0, lembrando que a opção “*Connection Type*” tem que estar “*ADSL-ATM*” para que essa configuração ocorra corretamente.

No quadro “*Src. Parameters*” foi colocado um VPI e VCI que se comunicará com o roteador do cliente, no caso 0 e 33 consecutivamente e o campo *UPC (Usage*

Parameter Control) que seleciona o que vai passar, ser sinalizado, ser descartado ou vai ser feito localmente um modelamento de tráfego. Essa opção no exemplo ficará sempre desligado (*off*), no quadro “*Dest. Parameters*” ficará a VPI 112 e VCI 300 que foi recebido da rede *newbridge* no exemplo, isso significa que os valores que vem da *Newbridge* tem que ser iguais na *cross* conexão para que haja a conexão.

Figura 182 - Tela de configuração de PVC.

The screenshot shows the 'Add P2P PVP/PVC' configuration window. It is divided into several sections:

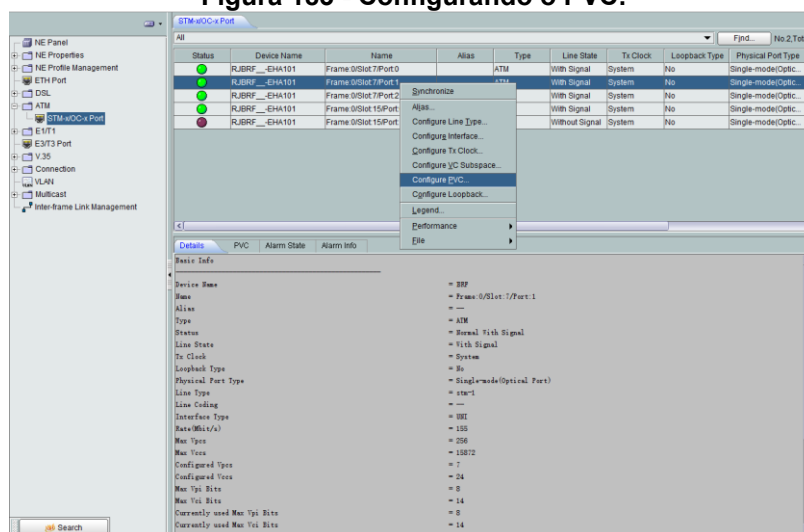
- Location:** Name: ADSL-ATM/0_0_6/0/33, Alias: (empty)
- Attributes:** PVP/PVC: PVC, Connection Type: ADSL-A...
- Traffic Consistency:** Set Rx and Tx traffic to be consistent. Tx Traffic Name: ubrPcr_512K, Rx Traffic Name: ubrPcr_512K.
- Src. Interface:** Frame: 0, Slot: 0, Port: 6-Frame:0/Slot...
- Dest. Interface:** Frame: 0, Slot: 7, Port: 0-Frame:0/Slot...
- Src. Parameters:** VPI (0-255): 0, VCI (32-255): 33, UPC: OFF.
- Dest. Parameters:** VPI (0-4095): 112, VCI (32-65535): 300, UPC: OFF.

Buttons: OK, Cancel, Apply.

Fonte: Autoria Própria

Se houver uma cascata de DSLAM's na topologia, basta voltar no menu esquerdo nas portas STM's, conforme figura 183, clicar com o botão direito do mouse na porta e escolher a opção configure PVC.

Figura 183 - Configurando o PVC.



Fonte: Autoria Própria

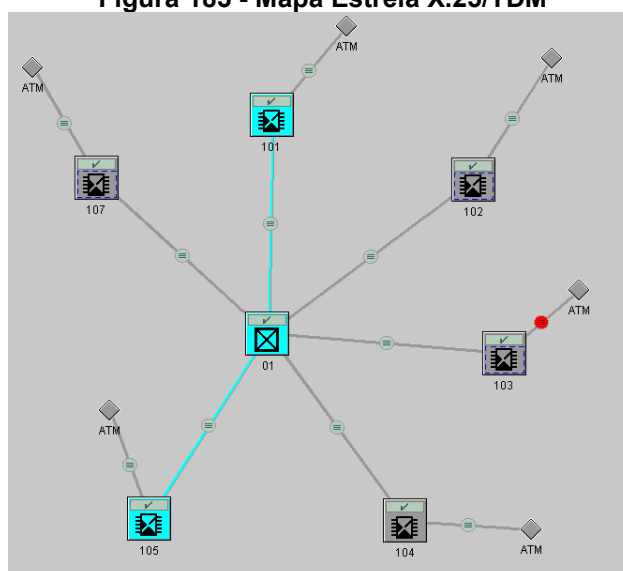
A figura 184 demonstra uma “*Connection Type*” com o parâmetro “ATM-ATM” necessário para fazer os saltos entre DSLAM’s. O quadro “*Src. Interface*” terá como parâmetros a prateleira 0, placa 7 e porta 0 que se comunica com a *Newbridge* e no quadro “*Dest. Interface*” tem a prateleira 0, placa 7 porta 1 que faz a comunicação a DSLAM de cascata. No quadro “*Src. Parameters*” foi deixado o VPI e VCI igual ao da *Newbridge* com UPC desativado (*off*). No quadro “*Dest. Parameters*” foi colocado no exemplo o mesmo da *Newbridge* para facilitar a configuração, mas pode ter VPI e VCI distintos, caso isso ocorra o próximo multiplexador receberá esse VPI e VCI. Esse passo se repete em todos os multiplexadores da cascata exceto no último que ficará igual ao da figura 170, lembrando que se no meio for alterado o VPI e o VCI deve casar as configurações no salto.

Figura 184 - Configurando PVC.

Fonte: Autoria Própria

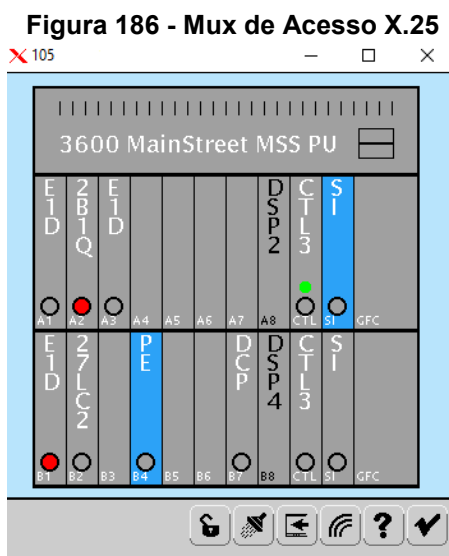
3.3.5 Cross conexão X.25 e outra gerência.

Na figura 185 mostra um mapa de uma topologia estrela na Newbridge, essa topologia é usada para X.25 devido o multiplexador 01 ser um equipamento que suporta a tecnologia X.25 e não ser PDH.

Figura 185 - Mapa Estrela X.25/TDM

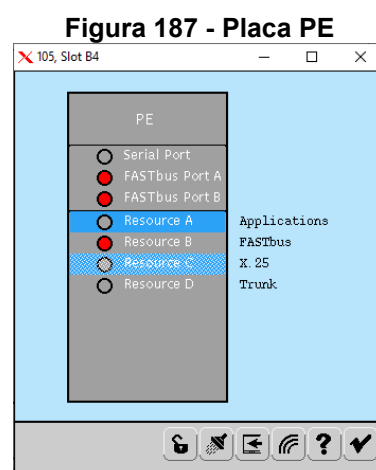
Fonte: Autoria Própria

A figura 186 demonstra o mux de acesso, a placa SI leva ao multiplexador 01 e a placa PE é a placa que suporta a tecnologia X.25.



Fonte: Autoria Própria

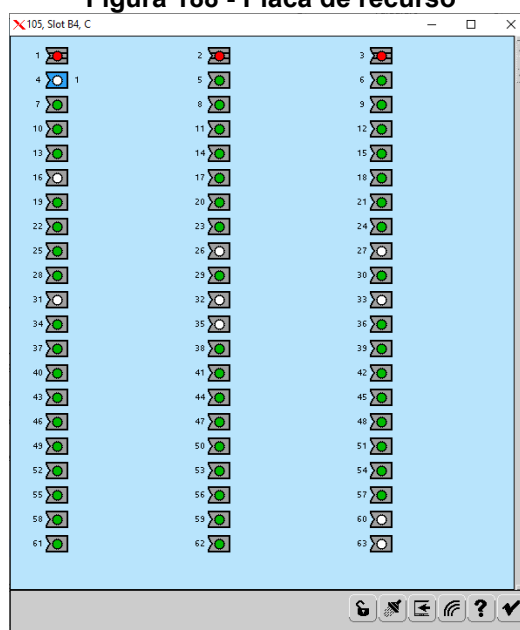
A figura 187 demonstra como é a placa PE, as placas *resource* serão chamadas como placas de recurso onde a qual nos importa é a placa de recurso C, onde terá a conexão X.25 propriamente dita, a placa de recurso A é usado para testes de loop e como a meta desse documento não é explicar a parte de testes de funcionamento e intermitência não será dado maiores detalhes sobre ela. As demais placas de recurso e portas seriais são usadas configurações de equipamento que já deve estar devidamente configurado pela operadora.



Fonte: Autoria Propria

A figura 188 ilustra a placa de recurso C, o circuito X.25 foi alocado na porta 4 com a descrição 1. Para acessar as configurações X.25 deve-se clicar duas vezes nela, caso necessite aprovisionar um circuito do zero deve-se escolher uma das portas que estão em verde usando como ponta A ou ponta B conforme tópico 3.2.4.

Figura 188 - Placa de recurso



Fonte: Autoria Própria.

A figura 189 demonstra a configuração da porta dentro da placa de recurso na aba *Link Layer* sendo os parâmetros:

- *Interface Type*: Escolhe se a interface irá ser DTE ou DCE, como normalmente a operadora vai trabalhar com DCE então aqui será ilustrado o modo de configuração DCE.
- *Frame Sequence Numbering*: Pode trabalhar com módulo 8 (básico) ou 128 (estendido), o módulo 128 deixa o quadro maior e acaba alterando a estrutura do quadro explicada no tópico 2.7, não é comum o uso de quadros grandes por isso só foi explicado o quadro de módulo 8. Existe o quadro de módulo 32768 (super), mas a rede *Newbridge* não suporta.
- *Retransmission Count (N2)*: tempo para retransmitir o pacote caso o mesmo não seja entregue.
- *Inactivity Timer (T3)*: Tempo em milissegundos para determinar inatividade.
- *Response Delay Time (T2)*: Temporizador de atraso na resposta permitido em milissegundos.
- *Frame Response Timer (T1)*: Temporizador de resposta do frame em milissegundos.
- *Congestion Timer*: Temporizador de congestionamento em milissegundos.

Figura 189 - Configuração camada de dados X25.

The screenshot shows a configuration window titled 'Config PE XAC - 105-B4-C-X4'. The 'Link Layer' tab is selected. The configuration details are as follows:

- Name: 1
- Service Type: X.25
- Profile: [dropdown]
- Interface Type: DCE
- Frame Sequence Numbering: Modulo 8
- Maximum Frame Window Size (K): 7
- Retransmission Count (N2): 10
- Data Link Timers:
 - Inactivity Timer (T3) (ms): 60000
 - Response Delay Timer (T2) (ms): 200
 - Frame Response Timer (T1) (ms): 3000
 - Congestion Timer (ms): 3000

On the right side, there are buttons for 'Save', 'Cancel', 'Delete', 'List NUAs', 'New NUA', 'List Profiles', and 'Save As Profile'.

Fonte: Autoria Própria

A figura 190 demonstra a configuração da camada de rede na aba *Network Layer*, nela consta as seguintes configurações:

- *Packet Layer Interface Type*: Pode ser DCE ou DTE, podendo ser diferente da camada de dados. Na operadora sempre será usado o DCE e no cliente estará o DTE.
- *Version*: Pode ser a versão 1984-1988 ou a versão 1992-1996, nesse caso depende do contrato com o cliente. No exemplo foi escolhido a versão mais antiga.
- *Default NPI*: Tem as opções X.121, E.164 Digital e E.164 Analógico. NPI (Numbering Plain Identification) determina o formato do bloco do endereço, sendo X.121 descrito em sua própria recomendação tendo tamanho maior de 15 dígitos e pode carregar os campos endereço alternativo de DTE, *call request* e *clear request* (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p. 60). A recomendação E.164 é endereçado com um máximo de 12 dígitos no plano de numeração antes de 1997 (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p.60).
- *Generate Alarms*: Marcando essa opção a porta poderá gerar alarmes ao DTE.
- *X.75 Calls Allowed*: Permite chamadas de recomendação X.75. Essa opção deve ser marcada conforme contrato do cliente.

- *Packet Sequence Numbering*: Determina se na camada de rede será modulo 8 ou módulo 128 a comunicação, conforme já explicado anteriormente nesse mesmo tópico na camada de dados.
- *Base LCN*: determina qual é a quantidade base de LCN (Logical Channel Number).
- *Number of LCNs*: determina o número de LCN que terá o circuito.
- *Number of PVCs*: determina o número de PVC que já foi explicado nos tópicos 2.3 e 2.8.
- *Number of incoming SVCs*: determina a quantidade SVC recebida no circuito que já foi explicado no tópico 2.3 e 2.8.
- *Number of outgoing SVCs*: determina a quantidade de SVC enviado do circuito.
- *Packet Layer Restart Timer (T10/T20)*: Temporizador de reinicialização na camada de pacote em segundos. T10 é quando o DCE expede uma indicação de reinicialização e T20 é quando o DTE expede uma requisição de reinicialização (INTERNATIONAL TELECOMUNICATION UNION, 1996, p.135/136).
- *Packet Layer Call Timer (T11/T21)*: Temporizador de chamada na camada de pacotes em segundos. T11 é quando o DCE expede uma chamada recebida e T21 é quando o DTE expede uma requisição de chamada (INTERNATIONAL TELECOMUNICATION UNION, 1996, p.135/136).
- *Reset Timer (T12/T22)*: Temporizador do restabelecimento da conexão em segundos. T12 é quando o DCE expede um indicador de restabelecimento e o T22 é quando o DTE expede uma requisição de restabelecimento (INTERNATIONAL TELECOMUNICATION UNION, 1996, p.135/136).
- *Clear Timer (T13/T23)*: Temporizador de limpeza em segundos. T13 é quando o DCE expede um indicador de limpeza e o T23 é quando DTE expede uma requisição de limpeza (INTERNATIONAL TELECOMUNICATION UNION, 1996, p.135/136).
- *Window Timer (T24)*: É o temporizador de registro do DTE. Não é mencionado no padrão mais novo da ITU-T para o X.25, porém segundo o padrão da CCITT (1988, p. 135) os temporizadores T24 ao T27 foram designados pela ISO na especificação da camada de pacotes para os DTEs X25. Para evitar ambiguidade e confusão, os números de tempo esgotado

foram designados ao T28.

- *Inactivity Timer*: Temporizador que determina a inatividade do circuito em milissegundos.
- *Flow Control Timer*: Temporizador de fluxo de controle de tráfego em segundos.
- *Incoming Maximum Address Length Allowed*: O maior tamanho permitido no campo endereço do pacote.
- *Suppress called address*: O endereço chamado será removido do quadro.
- *Suppress calling address*: O endereço que está sendo chamado será removido do quadro.
- *Local Address Validation*: Habilita a validação de endereço local na porta.
- *Flow Control Negotiation*: Habilita a negociação no controle de fluxo.
- *Throughput Class Negotiation*: Habilita a negociação de classe na taxa de transferência.
- *Extended Throughput Class Negotiation Format*: Habilita o formato de negociação estendida de classe na taxa de transferência.
- *Generate Cause Codes in DTE Format*: Gera um formato de erro para diagnóstico no modelo DTE.
- *Enhanced Diagnostic Codes*: Gera códigos de diagnóstico melhorado. Esse assunto não será abordado aqui, mas os diagnósticos ficam na placa de recurso A.
- *Hunt Group Member Address Substitution*: Habilita o modo *Hunt Group*. O modo *Hunt Group* distribui chamadas recebidas tendo um endereço associado com o *Hunt Group* cruzando um designado grupo de interfaces DTE e DCE (INTERNATIONAL TELECOMMUNICATION UNION, 1996, p. 100).
- *Allowable Packet Sizes*: Permite que pacotes de determinado tamanho possam passar pela porta.

Figura 190 - Configuração camada de rede X.25

The screenshot shows the 'Network Layer Parameters' configuration window. It is divided into several sections:

- Network General:** Packet Layer Interface Type (DCE), Version (1984-1988), Default NPI (X.121), Generate Alarms (unchecked), X.75 Calls Allowed (checked), Packet Sequence Numbering (Modulo 8).
- Logical Channel Number:** Base LCN (1), Number of LCNs (20), Number of PVCs (0), Number of Incoming SVCs (0), Number of Outgoing SVCs (0), Number of Two-Way SVCs (20).
- Network Timers:** Packet Layer Restart Timer (180s), Packet Layer Call Timer (200s), Reset Timer (180s), Clear Timer (180s), Window Timer (60s), Inactivity Timer (0ms), Flow Control Timer (1s).
- Network Call Processing:** Incoming Maximum Address Length Allowed (19), Suppress called address (unchecked), Suppress calling address (unchecked), Local Address Validation (checked), Flow Control Negotiation (unchecked), Throughput Class Negotiation (unchecked), Extended Throughput Class Negotiation Format (unchecked), Generate Cause Codes in DTE Format (unchecked), Enhanced Diagnostic Codes (checked), Hunt Group Member Address Substitution (unchecked).
- Allowable Packet Sizes:** 16 bytes (unchecked), 128 bytes (checked), 1024 bytes (unchecked), 32 bytes (unchecked), 256 bytes (checked), 2048 bytes (unchecked), 64 bytes (unchecked), 512 bytes (checked), 4096 bytes (unchecked).

Buttons on the right include Save, Cancel, Delete, List NUAs, New NUA, List Profiles, and Save As Profile.

Fonte: Autoria Própria

Na figura 191 tem-se a aba referente a tradução de endereço, nela temos as opções:

- *Translation Table*: é a tabela de tradução de um prefixo externo em um prefixo interno podendo ser unidirecional, bidirecional, ida ou volta. Os botões *add*, *update* e *remove* tem como objetivo adicionar, atualizar e remover consecutivamente, mas isto depende do NUA (Network User Address) que será explicado mais adiante nesse mesmo tópico.
- *Translation Table Index*: Determina o índice que será mudado, a quantidade caracteres no início do endereço.
- *External Prefix*: Prefixo padrão externo no início do endereço usado para todas as regras de tradução.
- *Internal Prefix*: Prefixo padrão interno no início do endereço para todas as regras de tradução.
- *Translate Address*: Pode ser definido como *Calling*, *Called* ou *Both*. Se for para o DCE fazer a tradução para o DTE será usado *Calling*, o inverso será usado *Called* e ambos será usado *Both*.
- *Direction*: Determina a direção que a regra é aplicada. Com os mesmos parâmetros do campo *Translate Address*, porém determina a direção do envio de pacotes.
- *Trap Incoming Calling*: Este parâmetro especifica se deve fazer a triagem

quando endereço que está sendo chamado é recebido ou enviado para uma linha de acesso originada bate com a cadeia de caracteres do prefixo de tradução externo (Newbridge Networks Corporation, 1997, p. 27.14-40).

- *Trap Incoming Called*: Este parâmetro especifica se deve fazer a triagem quando endereço que foi chamado é recebido ou enviado para uma linha de acesso originada bate com a cadeia de caracteres do prefixo de tradução externo (Newbridge Networks Corporation, 1997, p. 27.14-40).
- *Trap Outgoing Calling*: Este parâmetro especifica se deve fazer a triagem quando o endereço que está sendo chamado é enviado para certo destino que corresponde com a cadeia de caracteres do prefixo de tradução interno (Newbridge Networks Corporation, 1997, p. 27.14-40).
- *Trap Outgoing Called*: Este parâmetro especifica se deve fazer a triagem quando o endereço que foi chamado é enviado ou recebido para certo destino que corresponde com a cadeia de caracteres do prefixo de tradução interno (Newbridge Networks Corporation, 1997, p. 27.14-41).
- *Clear Call After Trap*: Este parâmetro decide se interromperá a chamada caso esbarre em uma das regras dos 4 tópicos acima.
- *Generate Alarm After Trap*: Gera um alarme na porta logo após esbarrar nas regras do *Trap Incoming Calling*, *Trap Incoming Called*, *Trap Outgoing Calling* e *Trap Outgoing Called*. A versão 1.2 do equipamento 36120 MainStreet X.25 não suporta mais esse tipo de recurso (Newbridge Networks Corporation, 1997, p. 27.14-41), mas as versões mais antigas como a que está sendo usada no exemplo ainda suportam.

A *translation table* tem algumas regras conforme quadro 16 e essas regras modificam conforme a se é usado X.121 ou E.164.

Quadro 16 - Sinalização Rede NWB X.25

Formato de endereço externo (Sinalizado no Link)	Formato de endereço interno (NPI, Endereço)
SS	x, DNIC + NTN + SS
NTN	x, DNIC + NTN
NTN + SS	x, DNIC + NTN + SS
DNIC + NTN	x, DNIC + NTN
DNIC + NTN + SS	x, DNIC + NTN + SS
P + DNIC + NTN	x, DNIC + NTN
P + DNIC + NTN + SS	x, DNIC + NTN + SS
SN	e ou m, CC + NSN
1 + NSN	e ou m, CC + NSN
011 + CC + NSN	e ou m, CC + NSN

Fonte: Newbridge Networks Corporation, 1997, p. 27.14-30

A sigla SS é conhecida como dígitos de sub endereço e quando recebido será transformado em x, DNIC que é o código de interface de dados de rede, NTN que é o número nacional do terminal e o sub endereço (SS). Quando o multiplexador recebe um NTN ele irá transformar na letra x junto com DNIC mais o NTN. Agora se vier NTN mais o SS ele irá tratar igual estivesse recebendo o SS e assim seguindo a tabela... O SN é chamado de número inscrito, CC é o código E.164 do país, o NSN é o número significativo nacional, o P é o dígito de prefixo internacional e as letras e, m e x tem como indicativo consecutivo endereço digital E.164, endereço analógico E.164 e o x é o X.121. Essa explicação determina o NUA.

Figura 191 - Tradução de endereços

Config PE XAC - 105-B4-C-X4

Name: 1

Service Type: X.25

Profile: [v]

Link Layer | Network Layer | Address Translation

Address Translation:

Translation Table:

Index	External Prefix	Internal Prefix	Address	Direction
1	1x0	1x	Both	Both
2	1x	1x7243	Both	Both

Add
Update
Remove

Save
Cancel
Delete

List NUAs
New NUA

List Profiles
Save As Profile

Translation Item:

Translation Table Index: 3 [v]

External Prefix: 1

Internal Prefix: 1

Translate Address: Both

Direction: Both

Trap Incoming Calling:

Trap Outgoing Calling:

Clear Call After Trap:

Generate Alarm After Trap:

Trap Incoming Called:

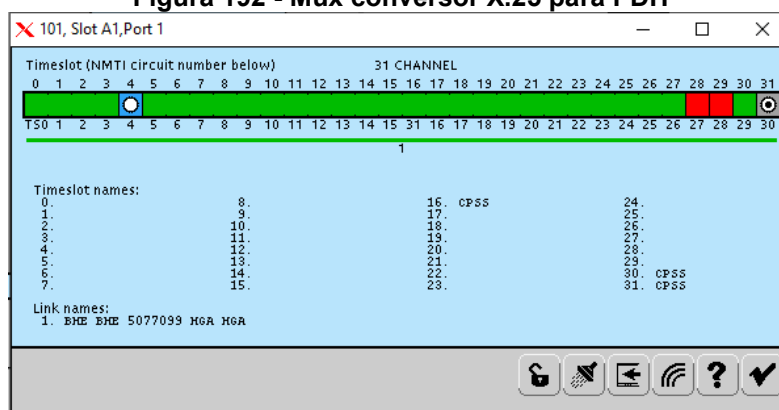
Trap Outgoing Called:

Fonte: Autoria Própria

O multiplexador 101 será responsável por receber o circuito X.25, lembrando que mesmo a gerência NWB trabalhe com as tecnologias X.25 e PDH ela não converte automaticamente uma tecnologia para outra, sendo necessário criar uma rota PDH/SDH e outra X.25.

Não é necessário que esse E1 vá para a rede NWB em uma segunda rota, pode ir para uma rede DTC usando a mesma lógica do tópico 3.3.1. A figura 192 demonstra o ponto B que será configurado a rota, nesse caso irá sair para o *timeslot* 4.

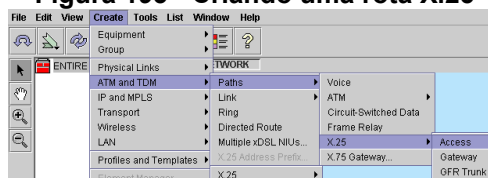
Figura 192 - Mux conversor X.25 para PDH



Fonte: Autoria Própria

A figura 193 demonstra a criação da rota, as opções que devem ser acessadas é “ATM and TDM”, “Paths”, “X.25” e “Access”.

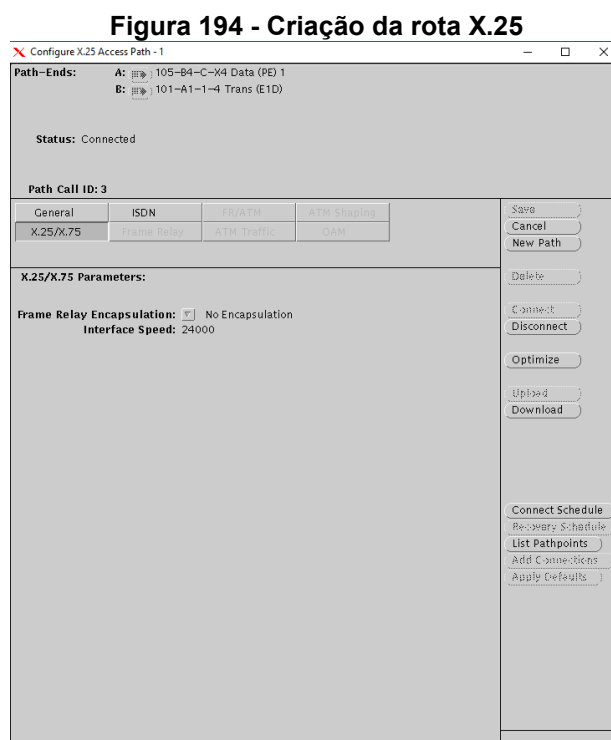
Figura 193 - Criando uma rota X.25



Fonte: Autoria Própria.

A criação da rota é igual o explicado no tópico 3.2.4, é escolhido a ponta A e a ponta B, sendo um o *timeslot* PDH e outro a placa de recurso C independente da ordem. As únicas abas habilitadas serão as “General”, “ISDN” e “X.25/X.75” conforme ilustrado na figura 194, as abas “General” e “ISDN” foram explicadas no tópico 3.2.4.

A aba “X.25/X.75” terá a opção de encapsulamento Frame Relay (“Frame Relay Encapsulation”), normalmente não será usado, mas pode haver necessidade de configurar. A opção “Interface Speed” determina em bits a velocidade do circuito.



Fonte: Autoria Própria

3.4 SERVIÇOS

3.4.1 Configurando a velocidade no roteador

Alguns serviços poderão rodar por fibra passiva, por redes EPON ou GPON. Como é passiva normalmente não há gerência no meio do caminho e é uma tendência que tudo passe por essa tecnologia futuramente, então há a necessidade de configurar a velocidade no roteador. Na rede *metroethernet* e satélite também é usada essa metodologia para configurar a velocidade.

A figura 195 ilustrará a configuração de velocidade no roteador Cisco. No mesmo deve-se criar uma *access-list*, isso não interfere na velocidade, mas é necessário para a inserção da linha que controla a velocidade no roteador, a linha “*ip access-list extended aciPermit*” cria a *access-list* chamada de “*aciPermit*” e a linha “*permite ip any any*” está configurado junto da linha anterior e isso é verificado pelo o espaço que tem antes da linha, e essa linha afirma que todo o IP está permitido para

se comunicar com essa porta. Caso seja necessário bloquear um IP isso deve ser feito no roteador entregue ao cliente.

Nas duas próximas linhas é criado um mapeamento de classe (*class-map*) onde existe a necessidade de criar uma classe, isso é feito apenas no roteador do cliente, raramente a operadora vai fazer algum tipo de configuração desse tipo, porém essas linhas são necessárias para configuração da velocidade. A linha "*class-map match-all Trafego*" cria a classe nomeada "Trafego", na segunda linha "*match access-group name aclPermite*" e insere nessa classe a *access-list* criada nas duas primeiras linhas.

Nas próximas três linhas é criada uma política (*policy*), na linha "*policy-map 45Kbps*" é criada a política nomeada de "45Kbps", na linha "*class Trafego*" é inserida a classe "Trafego" criada nas linhas anteriores e é obrigatória para a inserção da próxima linha, e na linha "*police cir 45000 bc 5625 be 5625 conform-action transmit exceed-action drop violate-action drop*". Essa linha define CIR, bc e be que segundo Kocharians e Vinson (2014, p. 212) é o "*Comitted Information Rate*", medido em bits por segundo, que define a taxa de um VC (*virtual circuit*) de acordo com o contrato do negócio, bc é o "*Comitted Burst Size*" medido em bits. Esta quantidade de trafego, que pode ser enviado durante o intervalo "tc" e o be que é o "*Excess Burst Size*", medido em bits, é o número de bits, além do BC que podem ser enviados após um período de inatividade. O intervalo "tc" também é definido por Kocharians e Vinson (2014, p. 212) como o intervalo de tempo, medido em milissegundos, sobre o que o "bc" pode ser enviado. A fórmula que calcula o "tc":

$$tc = \frac{bc}{CIR}$$

Seguindo a teoria, existirá uma velocidade 45 Kbps e terá nesse comando o trecho "*conform action transmit*" que afirma que será transmitido se o circuito estiver nessa velocidade, o trecho "*exceed-action drop*" que faz a porta recusar mais pacotes caso exceda os 45 Kbps e o trecho "*violate-action drop*" que afirma que caso exista alguma violação nessa regra ele recusa o pacote.

As cinco últimas linhas têm a configuração da porta, na linha "*interface FastEthernet 0/0*" informa que foi selecionada a interface *FastEthernet 0/0*, na linha "*ip address 192.168.10.1 255.255.255.252*" tem o endereço IP que será tratado no

tópico 3.4.3, na linha “*duplex full*” é explicado como ocorre a negociação, na linha “*service-policy input 45Kbps*” insere na entrada da porta a política de 45Kbps e a linha “*service-policy output 45Kbps*” insere na saída da porta a política de 45Kbps.

Figura 195 – Comandos para configurar velocidade Cisco.

```
ip access-list extended aclPermite
 permit ip any any
class-map match-all Trafego
 match access-group name aclPermite
policy-map 45Kbps
 class Trafego
  police cir 45000 bc 5625 be 5625 conform-action transmit exceed-action drop violate-action drop
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.252
 duplex full
 service-policy input 45Kbps
 service-policy output 45Kbps
```

Fonte: Autoria Própria

A figura 196 demonstra a configuração de velocidade conforme No roteador Nokia-Alcatel foi criado um serviço “*ies*” (comando “*configure service ies 1 customer 1 create*”, sendo “*create*” indicado para a criação do serviço, sem o *create* é acessado a caixa de configuração) nomeado como 1 na primeira linha, na segunda linha é criado uma interface lógica nomeado como “operadora” dentro da caixa de serviço, na terceira linha é configurado o IP que será tratado mais à frente, nas próximas 4 linhas tem a configuração de ICMP que segundo Mason e Newcomb (2001 ,p. 23) são mensagens encapsulados dentro do pacote IP que usando sem conectividade, um mecanismo de transferência inacessível, é usado para reportar erros dentro de uma rede, nesse documento não será debatido essas configurações.

Na linha “*sap 1/1/2:500 create*” é gerada uma nova caixa de configuração dentro da caixa de configuração da interface lógica, sendo essa caixa da porta física, dentro dessa caixa existe a linha “*ingress*” e “*egress*” que são responsáveis cada uma por uma caixa, sendo a de “*ingress*” a que controla o que entra na porta e a de “*egress*” o que sai da porta, as linhas “*queue-override*” reescreverá as regras de QOS caso exista alguma já pré-definida para entrada e saída, a linha “*queue*” define uma fila nesse caso nomeada como 1 e o comando “*rate 1000 cir 1000*” define o PIR e o CIR em Kbps.

Figura 196 - Configurando velocidade no Alcatel.

```

ies 1 customer 1 create
interface "operadora" create
address 192.168.1.1/30
icmp
no mask-reply
no redirects
no unreachable
exit
sap 1/1/2:500 create
ingress
queue-override
queue 1 create
rate 1000 cir 1000
exit
exit
exit
egress
queue-override
queue 1 create
rate 1000 cir 1000
exit
exit
exit

```

Fonte: Autoria Própria

3.4.2 Rotas

Existem duas formas para configurar uma rota para acesso, podendo ser estática ou BGP (*Border Gateway Protocol*).

A figura 197 demonstra a configuração de uma rota estática no equipamento Cisco. Usa-se “*configure terminal*” para entrar na configuração do roteador, o comando “*ip route 10.10.10.0 255.255.255.0 192.168.10.2*” sendo o IP 10.10.10.0 e a máscara de rede 255.255.255.0 e esse conjunto representa a rede destino e o IP 192.168.10.2 o endereço da porta no roteador que irá receber os pacotes referentes a essa rede, pode-se colocar a porta no lugar do IP nesse comando.

Figura 197 - Configurando rota estática Cisco.

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.10.10.0 255.255.255.0 192.168.10.2
Router(config)#

```

Fonte: Autoria Própria

A figura 198 demonstra a configuração de uma rota estática no equipamento Alcatel. Para configurar não há necessidade de entrar em nenhuma caixa de configuração, usa-se o comando “*configure router static-router 10.1.2.0/30 next-hop 192.168.1.2*” sendo 10.1.2.0/30 o endereço de rede destino com sua máscara de rede e 192.168.1.2 o endereço da porta que irá receber os pacotes que irão para tal destino.

Figura 198 - Configurando rota estática Alcatel.

```
*A:R1# configure router static-route 10.1.2.0/30 next-hop 192.168.1.2
```

Fonte: Autoria Própria

A configuração do BGP aqui no Alcatel, demonstrada na figura 199, tem um nível de complexidade maior que a rota estática. O primeiro comando deve ser o “*configure service vprn 1*” caso já exista o serviço vprn 1, caso não exista, o comando correto a ser aplicado é o “*configure service service vprn 1 customer 1 create*” sendo “*customer 1*” criado um valor criado anteriormente. Após isso entrará dentro da caixa da “*vprn*”. Um ponto importante é que o serviço que deve ser criado nesse ponto é o VPRN, o IES é apenas para circuitos de IP fixo e dedicado.

Na caixa da “*vprn*” se define o “*autonomous-system*” ou AS, que é definido como um grupo de rotas que está abaixo de uma única autoridade administrativa (Pyles; Carrel; Tidel, pag 696), por essa definição deve-se definir o AS vindo da operadora para que possa se comunicar com o AS do cliente, tudo isso é referente a linha “*autonomous-system 3*”.

O *router distinguisher* é apenas um separador de rotas que a operadora irá decidir sua numeração. A próxima linha gera uma interface lógica nomeada aqui como cliente, se já existir não precisa do “*create*” no comando, a partir daqui será acessada a caixa da interface.

Na caixa interface é inserido o comando “*address 192.168.5.1/30*” que determina o endereço IP que será explicado no próximo tópico. Na próxima linha é definido o MTU que é o tamanho do pacote que será usado, normalmente o valor é 1500 mas pode haver alterações dependendo do contrato com o cliente. Na linha “*sap 1/1/1 create*” é vinculada a porta física ou DOT1Q ou QINQ ao ip e serviços referentes a porta lógica. Dentro da porta física pode-se inserir QOS e mais alguns serviços interessantes, que já foi visto no tópico anterior, então o próximo comando será “*exit*” para sair da caixa da porta e mais um “*exit*” para sair da interface lógica e voltar para a caixa da VPRN.

Pode ser que tenha mais uma interface lógica aqui caso esse roteador tenha dois clientes da mesma VPN configurado, caso não tenha pode-se configurar a caixa referente ao protocolo BGP com o comando “*bgp*”. Na linha “*disable-communities extended*” desativa as “*communities*”, *community* provê um mecanismo pelo qual agrupa rotas que políticas de roteamento podem ser aplicadas em todas as rotas de

tal *community* (KOCHARIANS,VINSON, p.119).

Na próxima linha (*group* “cliente”) é criado um grupo nomeado cliente no qual será configurada a rota BGP para a interface criada, caso tenha mais de um cliente no roteador será necessário mais um grupo para cada interface criada. A linha “*neighbor 192.168.5.2*” declara o IP do roteador vizinho, a linha “*prefix-limit 100 log-only threshold 80*” define o limite de prefixos que esse cliente pode passar ao roteador com alerta a partir de 80 por cento do valor, prefixos são a quantidade de redes permitidas.

Logo após existe a linha “*passive* que apenas recebe mensagens de BGP e não envia mensagens ao vizinho (roteador do cliente). A linha “*as-override*” significa que o “AS” (*Autonomous System*) vindo do cliente será sobrescrito e a linha “*peer-as*” é indicado qual é o “AS” do cliente e por fim o comando “*split-horizon*” que é um comando que evita que as rotas entrem em um ciclo sem fim. Os demais comandos são para sair das caixas e ligar os serviços.

Figura 199 - BGP no Alcatel.

```
vprn 1 customer 1 create
  interface "cliente" create
  exit
exit
vprn 1 customer 1 create
  autonomous-system 3
  route-distinguisher 1:32
  interface "cliente" create
    address 192.168.5.1/30
    ip-mtu 1500
    sap 1/1/1 create
  exit
  exit
  bgp
    disable-communities extended
    group "cliente"
      neighbor 192.168.5.2
      prefix-limit 100 log-only threshold 80
      passive
      as-override
      peer-as 2
      split-horizon
    exit
  exit
  no shutdown
exit
no shutdown
exit
```

Fonte: Autoria Própria

Na figura 200 demonstra como no roteador do cliente deve estar configurado. Como no cliente normalmente será usado um roteador Cisco ou de baixo custo, no exemplo foi usado um roteador Cisco. Para configurar tem que inserir o comando “*configure terminal*” e depois o comando “*router bgp 2*” sendo 2 o AS do roteador do cliente.

A configuração “*bgp log-neighbor-changes*” é altamente necessária para poder gerar logs de queda, falha ou desligamento do protocolo BGP, então é

recomendável sua configuração. A linha “*neighbor 192.168.5.1 remote-as 3*” indica o AS e o IP do vizinho para que ocorra a negociação do protocolo BGP.

Figura 200 - BGP no cliente.

```
router bgp 2
  bgp log-neighbor-changes
  neighbor 192.168.5.1 remote-as 3
```

Fonte: Autoria Própria

Para verificar se a configuração foi feita corretamente, no roteador Alcatel deve-se usar o comando “*show router (número da vprn) bgp neighbor (IP do cliente) detail*”, com esse comando os campos “*State*” e “*Fsm Est. Time*” são importantes para verificar se está tendo conectividade.

O campo “*State*” pode ter os seguintes parâmetros:

- *Idle*: O BGP não está aceitando conexões, normalmente ocorre por falhas ou se o vizinho estiver com a bgp desligada;
- *Active*: O BGP está escutando e aceitando a conexão TCP;
- *Connect*: O BGP está tentando estabelecer a conexão TCP;
- *OpenSent*: O BGP enviou uma mensagem “OPEN” para o vizinho e está esperando uma mensagem de “OPEN” para abrir a conexão;
- *OpenConfirm*: O BGP recebeu a mensagem “OPEN” e está esperando uma notificação;
- *Established*: A conexão foi efetuada com sucesso.

O campo “*Fsm Est. Time*” demonstra a quanto tempo ocorreu a última queda.

Outro campo que é importante é o “*Last Error*”, mas esse pode receber várias mensagens de erro que podem ajudar no diagnóstico, porém não será discutido nesse documento. Todos esses parâmetros são demonstrados na figura 201.

Figura 201 - Estado da BGP.

```
A:RBGP# show router 1 bgp neighbor 192.168.5.2 detail
=====
BGP Neighbor
=====
Peer      : 192.168.5.2
Group    : cliente
-----
Peer AS      : 2           Peer Port      : 13260
Peer Address : 192.168.5.2
Local AS     : 3           Local Port     : 179
Local Address : 192.168.5.1
Peer Type    : External
State       : Established   Last State     : Established
Last Event   : rcvKeepAlive
Last Error   : Cease (Connection Collision Resolution)
Local Family : IPv4
Remote Family : IPv4
Connect Retry : 120          Local Pref.    : 100
Min Route Advt. : 30
Multihop     : 0 (Default) AS Override     : Enabled
Damping      : Disabled   Loop Detect     : Ignore
MED Out      : No MED Out Authentication : None
Next Hop Self : Disabled   AggregatorID Zero : Disabled
Remove Private : Disabled   Passive        : Enabled
Peer Identifier : 192.168.5.2   Fsm Est. Trans  : 1
Fsm Est. Time : 00h43m13s InUpd Elap. Time : 00h43m33s
Prefix Limit : 100       Pref Limit Idle Time* : forever
Prefix Log Only : Enabled   Prefix Threshold : 80
Hold Time     : 90       Keep Alive      : 30
Min Hold Time : 0
Active Hold Time : 90   Active Keep Alive : 30
Cluster Id    : None     Client Reflect   : Disabled
Preference    : 170     Num of Update Flaps : 0
Recd. Paths   : 0
```

Fonte: Autoria Própria.

No cliente pode ser visto se a conexão foi realizada com sucesso usando o comando “*show ip bgp neighbors* (ip da operadora)”. A linha “*BGP state = Established, up for 00:01:40*” demonstrada na figura 202 mostra o estado da BGP (com os mesmos parâmetros do roteador Alcatel) e a quantidade de tempo que está alinhado.

Figura 202 – Estado da BGP no cliente.

```
Router#show ip bgp neighbors 192.168.5.1
BGP neighbor is 192.168.5.1, remote AS 3, external link
BGP version 4, remote router ID 192.168.0.20
BGP state = Established, up for 00:01:40
Last read 00:00:23, last write 00:00:22, hold time is 90, keepalive interval is 30 seconds
Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1
Message statistics:
  InQ depth is 0
  OutQ depth is 0
```

Fonte: Autoria Própria.

A figura 203 demonstra a configuração do BGP. No roteador Cisco quando está na operadora tem uma configuração diferente do roteador Alcatel. Para iniciar a configuração deve-se entrar com o comando “*configure terminal*”. Ao entrar na caixa de configuração deve-se entrar na vrf que se quer configurar através do comando “*ip*

vrf (nome da *vrf*)” aqui usado “Cliente”, dentro da caixa *vrf* se configura o “*router distinguisher*” que já foi explicado no Alcatel. Para sair da caixa *vrf* usa-se o comando *exit*.

Ao voltar à caixa de configuração existe a necessidade de configurar o BGP. Para iniciar a configuração deve-se usar o comando “*router bgp* (número da AS desse roteador)” e acessar a caixa BGP, frisando que o AS desse equipamento será esse número. Na caixa BGP existe a obrigatoriedade de criar um ID para o roteador da operadora na rede, esse ID pode ser um IP qualquer, normalmente criado conforme o projeto do cliente. O comando “*bgp log-neighbor-changes*” que foi configurado roteador do cliente anteriormente nesse tópico tem a mesma finalidade.

Sem sair da caixa do BGP é necessário que seja anexado a *vrf* a ela. Para isso o comando “*address-family ipv4 vrf* (nome da *vrf* que já foi criada anteriormente)” será usado abrindo uma nova caixa. Na caixa “*address-family*” existe o comando “*redistribute connected*” afirmando que esse roteador vai distribuir as rotas e o comando “*redistribute static*” que é a forma que ocorrerá a distribuição, tem como ser ospf e demais protocolos, mas isso não será abordado.

O próximo comando usado é o “*neighbor* (IP da porta do cliente) *remote-as* (AS do cliente)” que indicará qual é o AS do cliente, o comando “*neighbor* (IP da porta do cliente) *transport connection-mode passive*” onde o roteador da operadora receberá as mensagens de BGP, *activate*” realiza a ativação do equipamento vizinho. Logo após existe o comando “*neighbor* (IP da porta do cliente) *send-community*” afirmando que quem cuidará das *communities* é o roteador do cliente, o comando “*neighbor* (IP da porta do cliente) *as-override*” é responsável pela troca do AS entre operadora e cliente e por fim o comando “*neighbor* (IP da porta do cliente) *maximum prefix* (valor do máximo de prefixos) (porcentagem de prefixos antes do alerta) *restart* (tempo para resetar a BGP)” que controla o número de redes que o cliente pode usar simultaneamente.

Saindo da caixa “*address-family*” e da caixa BGP e retornando para a caixa de configuração é necessário configurar a interface do cliente. Para isso necessita-se entrar na caixa de interface usando o comando “*interface* (número da interface que se comunica com cliente)”. Ao entrar nessa caixa, no exemplo, foi criada uma descrição para ela usando o comando “*description* (descrição desejada)” que é opcional, mas importante para a operadora para localizar informações pertinentes ao cliente. O comando posterior que é “*ip vrf forwarding* (nome da *vrf*)” é responsável

por vincular a vrf configurada com o cliente, seguindo em frente existe o comando “*ip address* (ip do cliente) (sub máscara de rede)” para endereçar a porta e que será explicado mais adiante e por fim é configurada a negociação da porta que aqui está configurada como “*full duplex*”.

Figura 203 - Configurando a BGP no Cisco da operadora.

```
ip vrf Cliente
rd 1:32
router bgp 3
  bgp router-id 192.168.100.1
  bgp log-neighbor-changes
  !
  address-family ipv4 vrf Cliente
    redistribute connected
    redistribute static
    neighbor 192.168.5.2 remote-as 2
    neighbor 192.168.5.2 transport connection-mode passive
    neighbor 192.168.5.2 activate
    neighbor 192.168.5.2 send-community
    neighbor 192.168.5.2 as-override
    neighbor 192.168.5.2 maximum-prefix 1000 80 restart 10
  exit-address-family
interface Ethernet1/0
  description Cliente
  ip vrf forwarding Cliente
  ip address 192.168.5.1 255.255.255.252
  duplex full
```

Fonte: Autoria Própria.

Na figura 204 está o comando “*show ip bgp vpnv4 vrf* (vrf do cliente) *neighbors* (ip da porta do roteador do cliente)” que mostra um resultado igual mostrado no roteador do cliente nesse capítulo.

Figura 204 - Estado da BGP.

```
Router#sh ip bgp vpnv4 vrf Cliente neighbors 192.168.5.2
BGP neighbor is 192.168.5.2, vrf Cliente, remote AS 2, external link
  BGP version 4, remote router ID 192.168.5.2
  BGP state = Established, up for 00:23:07
  Last read 00:00:11, last write 00:00:20, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multiseession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multiseession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

Fonte: Autoria Própria.

3.4.3 Endereçamento IP

O endereçamento IP é um conjunto de números como já explicado no tópico 2.8. e é usado para identificar um equipamento ou porta parecido como um número de telefone.

Para realizar a configuração de um IP para a operadora na rede de acesso normalmente terá que ser usado um IP com máscara de sub rede 255.255.255.252 ou /30 devido apenas dois IP's serem necessários, sendo um para o equipamento do cliente e outro para o equipamento da operadora. Mais IP's podem ser usados, mas nesse caso pode ter uma conexão satélite no meio, o que não será simulado nesse material.

Para configurar um IP no Cisco deve-se seguir as informações da figura 205, que está dentro da interface física, para isso deve-se usar o comando "*configure terminal*" para entrar na caixa de configuração, depois entrar na caixa da interface física usando o comando "interface (porta)" e por fim escolher o IP e colocar a máscara com o comando "*ip address (ip da porta) 255.255.255.252*".

Figura 205 - Configurando endereçamento IP no Cisco.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int Serial1/0/0.1/3/5/3:0
R1(config)#ip address 191.40.86.45 255.255.255.252
```

Fonte: Autoria Própria.

No Alcatel usa-se os passos da figura 206, onde a configuração ocorre dentro da caixa serviço do cliente usando o comando "*configure service (tipo do serviço) (número do serviço)*", sendo o tipo de serviço IES ou VPRN. Logo após deve-se entrar na interface lógica com o comando "interface (nome da interface do cliente)" e por fim o comando "*address (IP do cliente na notação CIDR)*" onde será configurado o endereçamento do cliente. Existem outras formas de configurar o endereçamento, mas não será abordado nesse documento.

Figura 206 - Configurando endereçamento IP no Alcatel.

```
A:B1# configure service ies 157985
A:B1>config>service>ies# interface "cliente"
A:B1>config>service>ies>if# address 187.6.60.165/30
```

Fonte: Autoria Própria.

3.4.4 Aplicação de QOS

Nesse tópico será tratado a implementação de QOS no roteador, a figura 207 demonstra a base de todo o tópico e para configurar uma QOS deve usar o comando "*configure qos*". Podemos trabalhar com as fileiras do que vai sair pela

porta através do comando “*sap-egress # create*” ou com o que vai ingressar “*sap-ingress # create*” onde “#” é um numeral entre 1 e 65535 ou uma cadeia de caracteres de tamanho máximo 64. Caso exista a necessidade de realizar uma reconfiguração o *create* no comando não deve ser utilizado.

Ao entrar na caixa “*sap-egress*” ou “*sap-ingress*” existe a opção de colocar uma descrição para identificar a quem pertence aquela QOS. O próximo comando “*queue # create*” é referente a criação de fila onde “#” é um numeral de 1 a 8, isto significa que o Alcatel aceita no máximo oito filas de QOS sendo cada uma personalizada conforme necessidade do cliente, o uso de do parâmetro *create* só deve ser usado para a criação e não para alteração da caixa.

Dentro da caixa das filas (*queue*) pode-se definir um pai com um nome de uma “*scheduler*” que seria um escalonador que permite a herança de seus atributos através do comando “*parent (nome do escalonador/scheduler) cir-level #*” no exemplo.

No exemplo da figura 207 não foi citado, porém, a critério de informação existe os parâmetros opcionais “*weight*”, “*level*”, “*cir-weight*” e o citado “*cir-level*” para o comando *parent*, onde *weight* é determinado como o peso dentro do nível “acima do CIR” dada para uma fila criança ou escalonador (ALCATEL-LUCENT, 2011, p.83), *level* define o nível de estrita prioridade para uma fila criança ou um escalonador com respeito para a alocação de banda durante a fase de distribuição acima do CIR no escalonador pai da fila criança (ALCATEL-LUCENT, 2011, p. 81), o *cir-weight* define o peso dentro de um nível de CIR dada a uma fila criança ou escalonador (ALCATEL-LUCENT, 2011, p. 81) e por fim o *cir-level* define o nível estrito a qual banda é alocada para a fila criança ou escalonador durante a fase de alocação de memória dentro da distribuição do CIR (ALCATEL-LUCENT, 2011, p.81).

O comando *percent-rate* determina o PIR que é o pico que a fila irá aceitar conforme abordado em outros tópicos e o parâmetro *cir-percent* determina o CIR conjuntamente que determina a taxa de transferência e o parâmetro *local-limit* é aplicável e é o padrão a qual não pode ser mudado quando a porta estiver operando em *percent-rate* (Alcatel-Lucent, 2011, p. 204).

A caixa *queue* tem vários parâmetros como CBS, MBS, *bust-limit*, *rate* entre outros, e os três primeiros citados trabalham com tráfego por rajada e o *rate* seria um comando substituto ao *percent-rate*, mas ao invés de porcentagem os

parâmetros seriam em Kbps.

O comando `fc` (forward class) pode ser definido entre `be`, `I2`, `af`, `I1`, `h2`, `ef`, `h1` e `nc`, boa parte definido no tópico 2.13, porém alguns foram usados apenas no sistema deles como o `nc` (Network Control) que seria `NC2` que é um dado de extrema prioridade usado apenas para o controle de rede (ALCATEL-LUCENT, 2011, p. 76) e não foi definido no DSCP assim como o `h1` que seria de uma prioridade um pouco menor do que o `NC2` e seria o `NC1`.

As classes `I2`, `I1` e `h2` são traduzidas respectivamente para `CS1`, `AF2` e `AF4` no padrão DSCP e as demais seguem o padrão DSCP. Dentro da caixa “`fc`” terá a fila (*queue*) criada anteriormente como parâmetro para definir qual é o DSCP dela.

Por fim o comando `dscp` que está dentro da caixa `sap-egress` ou `sap-ingress` fará a tradução das *forward class* (`fc`) da fabricante para o DSCP desejado.

Figura 207 - QOS Alcatel

```

qos sap-egress 15 create
description "CLIENTE"
queue 1 create
parent "ACESSO" cir-level 1
percent-rate 100.00 local-limit
exit
queue 2 create
parent "ACESSO" cir-level 1
percent-rate 100.00 cir 2.00 local-limit
exit
queue 3 create
parent "ACESSO" cir-level 1
percent-rate 100.00 cir 10.00 local-limit
exit
queue 4 create
parent "ACESSO" cir-level 1
percent-rate 100.00 cir 5.00 local-limit
exit
queue 5 create
parent "ACESSO" cir-level 1
percent-rate 100.00 cir 5.00 local-limit
exit
queue 6 create
parent "ACESSO" cir-level 1
percent-rate 20.00 cir 20.00 local-limit
exit
queue 7 create
parent "ACESSO" cir-level 1
percent-rate 20.00 cir 20.00 local-limit
exit
queue 8 create
parent "ACESSO" cir-level 1
percent-rate 25.00 cir 25.00 local-limit
exit
fc af create
queue 4
exit
fc be create
queue 1
exit
fc ef create
queue 8
exit
fc h1 create
queue 7
exit
fc h2 create
queue 6
exit
fc I1 create
queue 5
exit
fc I2 create
queue 3
exit
fc nc create
queue 2
exit
dscp af31 fc "af"
dscp ef fc "ef"
dscp af41 fc "h1"
dscp af42 fc "h2"
dscp af32 fc "I1"
dscp af12 fc "I2"
dscp cs2 fc "nc"

```

Fonte: Autoria Própria

Voltando a caixa `qos` dentro do roteador pode-se configurar o escalonador através das políticas de escalonamento (*scheduler-policy*), essas políticas serão passadas por herança conforme o escalonador anexado ao QOS na figura 208. Entrando na caixa *scheduler-policy* através do comando “*scheduler-policy (nome)*”

create” sendo nome uma cadeia de caracteres de tamanho 32 e *create* usado para criação e dispensável para alteração, pode-se configura um *tier*.

O *tier* é usado para colocar o escalonador dentro de uma hierarquia com 3 níveis (ALCATEL-LUCENT, 2011, p.26). O escalonador pode também ser filho (pegar banda) de um escalonador em maior nível, exceto para escalonadores criados em nível 1 (ALCATEL-LUCENT, 2011, p. 67). Para definir o nível será necessário entrar na caixa *tier* como o comando “*tier #*” sendo # um valor inteiro de 1 a 3.

Dentro do nível será criado o escalonador através do comando “*scheduler (nome) create*” sendo nome uma cadeia de caracteres de tamanho 32. Dentro do *scheduler* é posta a velocidade máxima do que os clientes terão através do comando “*rate # cir #*” sendo # um numeral que seja maior que 0 e vá até o valor máximo que a porta física ou conjunto de portas suportam e onde o cliente será configurado.

Voltando a caixa qos pode-se configurar a quantidade que quiser de políticas de escalonamento a quais poderão ser vinculados a *sap* na figura 209, lembrando que o conceito de herança é muito útil para não ter que criar várias linhas de códigos e gerar um encapsulamento de informações. Dependendo da versão do sistema Alcatel, talvez seja necessário criar o *scheduler* que nesse exemplo foi chamado de ACESSO dentro da caixa qos e para isso deve-se usar o comando “*scheduler “ACESSO” create*”, podendo “ACESSO” ser qualquer outra cadeia de caracteres que não ultrapasse o tamanho 32.

Figura 208 - Escalonador de QOS

```

scheduler-policy "2_MBPS" create
  tier 1
    scheduler "ACESSO" create
      rate 2048 cir 2048
scheduler-policy "3_MBPS" create
  tier 1
    scheduler "ACESSO" create
      rate 3072 cir 3072

```

Fonte: Autoria Própria

A figura 209 mostra a configuração da porta do cliente e para acessar a “*service*” precisa sair da caixa qos e usar o comando “*configure service*” conforme já explicado no tópico 3.1.3 e nenhuma das demais configurações serão explicadas aqui, exceto aquilo que estiver relacionado ao assunto QOS, afinal boa parte desse

assunto já foi abordado no tópico 3.1.3 e 3.4.3. Ao acessar a *sap* que nesse exemplo foi usado a *3/2/4/1.7.1.1*, existe a fila de *ingress* e *egress* .

Ao usar o comando *ingress* para acessar a caixa, para que a QOS tenha efeito tem que inserir uma *scheduler-policy* e um *qos*, a *scheduler-policy* é herdada da QOS inserida fazendo que o cliente receba a QOS desejada.

Figura 209 - Interface com QOS

```
service
  vprn 11 customer 3 create
  interface "420" create
    description "By DFID# = 20 (420)"
    address 10.12.12.1/30
    icmp
      no mask-reply
      no redirects
      no unreachable
    exit
    ip-mtu 1500
    sap 3/2/4.1.7.1.1 create
      ingress
        scheduler-policy "2_MBPS"
        qos 15
      exit
      egress
        scheduler-policy "2_MBPS"
        qos 15
      exit
    exit
  exit
```

Fonte: Autoria Própria

4 INTEGRANDO E CONFIGURANDO SOLUÇÃO DE VOZ

Nesse tópico será abordado a tecnologia de voz que está cada vez menos sendo utilizada, conforme dados da UOL (2018) houve uma redução de 94503 linhas entre os meses de fevereiro e março de 2018 por conta da telefonia celular. Nesse trabalho irá ser somente abordada a tecnologia EWSD da fabricante Siemens, porém existem outras como por exemplo a AXE da Ericsson, 5ESS da Lucent (Atual Nokia) entre outras.

4.1 DDR VIA NÚMERO CHAVE

Essa configuração normalmente é utilizada para clientes empresariais tendo os conceitos de ramais e canais, sendo ramais os números de telefones disponíveis e canais a quantidade simultânea máxima de ligações feitas ou recebidas. Este produto terá que ter na outra ponta uma central telefônica PABX para poder conectar os telefones nele, e a conexão terá um enlace de modem sendo digital.

Na figura 210 mostra o comando *STATDIU* que gera como resultado a LTG e suas DIU's, sendo que cada DIU tem 2 Mbps tendo 32 canais de 64 Kbps e cada LTG tem 4 DIU's, ou seja, uma LTG equivale a 8 Mbps ou uma E2 e a DIU equivale a um E1. Outra informação importante do comando são as colunas "*OST LTG*", "*OST DIU*" e "*OST PCM*", nas colunas "*OST LTG*" e "*OST DIU*" que representam a LTG e DIU respectivamente pode-se ter como resultado:

- ACT (*ACTIVE*): Ativo e sem falha na LTG ou DIU;
- CBL (*CONDITIONALLY BLOCKED*): Bloqueado condicionalmente por algum problema ou pode até ser usado por falta de pagamento do cliente;
- UNA (*UNAVAILABLE*): Indisponível por alguma falha na LTG ou DIU;
- MBL (*MAINTENANCE BLOCKED*): Bloqueio específico para configurações e em alguns casos pode ser usado para trabalhar com "loop";
- PLA (*PLANNED*): Planejado ou desativado por algum motivo, seja por configuração ou reset lógico.

A DIU em CASCAS na coluna "*APPLIC*" quer significar que essa placa trabalhará com a tecnologia DDR, qualquer coisa que difere disso não pertence à tecnologia DDR e pode ser usado para tecnologias ISDN, sinalização, tronco, linhas convencionais entre outros.

Figura 210 - Estado das DIU's.

```

STATDIU:LTG=0-47,DIU=X; EXEC'D

```

LTG	DIU	LTU TYPE	APPLIC	OST LTG	OST DIU	OST PCM
0-47	0	D30	CASCAS	ACT	ACT	ACT
0-47	1	D30	CASCAS	ACT	MBL	
0-47	2	D30	CASCAS	ACT	ACT	DIS-MA
0-47	3	D30	CASCAS	ACT	MBL	

```

END JOB 2340

```

Fonte: Autoria Própria.

Outro conceito importante é o de tronco chave ou número principal da faixa de ramais que é definido por um dos números dessa faixa. Na figura 211 é demonstrado como pegar esse tronco chave através da posição da DIU através do comando “*STATPORT*”. Observa-se aqui que existem 32 feixes que variam de 0 a 31, sendo que o 0 e o 16 são usados para controle restando apenas 30 feixes para ligações simultâneas. Na coluna “*STATUS*” pode-se obter os seguintes resultados:

- IDLE: Aguardando ficar ocupado;
- NLTG: Falha na LTG;
- NDIU: Falha na DIU;
- NCAR: Canais em curto ou não atingindo 2 Mbps;
- MPRT: Porta com DIU ou LTG em MBL;
- NMNT: Porta com DIU ou LTG em MBL;
- BUSY: Linha ocupada;
- BBAC: Falha na outra ponta, pode ter falha em algum equipamento de meio ou PABX do cliente;
- OUT: Linha fazendo ligações;
- INC: Linha recebendo ligações.

Outro campo interessante é o campo OPM que demonstra a direcionalidade dos feixes. Ele tem os seguintes parâmetros:

- ABW (*Analog Bothway*): Bidirecional;
- AIC (*Analog Incoming*): Apenas recebe chamadas;
- AOG (*Analog Outgoing*): Apenas faz ligação.

Figura 211 - Estado das linhas e direcionalidade.

```

STATPORT:LTG=0-47,LC=0;
EXEC'D LTG LC TGNO/PA DN LAC LNO CIC OPM
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
STATUS OF PORTS
0-47 0- 1 333333 041 1 ABW
0-47 0- 2 333333 041 2 ABW
0-47 0- 3 333333 041 3 ABW
0-47 0- 4 333333 041 4 ABW
0-47 0- 5 333333 041 5 ABW
0-47 0- 6 333333 041 6 ABW
0-47 0- 7 333333 041 7 ABW
0-47 0- 8 333333 041 8 ABW
0-47 0- 9 333333 041 9 ABW
0-47 0-10 333333 041 10 ABW
0-47 0-11 333333 041 11 ABW
0-47 0-12 333333 041 12 ABW
0-47 0-13 333333 041 13 ABW
0-47 0-14 333333 041 14 ABW
0-47 0-15 333333 041 15 ABW
0-47 0-16 333333 041 16 ABW
0-47 0-17 333333 041 17 ABW
0-47 0-18 333333 041 18 ABW
0-47 0-19 333333 041 19 ABW
0-47 0-20 333333 041 20 ABW
0-47 0-21 333333 041 21 ABW
0-47 0-22 333333 041 22 ABW
0-47 0-23 333333 041 23 ABW
0-47 0-24 333333 041 24 ABW
0-47 0-25 333333 041 25 ABW
0-47 0-26 333333 041 26 ABW
0-47 0-27 333333 041 27 ABW
0-47 0-28 333333 041 28 ABW
0-47 0-29 333333 041 29 ABW
0-47 0-30 333333 041 30 ABW
0-47 0-31 333333 041 30 ABW
END JOB 2347
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
LTG LC EQTYPE LCPOS OST STATUS
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
0-47 0- 0 NOTCOM ACT
0-47 0- 1 PBXLN ACT IDLE
0-47 0- 2 PBXLN ACT IDLE
0-47 0- 3 PBXLN ACT IDLE
0-47 0- 4 PBXLN ACT IDLE
0-47 0- 5 PBXLN ACT IDLE
0-47 0- 6 PBXLN ACT IDLE
0-47 0- 7 PBXLN ACT IDLE
0-47 0- 8 PBXLN ACT IDLE
0-47 0- 9 PBXLN ACT IDLE
0-47 0-10 PBXLN ACT IDLE
0-47 0-11 PBXLN ACT IDLE
0-47 0-12 PBXLN ACT IDLE
0-47 0-13 PBXLN ACT IDLE
0-47 0-14 PBXLN ACT IDLE
0-47 0-15 PBXLN ACT IDLE
0-47 0-16 NOTCOM ACT
0-47 0-17 PBXLN ACT IDLE
0-47 0-18 PBXLN ACT IDLE
0-47 0-19 PBXLN ACT IDLE
0-47 0-20 PBXLN ACT IDLE
0-47 0-21 PBXLN ACT IDLE
0-47 0-22 PBXLN ACT IDLE
0-47 0-23 PBXLN ACT IDLE
0-47 0-24 PBXLN ACT IDLE
0-47 0-25 PBXLN ACT IDLE
0-47 0-26 PBXLN ACT IDLE
0-47 0-27 PBXLN ACT IDLE
0-47 0-28 PBXLN ACT IDLE
0-47 0-29 PBXLN ACT IDLE
0-47 0-30 PBXLN ACT IDLE
0-47 0-31 PBXLN ACT IDLE
INTERRUPTION TEXT JOB 2347

```

Fonte: Autoria Própria.

Para ver a faixa de ramais usa-se o comando “DISPDN”, conforme figura 212, o mesmo demonstra no campo “PBXVOL” quais são os milhares, centenas ou dezenas configuradas para o cliente. No exemplo haverá no campo “PBXVOL” o 3 e 4, ou seja, os ramais começarão do 33333300 e irão até 33333499. Caso o cliente tenha a necessidade de ter duas faixas de ramais distintas no mesmo PABX pode-se vincular uma segunda chave a uma DIU. Para realizar a consulta usa-se o comando “STATPBXLN:DN=Chave” sendo que a chave pode não ter os últimos dígitos dependendo se ela terá unidades, dezenas, centenas ou milhares de ramais em tal faixa. Outro ponto a ressaltar é o campo “LAC” que representa o DDD do cliente.

Figura 212 - Sistema de numeração.

```
DISPDM:DN=333333;

DIRECTORY NUMBER DATA

LAC   = 041   DN     = 333333   ACT   = YES
        PEXVOL = 3&4
        STMGRP  = 0

DN      TYPE   INCEPT   EXTDM
-----+-----+-----+-----
333333  PEX
END JOB 3259
```

Fonte: Autoria Própria.

No comando “DISPPBX” terão os serviços desse DDR conforme ilustrado na figura 213, o LAC conforme já explicado é o DDD, o DN é o número que está o número chave, o COS contém os seguintes parâmetros:

- CLIP: Identificador de chamadas (BINA) ativo;
- CLIR: Identificador de chamadas (BINA) inativo;
- CONF3: Ativa conferência entre o cliente e duas chamadas;
- CT: Ativa a transferência e consulta de chamadas.

O TLIM tem como parâmetros os tempos limites de ligação, chamada e retorno, *opmode* terá opções referentes a direcionalidade conforme já explicado na figura 212 e por fim pode ter um outro parâmetro importante que é o “BLK”, esse parâmetro define os bloqueios e tem como resultado:

- ACCSPORI: Bloqueio para originar ligações;
- ACCSPTER: Bloqueio para receber ligações;
- ACCSUSP: Bloqueio total;
- ADMIN: Bloqueio total com interceptação de chamada.

Figura 213 - Verificando serviços atrelados a linha.

```
DISPPBX:DN=333333;

LAC   = 041   DN     = 333333   MASKNO:03793
COS   = CLIP   MASKNO:03777
TLIM  = CLEATM1 DIALTM1 RINGTM1   MASKNO:03802
OPMODE = AEW   MASKNO:03792
GCOS  = PROP8   PROP13   MASKNO:03782
HUNT  = SEQSRCH   MASKNO:03783
DIAL  = MFCR2   MASKNO:03779
SSDI  = 5       MASKNO:03798
DINO  = 2
MINMAX = 8- 8   MASKNO:03790
EOS   = SIGN   MASKNO:03781

END JOB 1292
```

Fonte: Autoria Própria.

4.2 CONFIGURAÇÃO DDR POR ROTA

Outra forma de configurar o acesso via DDR é por rota, assim como é feita a comunicação entre estações, foi pego de exemplo o número de telefone que se inicia com os dígitos “375333” considerando sua faixa de ramais entre 37533300 a 37533399.

O primeiro comando utilizado é o “DISPCPT:CODE=(número procurado),DEST=X” conforme figura 214, o X do destino significa que vai filtrar todos os resultados vinculados ao número procurado que está no parâmetro *CODE*. Na coluna *DEST* mostrou a rota “PIBV8” como resultado para coluna *CODE* com as dezenas 3753330, 3753331, 3753332 assim até o 3753339, isso significa que os intervalos serão 37533300 – 37533309, 37533310 – 37533319, 37533320 – 37533329 assim até o intervalo 37533390 – 37533399. Se juntar todos os intervalos fica 37533300 – 37533399 indo pela mesma rota PIBV8, ou seja, essa rota de destino é a do cliente.

Figura 214 - Configuração de rota.

```
DISPCPT:CODE=375333,DEST=X;
```

CODE POINTS FOR DEST					
DEST	CODE	MFCAT	ORIG1	LAC	SYM
		ROUTYP		ZDIG	CON
PIBV8	3753330	SUBORD	- 5 300 - 3		NO
PIBV8	3753331	SUBORD	- 5 300 - 3		NO
PIBV8	3753332	SUBORD	- 5 300 - 3		NO
PIBV8	3753333	SUBORD	- 5 300 - 3		NO
PIBV8	3753334	SUBORD	- 5 300 - 3		NO
PIBV8	3753335	SUBORD	- 5 300 - 3		NO
PIBV8	3753336	SUBORD	- 5 300 - 3		NO
PIBV8	3753337	SUBORD	- 5 300 - 3		NO
PIBV8	3753338	SUBORD	- 5 300 - 3		NO
PIBV8	3753339	SUBORD	- 5 300 - 3		NO

Fonte: Autoria Própria.

No EWSD existe a rota de destino “*DEST*” e o agrupamento de rota “*TGNO*”, os testes são sempre realizados com a “*TGNO*”, no caso tratado na figura 215 através do comando “*DISPROUTE*” existem duas rotas garantindo redundância devido à coluna “*TGNO*” ter “-T” ao lado do agrupamento “*PIBV*”. Caso não tenha o “-T” pode seguir para a figura 217, pois é uma rota apenas, sem necessidade de redundância.

Figura 215 - Verificação de destino.

```
DISPROUTE:DEST=PIBV8;
                                     DACT
TGNO   DEST      ROUTE  DINO      SSSI EOS  LNDES  TRACA  :
-----+-----+-----+-----+-----+-----+-----+
PIBV   -T PIBV8   1-Y-1 D8      1  SIGN  CLEARBA & NAT
                                     AMIRQD &
                                     DATIMM &
                                     PRIM
END TEXT 3340
DISPROUTE:DEST=PIBV8;
                                     ZDIG
TGNO   DEST      ROUTE  STAT :  DICON  DACT
-----+-----+-----+-----+-----+-----+
PIBV   -T PIBV8   1-Y-1   0 0
END JOB 3340
```

Fonte: Autoria Própria.

Então devido a existência do “-T” como parâmetro usa-se o comando “DISPTGCLU” conforme figura 216 para pegar as duas rotas, tendo na coluna “TGFCQ” a rota BV e PI, cada uma com 50% do total do tráfego.

Figura 216 - Divisão de tráfego.

```
DISPTGCLU:TGCLU=PIBV;
TRUNK GROUP CLUSTER
      ROU- FCQ- PRIM- RR-
TGCLU  SAL  SAL  ROUT  GRP  TGFCQ      OVSEQ
-----+-----+-----+-----+-----+-----+
PIBV   STD  EQDI  ALLTG  BV   - 50  PI   - 1
                                     PI   - 50  BV   - 1
END JOB 3394
```

Fonte: Autoria Própria.

A figura 217 retrata os canais da rota “BV” através do comando “STATTRUNK”. Na coluna LTG é demonstrada a LTG do cliente e na coluna LC demonstra a DIU e o canal separadas por traço “-”, outra coluna interessante é o de “STATUS” como explicado no tópico 4.1. Para verificar o estado da linha referente a rota “PI” é só usar o mesmo comando. Caso não tenha o “-T” na figura 214 pode-se usar a TGNO de lá direto.

Figura 217 – Estado das linhas.

```

STATTRUNK: TGNO=BV;
ACCEPTED

```

TGNO	LNO	CIC	EQTYP	OPMODE	LTG	LC	STATUS
BV	1	0-1	TRUNK	BW	2-12	1-1	IDLE
BV	2	0-2	TRUNK	BW	2-12	1-2	IDLE
BV	3	0-3	TRUNK	BW	2-12	1-3	IDLE
BV	4	0-4	TRUNK	BW	2-12	1-4	IDLE
BV	5	0-5	TRUNK	BW	2-12	1-5	OUT
BV	6	0-6	TRUNK	BW	2-12	1-6	IDLE
BV	7	0-7	TRUNK	BW	2-12	1-7	IDLE
BV	8	0-8	TRUNK	BW	2-12	1-8	IDLE
BV	9	0-9	TRUNK	BW	2-12	1-9	IDLE
BV	10	0-10	TRUNK	BW	2-12	1-10	IDLE
BV	11	0-11	TRUNK	BW	2-12	1-11	IDLE
BV	12	0-12	TRUNK	BW	2-12	1-12	IDLE
BV	13	0-13	TRUNK	BW	2-12	1-13	IDLE
BV	14	0-14	TRUNK	BW	2-12	1-14	IDLE
BV	15	0-15	TRUNK	BW	2-12	1-15	IDLE
BV	16	0-17	TRUNK	BW	2-12	1-17	IDLE
BV	17	0-18	TRUNK	BW	2-12	1-18	IDLE
BV	18	0-19	TRUNK	BW	2-12	1-19	IDLE
BV	19	0-20	TRUNK	BW	2-12	1-20	IDLE
BV	20	0-21	TRUNK	BW	2-12	1-21	IDLE
BV	21	0-22	TRUNK	BW	2-12	1-22	IDLE
BV	22	0-23	TRUNK	BW	2-12	1-23	IDLE
BV	23	0-24	TRUNK	BW	2-12	1-24	IDLE
BV	24	0-25	TRUNK	BW	2-12	1-25	IDLE
BV	25	0-26	TRUNK	BW	2-12	1-26	IDLE
BV	26	0-27	TRUNK	BW	2-12	1-27	IDLE
BV	27	0-28	TRUNK	BW	2-12	1-28	IDLE
BV	28	0-29	TRUNK	BW	2-12	1-29	IDLE
BV	29	0-30	TRUNK	BW	2-12	1-30	IDLE
BV	30	0-31	TRUNK	BW	2-12	1-31	IDLE

Fonte: Autoria Própria.

4.3 CONFIGURAÇÃO DE NÚMERO FIXO

As configurações de linha fixa são bem mais simples do que as configurações DDR, sendo separadas por DLU's que suportam até 1024 linhas fixas. Não há aqui ramais e canais e quase nenhuma complicação.

Com o comando "STATLINE" e mais o telefone fixo é obtido o EQN que é composto por número da DLU, numeração do armário, numeração do módulo e a identificação do canal, isto é ilustrado na figura 218. Pode-se ver o estado do canal através do "STATUS", que contém a mesma informação do tópico 4.1.

Figura 218 - Estado da linha fixa.

```

STATLINE: DN=33333333;

```

OBJECT	EQN	OPMODE	LNO	LSN	SERV	STATUS
ENHANCED STATUS OF LAC: 041 DN: 33333333						
SUB						
PORT	1330-1-		3-12			IDLE
END JOB 0625						

Fonte: Autoria Própria.

Com a DLU é possível ver os estados das LTG's interligadas a ele, que no caso exemplificado na figura 219, existe a LTG 3-29 e 3-30 ambas nas colunas "SIDE - 0: LTG" e "SIDE - 1 : LTG". Pode-se ver os estados LTG com o comando "DISPLTG:LTG=nº da LTG". Outro ponto de falha é a DLU que é demonstrado na coluna DLUC-OST e pode ter os seguintes parâmetros:

- ACT (*ACTIVE*): ativa e operante;
- DST (*DISTURBED*): com falhas e problemas;
- MBL (*MAINTENANCE BLOCKED*): bloqueado para manutenção;
- PLA (*PLANNED*): planejado;
- CBL (*CONDITONALLY BLOCKED*): bloqueado por operador;
- FLT (*FAULTY*): inoperante.

Figura 219 - Estado das LTG's.

```

STATDLU:DLU=1330; EXEC'D
+      SIDE - 0:      +      SIDE - 1:
+      ACCESS-      +      ACCESS-
DLU + DLUC-OST  LTG  DEG.  + DLUC-OST  LTG  DEG.
-----+-----+-----+-----+-----+-----+-----
1330  ACT    3-29  NON      ACT    3-30  NON
END JOB 0986

```

Fonte: Autoria Própria.

Com o comando *DISPSUB* que é ilustrado conforme figura 220 pode-se pegar configurações da linha como:

- LAC: é o DDD do número;
- DN: Número do cliente;
- EQN: Conforme já explicado, é a DLU, armário, posição e canal;
- CAT: Aqui é a categoria do assinante, sempre será para linha analógica "MS" (*main station (analog)*);
- LTT: Tipo de linha de transmissão, tem até 7 perfis que podem ser usados pela operadora que controla a parte sonora entregue ao cliente;
- LNATT: São alguns atributos da linha sendo:
 - PB: Pressionar algum botão para realizar chamada;
 - LNPROP0: São propriedades padrão da linha fixa.
- COS: são as classes de serviços que a linha possui:
 - ACTCW: Serviço de chamada em espera;
 - CWACTION: Autenticação do serviço de chamada em espera.

Figura 220 - Configurações da linha.

```

DISPSUB:DN=33333333;
                                     MASKNO:03800
LAC   = 041   DN   = 33333333   EQN   = 1330- 1- 3-12
CAT   = MS                                     MASKNO:03774
LTT   = COSLAC2                               MASKNO:03789
NUMCAL = 1                                     MASKNO:08641
ORIG1 = 1                                     ORIG2 = 1
LNATT = LNPROPO PB                             MASKNO:03787
COS   = ACTCW   CWACTION CLIP                 MASKNO:03777
END JOB 0995

```

Fonte: Autoria Própria.

Um comando que pode ser usado como substituto do comando “STATLINE” é o “STATSUB” da figura 221 que mostra na coluna “STATUS” o estado do link e na coluna “EQN” a facilidade aonde se encontra o circuito.

Figura 221 - Estado da EQN.

```

STATSUB:DN=33333333;
LAC   DN           CATYPE EQN           STATUS DNCTR LNCTR
-----+-----+-----+-----+-----+-----+-----
041   33333333    MS       1330- 1- 3-12 DIDDLE & 1- 0 1- 0
                                     IDLE
END JOB 1065

```

Fonte: Autoria Própria.

4.4 VOIP

Para configurar o H.323 num roteador Cisco é necessário entrar no modo de configuração, através do comando “configure terminal”. Ao entrar no modo de configuração pode-se entrar diretamente na placa e fazer algumas configurações através do comando “voice-card #” onde # é um numeral que representa o slot da placa que é demonstrado na figura 222. Nessa caixa não será feita nenhuma configuração no H.323, mas pode ser usada para os demais protocolos, inclusive pode ter configurações importante dependendo do fabricante da placa.

Voltando à caixa de configuração (configure terminal) será executado o comando “voice rtp send-recv”, esse comando de acordo Giralt, Hallmark e Smith (2002, p.408) é usado para problemas de chamadas unidirecionais quando se liga para certos números.

Continuando na caixa de configuração (*configure terminal*) podemos acessar a caixa “voice service pots”, lembrando que o POTS (*Plain Old Telephone Service*) e PSTN (*Plain Switched Telephone Network*) é uma terminologia usada com o mesmo

significado e já explicado no tópico 2.10.1. Dentro dessa caixa podemos inserir o comando *“fax rate disable”* que como o próprio comando sugere é a desativação de serviço de fax, lembrando que isso é apenas um exemplo de como configurar essa caixa, pode-se lançar diversos comandos para serviços telefônicos legados.

Voltando a caixa de configuração (*configure terminal*) pode-se iniciar a configuração do VOIP através do comando *“voice service voip”* para entrar nessa caixa. Nessa caixa existe a possibilidade de ativar o monitoramento de chamadas através do comando *“callmonitor”*, ao ativar essa configuração pode-se usar o comando *“show callmon”* fora das caixas para coletar o log de ligações.

Outro comando que é interessante ser explicado é o *“allow-connections”* que aqui no exemplo da figura 222 serve para permitir a conexão entre o SIP e o H323, vice-versa ou entre eles mesmos.

O próximo comando a ser explicado dentro dessa mesma caixa é o *“supplementary-service”* que liberará um serviço suplementar que nesse caso é o serviço h450.12 chamado de informação adicional de recurso de rede comum (*Common Information Additional Network Feature*) também chamado como ANF-CMN. Segundo a *International Telecommunication Union* (2001, p. 2) esse serviço é uma coleção de diversas informações que relatam ao ponto final ou equipamento em um fim de uma conexão e inclui um ou mais dos seguintes recursos de identificação, recurso de valores e recurso de controle.

O comando *“fax protocol pass-through g711alaw”* permite que o protocolo de fax passe pela codificação G.711 A-Law que é um protocolo PCM que está especificado pela norma G711 da ITU-T e codificado pelo método A-Law e não será explicado nesse material devido à complexidade do assunto.

O comando *“H323”* ativa o H323 no serviço e o comando *“sip”* entra nas configurações do protocolo SIP, abrindo uma nova caixa para configuração. Essa nova caixa de configuração que abriu abre um leque gigantesco de opções que podem ser realizadas como rotas de voz, volume, CODECS, autenticação, banda, entre outros. Aqui como exemplo será usado o comando *“registrar server expires max 3600 min 3600”* que serve para realizar o registro de chamadas locais com tempo de expiração de 1 hora.

Após essas configurações pode-se sair das duas caixas e entrar na caixa de configuração e lá acessar a caixa *“voice class codec 1”*. Nessa caixa pode-se configurar os CODECS de voz que serão usados pelo cliente e também os CODECS

de vídeo. No exemplo da figura 222 foram inseridos os CODECS através do comando “*codec preference*” seguido de um número inteiro que pode variar “1-24” sendo que 1 é a preferência mais alta seguido do CODEC que foi acordado contratualmente com o cliente. Ao configurar o que é necessário deve-se sair da caixa e voltar para a caixa de configuração.

A próxima caixa que deve ser configurada é a caixa “*voice class h323 1*”, que contempla algumas configurações do h323 como funcionalidades exclusivas do roteador Cisco, protocolos h225 e h245 e mais alguns serviços. Aqui foi decidido configurar o tempo máximo que pode ficar sem sinal TCP de 5 segundos através do comando “*h225 timeout tcp establish 5*” como exemplo.

Figura 222 - Configuração VOIP 1.

```
voice-card 0
!
!
voice rtp send-recv
!
voice service pots
fax rate disable
!
voice service voip
callmonitor
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
supplementary-service h450.12
fax protocol pass-through g711alaw
h323
sip
  registrar server expires max 3600 min 3600
!
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g711alaw
codec preference 3 g729r8
codec preference 4 g729br8
!
voice class h323 1
h225 timeout tcp establish 5
```

Fonte: Autoria Própria.

Após essas configurações deve-se criar uma interface lógica, que está sendo explicado na figura 223, para que se possa gerar a transição do IP ao VOIP. Entrando no modo de configuração do roteador CISCO deve-se usar o comando “*interface loopback#*” sendo “*#*” um número variável e que depende da versão do roteador do seu valor máximo. Ao criar uma interface *loopback* automaticamente se entra na caixa da interface e pode-se gerar uma descrição a ela.

Outro ponto importante dentro dessa caixa é a definição de IP's sendo necessário criar um IP para essa porta através do comando “*ip address* (número do IP) (máscara de sub rede)”. Aqui também se define essa interface como o gateway

ou interface de entrada/saída h323 através do comando “*h323-gateway voip interface*”.

O comando “*h323-gateway voip id (apelido) ipaddr (IP) (TCP) priority #*” sendo apelido uma sequência de caracteres, IP o endereço IP, TCP a porta TCP e # um numeral de 1-127 que define a prioridade do gateway que será usado e esse comando faz que seja direcionado o tráfego a esses endereços IP’s evitando que outros computadores da rede acessem a informação. Mais um comando importante é o apelido desse gateway que é definido pelo comando “*h323-gateway voip h323-id (apelido)*”. O comando “*h323-gateway voip tech-prefix 1#*” define o apelido do gateway para a tecnologia de voz e por fim o IP que irá ligar o protocolo com a porta através do comando “*h323-gateway voip bind srcaddr (ip)*” que será o mesmo endereço configurado na porta da interface de *loopback*.

Figura 223 - Configurando VOIP 2.

```
interface Loopback2
description Loopback rede de voz
ip address 192.0.2.1 255.255.255.255
h323-gateway voip interface
h323-gateway voip id exemplo ipaddr 192.0.3.1 1719 priority 1
h323-gateway voip id exemplo ipaddr 192.0.4.1 1719 priority 2
h323-gateway voip h323-id ex1
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 192.0.2.1
```

Fonte: Autoria Própria.

Na próxima configuração, demonstrada na figura 224, existem as configurações referentes à porta física, normalmente o equipamento VOIP aceitará a configuração padrão, porém pode ser necessário configurar tradutores, impedância, tronco chave, música e tom. Para acessar essa caixa de configuração, basta entrar no modo de configuração (“*conf t*”) e escolher a porta através do comando (“*voice-port (número da porta)*”).

Figura 224 - Configurando VOIP 3.

```
voice-port 1/0/0
description FXO 1/0/8
!
voice-port 1/0/1
!
voice-port 1/0/2
!
voice-port 1/0/3
!
voice-port 1/0/4
!
voice-port 1/0/5
!
voice-port 1/0/6
!
voice-port 1/0/7
```

Fonte: Autoria Própria.

O próximo passo, conforme figura 225, é a configuração do número da rede de telefonia que será vinculado ao IP. Para isso deve-se entrar na caixa de configuração e entrar na caixa “*dial-peer voice (valor) pots*” onde valor pode ser um ramal, um telefone ou até um identificador qualquer. Nesse caso será apenas configurado o ramal 3940 através do comando “*destination-pattern 3940*”, pode-se também usar “*prefix*” para configurar um prefixo, “*trunk-group*” para vincular um identificador de um grupo de troncos já criados, outro modo de configurar vários números para envio é usando a letra T após o prefixo ou todos os números usando “.T”. Logo após deve-se configurar o “*port 1/0/0*” para vincular a porta com o ramal.

Saindo dessa caixa deve-se fazer a configuração VOIP para o equipamento chamado na rede VOIP de “*gatekeeper*” para realizar a configuração e identificação dos equipamentos VOIP em toda a rede. Nesse caso é necessária a existência dessa configuração devido à topologia ser entre múltiplas filiais e uma unidade concentradora que faz a saída para a rede legada de telefonia.

Para fazer a configuração do *gatekeeper* em uma filial deve entrar na caixa de configuração do roteador Cisco (*configure terminal*) e depois entrar na caixa de comando “*dial-peer voice (número) voip*” onde número pode ser um identificador qualquer e VOIP é a sinalização para a rede VOIP.

Dentro dessa caixa pode-se colocar uma descrição através do comando “*description*”. Como será necessário criar um “*destination-pattern*” para envio dos dígitos e o *gatekeeper* vai receber todos que a filial mandar, pode-se configurar o “.T”. A configuração “*progress_ind setup enable 3*” configura a sinalização chamada PI, sem essa configuração tons de chamada podem não aparecer. No Brasil o valor padrão para essa configuração é 3, porém pode ser 8.

O comando “*session target (palavra)*” sendo essa palavra uma sequência de caracteres e ele atua analogicamente como uma rota estática para a rede de dados, porém para a rede de voz, nesse caso foi usado a palavra “ras” como apelido para identificar o destino e também pode ser usado “*ipv4:(endereço IPv4)*” para selecionar um endereço IPv4 como destino.

O comando “*voice-class h323 1*” serve para apontar a caixa criada anteriormente ao *gatekeeper*. No próximo comando “*dtmf-relay rtp-nte h245-alphanumeric*” é usado para o método de discagem sendo nesse caso usado “*rtp-nte*” que é um padrão definido pela norma RFC 2833 e “*h245-alphanumeric*” que usa

o padrão H245. O comando “*codec g728br8*” é o comando que seleciona o codificador e o decodificador do sinal, nesse caso foi usado o g728br8, porém pode ser usado outro, dependendo dos equipamentos do cliente.

O último comando é o “*ip qos dscp cs3 signaling*” e é referente ao QOS (*Quality of Service*) desse serviço, e refere-se à prioridade no envio desses pacotes pela rede IP, o recomendado é usar o “*best-effort*”, porém quem definirá esse parâmetro é o contrato do cliente.

Figura 225 - Configurando VOIP 4.

```
dial-peer voice 3940 pots
destination-pattern 3940
port 1/0/0
!
dial-peer voice 100 voip
description Gatekeeper
destination-pattern .T
progress_ind setup enable 3
session target ras
voice-class h323 1
dtmf-relay rtp-nte h245-alphanumeric
codec g729br8
ip qos dscp cs3 signaling
!
!
gateway
timer receive-rtp 1200
!
!
!
gatekeeper
shutdown
```

Fonte: Autoria Própria.

Esse é um exemplo de configuração, lembrando que o VOIP nesse caso será usado num sistema multifilial, porém pode ser usado para sair direto para um PABX e ir para a rede de telefonia legada.

5 APRESENTAÇÃO DE DADOS E TRABALHOS FUTUROS

A rede legada ainda existirá por mais alguns anos devido aos clientes empresariais que contrataram essa rede legada como bancos que usam para caixas eletrônicos com a rede plesiócrons e em regiões do interior do país. E esse é um problema dinâmico que tende sempre a ser estudado, afinal é extremamente necessário a humanidade todo esse tráfego de dados para a comunicação e o mundo mais integrado e que todo dia haverá novidades seja em aplicativos e novas tecnologia que entram e saem do mercado, garante-se ao leitor que não é fácil escrever sobre tal tema por seu nível de evolução.

Os serviços cada ano que passa estão mais robustos e específicos. Antigamente o sistema de telefonia era caro e importantíssimo, hoje é considerado algo arcaico, o mesmo ocorre em todas as áreas da tecnologia, desde vídeo games que o modo multijogador era no mesmo aparelho e hoje existem servidores pelo mundo para jogos em rede até vídeos que antigamente rodavam via fita magnética e hoje pode ser acessado via serviço de vídeo em rede. Com esse parágrafo conclui-se que esse tema futuramente será abordado com tecnologia ótica e sem fio.

Talvez os serviços requeiram em maior parte do tempo uma tecnologia sem fio para seu uso, não que os velhos cabos sejam totalmente aposentados. Assim como o legado Frame-Relay ainda é usado hoje para sistemas bancários e que exijam uma alta segurança e confiabilidade, afinal a segurança de tecnologias antigas já são comprovadas, enquanto das novas geram desconfiança nas grandes empresas que tem como prioridade a segurança de dados de seus usuários. Quem sabe se a tecnologia satélite se torne nos próximos anos mais barata e eficiente do que colocar muitas antenas e estações físicas para usuários que não priorizam a segurança em suas transações em uma cidade? Esse questionamento se guarda aos interessados em tais áreas.

Com o passar do tempo e com a implementação da 5G a internet tende a ser mais rápida e mais móvel, podendo até aposentar os computadores desktops e abrindo espaço para novas tecnologias móveis, além dos avanços com serviços a realidade aumentada e óculos de realidade virtual pode-se ocorrer um maior tráfego de dados da rede.

6 CONSIDERAÇÕES FINAIS

Com o tempo as empresas de telecomunicações vão evoluindo e existe a necessidade de pessoas do curso Sistemas de Telecomunicação ficarem mais necessárias, para as pessoas que convivem trabalhando com esse assunto sabe que existe muita coisa legada, mas conforme os desafios vão chegando a modernização se torna mais fácil e real.

Futuramente as coisas serão mais automatizadas e serão todas convertidas para a facilidade da tecnologia IP que também se modernizou que antigamente era IPV4 e hoje IPV6. Talvez futuramente a visão do profissional de telecomunicações fique mais na parte lógica e de cabeamento do que na parte de suporte que lentamente vai sendo automatizado.

REFERÊNCIAS

AGRELA, Lucas. Este é o hábito mais comum dos brasileiros no WhatsApp. **Exame**, [S. l.], n. 1, p. 1, 8 out. 2019. Disponível em: <https://exame.abril.com.br/tecnologia/este-e-o-habito-mais-comum-dos-brasileiros-no-whatsapp/>. Acesso em: 15 abr. 2020.

AKAMAI (Estados Unidos). **Akamai's [state of internet]**: Q1 2017 report. 1. ed. Estados Unidos da América: Akamai, 2017. 57 p. v. 10. Disponível em: <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-connectivity-report.pdf>. Acesso em: 9 jun. 2020.

ALCATEL-LUCENT. **7750 SR OS Quality of Service Guide**. Estados Unidos da América: Alcatel Lucent, 2011. 800 p. Disponível em: https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9300770801_V1_7750%20SR%20OS%20QUALITY%20F.pdf. Acesso em: 11 ago. 2021.

AMERICAN NATIONAL STANDARDS INSTITUTE. **T1.105: Synchronous Optical Network (SONET) – Basic Description Including Multiplex Structure, Rates and Formats**. Nova Iorque, 2001.

ANATEL (Brasil). **Telefonia Fixa**. [S. l.], 1 fev. 2020. Disponível em: <https://www.anatel.gov.br/paineis/acessos/telefonia-fixa>. Acesso em: 15 abr. 2020.

ANATEL (Brasil). **TV por assinatura**. [S. l.], 1 fev. 2020. Disponível em: <https://www.anatel.gov.br/paineis/acessos/tv-por-assinatura>. Acesso em: 15 abr. 2020.

BAGAD, Vilas; DHOTRE, Iresh. **Computer Communication Networks**. 1. ed. Shaniwar Peth, Pune, India: Technical Publication Pune, 2008. 386 p. ISBN 9788189411299.

BARBIARZ, Jozef; HO CHAN, Kwok; BAKER, Fred. **RFC 4594 – Guidelines for DiffServ Service Class**. Estados Unidos da América: IETF, 2006. 57 p. Disponível em: <https://datatracker.ietf.org/doc/html/rfc4594>. Acesso em: 10 ago. 2021.

BEASLEY, Jeffrey S.; NILKAEW, Piyasat. **Networking Essentials**. 3. ed. Estados Unidos da América: Pearson Education, 2012. 600 p. ISBN 9780133381702.

BEKAKOS, M. P.; GRAVVANIS, G. A.; ARABNIA, H.R. **Grid Technologies: Emerging from Distributed Architectures to Virtual Organizations**. Hampshire, Inglaterra: WIT Press, 2006. 475 p. ISBN 9781845640552.

BONEY, James. **Cisco IOS in a Nutshell: A desktop quick reference for IOS on IP networks**. 2. ed. Califórnia, Estados Unidos da América: O'Reilly Media, 2005. 798 p.

ISBN: 9780596553111.

BRADEN, Bob; et. al. **RFC 2309 – Internet Performance Recommendations**. Estados Unidos da América: IETF, 1998. 17 p. Disponível em: <https://datatracker.ietf.org/doc/html/rfc2309>. Acesso em: 10 ago. 2021.

BRUNO, A. Anthony; KIM, Jacqueline. **CCDA Self-study: CCDA Exam Certification Guide**. 2. ed. Indianapolis, Estados Unidos da América: Cisco Press, 2003. 666 p. ISBN 1587200767.

CASTELLI, Matthew. **Network Consultants Handbook**. Indianapolis, Estados Unidos da América: Cisco Press, 2002. 965 p. ISBN 9781587050398.

CHIN, Jonathan. **Cisco Frame Relay Solutions Guide**. 1. ed. Indianapolis, Estados Unidos da América: Cisco Press, 2004. 669 p. ISBN 1587051168.

CISCO SYSTEM INC. (Estados Unidos). **Configuração e Troubleshooting da conexão ATM e Cisco BPX 8600 Series Switches**. Califórnia, Estados Unidos: Cisco System Inc., 10 set. 2018. Disponível em: https://www.cisco.com/c/pt_br/support/docs/interfaces-modules/bpx-8600-modules/6502-atm-connection-abr.html. Acesso em: 3 jun. 2020.

CLARK, M. P. **Data Networks, IP and the Internet: Protocols, Design and Operation**. West Sussex, Inglaterra: John Wiley & Sons, 2003. 866 p. ISBN 9780470848562.

ELLIS, Juanita; PURSELL, Charles; RAHMAN, Joy. **Voice, Video, and Data Network Convergence: Architecture and Design, From VoIP to Wireless**. California, Estados Unidos: Elsevier, 2003. 330 p. ISBN 9780080474816.

FARID, Handy Mahmoud et al. **Packet switch network link**. Depositante: Alcatel. US 2006/0088033 A1. Depósito: 21 out. 2004. Concessão: 27 abr. 2006.

FREEMAN, R. L. **Fundamentals of Telecommunications**. 2. ed. New Jersey, Estados Unidos da América: John Wiley & Sons, 2005. 720 p. ISBN 9780471720935

FROEHLICH, Fritz; KENT, Allen. **The Froehlich/Kent Encyclopedia of Telecommunications: IEEE 802.3 and Ethernet Standards to Interrelationship of the SS7 Protocol Architecture and the OSI Reference Model and Protocols**. 9. ed. Nova Iorque, Estados Unidos da América: Marcel Dekker, 1995. 528 p. v. 9. ISBN 0824729072.

GIRALT, Paul; HALMARCK, Addis; SMITH, Anne. **Troubleshooting Cisco IP Telephony**. Indianapolis, Estados Unidos da América: Cisco Press, 2003. 973 p. ISBN 9781587050756.

GOLENIEWSKI, Lillian. **Telecommunications Essentials: The Complete Global**

Source for Communications Fundamentals, Data Networking and the Internet, and Next-generation Networks. Massachusetts, Estados Unidos: Addison-Wesley Professional, 2002. 582 p. ISBN 9780201760323.

GRABER, Herald; HERNANDEZ-VALENCIA, Enrique; HEIMUELLER, Bernd. **Optical/Packet Transport Convergence**. Bell Labs Technical Journal, DOI: 10.1002/bltj.20149, p 143-158, 2006.

IGI CONSULTING (Massachusetts). **Frame Relay: Market and Technology Assessment Study**. Massachusetts, Estados Unidos da América: Information Gatekeepers Inc, 1991.

INTERNATIONAL TELECOMMUNICATION UNION. **Common Information Additional Network Feature for H.323**. Geneva, Suíça, 2001.

INTERNATIONAL TELECOMMUNICATION UNION. **G.704: Synchronous Frame Structure Used at 1544, 6312, 2048, 8448 and 44736 kbit/s hierarchical levels**. 37 p. Geneva, 1998.

INTERNATIONAL TELECOMMUNICATION UNION. **G.707/Y.1322: Network node interface for the synchronous digital hierarchy (SDH)**. Geneva, 2008.

INTERNATIONAL TELECOMMUNICATION UNION. **G.780/Y.1351: Terms and definitions for synchronous digital hierarchy (SDH) networks**. Geneva, 2010.

INTERNATIONAL TELECOMMUNICATION UNION. **G.992.1: SERIES G: TRANSMISSION SYSTEMS AND MEDIA DIGITAL SYSTEM AND NETWORKS: Digital transmission systems – Digital sections and digital line system – Access networks**. 240 p. Geneva, 1999.

INTERNATIONAL TELECOMMUNICATION UNION. **I.326: Functional architecture of transport networks based on ATM**. Geneva, 2003.

INTERNATIONAL TELECOMMUNICATION UNION. **Séries G: Transmission Systems and Media Digital Systems and Networks – Digital Sections and Digital Line System – Optical Line Systems for Local and Access Network, Gigabit-capable passive optical networks (GPON): General characteristics**. Geneva, Suíça, 2008, 43 p.

INTERNATIONAL TELECOMMUNICATION UNION. **Séries G: Transmission Systems and Media Digital Systems and Networks – Digital Sections and Digital Line System – Optical Line Systems for Local and Access Network, Gigabit-capable passive optical networks (GPON): ONT management and control interface specification**. Geneva, Suíça, 2019, 50 p.

INTERNATIONAL TELECOMMUNICATION UNION. **Séries G: Transmission Systems and Media Digital Systems and Networks – Digital Sections and Digital**

Line System – Optical Line Systems for Local and Access Network, Gigabit-capable passive optical networks (GPON): Physical media dependent (PMD) layer specification. Geneva, Suíça, 2019, 50 p.

INTERNATIONAL TELECOMUNICATION UNION. **Séries G: Transmission system and media, digital systems and networks** – Multimedia Quality of Service and Performance – Generic and user-related aspects, Reference guide to quality of experience assessment methodologies. Geneva, Suíça, 2015, 57 p.

INTERNATIONAL TELECOMUNICATION UNION. **Séries H: Audiovisual and Multimedia Systems** – Infraestrutura of audiovisual services – System Aspects, Confidentiality system for audiovisual services. Geneva, Suíça, 2002, 28 p.

INTERNATIONAL TELECOMUNICATION UNION. **Séries Q: Switching and Signalling** – Signalling requirements and protocols for IMT-2000 – IMT-Advanced references to release 11 of LTE-Advanced evolved packet core network. Geneva, Suíça, 2006, 330 p.

INTERNATIONAL TELECOMUNICATION UNION. **Séries X: Data Networks And Open System Communication** – Interface between Data Terminal Equipment (DTE) Data Circuit-terminating (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit. Geneva, 1996.

INTERNATIONAL TELECOMUNICATION UNION. **Séries Y: Global Information Infraestructure, Internet Protocol Aspects and Next Generation Networks** – Internet Protocol Aspects – Quality of Services and Network Performance, Network performance objectives for IP-based services. Geneva, Suíça, 2011, 57 p.

INTERNATIONAL TELECOMUNICATION UNION. **Séries Y: Global Information Infraestructure, Internet Protocol Aspects and Next Generation Networks** – Next Generation Networks – Quality of Service and Performance, Admission control priority levels in Next Generation Networks. Geneva, Suíça, 2006, 12 p.

HEINANEN, Juha; GUERIN, Roch. **RFC 2698 – A Two Rate Three Color Marker**. Estados Unidos da América: IETF, 1999. 5 p. Disponível em: <https://datatracker.ietf.org/doc/html/rfc2698>. Acesso em: 10 ago. 2021.

HEINANEN, Juha; GUERIN, Roch. **RFC 2698 – A Single Rate Three Color Marker**. Estados Unidos da América: IETF, 1999. 6 p. Disponível em: <https://datatracker.ietf.org/doc/html/rfc2697>. Acesso em: 10 ago. 2021.

KASERA, Sumit. **Atm Networks Concepts And Protocols**. 2. ed. Gurgaon, India: Tata McGraw-Hill Education, 2006. 466 p. ISBN 9780070583535.

KOCHARIANS, Narbik; VINSON, Terry. **CCIE Routing and Switching v5.0 Official Cert Guide**. 5. ed. Indianapolis, Estados Unidos da América: Cisco Press, 2014. 656 p. v. 2. ISBN 9780133591064.

KOTA, S. L.; PAVALAN, Kaveh; LEPPANEN, Pentti. **Broadband Satellite Communications for Internet Access**. 1. ed. Nova Iorque, Estados Unidos da América: Springer Science & Business Media, 2004. 421 p. ISBN 9781441988959.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down**. 6^a. ed. rev. São Paulo: Pearson Education do Brasil, 2013. 658 p. ISBN 9788543014432.

LEE, Robert. **The ISDN Consultant: A Stress-free Guide to High-speed Communications**. New Jersey, Estados Unidos: Prentice Hall, 1997. 236 p. ISBN 9780132590525.

MASON, A. G.; NEWCOMB, M. J. **Cisco Secure Internet Security Solutions**. Indianapolis, Estados Unidos da América: Cisco Press, 2001. 499 p. ISBN 9781587050169.

MCQUERRY, Steve; MCGREW, Kelly; FOY, Stephen. **Cisco Voice Over Frame Relay, ATM, and IP**. Indianapolis, Estados Unidos da América: Cisco Press, 2001. 517 p. ISBN 9781578702275.

MISHRA, Ajay Ranjan. **Cellular Technologies for Emerging Markets: 2G, 3G and Beyond**. New Delhi, India: John Wiley & Sons, 2010. 326 p. ISBN 9780470975671.

NETO, Vicente Soares; NETO, Jarbas Gambogi. **Telecomunicações : redes de alta velocidade, sistemas PDH e SDH**. 2. ed. São Paulo, SP: Érica, 2002. 206 p. ISBN 8571946930.

NEWBRIDGE NETWORKS CORPORATION. **3600 Mainstreet Family: Bandwidth Managers**. Ontario, Canada, 1997. 1478 p.

NIC.BR (Brasil). **Endereçamento**. Brasil: Nic.br, 15 maio 2012. Disponível em: <http://ipv6.br/post/enderecamento/>. Acesso em: 7 jul. 2020.

OPPENHEIMER, Priscilla. **Top-down Network Design**. Indianapolis, Estados Unidos da América: Cisco Press, 2001. 560 p. ISBN 9781578700691.

OSHANA, Robert. **DSP for Embedded and Real-Time Systems**. Massachusetts, Estados Unidos: Elsevier, 2012. 656 p. ISBN 9780123865359.

PAGANI, Margherita. **Encyclopedia of Multimedia Technology and Network**. 2. ed. Pensilvânia, Estados Unidos da América: IGI Global, 2009. 1756 p. ISBN 9781605660158.

PYLES, J.; CARREL, J. L.; TITTEL, E. **Guide to TCP/IP: IPv6 and IPv4**. 5. ed. Massachusetts, Estados Unidos: Cengage Learning, 2016. 768 p. ISBN 9781337020541.

RIVEIRA, Carolina. **Estagnação? Base de usuários da Netflix no Brasil cresce cada vez menos.** Exame, [S. l.], p. 1, 17 jul. 2019. Disponível em: <https://exame.abril.com.br/negocios/estagnacao-base-de-usuarios-da-netflix-no-brasil-cresce-cada-vez-menos/>. Acesso em: 15 abr. 2020.

SREETHARAN, Muthuthamby; SUBRAMANIAM, Sivananda. **ATM Interworking in Broadband Wireless Applications.** Massachusetts, Estados Unidos da América: Artech House, 2002. 324 p. ISBN 9781580532853.

STRIGFIELD, Nakia; WHITE, Russ; MCKEE, Stacia. **Cisco Express Forwarding.** Indianapolis, Estados Unidos da América: Cisco Press, 2007. 288 p. ISBN: 9780132796873

SWEE, Poo G. **Towards Network Globalization:** Proceedings Of The 1991 Singapore International Conference Of Networks. Raffles, Singapura: World Scientific, 1991. 440 p. ISBN 9789814555630.

THE INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE. **Series X: Data Communication Networks:** Services And Facilities, Interfaces. Geneva, Suíça 1988. 152 p.

TUGAL, D. A.; TUGAL, O. **Data transmission:** Mcgraw-Hill Communications Series. 2. ed. rev. Michigan, Estados Unidos da América: McGraw-Hill, 1989. 493 p. ISBN 9780070654471.

UOL (Brasil). **Telefonia fixa no Brasil tem queda e registra 94,5 mil linhas a menos.** UOL, Brasil, p. 1, 30 abr. 2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/04/30/telefonia-fixa-no-brasil-tem-queda-e-registra-945-mil-linhas-a-menos.htm>. Acesso em: 11 jun. 2020.

XIAO, Tianyuan; FEI, Minrui; ZHANG, Lin **AsiaSim 2012** - Part II: Asia Simulation Conference 2012. Shanghai, China, 2012. 452 p.