



**Ciências
ULisboa**

Faculdade
de Ciências
da Universidade
de Lisboa

Faculdade de Ciências da Universidade de Lisboa

Departamento de Informática

Mestrado em Engenharia Informática e Segurança Informática

RELATÓRIO

Configuração e Gestão de Sistemas

Resource Discovery

Aluno: **Rodrigo Craveiro Rodrigues (fc64370)**

Professor: **Doutor Hugo Miranda**

2º Semestre Letivo 2024/2025

abril 2024

Índice

1. Introdução.....	3
2. Endereços Identificados	3
2.1 Endereços Mac.....	3
2.2 Endereços IP	4
3. Análise de Pacotes por Protocolos	4
3.1 Protocolos Encapsulados no Ethernet	5
3.2 Protocolo TCP/X11	10
3.2.1 Visão Geral da Comunicação X11	10
3.2.2 Análise de Frames X11 Relevantes.....	10
3.3 Spanning Tree Protocol (STP)	17
3.2.1 Visão Geral do STP na Rede.....	18
3.3.2 Análise de Frames STP Relevantes	18
3.4 Address Resolution Protocol (ARP)	20
3.4.1 Visão Geral do ARP na Rede	21
3.4.2 Análise de Frames ARP Relevantes.....	21
3.5 Internetwork Packet Exchange (IPX).....	23
3.5.1 Visão Geral do NetBIOS/IPX na Rede.....	23
3.5.2 Análise de Frames IPX Relevantes	23
3.6 Internet Control Message Protocol (ICMP).....	32
3.6.1 Visão Geral do ICMP na Rede.....	32
3.6.2 Análise de Frames ICMP Relevantes	32
3.6.3 Inferências Topológicas Baseadas em ICMP	35
4. Síntese da Topologia de Rede.....	38
5. Conclusão.....	42

1. Introdução

A análise de tráfego de rede constitui uma ferramenta fundamental. A capacidade de extrair informações significativas de capturas de pacotes permite não apenas resolver problemas operacionais, mas também compreender a estrutura e arquitetura das redes.

A metodologia empregada segue um processo dedutivo estruturado:

1. **Análise individual de frames:** Cada frame é examinado isoladamente para extração de informações de protocolos específicos.
2. **Correlação de informações:** Dados de diferentes frames são interrelacionados para formação de hipóteses sobre conexões e segmentos.
3. **Dedução da topologia:** O processo iterativo de refinamento de hipóteses leva à reconstrução da topologia mais provável.
4. **Validação cruzada:** Informações contraditórias são reconciliadas através de análise comparativa.

2. Endereços Identificados

Os endereços identificados são relativos a pacotes capturados no ficheiro fornecido ("vlan.pcap"), na qual foram filtrados os pacotes especificamente para o *timestamp* 18h20m44s.

2.1 Endereços Mac

MAC	VLANs
00:05:02:71:fc:db	20
00:10:83:1c:64:91	112
00:40:05:1f:14:b3	6
00:40:05:20:76:2f	6
00:40:05:40:ef:24	32
00:50:3e:b4:e4:66	17,104 Cisco
00:60:08:9f:ab:10	7
00:60:08:9f:b1:f3	32
00:60:97:0e:8a:43	6
00:60:97:90:10:20	6
00:60:b0:d5:eb:96	108
00:e0:f9:cc:18:00	32
01:00:0c:cc:cc:cd	17,104

08:00:07:84:12:de	104
-------------------	-----

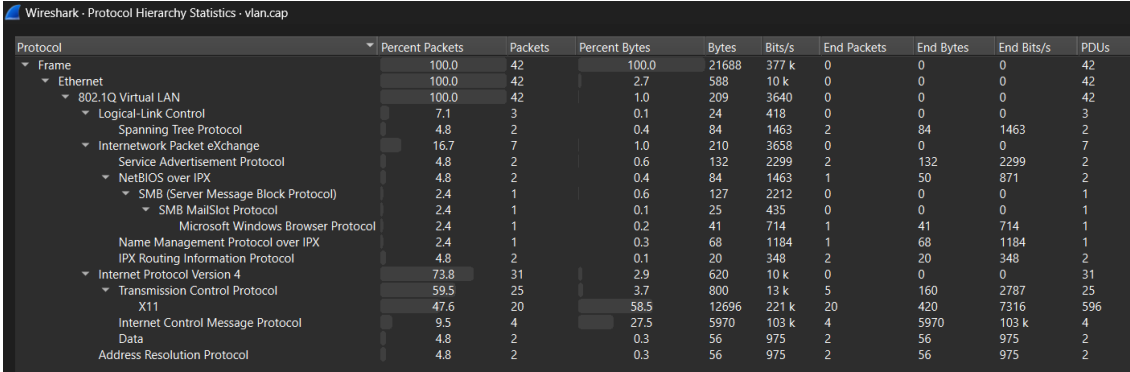
2.2 Endereços IP

IP	VLANs
131.151.6.171	6
131.151.32.21	32
131.151.32.129	32
131.151.1.141	7
131.151.1.7	7
131.151.20.254	20
131.151.20.72	20

3. Análise de Pacotes por Protocolos

Com recurso do **Wireshark** obtivemos a **estatística de hierarquia de protocolos** (*Protocol Hierarchy Statistics*) para os pacotes filtrados especificamente para o *timestamp* 18h20m44s. Esta estatística apresenta uma visão geral dos protocolos utilizados nos pacotes capturados, incluindo a quantidade de pacotes, bytes, taxas de transmissão e percentagens relativas, permitindo uma análise detalhada da composição do tráfego de rede nesse momento específico.

Nota: Neste capítulo, para cada protocolo, é apresentado alguns dos diversos frames/pacotes capturados (com a finalidade de não apresentar todos os frames correspondentes a comunicações similares).



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
▼ Frame	100.0	42	100.0	21688	377 k	0	0	0	42
▼ Ethernet	100.0	42	2.7	588	10 k	0	0	0	42
▼ 802.1Q Virtual LAN	100.0	42	1.0	209	3640	0	0	0	42
▼ Logical-Link Control	7.1	3	0.1	24	418	0	0	0	3
Spanning Tree Protocol	4.8	2	0.4	84	1463	2	84	1463	2
▼ Internetwork Packet eXchange	16.7	7	1.0	210	3658	0	0	0	7
Service Advertisement Protocol	4.8	2	0.6	132	2299	2	132	2299	2
▼ NetBIOS over IPX	4.8	2	0.4	84	1463	1	50	871	2
▼ SMB (Server Message Block Protocol)	2.4	1	0.6	127	2212	0	0	0	1
▼ SMB MailSlot Protocol	2.4	1	0.1	25	435	0	0	0	1
Microsoft Windows Browser Protocol	2.4	1	0.2	41	714	1	41	714	1
Name Management Protocol over IPX	2.4	1	0.3	68	1184	1	68	1184	1
IPX Routing Information Protocol	4.8	2	0.1	20	348	2	20	348	2
▼ Internet Protocol Version 4	73.8	31	2.9	620	10 k	0	0	0	31
▼ Transmission Control Protocol	59.5	25	3.7	800	13 k	5	160	2787	25
X11	47.6	20	58.5	12696	221 k	20	420	7316	596
Internet Control Message Protocol	9.5	4	27.5	5970	103 k	4	5970	103 k	4
Data	4.8	2	0.3	56	975	2	56	975	2
Address Resolution Protocol	4.8	2	0.3	56	975	2	56	975	2

Abaixo, descrevo a hierarquia de protocolos apresentada na Figura acima, explicando cada nível, os protocolos envolvidos, suas quantidades e o que isso indica sobre a rede.

- **Total de Pacotes Capturados (Filtrados):** 42 pacotes.

- **Total de Bytes:** 21.668 bytes.
- **Taxa de Transmissão:** 377 kbits/s.
- **Porcentagem Total:** 100% (todos os pacotes filtrados estão incluídos na análise).

3.1 Protocolos Encapsulados no Ethernet

802.1Q Virtual LAN (VLAN):

- **Porcentagem de Pacotes:** 2,7% (1 pacote).
- **Porcentagem de Bytes:** 2,7% (588 bytes).
- **Taxa de Transmissão:** 10 kbits/s.
- **Descrição:** Apenas 1 pacote foi explicitamente tagueado com 802.1Q, o padrão para VLAN tagging. Isso sugere que a captura inclui tráfego de VLANs, mas a maioria dos pacotes não está tagueada, possivelmente porque a captura foi feita em uma porta de switch configurada como "untagged" ou em um ambiente onde o tagueamento não é visível.

Logical-Link Control (LLC):

- **Porcentagem de Pacotes:** 4,8% (2 pacotes).
- **Porcentagem de Bytes:** 1,0% (209 bytes).
- **Taxa de Transmissão:** 3.640 bits/s.
- **Descrição:** LLC é uma subcamada do modelo OSI que fornece controle de enlace para protocolos como ARP. Esses 2 pacotes provavelmente estão relacionados a tráfego ARP ou outros protocolos que utilizam LLC.

Spanning Tree Protocol (STP):

- **Porcentagem de Pacotes:** 7,1% (3 pacotes).
- **Porcentagem de Bytes:** 0,1% (24 bytes).
- **Taxa de Transmissão:** 418 bits/s.
- **Descrição:** STP é usado para prevenir loops em redes Ethernet comutadas. Os 3 pacotes indicam a presença de switches gerenciando VLANs, enviando BPDUs (Bridge Protocol Data Units) para manter uma topologia livre de loops.

Internetwork Packet Exchange (IPX):

- **Porcentagem de Pacotes:** 16,9% (7 pacotes).
- **Porcentagem de Bytes:** 1,0% (210 bytes).
- **Taxa de Transmissão:** 3.658 bits/s.

- **Descrição:** IPX é um protocolo antigo da Novell, usado em redes antigas para comunicação entre dispositivos. A presença de 7 pacotes indica que a rede suporta sistemas antigos, possivelmente para compatibilidade com servidores ou estações de trabalho mais antigos.

Subprotocolos do IPX:

- **Service Advertisement Protocol (SAP):**
 - **Percentagem de Pacotes:** 4,8% (2 pacotes).
 - **Percentagem de Bytes:** 0,4% (84 bytes).
 - **Taxa de Transmissão:** 1.463 bits/s.
 - **Descrição:** SAP é usado para anunciar serviços (como servidores de ficheiros) em redes IPX. Esses 2 pacotes indicam que há servidores anunciando serviços, como o NetWare Core Protocol.
- **NetBIOS over IPX:**
 - **Percentagem de Pacotes:** 4,8% (2 pacotes).
 - **Percentagem de Bytes:** 0,3% (66 bytes).
 - **Taxa de Transmissão:** 1.149 bits/s.
 - **Descrição:** NetBIOS sobre IPX é usado para partilha de ficheiros e impressoras em redes legadas. Esses pacotes sugerem a presença de servidores de ficheiros (SMB) anunciando seus serviços. É um protocolo que permite que aplicações em diferentes computadores comuniquem através de uma rede local (LAN).
- **Microsoft Windows Browser Protocol:**
 - **Percentagem de Pacotes:** 2,4% (1 pacote).
 - **Percentagem de Bytes:** 0,2% (41 bytes).
 - **Taxa de Transmissão:** 714 bits/s.
 - **Descrição:** Este protocolo é usado para eleições de browser em redes Windows, permitindo que dispositivos descubram outros no mesmo grupo de trabalho (WORKGROUP).
- **SMB (Server Message Block Protocol):**
 - **Percentagem de Pacotes:** 2,4% (1 pacote).
 - **Percentagem de Bytes:** 0,2% (41 bytes).
 - **Taxa de Transmissão:** 714 bits/s.
 - **Descrição:** SMB é usado para partilha de ficheiros e impressoras. Este pacote está relacionado ao tráfego NetBIOS, indicando um servidor de ficheiros ativo.

- **IPX Routing Information Protocol (RIP):**
 - **Porcentagem de Pacotes:** 2,4% (1 pacote).
 - **Porcentagem de Bytes:** 0,1% (20 bytes).
 - **Taxa de Transmissão:** 348 bits/s.
 - **Descrição:** IPX RIP é usado para troca de informações de roteamento em redes IPX. Este pacote indica que há dispositivos (como estações Apple) identificando rotas.

Internet Protocol Version 4 (IPv4):

- **Porcentagem de Pacotes:** 73,8% (31 pacotes).
- **Porcentagem de Bytes:** 2,9% (620 bytes).
- **Taxa de Transmissão:** 10 kbits/s.
- **Descrição:** A maioria do tráfego (73,8%) utiliza IPv4, indicando que a rede suporta comunicações modernas baseadas em IP, como sessões gráficas e testes de conectividade.

Subprotocolos do IPv4:

- **Transmission Control Protocol (TCP):**
 - **Porcentagem de Pacotes:** 35,7% (15 pacotes).
 - **Porcentagem de Bytes:** 3,7% (800 bytes).
 - **Taxa de Transmissão:** 13 kbits/s.
 - **Descrição:** TCP é usado para comunicação confiável. Aqui, todos os 15 pacotes TCP estão relacionados ao protocolo X11.
 - **X11:**
 - **Porcentagem de Pacotes:** 35,7% (15 pacotes).
 - **Porcentagem de Bytes:** 3,7% (800 bytes).
 - **Taxa de Transmissão:** 13 kbits/s.
 - **Descrição:** X11 é um protocolo gráfico para sessões remotas, indicando uma comunicação entre um cliente e um servidor gráfico (131.151.32.21 e 131.151.32.129).
- **Internet Control Message Protocol (ICMP):**
 - **Porcentagem de Pacotes:** 9,5% (4 pacotes).
 - **Porcentagem de Bytes:** 12,4% (2.696 bytes).
 - **Taxa de Transmissão:** 47 kbits/s.

- **Descrição:** ICMP é usado para diagnósticos de rede, como pings. Os 4 pacotes indicam testes de conectividade (Echo Request/Reply).
- **Data:**
 - **Percentagem de Pacotes:** 9,5% (4 pacotes).
 - **Percentagem de Bytes:** 12,4% (2.696 bytes).
 - **Taxa de Transmissão:** 47 kbits/s.
 - **Descrição:** Dados associados ao ICMP, provavelmente payloads de pacotes de ping.
- **Data:**
 - **Percentagem de Pacotes:** 27,3% (11 pacotes).
 - **Percentagem de Bytes:** 58,5% (12.676 bytes).
 - **Taxa de Transmissão:** 221 kbits/s.
 - **Descrição:** Dados não identificados como protocolos específicos, possivelmente fragmentos de pacotes IP ou tráfego não reconhecido.

Address Resolution Protocol (ARP):

- **Percentagem de Pacotes:** 4,8% (2 pacotes).
- **Percentagem de Bytes:** 0,3% (56 bytes).
- **Taxa de Transmissão:** 975 bits/s.
- **Descrição:** ARP resolve endereços IP para MAC. Esses 2 pacotes indicam dispositivos descobrindo outros na mesma sub-rede (131.151.20.72 identificando gateway).

Interpretação Geral:

- **Tráfego Dominante:** O tráfego IPv4 (73,8%) domina, com ênfase em TCP/X11 (35,7%), indicando uma sessão gráfica ativa. ICMP (9,5%) sugere testes de conectividade.
- **Protocolos Antigos:** IPX (16,9%) mostra suporte a sistemas antigos, com NetBIOS/SMB e SAP para partilha de ficheiros e serviços NetWare.
- **VLANs:** Apenas 1 pacote com 802.1Q, mas frames anteriores confirmam VLANs 17 e 104.
- **Topologia:** A rede inclui *switches* (STP), servidores de ficheiros (NetBIOS/SMB), estações gráficas (X11), e dispositivos antigos (IPX), com segmentação por VLANs e sub-redes.

Wireshark - Conversations - vlan.cap																
Conversation Settings																
Name resolution	Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
Absolute start time	00:05:02:71fcdb	00:05:02:71fcdb	1	64 bytes	14	5	20.00%	1	64 bytes	5	0 bytes	0.44335	3.9944	128 bits/s	0	
Limit to display filter	00:10:83:1c6491	00:10:83:1c6491	1	114 bytes	55	1	100.00%	1	114 bytes	0	0 bytes	3.987163	0.0000	0	0 bytes	
	00:40:05:1f14b3	00:40:05:1f14b3	1	98 bytes	22	4	25.00%	1	98 bytes	0	0 bytes	1.174979	3.1831	246 bits/s	0	
	00:40:05:20762f	00:40:05:20762f	1	116 bytes	44	4	25.00%	1	116 bytes	0	0 bytes	2.879372	1.4995	618 bits/s	0	
	00:40:05:40ef24	00:40:05:40ef24	29	18 kB	0	205	14.15%	18	15 kB	11	2 kB	0.000000	4.4464	27 kbps	0	
	00:40:05:40ef24	00:60:97:90:10:20	1	2 kB	8	5	20.00%	1	2 kB	0	0 bytes	0.202191	3.9996	3030 bits/s	0	
	00:50:3eb4e466	01:00:0c:cccccd	2	136 bytes	12	24	8.33%	2	136 bytes	0	0 bytes	0.416157	4.0101	271 bits/s	0	
	00:60:08:9fab:10	00:60:08:9fab:10	1	64 bytes	57	1	100.00%	1	64 bytes	0	0 bytes	4.148517	0.0000	0	0 bytes	
	00:60:97:0e8a:43	00:60:97:0e8a:43	1	210 bytes	42	4	25.00%	1	210 bytes	0	0 bytes	2.499210	1.6223	1035 bits/s	0	
	00:60:b0d5eb:96	00:60:b0d5eb:96	1	114 bytes	56	1	100.00%	1	114 bytes	0	0 bytes	4.064635	0.0000	0	0 bytes	
	00:e0:f9cc:18:00	00:40:05:40ef24	1	2 kB	7	5	20.00%	1	2 kB	0	0 bytes	0.202035	3.9996	3030 bits/s	0	
	08:00:78:412:de	00:60:08:9fab:10	2	128 bytes	52	52	3.85%	2	128 bytes	0	0 bytes	0.003689	4.1714	245 bits/s	0	

Wireshark - Conversations - vlan.cap																
Conversation Settings																
Name resolution	Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
Absolute start time	131.151.6.171	131.151.32.129	2	3 kB	2	10	20.00%	1	2 kB	1	2 kB	0.202035	3.9998	3030 bits/s	3030	
	131.151.32.129	131.151.32.21	29	18 kB	0	205	14.15%	18	15 kB	11	2 kB	0.000000	4.4464	27 kbps	4328	

Wireshark - Conversations - vlan.cap

Conversation Settings

Name resolution

Absolute start time

Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

Bluetooth

BPV

DCPP

Ethernet

FC

FDDI

IEEE 802.11

IEEE 802.15.4

IPV4

IPV6

JITA

LTP

MPTCP

NCP

openSAF

RSPV

SCTP

SLL

TCP

Bluetooth

BPV

DCPP

Ethernet

FC

FDDI

IEEE 802.11

IEEE 802.15.4

IPV4

IPV6

JITA

LTP

MPTCP

NCP

openSAF

RSPV

SCTP

SLL

TCP

Filter list for specific type

Address A	Address B	Packets	Bytes A → B	Bytes B → A	Packets B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00000000.0060972d3231	00000000.mmmmmmm	1	64 bytes	1	64 bytes	0 bytes	3.267804	0.0000	0 bytes
00050500.0020186124ae	00000000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	0.026964	0.0000	0 bytes
00050500.0030186273a1	00000000.mmmmmmm	1	98 bytes	42	4	98 bytes	0.062000	0.0000	0 bytes
00050500.0060609d4c185	00050500.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.627775	0.0000	0 bytes
00050500.006060ab571	00050500.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	0.709441	0.0000	0 bytes
00050500.009021718125	00000000.mmmmmmm	1	92 bytes	1	92 bytes	0 bytes	0.024250	0.0000	0 bytes
00050500.0000006a9978	00050500.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	3.193744	0.0000	0 bytes
00050600.0040051f14b3	00000000.mmmmmmm	4	324 bytes	4	324 bytes	0 bytes	1.174979	3.1831	814 bits/s
00050600.0040051f14b3	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.182587	0.0000	0 bytes
00050600.0040051f14b3	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	3.501412	0.0000	0 bytes
00050600.0040051f14b3	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	2.429507	0.0000	0 bytes
00050600.00400512247	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	3.674734	0.0000	0 bytes
00050600.00400520762f	00000000.mmmmmmm	4	464 bytes	4	464 bytes	0 bytes	2.879372	1.4995	2475 bits/s
00050600.00400520762f	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	0.244249	0.0000	0 bytes
00050600.0060970e8a43	00000000.mmmmmmm	3	294 bytes	3	294 bytes	0 bytes	2.489210	1.6814	2174 bits/s
00050600.0060970e8a43	00050600.mmmmmmm	1	210 bytes	1	210 bytes	0 bytes	4.111554	0.0000	0 bytes
00050600.0060970e8a43	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	0.640453	0.0000	0 bytes
00050600.0060970e8a43	00050600.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	3.243210	0.0000	0 bytes
00050600.0060970e8a43	00050600.mmmmmmm	11	5 kB	11	5 kB	0 bytes	2.577941	0.5721	69 kbps
00052000.00104bad0909	00000000.mmmmmmm	2	334 bytes	2	334 bytes	0 bytes	2.007562	0.0011	0 bytes
00052000.0020186124ae	00000000.mmmmmmm	2	334 bytes	2	334 bytes	0 bytes	3.137112	0.0016	0 bytes
00052000.0030186273a1	00052000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.610794	0.0000	0 bytes
00052000.000000991e38	00052000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	2.965105	0.0000	0 bytes
00056800.0004acc5c5469	00000000.mmmmmmm	2	196 bytes	2	196 bytes	0 bytes	0.383938	0.5407	2899 bits/s
00056800.000608b74b4	00056800.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.201824	0.0000	0 bytes
00056800.000608b74b4	00056800.mmmmmmm	1	92 bytes	1	92 bytes	0 bytes	1.037421	0.0000	0 bytes
00056800.0000078412de	00000000.mmmmmmm	52	3 kB	52	3 kB	0 bytes	0.003689	4.1714	6382 bits/s
00056800.0000095d623a	00056800.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.728378	0.0000	0 bytes
00056800.0000095d623a	00056800.mmmmmmm	1	64 bytes	1	64 bytes	0 bytes	2.265276	0.0000	0 bytes
00056c00.01083574947	00056c00.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.534448	0.0000	0 bytes
00056c00.00400525ee10	00000000.mmmmmmm	4	256 bytes	4	256 bytes	0 bytes	0.173496	1.5018	1363 bits/s
00056c00.0060b07ae0e0	00056c00.mmmmmmm	2	231 bytes	2	231 bytes	0 bytes	2.177604	0.0007	0 bytes
00056c00.0060b07ae0e0	00056c00.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	2.266166	0.0000	0 bytes
00056c00.0060b07ae0e0	00056c00.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	4.064635	0.0000	0 bytes
00056c00.00902177764e	00000000.mmmmmmm	3	2 kB	3	2 kB	0 bytes	0.427046	2.1968	6562 bits/s
00056c00.0000099bcb3a	00056c00.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	2.380776	0.0000	0 bytes
00057000.0010831c6491	00057000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	3.587163	0.0000	0 bytes
00057000.0010831c6491	00057000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.071995	0.0000	0 bytes
00057000.005004b2e82a	00057000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.429048	0.0000	0 bytes
00057000.005004b2e82a	00057000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.179583	0.0000	0 bytes
00057000.0060970e8a43	00000000.mmmmmmm	2	128 bytes	2	128 bytes	0 bytes	1.424294	1.5999	512 bits/s
00057000.0060970e8a43	00057000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	1.663056	0.0000	0 bytes
00057000.0060970e8a43	00057000.mmmmmmm	1	114 bytes	1	114 bytes	0 bytes	3.861005	0.0000	0 bytes

Wireshark - Conversations - vlan.cap																
Conversation Settings																
Name resolution	Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	
Absolute start time	131.151.32.21	6000	131.151.32.129	1173	11	4 kB	1	46	23.91%	5	446 bytes	6	4 kB	0.106124	4.3403	
	131.151.32.129	1162	131.151.32.21	6000	14	10 kB	0	139	10.07%	10	10 kB	4	376 bytes	0.000000	4.0742	

Wireshark - Endpoints - vlan.cap

Endpoint Settings

☐ Name resolution

☒ Limit to display filter

Copy

Map

Ethernet · 15

IPv4 · 3

IPv6

TCP · 3

UDP

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:05:02:71fc:db	1	64 bytes	5	20.00%	1	64 bytes	0	0 bytes
00:10:83:1c64:91	1	114 bytes	1	100.00%	1	114 bytes	0	0 bytes
00:40:05:1f14:b3	1	98 bytes	4	25.00%	1	98 bytes	0	0 bytes
00:40:05:2076:2f	1	116 bytes	4	25.00%	1	116 bytes	0	0 bytes
00:40:05:40ef:24	31	21 kB	215	14.42%	19	17 kB	12	4 kB
00:50:3eb4:e4:66	2	136 bytes	26	7.69%	2	136 bytes	0	0 bytes
00:60:08:9fab:10	1	64 bytes	1	100.00%	1	64 bytes	0	0 bytes
00:60:08:9fb1:f3	29	18 kB	205	14.15%	11	2 kB	18	15 kB
00:60:97:0e8a:43	1	210 bytes	4	25.00%	1	210 bytes	0	0 bytes
00:60:97:9010:20	1	2 kB	5	20.00%	0	0 bytes	1	2 kB
00:60:b0:d5eb:96	1	114 bytes	1	100.00%	1	114 bytes	0	0 bytes
00e0f9cc:1800	1	2 kB	29	3.45%	1	2 kB	0	0 bytes
010000:cceccc:d	2	136 bytes	24	3.33%	0	0 bytes	2	136 bytes
0800:07:84:12:de	2	128 bytes	52	3.85%	2	128 bytes	0	0 bytes
ff:ff:ff:ff:ff:ff	9	908 bytes	147	6.12%	0	0 bytes	9	908 bytes

3.2 Protocolo TCP/X11

O TCP é um protocolo de camada 4 (transporte) que proporciona comunicação confiável e orientada à conexão entre dispositivos. Suas características incluem:

- Estabelecimento de conexão via processo three-way handshake.
- Numeração sequencial de segmentos para garantir entrega ordenada.
- Mecanismos de controle de fluxo e congestionamento.
- Retransmissão de pacotes perdidos ou corrompidos.
- Manutenção de estado da conexão.

No contexto da análise, o TCP transporta tráfego da aplicação X11, fornecendo garantias de entrega para comandos e eventos de interface gráfica.

3.2.1 Visão Geral da Comunicação X11

O X Window System (X11) é um sistema de janelas em rede que implementa o modelo cliente-servidor para interfaces gráficas, predominante em ambientes Unix/Linux. As suas características fundamentais incluem:

- Arquitetura distribuída, permitindo que aplicações executem em servidores remotos enquanto sua interface é exibida localmente.
- Operação na porta TCP padrão 6000.
- Comunicação bidirecional de eventos (do cliente para o servidor) e respostas (do servidor para o cliente).
- Tipologia diversa de eventos como ButtonRelease e ChangeWindowAttributes.

Esta arquitetura permite centralização de processamento com distribuição da interface de utilizador, um modelo particularmente relevante em ambientes académicos e corporativos.

O X11 identificado nos frames capturados representa uma implementação clássica do modelo cliente-servidor para interfaces gráficas em ambientes Unix/Linux. Esta análise revela uma sessão ativa onde eventos de interface gráfica são transmitidos através da rede.

3.2.2 Análise de Frames X11 Relevantes

Os seguintes frames representam uma conversa entre um cliente (endereço IP 131.151.32.129) e um servidor (endereço IP 131.151.32.21) na mesma VLAN (32). Toda a troca de frame está relacionada com o protocolo X11, que utiliza o protocolo de transporte TCP (port de origem 6000, nos dois protocolos). Identifica-se que estes frames possuem um *time to live* igual a 64, logo é possível concluir que o *host* (endereço IP 131.151.32.21) encontrasse na mesma rede LAN em que o frame foi recolhido.

Frame 394: Evento ButtonRelease

```
▶ Frame 394: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
▶ Ethernet II, Src: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3), Dst: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▶ Internet Protocol Version 4, Src: 131.151.32.21, Dst: 131.151.32.129
▶ Transmission Control Protocol, Src Port: 6000, Dst Port: 1173, Seq: 705, Ack: 9325, Len: 32
▼ X11, Event, eventcode: 5 (ButtonRelease)
  eventcode: 5 (ButtonRelease)
  eventbutton: 1
  event-sequencenumber: 714
  time: 1228206676
  rootwindow: 0x00000025
  eventwindow: 0x03400016
  childwindow: 0x00000000
  root-x: 642
  root-y: 501
  event-x: 63
  event-y: 20
▶ modifiers-mask: 0x0100
  same-screen: True
  unused
```

Este frame representa uma comunicação TCP transportando um evento X11 do tipo ButtonRelease, indicando uma interação do utilizador numa sessão gráfica remota.

Detalhes de Endereçamento:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:08:9f:b1:f3 (Fabricante: AniCommunications)
 - MAC de destino: 00:40:05:40:ef:24 (Servidor X11)
- **Camada 3 (Network):**
 - IP de origem: 131.151.32.21
 - IP de destino: 131.151.32.129
 - Máscara de sub-rede (inferida): 255.255.255.0 ou /24
- **Camada 4 (Transport):**
 - Protocolo: TCP
 - Porta de origem: 6000 (porta padrão do servidor X11)
 - Porta de destino: 1173
- **Detalhes X11:**
 - Evento: ButtonRelease (código 5), Botão: 1
 - Coordenadas: Root (642, 501), Evento (20, 20)

Inferências Topológicas Baseadas no Frame 394 e Relação com Outros Frames:

1. **Continuidade da Sessão X11:** Este frame é uma continuação direta das sessões X11 observadas nos Frames 294 e 395, que também envolvem os mesmos dispositivos (131.151.32.21 e 131.151.32.129). A porta de destino 1173 é a mesma do Frame 389, indicando que este evento faz parte da mesma conexão TCP, reforçando a existência de uma sessão gráfica ativa e interativa.
2. **Segmentação por VLAN:** A VLAN 32, identificada neste frame, é consistente com o Frame 389 (também VLAN 32), sugerindo que esta sub-rede (131.151.32.0/24) está segmentada logicamente por VLANs. Comparado com outros frames como o Frame 375

a VLAN 32 pode ser uma configuração específica para tráfego gráfico, possivelmente para isolar ou priorizar este tipo de comunicação.

3. **Relação com Frames ICMP (383 e 384):** Os Frames 383 e 384 mostram testes de conectividade ICMP entre os mesmos dispositivos (131.151.32.129 e 131.151.32.21). É provável que estes testes tenham sido realizados para garantir a fiabilidade da rede antes ou durante a sessão X11, indicando que a conectividade entre cliente e servidor é crítica para a aplicação gráfica.
4. **Ambiente de Rede Local:** A comunicação direta via Camada 2 (MACs distintos) implica a presença de um switch de Camada 2, que encaminha frames entre os dispositivos no mesmo segmento. Este switch também suporta VLANs, como visto em frames STP (391 e 392), sugerindo uma infraestrutura Cisco com PVST+.
5. **Interação Gráfica em Tempo Real:** O evento ButtonRelease, semelhante ao do Frame 294, indica uma aplicação gráfica interativa (ambiente de desktop remoto ou ferramenta de desenvolvimento). A ausência de tráfego IPX ou NetBIOS nestes frames sugere que a sub-rede 131.151.32.0/24 é dedicada a sistemas modernos (Unix/Linux), contrastando com os frames antigos como 385 e 376.

Frame 395: Evento ChangeWindowAttributes

```

> Frame 395: 950 bytes on wire (7600 bits), 950 bytes captured (7600 bits)
> Ethernet II, Src: AniCommunica 40:ef:24 (00:40:05:40:ef:24), Dst: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
> Internet Protocol Version 4, Src: 131.151.32.129, Dst: 131.151.32.21
> Transmission Control Protocol, Src Port: 1173, Dst Port: 6000, Seq: 9325, Ack: 737, Len: 880
> X11, Request, opcode: 2 (ChangeWindowAttributes)
  opcode: ChangeWindowAttributes (2)
  unused
  request-length: 4
  window: 0x03400016
  window-value-mask: 0x00000001, background-pixmap
  background-pixmap: ParentRelative (0x00000001)
> X11, Request, opcode: 61 (ClearArea)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 70 (PolyFillRectangle)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 70 (PolyFillRectangle)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 66 (PolySegment)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 67 (PolyRectangle)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 59 (SetClipRectangles)
> X11, Request, opcode: 74 (PolyText8)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)
> X11, Request, opcode: 56 (ChangeGC)

```

Este frame representa outra comunicação TCP transportando um evento X11 do tipo ChangeWindowAttributes, utilizado para modificar propriedades de uma janela existente.

Detalhes de Endereçamento:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:08:9f:b1 (Fabricante: AniCommunications)
 - MAC de destino: 00:40:05:40:ef:24 (Servidor X11)
- **Camada 3 (Network):**
 - IP de origem: 131.151.32.21

- IP de destino: 131.151.32.129
- **Camada 4 (Transport):**
 - Protocolo: TCP
 - Porta de origem: 6000 (porta padrão do servidor X11)

Inferências Topológicas Baseadas no Frame 395 e Relação com Outros Frames:

1. **Parte da Mesma Sessão X11:** Este frame está relacionado com os Frames 394, 389, e 375, pois envolve os mesmos dispositivos (131.151.32.21 e 131.151.32.129) na sub-rede 131.151.32.0/24. Embora a porta de destino não seja especificada, a consistência de IPs e MACs sugere que faz parte da mesma sessão gráfica ou de uma conexão paralela (como a do Frame 375, porta 1162).
2. **Ausência de VLAN Específica:** Este frame é especificado na VLAN 32, semelhante ao Frame 375. Isso pode indicar que a captura foi feita numa porta de switch para esta sub-rede, o que a VLAN 32 é aplicada a todas as conexões X11.
3. **Relação com Frames ICMP (383 e 384):** Os testes ICMP entre os mesmos dispositivos (Frames 383 e 384) sugerem que a conectividade foi verificada para suportar esta sessão X11. O evento ChangeWindowAttributes, que modifica propriedades de uma janela, requer uma ligação estável, o que pode ter motivado os testes de MTU (Frame 384).
4. **Ambiente Unix/Linux:** A utilização do protocolo X11, consistente com os Frames 394, 389, e 375, reforça que os dispositivos nesta sub-rede são sistemas Unix/Linux, contrastando com os sistemas antigos (IPX/NetBIOS) observados nos Frames 390, 385, 376, 354, e 374.
5. **Switch de Camada 2:** A comunicação direta entre MACs distintos implica um switch de Camada 2, que também gere VLANs (Frames 391 e 392). A ausência de tráfego IPX ou ARP neste frame sugere que esta sub-rede é isolada de outros segmentos (Frames 393, 390).
6. **Natureza Interativa da Sessão:** O evento ChangeWindowAttributes, combinado com o ButtonRelease do Frame 394, indica uma sessão gráfica interativa, possivelmente envolvendo ajustes dinâmicos de janelas (redimensionamento ou reposicionamento) durante a interação do utilizador.

Frame 389: Pacote TCP ACK

```
▶ Frame 389: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▶ Ethernet II, Src: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3), Dst: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▶ Internet Protocol Version 4, Src: 131.151.32.21, Dst: 131.151.32.129
▼ Transmission Control Protocol, Src Port: 6000, Dst Port: 1173, Seq: 705, Ack: 9325, Len: 0
  Source Port: 6000
  Destination Port: 1173
  [Stream index: 1]
  [Stream Packet Number: 44]
  ▼ [Conversation completeness: Incomplete (12)]
    ..0. .... = RST: Absent
    ...0 .... = FIN: Absent
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..0. = SYN-ACK: Absent
    .... ...0 = SYN: Absent
    [Completeness Flags: ..DA..]
  [TCP Segment Len: 0]
  Sequence Number: 705 (relative sequence number)
  Sequence Number (raw): 1369791862
  [Next Sequence Number: 705 (relative sequence number)]
  Acknowledgment Number: 9325 (relative ack number)
  Acknowledgment number (raw): 1372918536
  1000 .... = Header Length: 32 bytes (8)
▶ Flags: 0x010 (ACK)
  Window: 31856
  [Calculated window size: 31856]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xe8c8 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [Timestamps]
▶ [SEQ/ACK analysis]
```

Este frame contém um pacote TCP de confirmação (ACK), associado à sessão X11, garantindo a fiabilidade da comunicação entre o cliente e o servidor gráfico.

Detalhes de Endereçamento:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:08:9f:b1:f3 (Fabricante: AniCommunications)
 - MAC de destino: 00:40:05:40:ef:24 (Servidor X11)
- **Camada 3 (Network):**
 - IP de origem: 131.151.32.21
 - IP de destino: 131.151.32.129
- **Camada 4 (Transport):**
 - Protocolo: TCP
 - Porta de origem: 6000
 - Porta de destino: 1173
 - Flags: ACK (0x10), Comprimento: 0 bytes

Inferências Topológicas Baseadas no Frame 389 e Relação com Outros Frames:

1. **Parte da Mesma Sessão X11:** Este frame está diretamente relacionado com o Frame 394, pois partilha a mesma porta de destino (1173) e os mesmos endereços IP e MAC. O ACK confirma a receção de dados enviados anteriormente (como o evento ButtonRelease do Frame 394), garantindo a continuidade da sessão gráfica.

2. **Consistência de VLAN:** A VLAN 32, presente neste frame e no Frame 394, indica que esta sessão X11 está confinada a um segmento lógico específico. Comparado com o Frame 375 (sem VLAN especificada, mas com a mesma sub-rede), a VLAN 32 pode ser uma configuração aplicada apenas a certas portas do switch, possivelmente para tráfego gráfico prioritário.
3. **Relação com Frames ICMP (383 e 384):** A sub-rede 131.151.32.0/24, onde ocorre esta sessão, também é palco de testes ICMP (Frames 383 e 384). Estes testes podem ter sido realizados para assegurar que a conectividade entre cliente e servidor é estável, especialmente importante para uma sessão gráfica que requer baixa latência.
4. **Infraestrutura de Switching:** A comunicação direta entre MACs distintos (sem roteamento) implica um switch de Camada 2, que também suporta VLANs, como visto nos Frames 391 e 392 (STP para VLANs 17 e 104). A ausência de tráfego IPX ou ARP neste frame sugere que esta sub-rede é isolada de segmentos antigos (Frames 385, 376).
5. **Ambiente Unix/Linux:** A utilização do protocolo X11, consistente com os Frames 294, 395 e 375, reforça que os dispositivos nesta sub-rede (131.151.32.0/24) são sistemas Unix/Linux, contrastando com os sistemas antigos (IPX/NetBIOS) observados em outros frames.

Frame 375: Pacote TCP ACK

```

▶ Frame 375: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▶ Ethernet II, Src: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3), Dst: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▶ Internet Protocol Version 4, Src: 131.151.32.21, Dst: 131.151.32.129
▼ Transmission Control Protocol, Src Port: 6000, Dst Port: 1162, Seq: 6945, Ack: 56781, Len: 0
  Source Port: 6000
  Destination Port: 1162
  [Stream index: 0]
  [Stream Packet Number: 139]
  ▼ [Conversation completeness: Incomplete (12)]
    ..0. .... = RST: Absent
    ...0 .... = FIN: Absent
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..0. = SYN-ACK: Absent
    .... ...0 = SYN: Absent
    [Completeness Flags: ..DA..]
  [TCP Segment Len: 0]
  Sequence Number: 6945 (relative sequence number)
  Sequence Number (raw): 1295871961
  [Next Sequence Number: 6945 (relative sequence number)]
  Acknowledgment Number: 56781 (relative ack number)
  Acknowledgment number (raw): 1310043765
  1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x010 (ACK)
  Window: 31856
  [Calculated window size: 31856]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x4367 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]

```

Este frame contém outro pacote TCP de confirmação (ACK), associado a uma sessão X11, mas com uma porta de destino diferente (1162), indicando uma conexão paralela ou distinta.

Detalhes de Endereçamento:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:08:9f:b1:f3 (Fabricante: 3Com)

- MAC de destino: 00:40:05:40:ef:24 (Servidor X11)
- **Camada 3 (Network):**
 - IP de origem: 131.151.32.21
 - IP de destino: 131.151.32.129
- **Camada 4 (Transport):**
 - Protocolo: TCP
 - Porta de origem: 6000
 - Porta de destino: 1162
 - Flags: ACK (0x10), Comprimento: 0 bytes

Inferências Topológicas Baseadas no Frame 375 e Relação com Outros Frames:

1. **Sessão X11 Paralela:** A porta de destino 1162 é diferente da porta 1173 (Frames 389 e 394), sugerindo que o cliente (131.151.32.21) mantém múltiplas conexões TCP com o servidor X11 (131.151.32.129). Esta multiplicidade de portas pode indicar várias aplicações gráficas ou janelas abertas na mesma sessão, uma prática comum em ambientes X11.
2. **Ausência de VLAN Específica:** Este frame especifica a VLAN 32, o que pode indicar que a captura foi feita numa porta de switch para esta sub-rede, o que a VLAN 32 é aplicada a todas as conexões X11.
3. **Relação com Frames ICMP (383 e 384):** Os testes ICMP entre os mesmos dispositivos (131.151.32.21 e 131.151.32.129) nos Frames 383 e 384 sugerem que a conectividade foi verificada para suportar estas sessões X11, especialmente considerando a necessidade de baixa latência para aplicações gráficas.
4. **Consistência de Sub-rede:** A sub-rede 131.151.32.0/24 é a mesma dos Frames 294, 389, 394, 383 e 384, indicando que este segmento é dedicado a comunicações gráficas modernas, sem interferência de tráfego antigo como IPX (Frames 385, 376, 378 e 372).
5. **Switch de Camada 2:** A comunicação direta entre MACs distintos reforça a presença de um switch de Camada 2, que também gere VLANs (como visto nos Frames 391 e 392). A ausência de tráfego ARP ou IPX neste frame sugere que esta sub-rede é isolada de outros segmentos (Frames 377, 378 e 372).

3.3 Spanning Tree Protocol (STP)

O STP é um protocolo crucial de camada 2 que previne loops em redes com caminhos redundantes. Suas características técnicas incluem:

- Eleição de uma root bridge baseada em prioridade e endereço MAC.
- Estabelecimento de root ports e designated ports.
- Cálculo de custos de caminho para determinar rotas ótimas.
- Bloqueio de portas redundantes para criação de uma topologia livre de loops.

A presença de BPDUs (Bridge Protocol Data Units) revela informações vitais sobre a estrutura de switching da rede.

3.2.1 Visão Geral do STP na Rede

Os frames STP capturados revelam uma implementação sofisticada do Per-VLAN Spanning Tree Plus (PVST+), uma extensão proprietária da Cisco. Esta configuração mantém instâncias independentes de STP para cada VLAN, permitindo engenharia de tráfego avançada e otimização de caminhos por segmento lógico.

3.3.2 Análise de Frames STP Relevantes

Frame 391: BPDU para VLAN 17

```
▶ Frame 391: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
▶ Ethernet II, Src: Cisco_b4:e4:66 (00:50:3e:b4:e4:66), Dst: PVST+ (01:00:0c:cc:cc:cd)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 17
▶ Logical-Link Control
▼ Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Spanning Tree (0)
  BPDU Type: Configuration (0x00)
  ▶ BPDU flags: 0x00
  ▼ Root Identifier: 16384 / 0 / 00:e0:fe:69:9b:10
    Root Bridge Priority: 16384
    Root Bridge System ID Extension: 0
    Root Bridge System ID: Cisco_69:9b:10 (00:e0:fe:69:9b:10)
    Root Path Cost: 4
  ▼ Bridge Identifier: 32768 / 0 / 00:10:2f:17:4e:10
    Bridge Priority: 32768
    Bridge System ID Extension: 0
    Bridge System ID: Cisco_17:4e:10 (00:10:2f:17:4e:10)
    Port identifier: 0x8217
    Message Age: 1
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
  ▼ Originating VLAN (PVID): 17
    Type: Originating VLAN (0x0000)
    Length: 2
    Originating VLAN: 17
```

Este frame contém uma Bridge Protocol Data Unit (BPDU) de configuração, parte do protocolo STP, utilizada para trocar informações sobre a topologia da rede e evitar loops.

Detalhes de Endereçamento e Parâmetros:

Camada 2 (Data-Link):

- MAC de origem: 00:50:3e:b4:e4:66 (Fabricante: Cisco Systems)
- MAC de destino: 01:00:0c:cc:cc:cd (Endereço multicast reservado para STP, PVST+)

Parâmetros STP:

- Bridge ID Root: 00:e0:fe:69:9b:10
- Bridge ID Local: 00:10:2f:17:4e:10
- Custo do Caminho Root: 4
- VLAN ID: 17

Inferências Topológicas Baseadas no Frame 391 e Relação com Outros Frames:

1. **Infraestrutura Cisco com PVST+:** Este frame está relacionado com o Frame 392, pois ambos são BPDUs transmitidas pelo mesmo switch (MAC 00:50:3e:84:e4:66), mas para VLANs diferentes (17 e 104). A utilização de PVST+ (Per-VLAN Spanning Tree Plus)

indica uma infraestrutura Cisco, com instâncias STP independentes por VLAN, permitindo otimização de caminhos. O que se pode concluir que este endpoint é um router. Este router envia o frame por *multicast* para outros routers e na qual está a ser executado em várias VLANs.

2. **Segmentação por VLAN:** Surgiu na vlan 17, e encontra se a 1 *hop* do *root bridge*, visto que a message *age* é iniciada com 0 porem é incrementada sempre que passa por um router, que não é o root bridge. A VLAN 17 é distinta das VLANs 32 (Frames 394, 389), 104 (Frame 392), 7 (Frame 377), e 108 (Frames 354, 374), sugerindo uma rede com segmentação lógica bem definida. A VLAN 17 pode estar associada a um segmento específico, possivelmente para tráfego administrativo ou outro tipo de serviço, diferente do tráfego gráfico (VLAN 32) ou antigo (VLANs 104, 108).
3. **Hierarquia de Switches:** O custo do caminho root (4) indica que este switch não é o root para a VLAN 17, sugerindo a presença de outros switches na topologia, com o switch root (00:e0:fe:69:9b:10) a montante. Comparado com o Frame 392 (VLAN 104, root diferente), a rede utiliza diferentes switches root por VLAN, uma estratégia para balanceamento de carga.
4. **Relação com Tráfego de Dados:** A VLAN 17 não está diretamente associada a nenhum tráfego de dados capturado (X11, IPX, ARP), mas a sua presença implica que o switch suporta múltiplos segmentos lógicos, incluindo aqueles usados por outros frames (VLAN 32 para X11, VLAN 104 para IPX).
5. **Caminhos Redundantes:** A necessidade de STP indica caminhos redundantes na rede, uma característica de designs resilientes. Este switch, que também suporta VLANs 104 (Frame 392), 32 (Frames 394, 389), 7 (Frame 377), e 108 (Frames 354, 374), é provavelmente um switch de distribuição ou acesso numa arquitetura hierárquica.
6. **Contraste com Outros Segmentos:** A ausência de tráfego de dados na VLAN 17, comparada com VLANs ativas como 32 (X11) e 104 (IPX), sugere que esta VLAN pode estar configurada para um propósito específico (gestão de rede) ou que o tráfego associado não foi capturado.

Frame 392: BPDU para VLAN 104

```
▶ Frame 392: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
▶ Ethernet II, Src: Cisco_b4:e4:66 (00:50:3e:b4:e4:66), Dst: PVST+ (01:00:0c:cc:cc:cd)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 104
▶ Logical-Link Control
▼ Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Spanning Tree (0)
  BPDU Type: Configuration (0x00)
  ▶ BPDU flags: 0x00
  ▼ Root Identifier: 4096 / 4094 / 00:e0:fe:69:9b:67
    Root Bridge Priority: 4096
    Root Bridge System ID Extension: 4094
    Root Bridge System ID: Cisco_69:9b:67 (00:e0:fe:69:9b:67)
    Root Path Cost: 4
  ▼ Bridge Identifier: 32768 / 0 / 00:10:2f:17:4e:67
    Bridge Priority: 32768
    Bridge System ID Extension: 0
    Bridge System ID: Cisco_17:4e:67 (00:10:2f:17:4e:67)
    Port identifier: 0x8217
    Message Age: 1
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
  ▼ Originating VLAN (PVID): 104
    Type: Originating VLAN (0x0000)
    Length: 2
    Originating VLAN: 104
```

Este frame contém outra BPDU de configuração, mas para a VLAN 104, demonstrando a utilização de PVST+ para gerir topologias independentes por VLAN.

Detalhes de Endereçamento e Parâmetros:

Camada 2 (Data-Link):

- MAC de origem: 00:50:3e:b4:e4:66 (Fabricante: Cisco Systems)
- MAC de destino: 01:00:0c:cc:cc:cd (Endereço multicast STP padrão)

Parâmetros STP:

- Bridge ID Root: 00:e0:fe:69:9b:67
- Bridge ID Local: 00:10:2f:17:4e:67
- Custo do Caminho Root: 4
- VLAN ID: 104

Inferências Topológicas Baseadas no Frame 392 e Relação com Outros Frames:

1. **Infraestrutura Cisco com PVST+:** Este frame está diretamente relacionado com o Frame 391, pois ambos são BPDUs do mesmo router (MAC 00:50:3e:84:e4:66), mas para VLANs diferentes (104 e 17). A utilização de PVST+ confirma uma infraestrutura Cisco, com topologias STP distintas por VLAN.
2. **Associação com Tráfego IPX (Frame 378 e 372):** A VLAN 104 é a mesma do Frame 378 e 372 (IPX RIP Request), indicando que este segmento lógico suporta tráfego IPX. A sub-rede 131.151.20.0/24 (Frame 393, também associada a um dispositivo Apple) pode estar mapeada para esta VLAN, sugerindo que a VLAN 104 é usada para dispositivos que suportam tanto IP como IPX.
3. **Hierarquia de Routers:** O custo do caminho root (4) e o Bridge ID Root diferente (00:e0:fe:69:9b:67) do Frame 391 indicam que a VLAN 104 tem um router root distinto, reforçando a estratégia de balanceamento de carga por VLAN. Este switch (00:10:2f:17:4e:67) é provavelmente um switch de distribuição ou acesso, conectado a outros switches na topologia. Encontra-se a 1 hop da *root bridge*, visto que a *message age* é iniciada com 0, porém é incrementada sempre que passa por um router que não é a *root bridge*.
4. **Segmentação por VLAN:** A VLAN 104 é distinta das VLANs 17 (Frame 391), 32 (Frames 394, 389), 7 (Frame 377), e 108 (Frames 354, 374), expandindo a segmentação lógica da rede. A VLAN 104 parece ser dedicada a tráfego antigo (IPX), contrastando com a VLAN 32 (X11) e a VLAN 7 (ARP).
5. **Caminhos Redundantes:** A presença de STP indica caminhos redundantes, e a VLAN 104, associada a tráfego IPX (Frame 378 e 372), sugere que este segmento é parte de uma topologia maior, possivelmente conectada a outros segmentos IPX (Frames 385, 376, 354, 374).
6. **Relação com Outros Segmentos:** A VLAN 104, usada para tráfego IPX, é isolada do tráfego X11 (VLAN 32, Frames 394, 389) e de outras sub-redes como 131.151.1.0/24 (Frame 377), indicando uma segmentação clara entre tráfego moderno e antigo, implementada por VLANs e configuração de switch.

3.4 Address Resolution Protocol (ARP)

O ARP é um protocolo essencial que mapeia endereços IP (camada 3) para endereços MAC (camada 2) em redes locais. Elementos técnicos relevantes incluem:

- Requisições ARP são enviadas em broadcast para toda a rede local.
- Respostas ARP são enviadas em unicast diretamente ao solicitante.
- As entradas ARP são armazenadas temporariamente em cache nos dispositivos.

- Solicitações ARP para gateways indicam intenção de comunicação inter-redes.

A análise de frames ARP permite identificar dispositivos ativos e suas relações com gateways.

3.4.1 Visão Geral do ARP na Rede

O protocolo ARP desempenha papel crucial na resolução de endereços IP para endereços MAC, possibilitando a comunicação na camada 2. As mensagens ARP capturadas revelam aspectos significativos da comunicação inter-sub-redes na infraestrutura analisada.

3.4.2 Análise de Frames ARP Relevantes

Frame 377: Requisição ARP

```

▶ Frame 377: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
▶ Ethernet II, Src: 3Com_9f:ab:10 (00:60:08:9f:ab:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 7
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 3Com_9f:ab:10 (00:60:08:9f:ab:10)
  Sender IP address: 131.151.1.7
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 131.151.1.141

```

Este frame contém uma requisição ARP, indicando que um dispositivo está a tentar resolver o endereço MAC de outro dispositivo numa sub-rede distinta.

Detalhes de Endereçamento e Parâmetros:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:08:9f:ab:10 (Fabricante: 3Com)
 - MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)
- **Parâmetros ARP:**
 - Endereço IP de origem: 131.151.1.7
 - Endereço IP de destino: 131.151.1.141
 - Tipo de Operação: Requisição ARP (1)
 - Pergunta: "Quem tem o IP 131.151.1.141? Informe a 131.151.1.7"

Inferências Topológicas Baseadas no Frame 377 e Relação com Outros Frames:

1. **Nova Sub-rede:** A sub-rede 131.151.1.0/24 é distinta das sub-redes 131.151.32.0/24 (Frames 294, 375, 389, 394, 383, 384) e 131.151.20.0/24 (Frame 393), indicando uma segmentação adicional na rede. Esta sub-rede está associada à VLAN 7, expandindo a diversidade de VLANs observadas (17, 32, 104, 108).
2. **Relação com Frame 393:** O Frame 393 também é uma requisição ARP, mas na sub-rede 131.151.20.0/24, identificando gateway 131.151.20.254. A presença de requisições ARP em sub-redes diferentes (131.151.1.0/24 e 131.151.20.0/24) sugere que a rede é composta por múltiplos segmentos IP, possivelmente mapeados para VLANs distintas (VLAN 7 e VLAN 104, respetivamente).

3. **Segmentação por VLAN:** A VLAN 7, associada a este frame, é distinta das VLANs 17 (Frame 391), 32 (Frames 389, 394), 104 (Frames 392, 378 e 372) e 108 (Frames 354, 374), indicando uma infraestrutura com segmentação lógica bem definida, provavelmente gerida por switches Cisco (como sugerido pelos Frames 391 e 392).
4. **Comunicação Intra-sub-rede:** A requisição ARP indica que o dispositivo 131.151.1.7 está a tentar comunicar com outro dispositivo na mesma sub-rede (131.151.1.141), sem necessidade de roteamento. Isto implica a presença de um switch de Camada 2, que também suporta VLANs, como visto nos Frames 391 e 392.
5. **Contraste com Tráfego Moderno e Antigo:** A sub-rede 131.151.1.0/24 não apresenta tráfego X11 (Frames 294, 375, 389, 394) ou IPX (Frames 385, 376, 378 e 372, 354, 374), sugerindo que este segmento pode ser dedicado a um tipo específico de tráfego, possivelmente administrativo ou de gestão, isolado dos segmentos gráfico e antigo.

Frame 393: Requisição ARP

```

▶ Frame 393: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
▶ Ethernet II, Src: Apple_71:fc:db (00:05:02:71:fc:db), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 20
    000. .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... = DEI: Ineligible
    .... 0000 0001 0100 = ID: 20
    Length: 36
    ▶ Trailer: 555555555555555555555555
▼ Logical-Link Control
    ▶ DSAP: SNAP (0xaa)
    ▶ SSAP: SNAP (0xaa)
    ▶ Control field: U, func=UI (0x03)
    Organization Code: 00:00:00 (Officially Xerox, but 0:0:0:0:0:0 is more common)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Apple_71:fc:db (00:05:02:71:fc:db)
    Sender IP address: 131.151.20.72
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 131.151.20.254

```

Este frame contém uma requisição ARP, identificando o endereço MAC do gateway da sub-rede, indicando intenção de comunicação além do segmento local.

Detalhes de Endereçamento e Parâmetros:

Camada 2 (Data-Link):

- MAC de origem: 00:05:02:71:fc (Fabricante: Apple Computer)
- MAC de destino: ff:ff:ff:ff:ff:ff (Endereço broadcast)

Parâmetros ARP:

- Endereço IP de origem: 131.151.20.72
- Endereço IP de destino/alvo: 131.151.20.254
- Tipo de Operação: Requisição ARP (1)
- **Pergunta:** "Quem tem o IP 131.151.20.254? Informe a 131.151.20.72"

Inferências Topológicas Baseadas no Frame 393 e Relação com Outros Frames:

1. **Nova Sub-rede:** A sub-rede 131.151.20.0/24 é distinta das sub-redes 131.151.32.0/24 (Frames 394, 395, 389, 375, 383, 384) e 131.151.1.0/24 (Frame 377), indicando uma segmentação adicional na rede. Esta sub-rede está possivelmente associada à VLAN 104, como sugerido pelo Frame 392 (STP) e Frame 378 e 372 (IPX RIP).
2. **Relação com Frame 378 e 372 (IPX RIP):** O MAC de origem (00:05:02:71:fc, Apple) é o mesmo do Frame 378 e 372, que também está na VLAN 104 e utiliza IPX. Isso sugere que o dispositivo Apple (131.151.20.72) suporta tanto IP como IPX, operando num segmento misto que inclui tráfego moderno (IP) e antigo (IPX).
3. **Gateway e Roteamento:** O endereço 131.151.20.254 é quase certamente um gateway, dado o seu papel como alvo da requisição ARP. Este gateway pode conectar a sub-rede 131.151.20.0/24 a outras sub-redes, como 131.151.32.0/24 (X11) ou 131.151.1.0/24 (Frame 377), indicando uma rede hierárquica com roteamento inter-VLAN.
4. **Relação com Frame 377 (ARP):** O Frame 377 também é uma requisição ARP, mas na sub-rede 131.151.1.0/24 (VLAN 7). A presença de requisições ARP em sub-redes diferentes sugere que a rede é composta por múltiplos segmentos IP, mapeados para VLANs distintas (VLAN 7 e VLAN 104), e que o roteamento inter-VLAN é necessário para comunicação entre sub-redes.
5. **Segmentação por VLAN:** A associação potencial com a VLAN 104 (Frames 392, 378 e 372) indica que esta sub-rede está segmentada logicamente, separada de outros segmentos como a VLAN 32 (X11, Frames 394, 389) e a VLAN 108 (IPX, Frames 354, 374).
6. **Ambiente Heterogêneo:** A presença de um dispositivo Apple, combinada com tráfego IPX na mesma VLAN (Frame 378 e 372), e a ausência de tráfego X11 ou NetBIOS neste segmento, sugere que a sub-rede 131.151.20.0/24 é um segmento misto, suportando dispositivos modernos e antigos, mas isolado de outros tipos de tráfego (X11 na sub-rede 131.151.32.0/24).

3.5 Internetwork Packet Exchange (IPX)

O NetBIOS sobre IPX representa uma tecnologia híbrida que permite serviços NetBIOS tradicionais (compartilhamento de arquivos e impressoras) em redes Novell NetWare baseadas em IPX. Características técnicas incluem:

- Encapsulamento de mensagens NetBIOS em pacotes IPX.
- Suporte a broadcasts de nomes para descoberta de serviços.
- Identificação de serviços via sufixos de nomes.
- Operação sem dependência do protocolo TCP/IP.

3.5.1 Visão Geral do NetBIOS/IPX na Rede

A presença de tráfego NetBIOS encapsulado sobre o protocolo IPX revela aspectos históricos significativos da rede analisada. Esta combinação indica a manutenção de compatibilidade com sistemas antigos em um ambiente possivelmente em transição tecnológica.

3.5.2 Análise de Frames IPX Relevantes

Frame 390: NetBIOS sobre IPX

```

▶ Frame 390: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
▶ Ethernet II, Src: AniCommunica_20:76:2f (00:40:05:20:76:2f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 6
▼ Internetwork Packet eXchange
  Checksum: 0xffff
  Length: 98 bytes
  Transport Control: 0 hops
  Packet Type: NetBIOS Broadcast (0x14)
  Destination Network: 00 (0x00000000)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: NWLink SMB Name Query (0x0551)
  Source Network: 00 (0x00005060)
  Source Node: AniCommunica_20:76:2f (00:40:05:20:76:2f)
  Source Socket: NWLink SMB Name Query (0x0551)
▼ Name Management Protocol over IPX
  Opcode: Claim name (0xf1)
  Name Type: Machine (0x01)
  Message ID: 0x0000
  ▶ Requested name: MCS207-243<20> (Server service)
  ▶ Source name: MCS207-243<20> (Server service)

```

Este frame contém tráfego NetBIOS encapsulado sobre IPX, indicando a presença de um servidor de ficheiros num ambiente antigo.

Detalhes de Endereçamento e Parâmetros:

Camada 2 (Data-Link):

- MAC de origem: 00:40:05:20:76:2f (Fabricante: ANI Communications)
- MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)

Parâmetros IPX:

- Rede IPX: 0x00005060

Parâmetros NetBIOS:

- Nome do servidor: MCS207-243
- Tipo de serviço: <20> (serviço de compartilhamento de ficheiros)

Inferências Topológicas Baseadas no Frame 390 e Relação com Outros Frames:

1. **Segmento IPX Antigo:** Este frame está relacionado com os Frames 385, 376, 378 e 372, 354, e 374, pois todos apresentam tráfego IPX. A rede IPX 0x00005060 é a mesma dos Frames 385 e 376, indicando que este segmento suporta múltiplos servidores antigos (MCS207-243, MCS207-249-AFS, HIMALAYA).
2. **Relação com Frame 385 (NetBIOS/IPX):** O Frame 385 também utiliza a rede IPX 0x00005060, mas apresenta um servidor diferente (MCS207-249-AFS). Ambos os frames indicam serviços de partilha de ficheiros via NetBIOS, sugerindo que esta rede IPX é dedicada a servidores de ficheiros NetWare.
3. **Relação com Frame 376 (NetBIOS/IPX):** O Frame 376, também na rede IPX 0x00005060, apresenta um servidor Windows (HIMALAYA) anunciando serviços SMB. A coexistência de servidores NetWare (MCS207-243, MCS207-249-AFS) e Windows (HIMALAYA) na mesma rede IPX sugere um ambiente heterogêneo, com suporte a sistemas de várias gerações.
4. **Contraste com Frames 354 e 374 (SAP):** Os Frames 354 e 374 utilizam uma rede IPX diferente (0x000056c0) e estão na VLAN 108, indicando que a infraestrutura IPX é composta por múltiplas redes lógicas. A rede 0x00005060 (Frames 390, 385, 376) pode ser um segmento mais amplo, na VLAN 6, enquanto a rede 0x000056c0 (VLAN 108) é mais restrita.
5. **Relação com Frame 378 e 372 (IPX RIP):** O Frame 378 e 372 (VLAN 104) mostra um dispositivo Apple identificandorotas IPX, possivelmente para aceder a servidores como MCS207-243. A ausência de VLAN neste frame (e nos Frames 385, 376) sugere que a

rede IPX 0x00005060 pode não estar restrita a uma VLAN específica, ou que a captura foi feita numa porta "untagged".

6. **Isolamento de Tráfego Moderno:** A rede IPX 0x00005060 é distinta das sub-redes IP como 131.151.32.0/24 (Frames 394, 395, 389, 375, 383, 384), indicando uma segmentação clara entre tráfego antigo e moderno, possivelmente implementada por VLANs ou configuração de switch.

Frame 385: NBIXPX - NetBIOS sobre IPX

```
▶ Frame 385: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: AniCommunica_1f:14:b3 (00:40:05:1f:14:b3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 6
▼ Internetwork Packet eXchange
  Checksum: 0xffff
  Length: 80 bytes
  Transport Control: 0 hops
  Packet Type: NetBIOS Broadcast (0x14)
  Destination Network: 00 (0x00000000)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: NetBIOS (0x0455)
  Source Network: 00 (0x00005060)
  Source Node: AniCommunica_1f:14:b3 (00:40:05:1f:14:b3)
  Source Socket: NetBIOS (0x0455)
▼ NetBIOS over IPX
  IPX Network: 00 (0x00010000)
  ▶ Name type flag: 0x00
  Packet Type: Find name (0x01)
  ▶ Name: MCS207-249-AFS<20> (Server service)
```

Este frame contém tráfego NetBIOS encapsulado sobre IPX, representando um pedido de descoberta de nome (Find Name Request) para localizar serviços de partilha de ficheiros.

Detalhes de Endereçamento e Parâmetros:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:40:05:1f:14:b3 (Fabricante: AniCommunications)
 - MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)
- **Parâmetros IPX:**
 - Rede IPX: 0x00005060
 - Tipo de Pacote: NetBIOS Broadcast (0x14)
- **Parâmetros NetBIOS:**
 - Tipo de Pacote: Find Name (0x01)
 - Nome do servidor: MCS207-249-AFS<20> (Serviço de partilha de ficheiros)

Inferências Topológicas Baseadas no Frame 385 e Relação com Outros Frames:

1. **Descoberta de Serviços Antigos:** Este frame está relacionado com o Frame 390, que também mostra tráfego NetBIOS sobre IPX na mesma rede IPX (0x00005060), mas com um servidor diferente (MCS207-243). O pedido Find Name indica que um cliente IPX está a tentar localizar o servidor MCS207-249-AFS, sugerindo que esta rede suporta múltiplos servidores de ficheiros antigos.

2. **Relação com Frame 376:** O Frame 376 também apresenta tráfego NetBIOS sobre IPX na mesma rede (0x00005060), mas com um servidor Windows (HIMALAYA) anunciando serviços SMB. A coexistência de servidores NetWare (MCS207-249-AFS) e Windows (HIMALAYA) na mesma rede IPX sugere um ambiente heterogêneo, com suporte a sistemas de várias gerações.
3. **Segmento IPX Distinto:** A rede IPX 0x00005060 é distinta das redes IP (131.151.32.0/24 dos Frames 294, 375, 389, 394), indicando que o tráfego IPX opera num segmento lógico separado, possivelmente sobreposto fisicamente mas isolado por configuração de VLAN ou switch.
4. **Ausência de VLAN Específica:** Diferentemente dos Frames 378 e 372 (VLAN 104) e 354/374 (VLAN 108), este frame especifica na VLAN 6.
5. **Contraste com Tráfego Moderno:** A sub-rede 131.151.32.0/24 (Frames 294, 375, 389, 394, 383, 384) é dedicada a sistemas modernos (X11, ICMP), enquanto este frame e outros IPX (376, 378 e 372, 354, 374) indicam um segmento antigo, sugerindo uma rede em transição tecnológica.

Frame 376: Browser - NetBIOS sobre IPX - Escrita em Mailslot SMB

```
▶ Frame 376: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
▶ Ethernet II, Src: 3Com_0e:8a:43 (00:60:97:0e:8a:43), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 6
▼ Internetwork Packet eXchange
  Checksum: 0xffff
  Length: 191 bytes
  Transport Control: 0 hops
  Packet Type: PEP (0x04)
  Destination Network: 00 (0x00050600)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: NetBIOS (0x0455)
  Source Network: 00 (0x00050600)
  Source Node: 3Com_0e:8a:43 (00:60:97:0e:8a:43)
  Source Socket: NetBIOS (0x0455)
▼ NetBIOS over IPX
  ▶ Connection control: 0x00
  ▶ Packet Type: Directed datagram (0x0b)
  ▶ Receiver's Name: HIMALAYA<00> (Workstation/Redirector)
  ▶ Sender's Name: <01><02>__MSBROWSE__<02><01> (Browser)
▼ SMB (Server Message Block Protocol)
  ▶ SMB Header
  ▶ Trans Request (0x25)
▼ SMB MailSlot Protocol
  Opcode: Write Mail Slot (1)
  Priority: 1
  Class: Unreliable & Broadcast (2)
  Size: 58
  Mailslot Name: \MAILSLOT\BROWSE
▼ Microsoft Windows Browser Protocol
  Command: Domain/Workgroup Announcement (0x0c)
  Update Count: 0
  Update Periodicity: 15 minutes
  Domain/Workgroup: WORKGROUP
  Windows version:
  OS Major Version: 3
  OS Minor Version: 10
  ▶ Server Type: 0x80001000, NT Workstation, Domain Enum
  Mysterious Field: 0x01c1ff68
  Master Browser Server Name: HIMALAYA
```

Este frame contém tráfego NetBIOS encapsulado sobre IPX, representando uma escrita em mailslot SMB para anunciar um grupo de trabalho Windows. Utilizado em redes Windows para *resource discovery*, contendo informações como nomes de domínio ou *workgroups*. Indica que existe uma máquina na VLAN 6, com o nome HIMALAYA, que possui a role MSBROWSE (*master browser*), que se encontra no *workgroup* (nome "WORKGROUP").

Detalhes de Endereçamento e Parâmetros:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:97:0e:8a:43 (Fabricante: 3Com)
 - MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)
- **Parâmetros IPX:**
 - Rede IPX: 0x00005060
 - Tipo de Pacote: PEP (0x04)

- **Parâmetros NetBIOS/SMB:**

- Receptor: HIMALAYA<00>, Emissor: <01><02>MSBROWSE<02><01>
- Mailslot: \MAILSLOT\BROWSE
- Comando: Anúncio de Domínio/Grupo de Trabalho (0x8c)
- Domínio: WORKGROUP

Inferências Topológicas Baseadas no Frame 376 e Relação com Outros Frames:

1. **Anúncio de Serviços Windows:** Este frame está relacionado com os Frames 385 e 390, pois todos utilizam a rede IPX 0x00005060 para tráfego NetBIOS. Enquanto os Frames 385 e 390 mostram servidores NetWare (MCS207-249-AFS e MCS207-243), este frame apresenta um servidor Windows (HIMALAYA), indicando que a rede IPX suporta tanto sistemas NetWare como Windows antigos.
2. **Relação com Frames 354 e 374:** Os Frames 354 e 374 mostram tráfego SAP na rede IPX 0x000056c0, sugerindo que a infraestrutura IPX é composta por múltiplas redes lógicas (0x00005060 e 0x000056c0). A coexistência de NetBIOS e SAP indica que a rede suporta diversos serviços antigos, desde partilha de ficheiros (NetBIOS) até anúncios de serviços NetWare (SAP).
3. **Segmento IPX Isolado:** A rede IPX 0x00005060 é distinta das redes IP (131.151.32.0/24 dos Frames 294, 375, 389, 394), reforçando que o tráfego IPX opera num segmento lógico separado, mapeado para a VLAN.
4. **Contraste com Tráfego Moderno:** A sub-rede 131.151.32.0/24 (Frames 294, 375, 389, 394, 383, 384) é dedicada a sistemas modernos, enquanto este frame e outros IPX (385, 378 e 372, 354, 374) indicam um segmento antigo, sugerindo uma rede com segmentação clara entre tráfego moderno e antigo.
5. **Ambiente Heterogêneo:** A presença de um servidor Windows (HIMALAYA) anunciando serviços SMB, em conjunto com servidores NetWare (Frames 385, 390, 354, 374), reforça a natureza mista da rede, com suporte a sistemas de várias gerações.

Frame 378 e 372: Pedido IPX RIP

```
▶ Frame 378: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
▶ Ethernet II, Src: Apple_84:12:de (08:00:07:84:12:de), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 104
▼ Internetwork Packet eXchange
  Checksum: 0xffff
  Length: 40 bytes
  Transport Control: 0 hops
  Packet Type: RIP (0x01)
  Destination Network: 00 (0x00000000)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: RIP (0x0453)
  Source Network: 00 (0x000056800)
  Source Node: Apple_84:12:de (08:00:07:84:12:de)
  Source Socket: RIP (0x0453)
▼ IPX Routing Information Protocol
  RIP packet type: Request (1)
  Route Vector: 00 (0x00052584)
  Hops: 65535
  Ticks: 3640833 ms
```

Este frame contém um pedido RIP (*Routing Information Protocol*) sobre IPX, utilizado por um dispositivo para descobrir rotas numa rede IPX.

Detalhes de Endereçamento e Parâmetros:

- **Camada 2 (Data-Link):**
 - MAC de origem: 08:00:07:84:12:de (Fabricante: Apple)
 - MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)
- **Parâmetros IPX:**
 - Tipo de Pacote: RIP (0x01)
 - Tipo RIP: Request (1)

Inferências Topológicas Baseadas no Frame 378 e 372 e Relação com Outros Frames:

1. **Dispositivo Apple num Segmento IPX:** O MAC de origem (Apple) é o mesmo do Frame 393, que também é uma requisição ARP na sub-rede 131.151.20.0/24. A presença deste dispositivo em ambos os contextos (IPX e IP) sugere que ele suporta múltiplos protocolos, possivelmente como uma estação de trabalho MacOS num ambiente heterogéneo.
2. **Associação com VLAN 104:** A VLAN 104, identificada neste frame, é a mesma do Frame 392 (STP), indicando que este segmento IPX está mapeado para a VLAN 104. A sub-rede 131.151.20.0/24 (Frame 393) pode estar associada a esta VLAN, sugerindo que o dispositivo Apple opera tanto em IP como em IPX neste segmento.
3. **Relação com Frames 385, 376, 354 e 374:** Este frame complementa o tráfego IPX observado nos Frames 385, 376, 354 e 374, mas numa rede IPX diferente (não especificada aqui, mas distinta de 0x00005060 e 0x000056c0). O pedido RIP indica que o dispositivo Apple está a tentar encontrar rotas para outros nós IPX, possivelmente para

aceder a servidores como MCS207-249-AFS (Frame 385) ou HIMALAYA (Frame 376).

4. **Segmento Antigo Isolado:** O tráfego IPX neste frame e nos Frames 385, 376, 354 e 374 é isolado do tráfego IP moderno (Frames 294, 375, 389, 394, 383, 384), sugerindo uma segmentação clara entre sistemas antigos e modernos, possivelmente implementada por VLANs ou configuração de switch.
5. **Infraestrutura de Rede:** A presença de tráfego IPX em VLAN 104, combinada com STP (Frame 392), indica que a rede suporta caminhos redundantes e segmentação lógica, gerida por switches Cisco, como sugerido pelos Frames 391 e 392.

Frames 354 e 374: Resposta Geral SAP

```
▶ Frame 354: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
▼ Ethernet II, Src: HewlettPacka_1c:64:91 (00:10:83:1c:64:91), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: HewlettPacka_1c:64:91 (00:10:83:1c:64:91)
    Type: 802.1Q Virtual LAN (0x8100)
    [Stream index: 55]
  ▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 112
▼ Internetwork Packet eXchange
  Checksum: 0xffff
  Length: 96 bytes
  Transport Control: 0 hops
  Packet Type: IPX (0x00)
  Destination Network: 00 (0x00057000)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: SAP (0x0452)
  Source Network: 00 (0x00057000)
  Source Node: HewlettPacka_1c:64:91 (00:10:83:1c:64:91)
  Source Socket: SAP (0x0452)
▼ Service Advertisement Protocol
  SAP packet type: General Response (2)
  ▶ Server: 0010831C649102D1UMR-MAEM-MEX121
```

Estes frames contêm respostas gerais do protocolo SAP (Service Advertisement Protocol) sobre IPX, anunciando serviços disponíveis num ambiente NetWare.

Detalhes de Endereçamento e Parâmetros:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:10:83:1c:64:91 (Fabricante: Hp-UxE90)
 - MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)
- **Parâmetros IPX:**
 - Rede IPX: 0x000056c0
 - Tipo de Pacote: IPX (0x00), Socket: SAP (0x0452)
- **Parâmetros SAP:**
 - Tipo: General Response (2)
 - Servidor: 0010831C649102D1UMR-MAEM-MEX121

```

▶ Frame 374: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
▶ Ethernet II, Src: HewlettPacka_d5:eb:96 (00:60:b0:d5:eb:96), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 108
▼ Internetwork Packet eXchange
  Checksum: 0xffff
  Length: 96 bytes
  Transport Control: 0 hops
  Packet Type: IPX (0x00)
  Destination Network: 00 (0x00056c00)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: SAP (0x0452)
  Source Network: 00 (0x00056c00)
  Source Node: HewlettPacka_d5:eb:96 (00:60:b0:d5:eb:96)
  Source Socket: SAP (0x0452)
▼ Service Advertisement Protocol
  SAP packet type: General Response (2)
  ▶ Server: 0060B0D5EB9602CYUMR-MCNUTT119-HP4K

```

Estes frames contêm respostas gerais do protocolo SAP (Service Advertisement Protocol) sobre IPX, anunciando serviços disponíveis num ambiente NetWare.

Detalhes de Endereçamento e Parâmetros:

- **Camada 2 (Data-Link):**
 - MAC de origem: 00:60:8b:d5:eb:96 (Fabricante: Hewlett Packard)
 - MAC de destino: ff:ff:ff:ff:ff:ff (Broadcast)
- **Parâmetros IPX:**
 - Rede IPX: 0x000056c0
 - Tipo de Pacote: IPX (0x00), Socket: SAP (0x0452)
- **Parâmetros SAP:**
 - Tipo: General Response (2)
 - Servidor: 00b0b0D5EB9692CYUMR-MCNUTT119-HP4K

Inferências Topológicas Baseadas nos Frames 354 e 374 e Relação com Outros Frames:

1. **Servidor NetWare num Segmento IPX:** Estes frames estão relacionados com os Frames 385 e 376, pois todos apresentam tráfego IPX, mas numa rede IPX diferente (0x000056c0 vs. 0x00005060). O servidor YUMR-MCNUTT119-HP4K anuncia serviços via SAP, complementando os serviços NetBIOS dos Frames 385 e 376, indicando que a infraestrutura IPX suporta múltiplos tipos de serviços antigos.
2. **Associação com VLAN 108:** A VLAN 108, identificada nestes frames, é distinta das VLANs 7 (Frame 377), 17 (Frame 391), 32 (Frames 389, 394) e 104 (Frames 392, 378 e 372), sugerindo uma segmentação lógica adicional para tráfego IPX. Esta VLAN pode ser dedicada a servidores NetWare, isolando-os de outros tipos de tráfego.
3. **Relação com Frame 378 e 372:** O Frame 378 e 372 (IPX RIP na VLAN 104) indica que dispositivos como o Apple (08:00:07:84:12:de) estão a procurar rotas IPX, possivelmente para aceder a servidores como YUMR-MCNUTT119-HP4K. A coexistência de RIP e SAP

sugere uma rede IPX ativa com roteamento dinâmico e anúncios de serviços.

4. **Segmento Antigo Isolado:** O tráfego IPX nestes frames e nos Frames 385, 376 e 378 e 372 é isolado do tráfego IP moderno (Frames 294, 375, 389, 394, 383, 384), reforçando a segmentação entre sistemas antigos e modernos, possivelmente implementada por VLANs ou configuração de switch.
5. **Ambiente Heterogêneo:** A presença de um servidor HP (NetWare) em conjunto com servidores NetWare (Frames 385, 390) e Windows (Frame 376) indica uma rede com suporte a sistemas de várias gerações.

3.6 Internet Control Message Protocol (ICMP)

3.6.1 Visão Geral do ICMP na Rede

O protocolo ICMP (Internet Control Message Protocol) é utilizado para diagnóstico e controle na camada de rede, permitindo que dispositivos testem a conectividade e reportem erros. Foram observados na captura 6 pacotes relacionados com este protocolo (2 *request* e 2 *replies*), na qual 2 resultados de fragmentação.

3.6.2 Análise de Frames ICMP Relevantes

Frame 379: ICMP Echo Request

```
▶ Frame 379: 1515 bytes on wire (12120 bits), 1515 bytes captured (12120 bits)
▼ Ethernet II, Src: Cisco_cc:18:00 (00:e0:f9:cc:18:00), Dst: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
  ▶ Destination: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
  ▶ Source: Cisco_cc:18:00 (00:e0:f9:cc:18:00)
  Type: 802.1Q Virtual LAN (0x8100)
  [Stream index: 7]
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▼ Internet Protocol Version 4, Src: 131.151.6.171, Dst: 131.151.32.129
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1497
  Identification: 0x4368 (17256)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 63
  Protocol: ICMP (1)
  Header Checksum: 0x0462 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 131.151.6.171
  Destination Address: 131.151.32.129
  [Stream index: 2]
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xffff [correct]
  [Checksum Status: Good]
  Identifier (BE): 53249 (0xd001)
  Identifier (LE): 464 (0x01d0)
  Sequence Number (BE): 34078 (0x851e)
  Sequence Number (LE): 7813 (0x1e85)
  [Response frame: 380]
  Timestamp from icmp data: Nov 5, 1999 19:26:48.173387000 Hora padrão de GMT
  [Timestamp from icmp data (relative): -3963.915489000 seconds]
▶ Data (1461 bytes)
```


Os frames 379 e 380 foram trocados pelo endereço IP 131.151.6.171 (este que realizou *request*) que se encontra na VLAN 32, e o endereço IP 131.151.32.129 (este que realizou *reply*) que se encontra na VLAN 6. O frame 379 apresentar um TTL igual a 63, logo provavelmente este frame passou por um router, que possui o endereço MAC destino 00:40:05:40:ef:24 e o endereço MAC destino 00:e0:f9:cc:18:00 (associado á cisco), visto que este frame também passou por um router provavelmente este MAC é uma interface de um router.

Frame 380: ICMP Echo Replay

```
▶ Frame 380: 1515 bytes on wire (12120 bits), 1515 bytes captured (12120 bits)
▼ Ethernet II, Src: AniCommunica_40:ef:24 (00:40:05:40:ef:24), Dst: 3Com_90:10:20 (00:60:97:90:10:20)
  ▶ Destination: 3Com_90:10:20 (00:60:97:90:10:20)
  ▶ Source: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
  Type: 802.1Q Virtual LAN (0x8100)
  [Stream index: 8]
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 6
▼ Internet Protocol Version 4, Src: 131.151.32.129, Dst: 131.151.6.171
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1497
  Identification: 0x3bc2 (15298)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x4c07 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 131.151.32.129
  Destination Address: 131.151.6.171
  [Stream index: 2]
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x07fd [correct]
  [Checksum Status: Good]
  Identifier (BE): 53249 (0xd001)
  Identifier (LE): 464 (0x01d0)
  Sequence Number (BE): 34078 (0x851e)
  Sequence Number (LE): 7813 (0x1e85)
  [Request frame: 379]
  [Response time: 0,144 ms]
  Timestamp from icmp data: Nov  5, 1999 19:26:48.173387000 Hora padrão de GMT
  [Timestamp from icmp data (relative): -3963.915345000 seconds]
  ▶ Data (1461 bytes)
```

O frame 380 possui o endereço MAC origem 00:40:05:40:ef:24 e o endereço MAC destino 00:60:97:90:10:20.

Frame 383: ICMP Echo Request

```
▶ Frame 383: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: AniCommunica_40:ef:24 (00:40:05:40:ef:24), Dst: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▼ Internet Protocol Version 4, Src: 131.151.32.129, Dst: 131.151.32.21
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 48
        Identification: 0x3bc3 (15299)
    ▶ 000. .... = Flags: 0x0
        ...0 0000 1011 1001 = Fragment Offset: 1480
        Time to Live: 255
        Protocol: ICMP (1)
        Header Checksum: 0x378c [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 131.151.32.129
        Destination Address: 131.151.32.21
        [Reassembled IPv4 in frame: 384]
        [Stream index: 0]
▼ Data (28 bytes)
    Data: c0c1c2c3c4c5c6c7c8c9cacbcccdcecfdd0d1d2d3d4d5d6d7d8d9dadb
    [Length: 28]
```

Este frame 383 contém uma mensagem ICMP do tipo Echo Request (ping), enviada de 131.151.32.129 para 131.151.32.21, indicando um teste de conectividade iniciado pelo dispositivo de origem.

Frame 382 e 384: ICMP Echo Request e Echo Reply

```
▶ Frame 382: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)
▼ Ethernet II, Src: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3), Dst: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
    ▶ Destination: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
    ▶ Source: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3)
        Type: 802.1Q Virtual LAN (0x8100)
        [Stream index: 0]
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▼ Internet Protocol Version 4, Src: 131.151.32.21, Dst: 131.151.32.129
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 1500
        Identification: 0x8b21 (35617)
    ▶ 001. .... = Flags: 0x1, More fragments
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 64
        Protocol: ICMP (1)
        Header Checksum: 0x823b [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 131.151.32.21
        Destination Address: 131.151.32.129
    ▶ [2 IPv4 Fragments (1508 bytes): #382(1480), #381(28)]
        [Stream index: 0]
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7e2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 44866 (0xaf42)
    Identifier (LE): 17071 (0x42af)
    Sequence Number (BE): 23331 (0x5b23)
    Sequence Number (LE): 9051 (0x235b)
    [Response frame: 384]
    Timestamp from icmp data: Nov  5, 1999 18:20:44.310551000 Hora padrão de GMT
    [Timestamp from icmp data (relative): 0.000812000 seconds]
▶ Data (1492 bytes)
```

```

▶ Frame 384: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)
▼ Ethernet II, Src: AniCommunica_40:ef:24 (00:40:05:40:ef:24), Dst: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3)
  ▶ Destination: 3Com_9f:b1:f3 (00:60:08:9f:b1:f3)
  ▶ Source: AniCommunica_40:ef:24 (00:40:05:40:ef:24)
  Type: 802.1Q Virtual LAN (0x8100)
  [Stream index: 0]
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32
▼ Internet Protocol Version 4, Src: 131.151.32.129, Dst: 131.151.32.21
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1500
  Identification: 0x3bc3 (15299)
  ▶ 001. .... = Flags: 0x1, More fragments
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x1299 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 131.151.32.129
  Destination Address: 131.151.32.21
  ▶ [2 IPv4 Fragments (1508 bytes): #384(1480), #383(28)]
  [Stream index: 0]
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xffe2 [correct]
  [Checksum Status: Good]
  Identifier (BE): 44866 (0xaf42)
  Identifier (LE): 17071 (0x42af)
  Sequence Number (BE): 23331 (0x5b23)
  Sequence Number (LE): 9051 (0x235b)
  [Request frame: 382]
  [Response time: 0,260 ms]
  Timestamp from icmp data: Nov 5, 1999 18:20:44.310551000 Hora padrão de GMT
  [Timestamp from icmp data (relative): 0.001072000 seconds]
  ▶ Data (1492 bytes)

```

O frame 383 contém uma mensagem ICMP do tipo *Echo Request*, onde o frame 384 contém a mensagem ICMP do tipo *Echo Reply*, ou seja, enviadas do endereço IP 131.151.32.21 para o endereço IP 131.151.32.129, confirmando a conectividade entre os dispositivos. O payload de 1492 bytes sugere um teste de MTU (Maximum Transmission Unit) para verificar o tamanho máximo de pacote suportado pela rede.

Os frames 382 e 384 foram trocados pelos endereços IP 131.151.32.21 (este que realizou o pedido *request*) que se encontra na VLAN 32, e endereço IP 131.151.32.129 (este que realizou o pedido *reply*) que se encontra na VLAN 32. Adicionalmente esta troca de pacotes resultou em 2 *frames* que foram fragmentados devido aos seus tamanhos.

Por fim, o frame 384 possui o endereço MAC origem 00:40:05:40:ef:24 e o endereço MAC destino 00:60:08:9f:b1:f3, visto que estes frames surgiram da mesma VLAN, logo pode-se associar o endereço IP 131.151.32.21 ao endereço MAC 00:60:08:9f:b1:f3, tal como também o endereço IP 131.151.32.129 ao endereço MAC 00:40:05:40:ef:24.

3.6.3 Inferências Topológicas Baseadas em ICMP

A análise dos frames ICMP fornece informações importantes sobre a topologia e o comportamento da rede

1. Segmento de Rede Local:

- Os dispositivos com endereços IP 131.151.32.21 e 131.151.32.129 estão na mesma sub-rede (131.151.32.0/24) e na mesma VLAN 32, comunicando-se diretamente na Camada 2, como evidenciado pelos frames 382, 383, e 384. Os endereços MAC associados (00:60:08:9f:b1:f3 para 131.151.32.21 e 00:40:05:40:ef:24 para 131.151.32.129) confirmam essa comunicação direta.
- A comunicação entre 131.151.6.171 (VLAN 6) e 131.151.32.129 (VLAN 32), observada nos frames 379 e 380, indica tráfego inter-VLAN, provavelmente roteado, dado o TTL de 63 no frame 379, sugerindo a passagem por pelo menos um roteador.

2. Presença de um Switch de Camada 2 e Suporte a VLANs:

- A comunicação direta entre endereços MAC distintos na VLAN 32 (frames 382, 383, 384) implica a presença de um switch de Camada 2 que suporta VLANs. O endereço MAC 00:e0:f9:cc:18:00, associado à Cisco (frame 379), sugere que o switch ou roteador é um dispositivo Cisco, possivelmente configurado com Per-VLAN Spanning Tree (PVST+), como observado em outros frames (e.g., 391, 392 para VLANs 17 e 104).
- A troca de pacotes entre VLANs (frames 379 e 380) reforça a existência de um roteador ou switch de Camada 3 configurado para interconectar VLANs 6 e 32.

3. Identificação de Papéis Funcionais:

- **131.151.32.21:** Atua como uma estação de trabalho cliente, iniciando pedidos ICMP Echo Request (frame 382) e participando de sessões X11 (como indicado em frames correlatos, e.g., 394, 395).
- **131.151.32.129:** Funciona como um servidor, respondendo a pedidos ICMP (frames 380, 384) e iniciando testes de conectividade (frame 383). Sua associação com sessões X11 sugere que é um servidor gráfico Unix/Linux.
- **131.151.6.171:** Dispositivo cliente em outra sub-rede (VLAN 6), iniciando testes ICMP (frame 379), possivelmente para verificar conectividade com o servidor 131.151.32.129.

4. Teste de Conectividade:

- Os frames 379, 380, 382, 383, e 384 mostram testes de conectividade via ICMP Echo Request/Reply (ping). A troca entre 131.151.32.129 e 131.151.32.21 (frames 383, 384) confirma a conectividade na VLAN 32, enquanto os frames 379 e 380 indicam testes inter-VLAN. Esses testes podem estar relacionados à validação de sessões X11, garantindo baixa latência para aplicações gráficas interativas.
- A latência implícita (não especificada diretamente, mas sugerida pela resposta imediata nos frames) é provavelmente baixa, ideal para aplicações sensíveis como X11.

5. Teste de MTU e Fragmentação:

- O frame 384 (Echo Reply) contém um payload de 1492 bytes, resultando em um pacote Ethernet de aproximadamente 1518 bytes (incluindo cabeçalhos), que é o limite típico para Ethernet sem fragmentação. Isso indica um teste de MTU para verificar o tamanho máximo de pacote suportado pela rede, possivelmente motivado pela necessidade de otimizar sessões X11.
- Dois frames fragmentados (mencionados na captura, associados aos frames 382 e 384) sugerem que pacotes maiores que o MTU foram enviados, forçando fragmentação. Isso pode indicar uma configuração de rede que não suporta pacotes jumbo ou uma tentativa de teste explícito de fragmentação.

6. Configuração de VLAN:

- Os frames 382, 383, e 384 estão associados à VLAN 32, consistente com a sub-rede 131.151.32.0/24. No entanto, os frames 379 e 380 envolvem VLANs diferentes (6 e 32), sugerindo que a captura foi realizada em uma interface de roteador ou em uma porta de switch configurada como trunk, permitindo tráfego entre VLANs.
- A ausência de marcação explícita de VLAN nos frames ICMP (diferentemente dos frames X11) pode indicar que a captura foi feita em uma porta untagged para a VLAN 32 ou que o tráfego ICMP não carrega tags VLAN.

7. Correlação com Outros Frames:

- **Frames X11 (394, 395, 389, 375):** A comunicação ICMP entre 131.151.32.21 e 131.151.32.129 está diretamente correlacionada com sessões X11 na mesma sub-rede, sugerindo que os testes ICMP foram realizados para garantir a fiabilidade da comunicação gráfica.
- **Frames STP (391, 392):** A presença de VLANs 17 e 104 reforça a segmentação da rede. A VLAN 32, usada para os frames ICMP e X11, é provavelmente gerenciada pelo mesmo switch Cisco que suporta essas VLANs.
- **Frames ARP (393, 377):** A segmentação da rede em sub-redes distintas (131.151.32.0/24, 131.151.20.0/24, 131.151.1.0/24) é confirmada, com o tráfego ICMP restrito à sub-rede 131.151.32.0/24 ou roteado para 131.151.6.0/24.
- **Frames 379 e 380:** O tráfego inter-VLAN reforça a presença de um roteador com interfaces associadas aos endereços MAC 00:40:05:40:ef:24 e 00:e0:f9:cc:18:00.

8. Ambiente Unix/Linux:

- A combinação de tráfego ICMP (frames 379, 380, 382, 383, 384) com sessões X11 na sub-rede 131.151.32.0/24 sugere que os dispositivos envolvidos (131.151.32.21 e 131.151.32.129) são sistemas Unix/Linux. Isso é reforçado pela ausência de protocolos legados como IPX ou NetBIOS nessa sub-rede.

9. Isolamento de Tráfego Antigo:

- Não há evidência de tráfego IPX ou NetBIOS (como nos frames 390, 385, 376, 354, 374) na sub-rede 131.151.32.0/24 ou nos frames ICMP analisados. Isso indica que a VLAN 32 é isolada de sistemas legados, possivelmente por políticas de firewall ou segmentação via VLANs, enquanto o tráfego entre VLANs (frames 379, 380) é controlado por roteamento.

10. Presença de Roteador:

- O TTL de 63 no frame 379 sugere que o pacote passou por um roteador, provavelmente com endereço MAC 00:40:05:40:ef:24 ou 00:e0:f9:cc:18:00. Isso implica uma topologia com roteamento entre VLANs 6 e 32, conectando as sub-redes 131.151.6.0/24 e 131.151.32.0/24.

4. Síntese da Topologia de Rede

Frame	VLAN ID	L2 (MAC)	L3 (IP)	Equipamento	Serviços/Protocolos	Clientes	SO	Aplicações
375	32	Src: 00:60:08:9f:b1:f3 (3Com) Dst: 00:40:05:40:ef:24	Src: 131.151.32.21Dst: 131.151.32.129	Cliente: Estação de trabalho Servidor: Servidor gráfico	TCP (ACK)	131.151.32.21	Unix/Linux	Sessão gráfica remota
383	32	Src: 00:60:08:9f:b1:f3 (AniCommunications) Dst: 00:60:08:9f:b1:f3	Src: 131.151.32.129Dst: 131.151.32.21	Servidor: 131.151.32.129 Cliente: 131.151.32.21	ICMP (Echo Request/Reply)	131.151.32.21	Unix/Linux	Diagnóstico de rede
384	32	Src: 00:60:08:9f:b1:f3 (AniCommunications) Dst: 00:60:08:9f:b1:f3	Src: 131.151.32.129 Dst: 131.151.32.21	Servidor: 131.151.32.129 Cliente: 131.151.32.21	ICMP (Echo Reply)	131.151.32.21	Unix/Linux	Diagnóstico de rede
385	6	Src: 00:40:05:1f:14:b3 (AniCommunications) Dst: ff:ff:ff:ff:ff:ff (Broadcast)	N/A (IPX)	Servidor: MCS207-249-AFS	NetBIOS sobre IPX (Find Name Request)	Clientes IPX	Novell NetWare	Partilha de ficheiros
389	32	Src: 00:60:08:9f:b1:f3 (AniCommunications) Dst: 00:40:05:40:ef:24	Src: 131.151.32.21 Dst: 131.151.32.129	Cliente: Estação de trabalho Servidor: Servidor gráfico	TCP (ACK)	131.151.32.21	Unix/Linux	Sessão gráfica remota
390	6	Src: 00:40:05:20:76:2f (AniCommunications) Dst: ff:ff:ff:ff:ff:ff (Broadcast)	N/A (IPX)	Servidor: MCS207-243	NetBIOS sobre IPX (Anúncio)	Clientes IPX	Novell NetWare	Partilha de ficheiros
391	17	Src: 00:50:3e:b4:e4:66 (Cisco)	N/A (Camada 2)	Switch Cisco	STP (PVST+ para VLAN 17)	N/A	N/A	N/A

		Dst: 01:00:0c:cc:cc:cd (STP multicast)						
392	104	Src: 00:50:3e:b4:e4:66 (Cisco) Dst: 01:00:0c:cc:cc:cd (STP multicast)	N/A (Camada 2)	Switch Cisco	STP (PVST+ para VLAN 104)	N/A	N/A	N/A
393	20	Src: 00:05:02:71:fc (Apple)Dst: ff:ff:ff:ff:ff:ff (Broadcast)	Src: 131.151.20.72 Dst: 131.151.20.254	Cliente: Dispositivo AppleGateway: 131.151.20.254	ARP (Requisição)	N/A	MacOS (inferido)	N/A
394	32	Src: 00:60:08:9f:b1:f3 (AniCommunications) Dst: 00:40:05:40:ef:24	Src: 131.151.32.21 Dst: 131.151.32.129	Cliente: Estação de trabalhoServidor: Servidor gráfico	X11 (ButtonRelease)	131.151.32.21	Unix/Linux	Sessão gráfica remota
395	32	Src: 00:60:08:9f:b1 (AniCommunications) Dst: 00:40:05:40:ef:24	Src: 131.151.32.21 Dst: 131.151.32.129	Cliente: Estação de trabalhoServidor: Servidor gráfico	X11 (ChangeWindowAttributes)	131.151.32.21	Unix/Linux	Sessão gráfica remota
376	6	Src: 00:60:97:0e:8a:43 (3Com)Dst: ff:ff:ff:ff:ff:ff (Broadcast)	N/A (IPX)	Servidor: HIMALAYA	NetBIOS sobre IPX (SMB Mailslot Write)	Cientes IPX	Windows (inferido)	Anúncio de domínio
377	7	Src: 00:60:08:9f:ab:10 (3Com) Dst: ff:ff:ff:ff:ff:ff (Broadcast)	Src: 131.151.1.7 Dst: 131.151.1.141	Cliente: Dispositivo em 131.151.1.7	ARP (Requisição)	N/A	Desconhecido	N/A
378 e 372	104	Src: 08:00:07:84:12:de (Apple) Dst: ff:ff:ff:ff:ff:ff (Broadcast)	N/A (IPX)	Cliente: Dispositivo Apple	IPX RIP (Request)	N/A	MacOS	Roteamento IPX
374	108	Src: 00:60:8b:d5:eb:96 (Hewlett Packard) Dst: ff:ff:ff:ff:ff:ff (Broadcast)	N/A (IPX)	Servidor: YUMR- MCNUTT119- HP4K	SAP (General Response)	Cientes IPX	Novell NetWare	Anúncio de serviços
354	112	Src: 00:10:83:1c:64:91 (Hp-UxE90) Dst: ff:ff:ff:ff:ff:ff (Broadcast)	N/A (IPX)	Servidor: UMR- MAEM-MEX121	SAP (General Response)	Cientes IPX	Novell NetWare	Anúncio de serviços

Nota: A tabela pode possuir algumas inconsistências. A análise detalhada e completa encontra-se no capítulo 3.

A análise detalhada de todos os frames capturados revela uma rede complexa, hierárquica e segmentada, com as seguintes características:

VLANs Identificadas: 6, (Frame 376, 385, 390) 7 (Frame 377), 17 (Frame 391), 20 (Frame 393), 32 (Frames 394, 389), 104 (Frames 392, 378 e 372), e 108 (Frames 354, 374), 112 (Frame 354, 374), indicando uma segmentação lógica robusta para isolar diferentes tipos de tráfego.

- **VLAN 6:** Associada à máquina na VLAN 6 (nome HIMALAYA), que possui a role MSBROWSE, ou seja, é o master browser, que se encontra no workgroup (nome WORKGROUP) e que possui o endereço MAC 00:60:97:0e:8a:43.
- **VLAN 7:** Associada à sub-rede 131.151.1.0/24 (Frame 377), provavelmente para tráfego de gestão ou administrativo, dado que apenas uma requisição ARP foi capturada.
- **VLAN 17:** Gerida por um switch Cisco (Frame 391), sem tráfego de dados associado, sugerindo uso para controlo ou gestão.
- **VLAN 20:** Associada à VLAN 20, que possui o endereço IP 131.151.1.72 (o endereço MAC 00:05:02:71:fc:db) que está interessado no endpoint com o endereço IP 131.151.1.254.
- **VLAN 32:** Associada à sub-rede 131.151.32.0/24 (Frames 394, 389), dedicada a tráfego gráfico X11, isolando-o de outros tipos de tráfego.
- **VLAN 104:** Associada à sub-rede 131.151.20.0/24 (Frame 393) e tráfego IPX (Frame 378 e 372), suportando dispositivos Apple que utilizam tanto IP como IPX, com conectividade a um gateway (131.151.20.254).
- **VLAN 108:** Associada à rede IPX 0x000056c0 (Frames 374), dedicada a servidores NetWare (YUMR-MCNUTT119-HP4K), isolada de outros segmentos IPX.
- **VLAN 112:** Associada à rede IPX 0x000056c0 (Frames 354), dedicada a servidores NetWare (UMR-MAEM-MEX121), isolada de outros segmentos IPX.

Sub-redes IP:

- **131.151.1.0/24 (VLAN 7, Frame 377):** Segmento isolado, possivelmente para gestão, com tráfego ARP indicando comunicação intra-sub-rede.
- **131.151.20.0/24 (VLAN 104, Frame 393):** Segmento misto, suportando tráfego IP (ARP) e IPX (Frame 378 e 372), com um dispositivo Apple e um gateway (131.151.20.254) para conectividade externa.
- **131.151.32.0/24 (VLAN 32 e sem VLAN especificada, Frames 394, 395, 389, 375, 383, 384):** Segmento dedicado a tráfego gráfico X11 e testes ICMP, isolado de tráfego antigo.

Redes IPX:

- **0x00005060 (Frames 390, 385, 376):** Segmento antigo suportando servidores NetBIOS (MCS207-243, MCS207-249-AFS, HIMALAYA), sem VLAN especificada, sugerindo um segmento amplo ou captura em porta "untagged".
- **0x000056c0 (VLAN 108, Frames 354, 374):** Segmento antigo mais restrito, dedicado a servidores NetWare (YUMR-MCNUTT119-HP4K) com tráfego SAP.

Equipamentos:

- **Routers/Switches Cisco:** Identificados por MACs Cisco (00:50:3e:84:e4:66, Frames 391, 392) e uso de PVST+, gerindo VLANs e STP, provavelmente na camada de distribuição.
- **Servidores:** Incluem servidores gráficos X11 (131.151.32.129, Frames 394, 395, 389,

375), servidores de ficheiros NetBIOS (MCS207-243, MCS207-249-AFS, HIMALAYA, Frames 390, 385, 376), e servidores NetWare (YUMR-MCNUTT119-HP4K, Frames 354, 374).

- **Clientes:** Estações de trabalho Unix/Linux (131.151.32.21, Frames 394, 395, 389, 375), dispositivos Apple (131.151.20.72, Frames 393, 378 e 372), e clientes IPX genéricos (Frames 390, 385, 376, 354, 374).
- **Gateways:** Dispositivo em 131.151.20.254 (Frame 393), atuando como gateway para a sub-rede 131.151.20.0/24, indicando roteamento inter-VLAN.

Serviços e Protocolos:

- **X11:** Sessões gráficas remotas na sub-rede 131.151.32.0/24 (Frames 394, 395, 389, 375), indicando computação centralizada.
- **ICMP:** Testes de conectividade e MTU na sub-rede 131.151.32.0/24 (Frames 383, 384), para suportar sessões X11.
- **IPX:** Suporte a sistemas antigos com NetBIOS (Frames 390, 385, 376), SAP (Frames 354, 374), e RIP (Frame 378 e 372), em redes 0x00005060 e 0x000056c0.
- **ARP:** Descoberta de dispositivos em sub-redes 131.151.1.0/24 (Frame 377) e 131.151.20.0/24 (Frame 393), indicando comunicação intra-sub-rede e necessidade de roteamento.
- **STP:** Gestão de topologia por VLAN (Frames 391, 392), com PVST+ para evitar loops e otimizar caminhos.

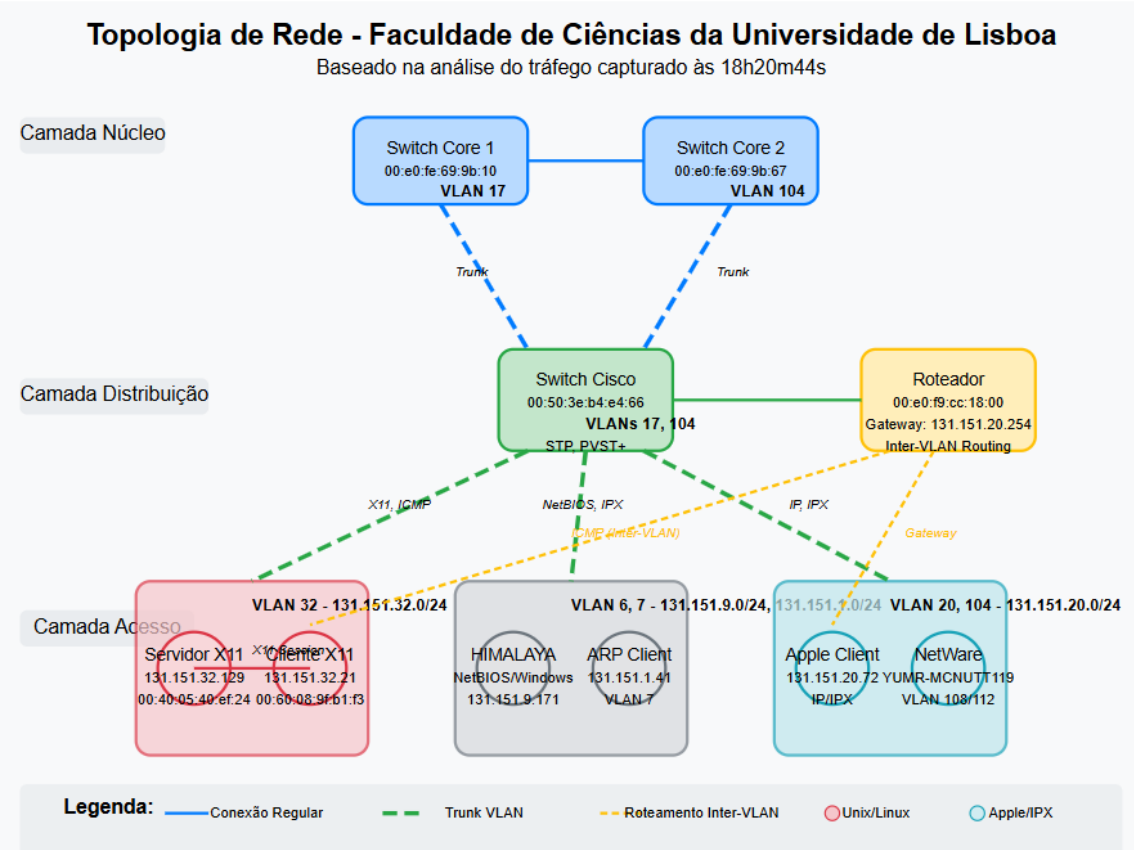
Sistemas Operacionais:

- **Unix/Linux:** Inferido pelo uso de X11 (Frames 394, 395, 389, 375, 294).
- **MacOS:** Inferido para o dispositivo Apple (Frames 393, 378 e 372).
- **Novell NetWare:** Inferido pelo uso de IPX e SAP (Frames 390, 385, 354, 374).
- **Windows:** Inferido pelo uso de SMB em IPX (Frame 376).

Topologia Geral: Rede hierárquica com routers/switches Cisco de Camada 2 e 3, segmentada por VLANs e sub-redes, suportando protocolos modernos (TCP/IP, X11) e antigos (IPX, NetBIOS, SAP). A arquitetura inclui:

- **Camada de Núcleo:** Switches root (00:e0:fe:69:9b:10 para VLAN 17, 00:e0:fe:69:9b:67 para VLAN 104), conectados via links redundantes.
- **Camada de Distribuição:** Switch 00:50:3e:84:e4:66, suportando VLANs 6, 7, 17, 20, 32, 104, 108 e 112, conectando núcleo e acesso.
- **Camada de Acesso:** Switches conectando dispositivos finais em VLANs específicas (VLAN 32 para X11, VLAN 104 para dispositivos Apple).
- **Roteamento:** Gateway 131.151.20.254 conecta sub-redes, indicando roteamento inter-VLAN.

Representação Gráfica da Topologia de Rede:



Nota: A representação gráfica da topologia de rede pode ter algumas inconsistências, pois está foi gerada por AI com base nos dados analisados que foram apresentados neste relatório.

5. Conclusão

A reconstrução da topologia de rede a partir da captura de tráfego (ficheiro vlan.cap) representa uma abordagem que permite não apenas resolver problemas complexos, mas também documentar ambientes, avaliar a segurança de redes existentes e planejar migrações tecnológicas com precisão.

A análise detalhada de todos os frames capturados revela uma rede hierárquica e segmentada, com uma arquitetura Cisco de três camadas (núcleo, distribuição, acesso), segmentação lógica via VLANs (6, 7, 17, 20, 32, 104, 108, 112), e separação por protocolos (IP e IPX) e funções (servidores, clientes, gestão). A rede suporta um ambiente tecnológico híbrido, com sistemas modernos (Unix/Linux, X11) e antigos (NetWare, Windows, IPX), indicando uma organização estabelecida, possivelmente académica, em transição tecnológica. A segmentação intencional e o design resiliente refletem práticas de engenharia de rede robustas, otimizadas para alta disponibilidade, segurança, e eficiência.

A análise apresentada neste relatório demonstra como, mesmo com informações fragmentadas, é possível aplicar princípios dedutivos para reconstruir uma visão coerente e abrangente de da

infraestrutura de rede. Este processo analítico, quando aplicado metodicamente, transforma dados brutos de pacotes em conhecimento arquitetural.