



LNET-RX

Análise de Rede

INTRODUÇÃO:

A análise de rede é um processo de estudo detalhado da rede LAN/WAN pelo qual se busca atender umas das necessidades listadas abaixo:

- Levantamento de toda **Documentação da Rede**;
- **Identificação de Problemas na rede**;
- **Diagnóstico para Implementação de Mudanças ou Expansões da Rede**.

Este trabalho apresentará informações detalhadas referentes à sua Rede, como Topologia, relação de equipamentos, plano de endereçamento, portas utilizadas, diagnóstico da sua da rede, desempenho, consumo, estatísticas de utilização, aplicações e erros.

OBJETIVOS:

Documentação da Rede:

Mesmo esteja funcionando, na maioria das vezes o cliente não conhece detalhadamente a topologia e características de tráfego da própria rede. Em geral, não se preocupa com isso até que o primeiro problema aconteça. Com a documentação da rede disponibilizada, o cliente passa a ter um retrato fiel de todo tráfego, identificando gargalos, tráfegos indesejados, e possíveis necessidades de reestruturação, redimensionamento dos links e equipamentos.

Identificação de problemas na rede:

Através de serviços emergenciais, seja pela simples análise do profissional, pelo uso de ferramentas de diagnóstico ou pela utilização de equipamentos provisórios, o objetivo é identificar problemas de desempenho ou indisponibilidades permanentes e/ou intermitentes na rede LAN/WAN que possam estar impactando na produtividade e/ou negócio do cliente.



Diagnóstico para Implementação de Mudanças ou Expansões da Rede:

Uma expansão e/ou mudança no ambiente atual requer uma análise detalhada da rede. O Diagnóstico permitirá ao gestor dimensionar de forma correta os recursos necessários, tecnologias e equipamentos a serem agregados na Rede. Essa informação constitui-se assim como uma importante fonte de informação, que auxiliará no gestor nas tomadas de decisão.

RELATÓRIOS GERADOS:

Fazem parte da documentação gerada nessa Análise de rede:

- Desenho da topologia Física e Lógica da rede;
- Identificação dos protocolos, portas, endereços e aplicações em uso na rede com estatísticas de tráfego e consumo;
- Análise de performance da rede, usando métodos estatísticos para geração de indicadores de desempenho (tráfego de pico, hora de tráfego de pico, tráfego médio, tráfego mínimo, etc.);
- Estatísticas de consumo dos links, up-links e pontos de intercessões da rede;
- Identificação de problemas como colisões e níveis de broadcast;
- Identificação de pontos de falha críticos para o negócio;
- Identificação dos pontos de falhas em topologias redundantes;
- Identificação de equipamentos descontinuados (end of Sales) e/ou de tecnologias ultrapassadas.



PROTOCOLOS E FERRAMENTAS:

Protocolos e ferramentas utilizadas para Análise de rede:

- SNMP;
- RMON/RMON2;
- SNIFFER;
- MRTG / PRTG / CACTI;
- NetFlow / JFlow / IPFix;

Análise com SNIFFER:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.60? Tell 10.23.173.1
2	0.051714	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.6? Tell 10.23.173.1
3	0.066529	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.63? Tell 10.23.173.1
4	0.169234	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.150? Tell 10.23.173.1
5	0.224387	Cameocom_4a:b6:b6	Broadcast	ARP	who has 10.23.173.6? Tell 10.23.173.193
6	0.409434	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.165? Tell 10.23.173.1
7	0.546460	3comEuro_4a:35:10	Spanning-tree-(for-br STP	Conf. Root = 49152/0/00:1e:c1:4a:35:10 Cost = 0 Port = 0x8008	
8	0.619905	10.23.173.202	87.246.30.101	TCP	global-dtserv > 63498 [SYN] Seq=0 win=65535 Len=0 MSS=1260
9	0.619921	10.23.173.202	213.138.247.10	TCP	1775 > 8323 [SYN] Seq=0 win=65535 Len=0 MSS=1260
10	0.619930	10.23.173.202	115.134.6.231	TCP	femis > 51127 [SYN] Seq=0 win=65535 Len=0 MSS=1260
11	0.727793	Cameocom_4a:ae:85	Broadcast	ARP	who has 10.23.173.6? Tell 10.23.173.191
12	0.886011	10.23.173.202	87.246.30.101	TCP	dpkeyserv > http [SYN] Seq=0 win=65535 Len=0 MSS=1260
13	0.886910	10.23.173.202	213.138.247.10	TCP	answersoft-lm > http [SYN] Seq=0 win=65535 Len=0 MSS=1260
14	0.887754	10.23.173.202	115.134.6.231	TCP	hp-hcip > http [SYN] Seq=0 win=65535 Len=0 MSS=1260
15	1.224399	Cameocom_4a:b6:b6	Broadcast	ARP	who has 10.23.173.6? Tell 10.23.173.193
16	1.385526	10.23.173.202	94.189.149.122	TCP	vaultbase > 60415 [SYN] Seq=0 win=65535 Len=0 MSS=1260
17	1.631608	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.68? Tell 10.23.173.1
18	1.654955	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.207? Tell 10.23.173.1
19	1.728555	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.173? Tell 10.23.173.1
20	2.067181	Cisco_c0:12:20	Broadcast	ARP	who has 10.23.173.137? Tell 10.23.173.1
21	2.260538	10.23.173.202	87.246.30.101	TCP	powerguardian > https [SYN] Seq=0 win=65535 Len=0 MSS=1260
22	2.260555	10.23.173.202	213.138.247.10	TCP	prodigy-internet > https [SYN] Seq=0 win=65535 Len=0 MSS=1260
23	2.260563	10.23.173.202	115.134.6.231	TCP	pharmasoft > https [SYN] Seq=0 win=65535 Len=0 MSS=1260
24	2.548870	3comEuro_4a:35:10	Spanning-tree-(for-br STP	Conf. Root = 49152/0/00:1e:c1:4a:35:10 Cost = 0 Port = 0x8008	
25	2.761357	10.23.173.202	213.21.18.84	TCP	1783 > 15336 [SYN] Seq=0 win=65535 Len=0 MSS=1260

Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_c0:12:20 (00:14:f2:c0:12:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff 00 14 f2 c0 12 20 08 06 00 01 .....
0010 08 00 06 04 00 01 00 14 f2 c0 12 20 0a 17 ad 01 .....
0020 00 00 00 00 00 0a 17 ad 50 00 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Figura1: exemplo de análise com sniffer



Análise com NetFlow:

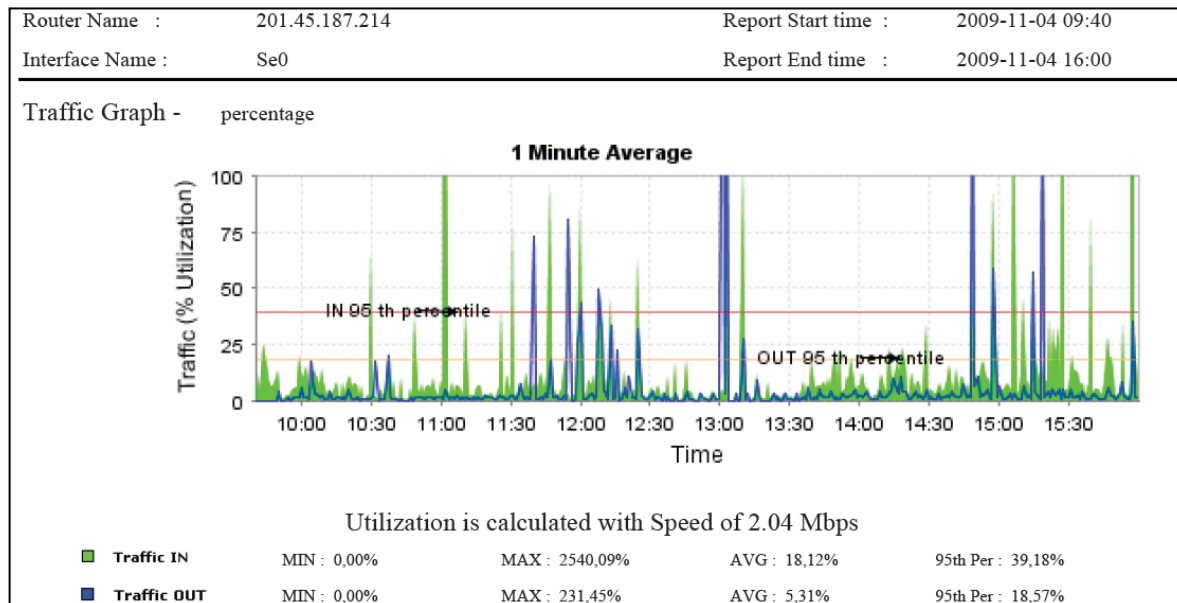


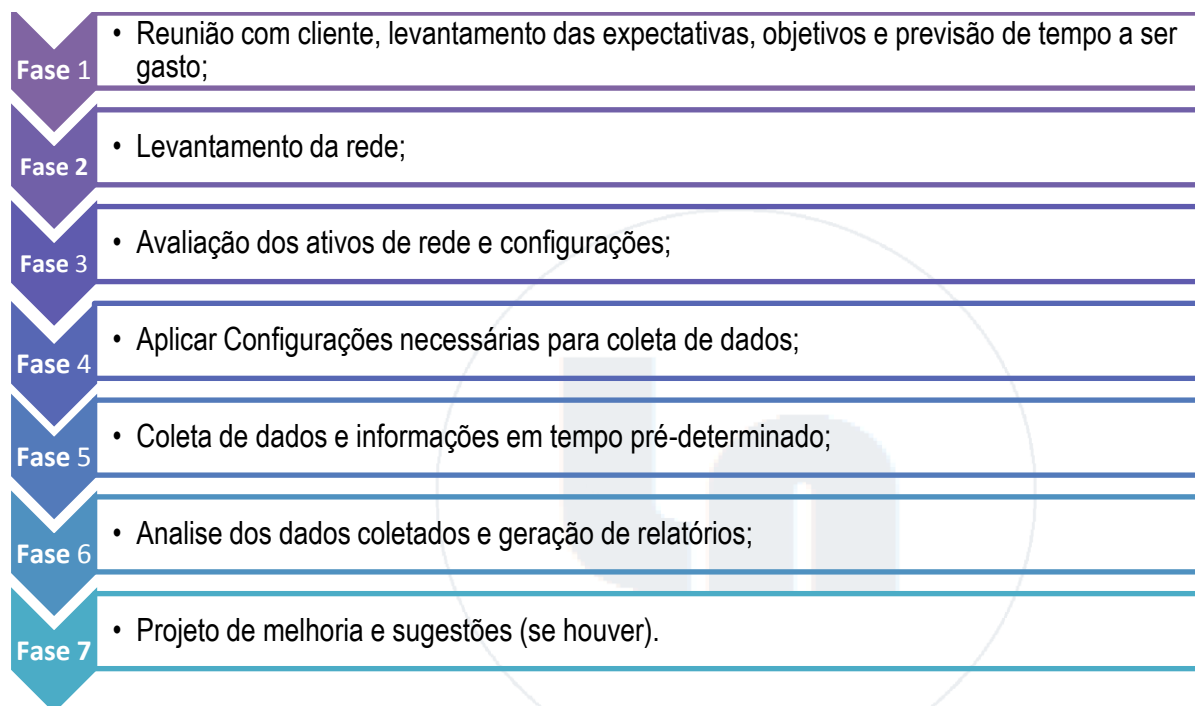
Figura2: exemplo de análise com netflow

Application	Traffic (1.03 GB)	Percentage of total traffic
lotusnote	574.62 MB	55%
http	399.86 MB	39%
UDP_App	26.97 MB	3%
Video Conferencia	25.3 MB	2%
TCP_App	4.93 MB	<1%
microsoft-ds	1.75 MB	<1%
domain	1.3 MB	<1%
icmp	454.83 KB	<1%
ftp-data	239.2 KB	<1%
netbios-ssn	113.14 KB	<1%
snmp	50.69 KB	<1%
ftp	42.85 KB	<1%
netbios-ns	25.19 KB	<1%
Oracle	20.83 KB	<1%
rmiactivation	20.56 KB	<1%
nessus	17.66 KB	<1%
jrun_ejb	3.1 KB	<1%
rmiregistry	2.56 KB	<1%
skinny	1.68 KB	<1%
wins	1.35 KB	<1%
Unaccounted	1.79 KB	<1%

Figura3: exemplo de análise com netflow(2)



METODOLIGIA PARA ANÁLISE DE REDE:



BENEFÍCIOS

A Análise de Rede traz os seguintes benefícios para empresa:

- Disponibilização de toda documentação da rede;
- Auxílio na visualização de possíveis problemas de performance, paralisia parcial ou total da rede;
- Possibilita melhorias de desempenho da rede baseadas em alterações da topologia ou configuração atual;
- Auxílio no dimensionamento do crescimento e melhorias na rede de forma adequada;
- Aumento da segurança, controle das aplicações, portas e endereçamento de rede;



- Possibilidade de redução de custos, evitando possíveis upgrades de link, ou mesmo, a redução dos atuais;
- Aumento potencial da capacidade e produtividade dos processos da empresa.

PROPOSTA:



logicnet

LogicNet Tecnologia Ltda.

LogicNet Tecnológica Ltda.
Tel: 31 2526-0217
Fax: 31 2526-5317
www.logicnet.com.br