

**FACULDADE ESTÁCIO DE SÁ DE OURINHOS
TECNOLOGIA EM REDES DE COMPUTADORES**

RICARDO DALIO DA CUNHA

**PROTOCOLO DE COMUNICAÇÃO
TRABALHO SMNP**

OURINHOS

2010

FACULDADE ESTÁCIO DE OURINHOS
TECNOLOGIA EM REDES DE COMPUTADORES

RICARDO DALIO DA CUNHA

PROTOCOLO DE COMUNICAÇÃO
TRABALHO SMNP

Faculdade Estácio de Sá de Ourinhos,

Curso: Redes de computadores

Matéria : protocolo de comunicação

RA: 2006200076

Professor (a): Maria Alessandra

OURINHOS

2010

SUMÁRIO

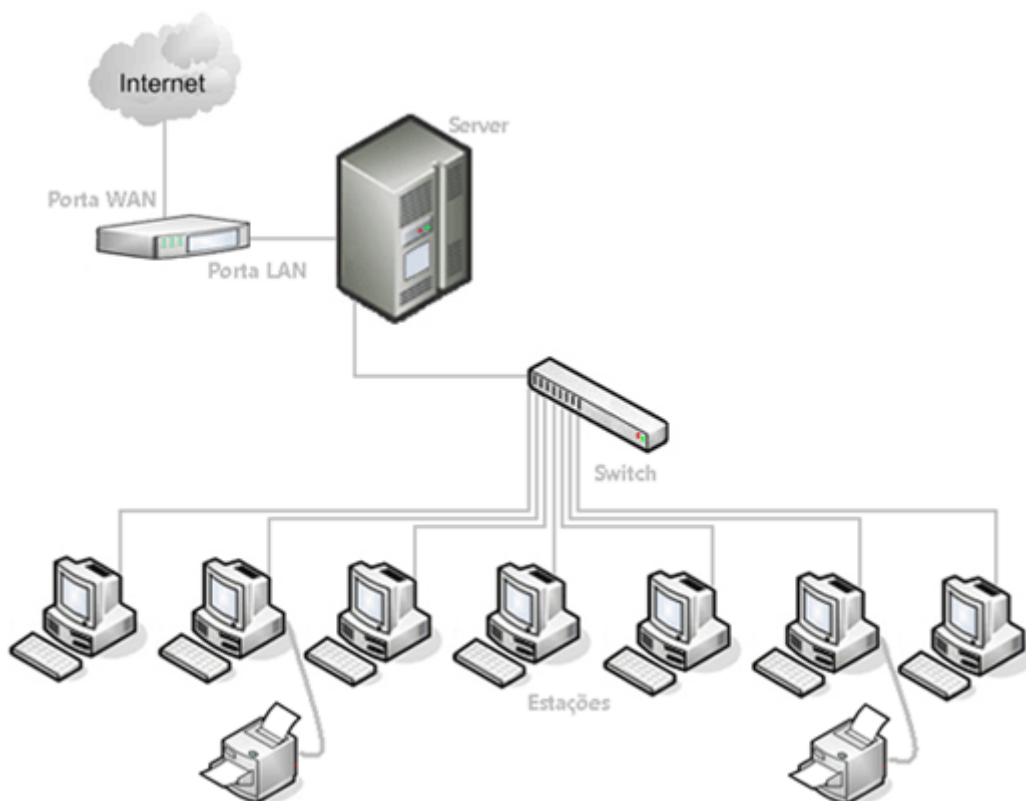
1 INTRODUÇÃO	3
2 REDES DE COMPUTADORES	4
3 SOFTWARES	5
3.1 Gerência de Segurança	5
3.2 Gerência de Desempenho	8
4 Rede Fábrica de softwares	10
5 Conclusão	12
6 Bibliografia	13

1 INTRODUÇÃO

Este projeto tem como idéia mostrar como seria a configuração simples de uma rede e alguns softwares que podem facilitar o funcionamento desta rede, foi simulado uma fábrica de softwares, onde há diversas áreas a ser explorada por uma rede, lembrando que é só para entender um conceito.

2 REDES DE COMPUTADORES

Bom todo mundo se pergunta o que é exatamente uma rede de computadores e como funciona, redes como o próprio nome sugere são ligações, elo de comunicação de um computador com outro ou vários computadores, se achar difícil entender então segue uma imagem do que seria uma rede simples:



Repare que há vários computadores algumas impressoras, isso é uma rede básica, há também um switch “repassando” o sinal que provem do servidor, mas se notarmos bem há um roteador que autentica a internet na rede acima. tendo base nesse conceito damos inicio ao projeto, conforme mencionado será uma fábrica de software onde há muito tráfego de dados assim veremos verificar uma forma boa de se construir uma rede eficiente.

Dando inicio ao projeto, primeiro temos de analisar quais softwares serão necessários, tendo em vista da imensa opção que o mercado nos oferece. Neste projeto utilizaremos dois softwares de gerenciamento um de segurança e outro de desempenho.

3 SOFTWARES

3.1 Gerência de Segurança

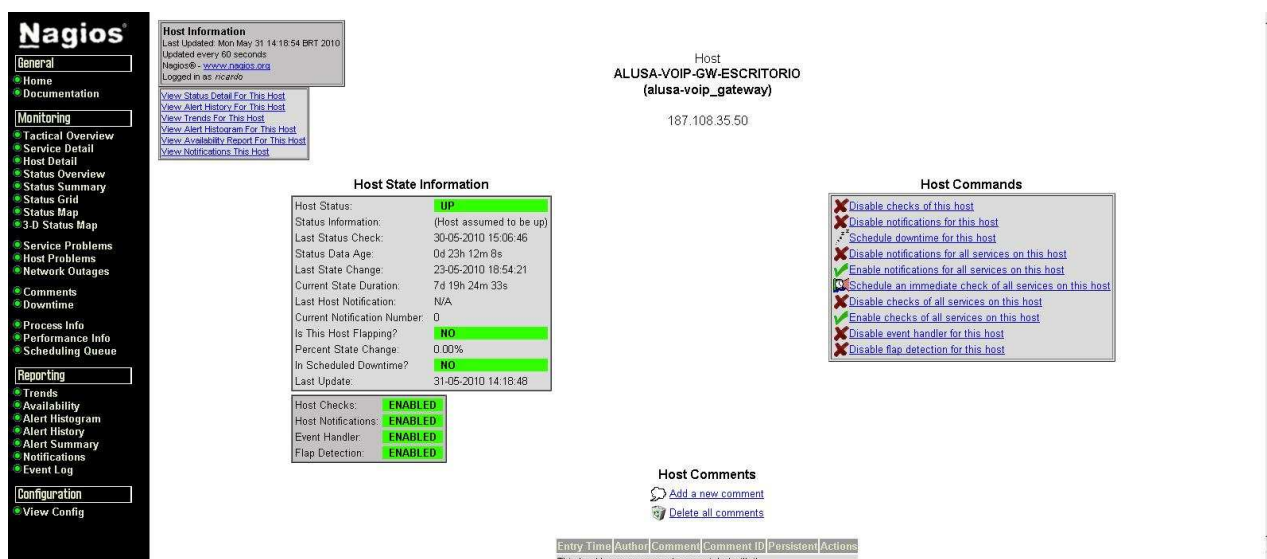
Para nossa rede será utilizado em gerenciamento de segurança a ferramenta “Nagios”, por ser open source ou seja “free”.



Tela de inicialização do Nagios

É uma ferramenta com fácil manuseio, serve para gerenciar possíveis problemas em uma rede, como máquinas desligadas servidores parados entre outros além de enviar notificações por e-mail e celular caso configurados.

Exemplo de configuração :



Nota-se que do lado esquerdo da tela há o status do host com alguns dados por exemplo, quanto tempo está “on”, se já foi atualizado, quantos dias está nessa condição etc..

Já no lado direito da tela há uma área de comandos, por exemplo, o que você quer que o Nagios notifique caso ocorra um problema como:

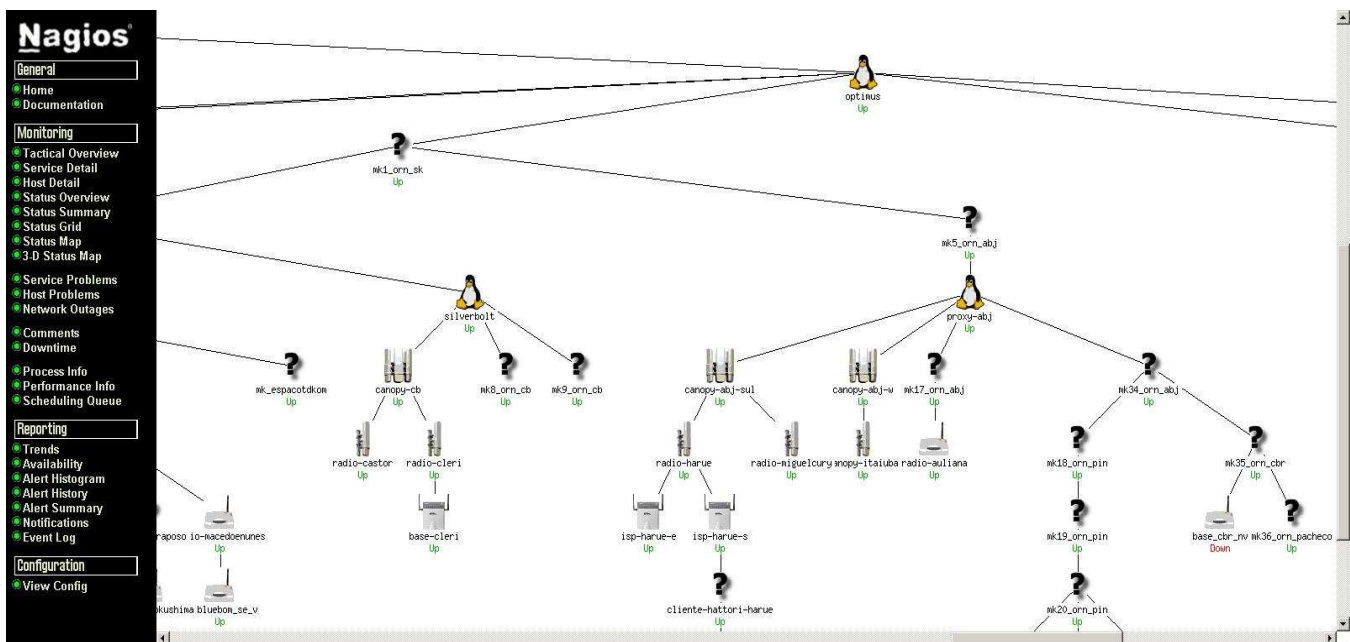
Notificação por e-mail;

Notificação via celular;

Disparo sonoro etc...

Para uma rede simples só notificação por e-mail é mais que suficiente, se o Nagios ficar constantemente aberto em uma máquina com áudio, colocar disparo sonoro é uma boa idéia, lembrando que, se o Nagios não for corretamente configurado isso se torna irritante.

Nesta ferramenta há opções como mapear a rede (Nagios faz um desenho de sua rede, se for devidamente configurado), opção de ver só máquinas “on” (ligado) ou só máquinas com problemas, pode –se configurar serviços das máquinas como apache, http, proxy entre outros.



Exemplo de uma rede mapeada pelo Nagios

- General
- Home
- Documentation
- Monitoring
 - Tactical Overview
 - Service Detail
 - Host Detail
 - Status Overview
 - Status Summary
 - Status Grid
 - Status Map
 - 3-D Status Map
- Service Problems
- Host Problems
- Network Outages
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Reporting
 - Trends
 - Availability
 - Alert Histogram
 - Alert History
 - Alert Summary
 - Notifications
 - Event Log
- Configuration
 - View Config

[View history for all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

3

196

20

355

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
58-ispso-silo	PING	OK	31-05-2010 14:33:26	0d 1h 22m 0s	1/3	PING OK - Packet loss = 0%, RTA = 32.50 ms
alusa-voip_gateway	PING	OK	31-05-2010 14:34:18	7d 19h 41m 4s	1/5	PING OK - Packet loss = 20%, RTA = 76.20 ms
argonmail	Apache	OK	31-05-2010 14:33:02	13d 12h 40m 13s	1/5	HTTP ok: HTTP/1.1 200 OK - 0.090 second response time
	IMAP	OK	31-05-2010 14:33:50	31d 20h 1m 0s	1/5	IMAP OK - 0.003 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION Courier-IMAP ready. Copyright 1998-2005 Double Precision, Inc. See COPYING for distribution information.]
	POP3	OK	31-05-2010 14:33:26	0d 12h 2m 42s	1/3	POP OK - 0.026 second response time on port 110 [+OK <31482.1275331642@argon.com.br>]
	SMTP	OK	31-05-2010 14:33:26	13d 12h 26m 13s	1/5	SMTP OK - 0 second response time
	SSH	OK	31-05-2010 14:34:59	0d 9h 5m 32s	1/5	SSH OK - OpenSSH_3.9p1 (protocol 2.0)
argonweb	DNS	OK	31-05-2010 14:35:02	0d 11h 37m 22s	1/3	DNS ok - 1 seconds response time, Address(es) is/are (null)
	DNS-AXFR	OK	31-05-2010 14:33:26	0d 11h 37m 12s	1/5	TCP OK - 0.022 second response time on port 53
	FTP	OK	31-05-2010 14:33:47	22d 10h 56m 47s	1/3	FTP OK - 0.018 second response time on port 21 [220 Microsoft FTP Service]
	IS	OK	31-05-2010 14:33:28	31d 20h 24m 47s	1/3	TCP OK - 0.014 second response time on port 80
	MySQL	OK	31-05-2010 14:33:45	31d 21h 0m 26s	1/3	TCP OK - 0.028 second response time on port 3306
asteriskbrasil	Apache	OK	31-05-2010 14:35:02	0d 1h 27m 2s	1/3	HTTP ok: HTTP/1.1 200 OK - 0.597 second response time
bacamarte	PING	OK	31-05-2010 14:34:35	5d 4h 7m 25s	1/3	PING OK - Packet loss = 0%, RTA = 66.90 ms
	SSH	OK	31-05-2010 14:33:20	2d 22h 59m 32s	1/5	TCP OK - 0.161 second response time on port 22
base-cleri	PING	OK	31-05-2010 14:30:12	1d 19h 29m 23s	1/5	PING OK - Packet loss = 0%, RTA = 23.80 ms
base-danielalabs	PING	OK	31-05-2010 14:33:31	0d 1h 22m 0s	1/5	PING OK - Packet loss = 0%, RTA = 22.80 ms
base-kennedy	PING	OK	31-05-2010 14:34:25	0d 0h 2m 42s	1/5	PING OK - Packet loss = 0%, RTA = 64.00 ms
base-nionovo	PING	OK	31-05-2010 14:33:39	0d 0h 47m 52s	1/3	PING OK - Packet loss = 0%, RTA = 14.70 ms
base-tsunami	PING	OK	31-05-2010 14:34:36	4d 4h 58m 55s	1/5	PING OK - Packet loss = 0%, RTA = 14.30 ms
base-usi	PING	OK	31-05-2010 14:33:31	0d 0h 47m 52s	1/3	PING OK - Packet loss = 0%, RTA = 12.70 ms
base2-distrito-scrp	PING	OK	31-05-2010 14:34:34	1d 11h 59m 6s	1/5	PING OK - Packet loss = 0%, RTA = 17.00 ms

Exemplo de serviços configurados pela ferramenta Nagios

Nagios é um software de gerenciamento de segurança muito utilizado pela comunidade de software livre, vem sendo substituído por Cacti, outro software livre com grande potencial.

Um bom motivo de o Nagios estar sendo colocado de canto é o descaso em suas atualizações, simplesmente pararam já à algum tempo.

3.2 Gerência de Desempenho

Outra ferramenta que utilizaremos em nossa rede, mantendo o conceito de software livre é o Tcpdump,.

Tcpdump é uma ferramenta que “escuta” a porta de rede, no caso placa ethernet; Com ela podemos saber se há um problema na placa , broadcast na rede entre outros problemas que incomodam. Existem vários comando para utilizar esta ferramenta de sniffer de rede segue abaixo um exemplo:

```
17:36:37.511845 IP 10.192.242.122.63284 > 200.152.65.10.22: P 157:209(52) ack 40552 win 64259
17:36:37.516599 IP 200.152.65.10.22 > 10.192.242.122.63284: P 42964:43208(244) ack 209 win 8576

933 packets captured
933 packets received by filter
0 packets dropped by kernel
[root@silverbolt root]# tcpdump -i eth2 host 10.192.242.122 -Nnl
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 96 bytes
17:36:54.322975 IP 74.125.107.93.80 > 10.192.242.122.63290: S 1420272515:1420272515(0) ack 1964573612 win 5840 <msg 1460,nop,nop,ackOK,nop,wscale 6>
17:36:54.323105 IP 200.152.65.10.22 > 10.192.242.122.63284: P 3152948901:3152949017(116) ack 363714774 win 8576
17:36:54.323107 IP 200.152.65.10.22 > 10.192.242.122.63284: P 1161232(116) ack 1 win 8576
17:36:54.336565 IP 10.192.242.122.63290 > 74.125.107.93.80: . ack 1 win 32768
17:36:54.336305 IP 10.192.242.122.63290 > 74.125.107.93.80: P 11407(506) ack 1 win 32768
17:36:54.344122 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 232 win 64103
17:36:54.350351 IP 200.152.65.10.22 > 10.192.242.122.63284: P 2321900(668) ack 1 win 8576
17:36:54.350355 IP 200.152.65.10.22 > 10.192.242.122.63284: P 9001032(132) ack 1 win 8576
17:36:54.356145 IP 200.152.65.10.22 > 10.192.242.122.63284: P 10321260(228) ack 1 win 8576
17:36:54.378054 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 1032 win 65535
17:36:54.381800 IP 200.152.65.10.22 > 10.192.242.122.63284: P 12601392(132) ack 1 win 8576
17:36:54.382928 IP 200.152.65.10.22 > 10.192.242.122.63284: P 13921524(132) ack 1 win 8576
17:36:54.384438 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 1392 win 65178
17:36:54.388411 IP 200.152.65.10.22 > 10.192.242.122.63284: P 15241464(132) ack 1 win 8576
17:36:54.387164 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 1656 win 64911
17:36:54.388092 IP 200.152.65.10.22 > 10.192.242.122.63284: P 16561788(132) ack 1 win 8576
17:36:54.388659 IP 200.152.65.10.22 > 10.192.242.122.63284: P 17881920(132) ack 1 win 8576
17:36:54.390572 IP 200.152.65.10.22 > 10.192.242.122.63284: P 192012052(132) ack 1 win 8576
17:36:54.391560 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 1920 win 64647
17:36:54.392395 IP 200.152.65.10.22 > 10.192.242.122.63284: P 205212280(228) ack 1 win 8576
17:36:54.399649 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 2280 win 64287
17:36:54.429747 IP 200.152.65.10.22 > 10.192.242.122.63284: P 228012508(228) ack 1 win 8576
17:36:54.429775 IP 200.152.65.10.22 > 10.192.242.122.63284: P 250812640(132) ack 1 win 8576
17:36:54.429777 IP 200.152.65.10.22 > 10.192.242.122.63284: P 264012772(132) ack 1 win 8576
17:36:54.429779 IP 200.152.65.10.22 > 10.192.242.122.63284: P 277212904(132) ack 1 win 8576
17:36:54.445940 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 2640 win 65535
17:36:54.446247 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 2808 win 65275
17:36:54.446285 IP 200.152.65.10.22 > 10.192.242.122.63284: P 28081323(132) ack 1 win 8576
17:36:54.456658 IP 200.152.65.10.22 > 10.192.242.122.63284: P 322813360(132) ack 1 win 8576
17:36:54.456861 IP 200.152.65.10.22 > 10.192.242.122.63284: P 336013492(132) ack 1 win 8576
17:36:54.471153 IP 200.152.65.10.22 > 10.192.242.122.63284: P 349213624(132) ack 1 win 8576
17:36:54.471151 IP 200.152.65.10.22 > 10.192.242.122.63284: P 362413756(132) ack 1 win 8576
17:36:54.471123 IP 200.152.65.10.22 > 10.192.242.122.63284: P 375613884(228) ack 1 win 8576
17:36:54.485204 IP 200.152.65.10.22 > 10.192.242.122.63284: P 398414308(324) ack 1 win 8576
17:36:54.493964 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 3360 win 64815
17:36:54.497219 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 3624 win 64551
17:36:54.500167 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 3984 win 64191
17:36:54.507524 IP 200.152.65.10.22 > 10.192.242.122.63284: P 430814440(132) ack 1 win 8576
17:36:54.507799 IP 200.152.65.10.22 > 10.192.242.122.63284: P 444014732(292) ack 1 win 8576
17:36:54.519137 IP 200.152.65.10.22 > 10.192.242.122.63284: P 473214960(228) ack 1 win 8576
17:36:54.528427 IP 200.152.65.10.22 > 10.192.242.122.63284: P 496015092(132) ack 1 win 8576
17:36:54.544085 IP 200.152.65.10.22 > 10.192.242.122.63284: P 509215224(132) ack 1 win 8576
17:36:54.545678 IP 10.192.242.122.63284 > 200.152.65.10.22: . ack 4440 win 65535
17:36:54.560585 IP 200.152.65.10.22 > 10.192.242.122.63284: P 522415452(228) ack 1 win 8576
```

Comando: tcpdump -i eth2 host “ip a ser escutado” -Nnl (comando para o tcpdump não resolver nome).

Este comando faz com que a máquina analise todo trafego que venha do ip escolhido na placa escolhida, quando menciono “todo” é todo mesmo, mas se você quer escolher uma adeterminada porta, exemplo:

Quero saber se há envio de spam em uma das minhas máquinas?

Sim isso é possível com um simples comando

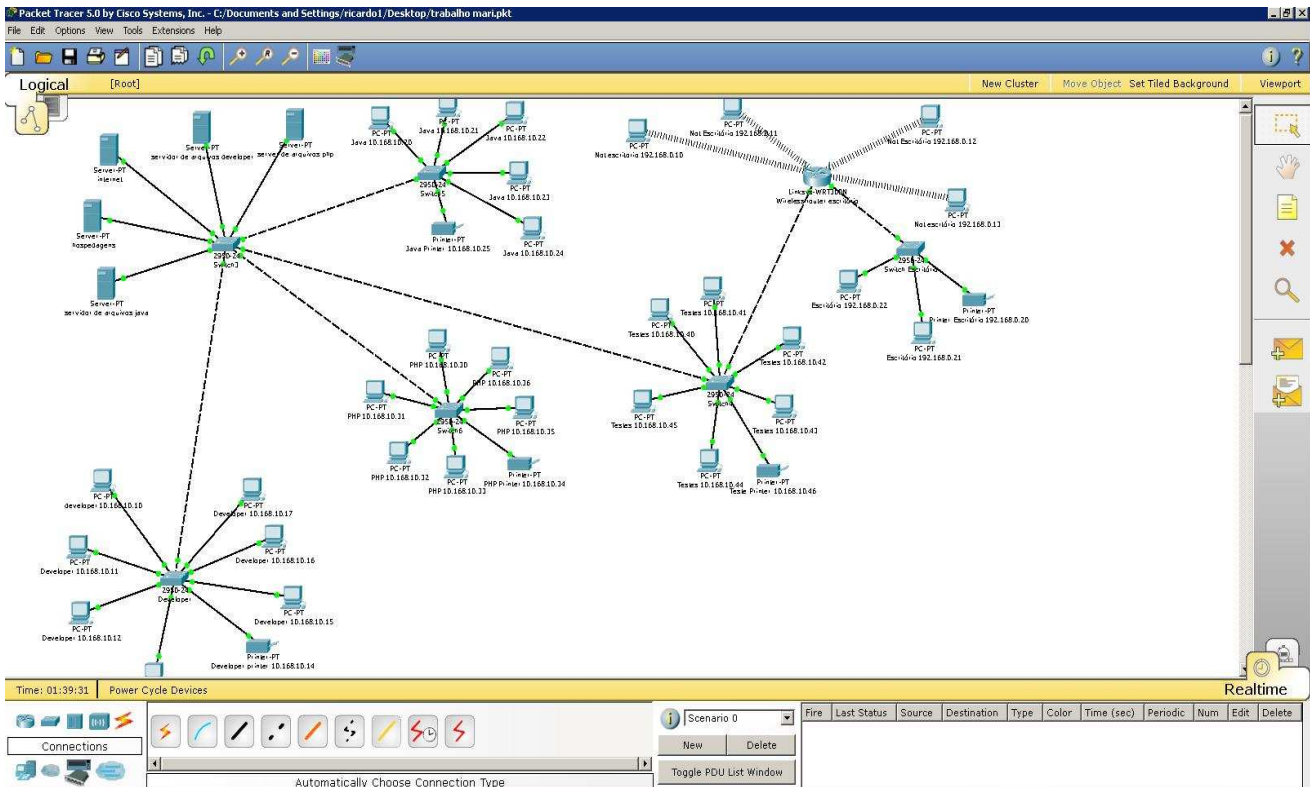
tcpdump -i eth? (placa escolhida) host (ip desejado) -Nnl and port ? (porta escolhida neste caso será a 25)

Ficaria mais ou menos assim :

tcpdump -t eth2 host 10.168.10.32 -Nnl and port 25

Se houver um tráfego absurdo com blocos de 6 (seis) mensagens seguidas sempre no envio e recebimento, isso é constado presença de vírus SPAM em sua rede, mas há um cuidado nem sempre bloco seqüenciais são vírus, somente em portas específicas, por um motivo simples, vírus são burros não atacam portas aleatórias, mas os outros blocos podem ser antivírus atualizando, “webcan” sendo executada, acesso remoto entre outras coisas.

4 Rede Fábrica de softwares



Baseado no conceito de ilhas a fábrica irá ter 6 ilhas uma principal e as outras dependendo do funcionamento da principal.

A primeira ilha ou a principal contem os servidores, foi utilizado uma mascara /24, pois não houve necessidade de múltiplas redes.

Ilha principal : Lá se encontra os servidores :

PHP : contendo tutorial, bibliotecas , arquivos de projetos passados, e softwares para instalação rápidas.

Java: contendo tutorial, bibliotecas , arquivos de projetos passados, e softwares para instalação rápidas

Developer: contendo tutorial, bibliotecas, arquivos de projetos passados, e softwares para instalação rápidas,

Hospedagem: antes de ter toda certeza do funcionamento de produtos , o mesmo é instalado no servidor de hospedagens, onde sofre uma bateria para analisar possíveis "bugs" e assim sendo corrigidos:

Ilha 2: Onde se encontra a área de Developer, usuários de flash, photoshop entre outras ferramentas de imagens, também há um acerto desenvolvimento, mas a maioria se aloca nas outras ilhas.

Ilha 3: Pessoal de PHP, desenvolvedores de ferramentas rápidas voltadas para WEB, e também suporte para equipe de Java

Ilha 4: Equipe Java, criação soluções para web e off web, sites, ferramentas ERP entre outras.

Ilhas 5: Área de testes, quando a nova ferramenta está pronta é preciso ser testada, para isso a ilha de testes existe, a nova ferramenta é hospedada a partir logo se iniciam os testes para correção do produto.

Ilha 6: esta ilha é independente, somente necessitando da internet, pois é uma ilha q tem wi-fi roteador entre outros, sua rede é outra, não interferindo nos dados da fábrica, motivo simples, essa ilha é voltada para financeiro, comercial, denominada escritório, onde se concentra toda parte administrativa.

5 Conclusão

Este projeto foi elaborado para demonstrar que hoje em dia há muita necessidade de profissionais na área de rede, para que uma fábrica de software tenha andamento é preciso um projeto, com início, meio e fim, lembrando que este só foi um exemplo, um projeto sério necessita de mais tempo e mais análise.

Com isso aprendemos que uma rede tem muitas dificuldades, e para sanar e analisar cada problema, não é uma simples pessoa que resolve.

Vale também mencionar o fato da equipe que gerência uma rede, tem de ter a serenidade de não utilizar de seu “poder” para más intenções, como por exemplo utilizar sniffer de redes para hackear senhas .

6 Bibliografia

Não houve, pois todo o projeto foi baseado nas aplicações do curso de Rede de computadores.