

++50 Dicas para Administradores de Redes



Eduardo Maroñas Monks

++50 Dicas para Administradores de Redes

Eduardo Maroñas Monks

ISBN: 978-65-01-59121-6

2025



Dedicatória

Dedico este livro a minha família, em especial a minha esposa Vanessa e ao meu filho Gregory, aos meus pais, Pedro e Maria, aos meus amigos e colegas que estiveram e estão comigo dando o apoio para seguirmos em frente trilhando novos caminhos e desafios.



Sumário

Sobre o Autor.....	4
Sobre esta Obra.....	5
Introdução.....	6
1) Scripts para montagem de linhas de comando.....	6
2) Testes de conexão com Tcpdump.....	9
3) Depurar a configuração de VLANs.....	11
4) Jumbo Frames.....	13
5) Fixar um endereço MAC para uso com IPs default em equipamentos.....	15
6) Monitoramento por SNMP de DHCP leases em Linux.....	17
7) Backup de Banco de Dados: Dump x Cópia de arquivos.....	20
8) Níveis de alertas e notificações.....	22
9) Liberação de regras para DNS e navegação Web no firewall.....	24
10) Forçar o uso do endereço MAC como identificação no serviço de DHCP.....	26
11) Ativar os logs de DNS para identificação de malware e domínios indesejados.....	29
12) DHCP Snooping.....	31
13) Limitar tráfego em broadcast e multicast.....	35
14) Ativar agregação (Link Aggregation) em uplinks.....	38
15) Multihoming em servidores de arquivos.....	41
16) Uso de VLANs.....	45
17) Servidor de logs centralizado.....	47
18) Backup de banco de dados.....	50
19) Bloqueios por consumo de tráfego.....	52
20) Janela de manutenção.....	55
21) Remoção de regras de firewall no Linux.....	57
22) Temperatura de data center/sala de servidores.....	59
23) Emulador CORE.....	62
24) Snapshots antes de alterações em VMs.....	64
25) Descoberta de IPs em uso.....	65
26) Backup de configurações de serviços.....	67
27) Usar comentários nos arquivos de configuração.....	68



28) Revisar a sala dos servidores diariamente.....	70
29) Ativar o gerenciamento SNMP em todos os dispositivos compatíveis.....	72
30) Documentar os disjuntores de racks e demais equipamentos importantes.....	75
31) Criar um repositório para toda a documentação.....	77
32) Monitorar o espaço em disco consumido por arquivos/pastas/tabelas temporárias....	79
33) Ativação do protocolo Netflow.....	80
34) Evitar cabos soltos dentro de racks e em mesas de usuários.....	82
35) Cuidados com sistemas legados.....	84
36) Criar um ambiente de testes.....	86
37) Revisar as ferramentas de gerenciamento.....	88
38) Ativar um servidor de gerenciamento fora da infraestrutura principal.....	90
39) Revisar as baterias dos nobreaks e realizar trocas periódicas.....	92
40) Criação de políticas de uso de recursos de TI e de segurança.....	95
41) Uso de sistemas de chamados para atendimento.....	97
42) Gerenciamento de backups.....	99
43) Anotar os telefones importantes para caso de tudo dar errado.....	101
44) Montar um kit de ferramentas e acessórios.....	102
45) Utilizar um sistema de gerenciamento de senhas.....	104
46) Conhecimento básico da linguagem Python para scripts.....	106
47) Escaneamento de vulnerabilidades.....	110
48) Manter os sistemas e serviços atualizados.....	114
49) Certificações Profissionais.....	116
50) Antes de tudo, o mais simples.....	118
51) Rotinas de Validação de Procedimentos.....	119
52) Evitar a postergação de atividades.....	120
53) O problema é na rede?.....	122
54) Entender os “milagres”.....	124
55) Conhecimentos dos fundamentos de Redes.....	125
56) Conhecimentos Não Técnicos.....	128
57) Serviços em Nuvem.....	130
58) Conhecimentos de outras áreas.....	133
59) Padrões e Melhores Práticas.....	134
60) Metodologia para diagnosticar problemas.....	136
61) Analisar as condições de licenciamento e garantia em aquisições.....	139
62) Verificar a conexão no servidor correto.....	141



63) Testes com ferramentas em ambiente de produção.....	142
64) Viabilidade técnica.....	144
Considerações Finais.....	146
Referências bibliográficas.....	147



Sobre o Autor

Possui graduação em Bacharel em Análise de Sistemas pela Universidade Católica de Pelotas (1998), Mestrado em Computação pela Universidade Federal do Rio Grande do Sul (2006) e Doutorado pela Universidade Federal de Pelotas (2023). Começou a atuar na área de redes em 1995 como estagiário na UCPEL, onde trabalhou por 14 anos. No período de 1999 a 2004 e 2006 a 2007, atuou como docente em cursos de Ciência da Computação e Tecnologia em Análise e Desenvolvimento de Sistemas na UCPEL. Em 2007, passou a exercer a função de docente da UniSenac Pelotas, em que esteve na coordenação da criação do curso superior em Redes de Computadores, curso que atingiu a nota máxima no ENADE de 2017. Em 2014 tornou-se Analista de TI na UFPEL, atuando na administração de redes. Possui certificados Cisco CCAI, Cisco CCNA e LPIC-1.



Para saber mais: Canal do Youtube criado em 2009 com mais de 600 vídeos sobre a área de redes, disponível em <http://www.youtube.com/emmonks>



Aviso Importante

Sobre esta Obra

Este livro pode ser usado de forma livre, desde que os créditos e as referências sejam publicados. As informações contidas no documento são de minha autoria, fruto de experiências de mais de 30 anos atuando na área. Nos casos em que são apontadas ferramentas ou sites, poderá haver inconsistências no acesso futuro e poderão causar indisponibilidades.

Se este livro tiver ajudado de alguma forma, por favor, contribua com o valor que achar justo como forma de agradecimento, um cafezinho está ótimo. Obrigado!

Chave do PIX: **7f7fa84a-6ce9-45da-a42f-a77d18eb232c**



Este livro também pode ser obtido em formato físico na loja da editora UICLAP, disponível em <https://loja.uiclap.com/>



Introdução

Este livro tem como objetivo publicar dicas para administradores de redes que foram experimentadas durante a minha vivência na área. São mais de 25 anos, começando como estagiário no ano de 1995 e chegando em 2024 atuando diretamente na área como técnico e docente. São dicas valiosas que poderão ajudar muito os iniciantes na área e aos mais experientes ajudar nas melhorias de alguns procedimentos e rotinas que podem salvar o final de semana e até mesmo o emprego.

Um ótimo administrador de redes é um profissional raro no mercado de trabalho. Esta raridade é resultante de um perfil específico, focado na responsabilidade, em querer aprender e na pró-atividade na execução das tarefas. Na minha experiência como profissional e docente na área é nítida a percepção de quando este perfil se manifesta. Na área de TI existem vários campos de atuação e cada um deles tem um perfil específico. Por mais que todos sejam da TI, um gestor de projetos, um desenvolvedor, um devops e um administrador de redes são espécies distintas em grande parte das atividades que realizam. O que há em comum com todos eles são os computadores e todos atuam com o mesmo objetivo em trilhas diferentes. Este livro é dedicado para o pessoal que trilha a área de redes.

As dicas não estão em ordem de importância, não há dica mais ou menos relevante. Entretanto, são percepções que foram vividas, às vezes com um certo sofrimento, e são apresentadas neste livro para que sejam evitadas ou enfrentadas com menos trabalho e sustos.

Espero que seja uma leitura proveitosa e que ajude a melhorar as rotinas de administração de redes.

Boa leitura!

1) Scripts para montagem de linhas de comando

Em várias situações será necessário tratar arquivos com campos para aplicar comandos. Por exemplo, para criar ou remover usuários em massa, montar listas de



comandos, realizar testes em listas de endereços IP e outros casos similares. O uso de scripts em Shell ou em Python, com o mínimo de programação, poderão resolver problemas complexos de forma simples e rápida. Deverá haver bastante cuidado quando se utilizam scripts para gerar comandos. Uma coisa é executar UM comando errado, outra bem diferente é executar 1000 comandos errados!

Em Linux, o utilitário **xargs** realiza o recebimento como variável a saída de uma linha de comando e possibilita a execução de uma nova linha de comando. No Exemplo 1.1, o arquivo “servidores.txt” possui uma lista de nomes e endereços IP separados por “;”. A linha de comando lê o 2º campo, que seria o endereço IP, joga como entrada para o **xargs** na variável de nome **ende** e executa duas requisições de ping em cada endereço IP.

Exemplo 1.1

Arquivo **servidores.txt**

```
servA192.168.100.9  
servB;192.168.100.11  
servC;192.168.100.13  
servD;192.168.100.90  
servE;192.168.100.91
```

Comando

```
cat servidores.txt | awk '{ print $2 }' | xargs -lende ping -c2
```

No Exemplo 1.2, o script em Bash **pinga_serv.sh** realiza a mesma tarefa do Exemplo 1.1. Entretanto, mostra o nome do servidor antes de realizar duas tentativas de ping para cada endereço IP.

Exemplo 1.2

```
#!/bin/bash  
  
for cada in $(cat servidores.txt);do  
  
    nome=$(echo $cada | awk '{ print $1 }')
```



```
ende=$(echo $cadalawk '{ print $2 }')

echo "Pingando no servidor $nome"

ping -c2 $ende
```

Done

Os scripts dos exemplos são simplificados e podem ser melhorados incluindo validações para se existe o arquivo, se está no formato correto, se o retorno do ping foi com sucesso entre outros. Entretanto, esta dica tem como objetivo indicar o uso de scripts simples para ajudar em tarefas chatas e que demandam trabalho repetitivo.



A criação ou a importação de usuários tem alguns desafios. Quando não se utiliza um número de documento único como CPF ou há necessidade de criar identificações com letras e números como no caso de e-mails, os desafios são mais complexos. Para auxiliar nesta tarefa foram desenvolvidos alguns scripts que poderão ajudar e estão disponíveis em https://github.com/emmonks/monta_users



2) Testes de conexão com Tcpdump

Analizar o tráfego de rede possibilita ao administrador de redes depurar com maior assertividade problemas relacionados a falhas de conexão, regras de firewall e relatos de indisponibilidade de serviços. A ferramenta Tcpdump está disponível na maioria das distribuições Linux e em soluções proprietárias baseadas em Linux ou na biblioteca Libpcap.

Uma das situações comuns na qual o uso do Tcpdump indica a resolução do problema acontece com validação de regras de firewall. Quando há um relato de impossibilidade de conexão por parte do usuário, por exemplo uma conexão ao banco de dados MySQL, as causas podem ser diversas. O usuário pode estar com o endereço IP incorreto, a porta de conexão incorreta, o usuário do banco incorreto, a senha incorreta, o nome do banco de dados incorreto ou usando um navegador Firefox para acessar o banco de dados MySQL. Do lado servidor pode estar ativado um firewall, o serviço do banco de dados inativo, restrição de acesso ao usuário/senha do cliente ou até mesmo o servidor estar desligado.

De forma remota, o uso do Tcpdump pode ser executado em um roteador entre a máquina cliente do usuário e o servidor. Caso seja na mesma rede, o uso do Tcpdump pode ser feito no próprio servidor. No Exemplo 2.1 estão listados filtros de captura do Tcpdump para coletar pacotes de acordo com os endereços e portas de interesse.

Exemplo 2.1

```
# Filtra pacotes que possuem a porta TCP 3306 e o endereço IP 10.10.1.101 (cliente) como destino ou origem e o endereço IP 10.10.99.5 (servidor)
```

```
tcpdump -nn -i eth0 tcp port 3306 and host 10.10.1.101 and host 10.10.99.5
```

O filtro usado no Exemplo 2.1 aplica-se em um roteador entre o cliente e o servidor. A porta TCP 3306 é a porta padrão do MySQL. Quando o cliente realizar a conexão com o banco, se a conexão estiver correta, o filtro mostraria o início de conexão TCP (*3-Way Handshake*) e segmentos TCP PSH / TCP ACK sendo trocados entre cliente e servidor. Se neste caso, ainda não houver sucesso na conexão por parte do cliente, o problema não está na rede e nem no firewall. A conexão foi estabelecida com sucesso e dados foram trocados. O provável problema está em nível de aplicação, no usuário, na senha ou nas permissões de



acesso ao banco de dados que devem ser revisados. Isto também pode ser verificado nos logs do servidor de banco de dados.

Em caso de não haver o estabelecimento da conexão TCP entre cliente e servidor, haverá apenas as tentativas de início de conexão por parte do cliente com segmentos TCP SYN sem resposta do servidor. Neste caso, há um firewall ativado que impede a conexão, porém pode haver um firewall e também o serviço do banco de dados estar inativo. Se não houver firewall e o serviço do banco de dados estiver inativo, a resposta do servidor será um segmento TCP RST para cada segmento TCP SYN.

Se não houver nenhum pacote sendo mostrado no filtro do Tcpdump, algumas condições podem estar causando isto:

- Existe um outro firewall bloqueando tráfego entre o cliente e o servidor
- Há problema de conectividade entre o cliente e o servidor, pode-se usar os utilitários *ping* e *traceroute* para verificar se existe caminho entre os hosts
- A porta de comunicação do serviço sendo filtrado não é a padrão (ao invés da porta TCP 3306 pode estar sendo usada outra porta, por exemplo, TCP 9801)
- A interface de rede usada no filtro não está correta ou não é a interface de entrada do tráfego. Se houver duas interfaces no firewall, os pacotes recebidos em uma interface interna não serão repassados para a interface externa



O *Tcpdump* é a ferramenta mais disponível em sistemas operacionais Linux e é a padrão. Para realizar análise de tráfego com mais recursos a ferramenta *Wireshark* é a recomendada. Está disponível uma série de vídeos sobre o *Wireshark* em <https://www.youtube.com/playlist?list=PLJE51qhGRWYVQbUMvf5yXIRrqMEiLOutW>

Para saber mais



Tcpdump - <https://www.youtube.com/watch?v=1LUk6fw6W6M>



3) Depurar a configuração de VLANs

Ao se fazer uso de VLANs alguns problemas são comuns e não tão simples de formar um diagnóstico. As VLANs tem como objetivo isolar domínios de broadcast, fazendo com que hosts conectados em uma VLAN só alcancem hosts em outra VLAN por meio de um roteador. Este isolamento acontece internamente no sistema operacional do switch que utiliza uma *tag* numérica para separar os endereços físicos (endereço MAC) pertencentes a cada VLAN. Portanto, se um endereço físico foi aprendido em uma VLAN, o switch não fará a comunicação deste endereço físico com uma VLAN diferente.

Quando um host não aparece na VLAN correta, a primeira coisa a fazer é verificar a configuração da porta onde está conectado. Um equipamento pode ser ligado em uma porta do tipo acesso, tronco ou híbrida. A porta do tipo acesso espera que o equipamento conectado a ela não saiba nada sobre VLAN (pacotes entram e saem da porta sem nenhuma *tag* de VLAN). A porta do tipo tronco espera que o equipamento conectado a ela trate as marcações de VLAN, portanto, os pacotes entram e saem da porta marcados. Uma porta híbrida trata de pacotes com marcações e caso receba pacotes sem nenhuma marcação, fará o tratamento destes pacotes usando uma VLAN sem marcação. Desta forma, ao conectar um equipamento que não trata VLAN em uma porta tronco não haverá comunicação. Se conectar um equipamento esperando marcação de VLAN em uma porta de acesso não haverá a comunicação como esperado, o mesmo para uma porta híbrida.

Em casos em que o equipamento está conectado na porta de tipo correto, o endereço físico do equipamento deverá aparecer na tabela MAC do switch na VLAN correta. Entretanto, são usados diversos switches em uma rede e com conexões de portas uplink entre eles. Estas portas são do tipo tronco ou híbrida. Para encontrar o endereço físico de um equipamento no restante dos switches deve-se verificar as portas de uplink desde a origem até o destino. Caso o endereço físico não esteja sendo propagado entre os switches, é provável que tenha faltado a configuração da VLAN nas portas de conexão do uplink nos dois switches. O efeito para o usuário é que não está com conexão plena, sem endereço IP ou com o endereço IP “errado” (porta configurada com a VLAN incorreta). Para identificar os switches que fazem vizinhança se pode utilizar o protocolo LLDP (*Link Layer Discovery Protocol*), disponível na quase totalidade dos switches gerenciáveis.





Os conceitos de VLAN possuem algumas particularidades quando implementados nos dispositivos. A forma como são definidas as portas de acesso e tronco podem variar. Em alguns casos as portas são denominadas untagged (acesso) e tagged (tronco). As portas trunk se referem a portas em agregação (link aggregation) e não possuem a mesma funcionalidade de portas tronco (tagged) usadas em VLANs.

Para saber mais



VLAN: Conceitos Básicos -

<https://www.youtube.com/watch?v=xZ-SOGYkafA>



4) Jumbo Frames

Os jumbo frames são quadros Ethernet maiores que 1518 Bytes e são usados para aumentar o espaço de dados e diminuir a relação de bytes usado em cabeçalho (controle) com os bytes usados na área de dados (carga útil). Esta possibilidade de utilizar pacotes maiores depende da interface de rede e do switch para poder funcionar. O tamanho do pacote pode chegar aos 9 KB. O tamanho máximo de um pacote é definido de acordo com a tecnologia de rede da camada de enlace de dados e chama-se MTU (*Maximum Transfer Unit*). Portanto, para ativar o modo jumbo frame em uma interface de rede deve-se alterar o MTU da interface. Na Figura 4.1, é apresentada a configuração em uma interface de rede no sistema operacional Microsoft Windows 11.

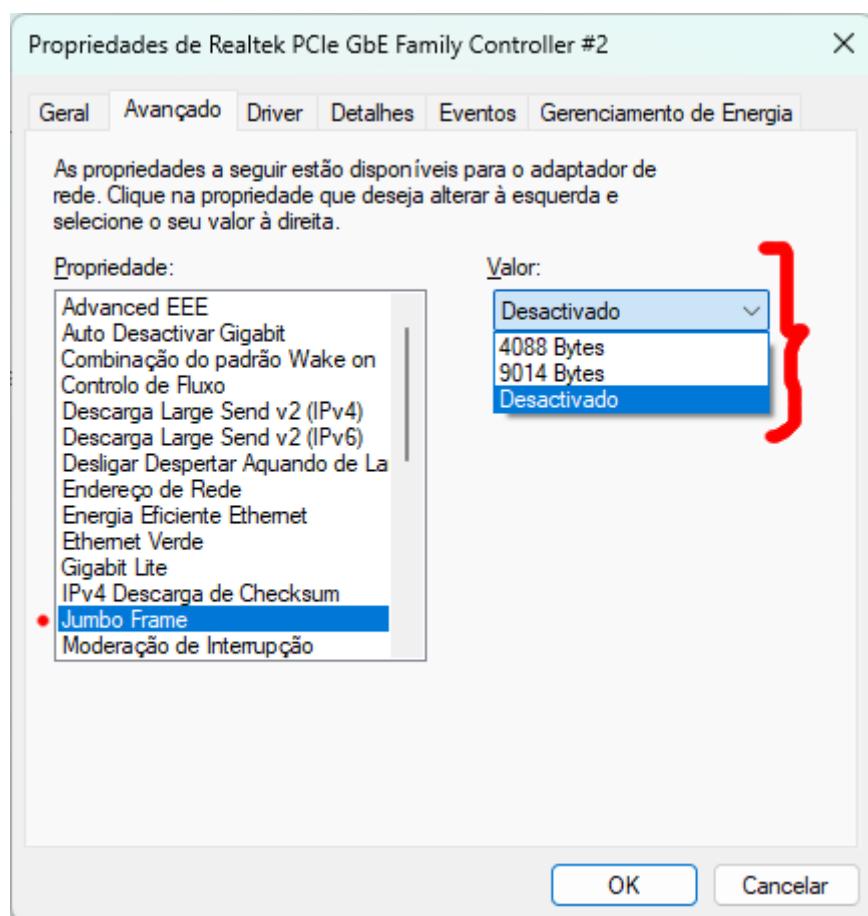


Figura 4.1 - Configurações da interface de rede para ativação do jumbo frame.

Em Linux, a mudança do MTU pode ser realizada com os comandos ip ou ifconfig. No Exemplo 4.1 estão listadas duas linhas de comando para ativação de jumbo frame na interface de nome eth0.

Exemplo 4.1

```
ip link set dev eth0 mtu 9000  
ifconfig eth0 mtu 9000 up
```

E qual o motivo desta configuração não estar ativa por padrão, se aumentaria o desempenho da rede? Um dos principais motivos está na compatibilidade com os demais equipamentos na rede. Mesmo que o switch tenha esta funcionalidade, outros hosts conectados podem não estar com o jumbo frame ativado ou não serem compatíveis. Um outro motivo é que poderá causar lentidão ao iniciar a conexão devido ao rebaixamento do tamanho do pacote que será feito pelo ICMP por meio do Path MTU e a fragmentação que ocorrerá nos roteadores quando houver comunicação entre VLANs com um host usando jumbo frame e outro não.

E para que serve o jumbo frame? Em um ambiente de virtualização, com uso de storages, pode-se ativar o jumbo frame nas interfaces dos virtualizadores e dos storages. O ganho estimado é por volta de 11%, sem contar a redução no número de pacotes por segundo que reflete no uso de recursos de CPU do host. Normalmente, os fabricantes de storages recomendam ativação de jumbo frame nas interfaces para melhor desempenho. No caso deste tipo de tráfego, os pacotes são grandes e aproveitam melhor o aumento do espaço para a carga útil. Em um tráfego com SSH, VoIP ou jogos, onde os pacotes são pequenos, não haveria ganho nenhum de desempenho.



Atualmente, é raro uma interface de rede não ter compatibilidade com jumbo frames. Entretanto, em switches mais antigos é bem provável que não tenham compatibilidade. Para verificar isto, observar os erros nas portas do switch para giants (pacotes maiores do que o padrão 1518 ou 1522 bytes).



5) Fixar um endereço MAC para uso com IPs default em equipamentos

Quando existem dispositivos com IPs iguais em uma mesma rede configura-se um conflito de endereços. Isto acontece devido ao uso de IPs configurados manualmente, sem levar em consideração a distribuição dos endereços de forma automática por DHCP, por uso malicioso para causar negação de serviço ou roubo de informações (usar o IP do gateway ou do servidor de autenticação) ou quando existem dispositivos que perdem a configuração e voltam ao padrão de fábrica com o mesmo IP. Uma alternativa para identificar de forma exclusiva um dispositivo é por meio do endereço físico (MAC address).

No caso de dispositivos que perdem a configuração e voltam para o mesmo IP pode-se tornar estático o endereço físico no sistema operacional para não haver descoberta dinâmica com o protocolo ARP ou com ICMPv6. Em IPv4, pode-se cadastrar um IP para um endereço físico de forma estática. Desta forma, o acesso ao dispositivo não ficará “pulando” de um endereço físico para outro quando expirar o tempo de cache da tabela ARP. O Administrador de Redes poderá fazer a configuração de um dispositivo por vez, ao trocar o IP depois de terminado e após fixar outro MAC para o mesmo IP padrão de fábrica.

No Exemplo 5.1, os comandos para fixar e remover um IP com um endereço físico no sistema operacional Microsoft Window. No Exemplo 5.2, os comandos para realizar os mesmos procedimentos no sistema operacional Linux. Estes comandos devem ser executados com níveis privilegiados de permissões (root/sudo/administrador).

Exemplo 5.1

```
# Fixa o endereço IP 10.0.0.100 com o endereço físico 00-50-56-C0-00-01  
arp -s 10.0.0.100 00-50-56-C0-00-01  
  
# Remove o mapeamento estático do endereço IP 10.0.0.100  
arp -d 10.0.0.100
```



Exemplo 5.2

```
# Fixa o endereço IP 10.115.233.132 com o endereço físico 00:70:56:9b:e3:1b  
arp -s 10.115.233.132 00:70:56:9b:e3:1b  
  
# Remove o mapeamento estático do endereço IP 10.115.233.132  
arp -d 10.115.233.132
```



Uma medida de segurança simples de implementar é a fixação do endereço MAC do gateway ou servidor na tabela ARP. Desta forma, caso seja ativado uma interface de rede com o mesmo IP do gateway ou servidor, de forma involuntária ou maliciosa, o host com o endereço MAC fixado na tabela ARP não seria afetado.

Para saber mais



ARP Estático - Acesso a dispositivos com o mesmo endereço IP -



<https://www.youtube.com/watch?v=JqQsMz9WlfU>



6) Monitoramento por SNMP de DHCP leases em Linux

O serviço de DHCP (*Dynamic Host Control Protocol*) costuma ser um dos mais tranquilos de configurar e administrar no sistema operacional Linux. O monitoramento é feito por meio dos logs de empréstimos (leases) que ficam em /var/lib/dhcp/dhcpd.leases ou nos logs do sistema operacional para serviços como /var/log/messages ou /var/log/syslog. Para obter estatísticas de consumo do range de IPs que estão em uso pode-se utilizar a ferramenta dhcpcd-snmp, disponível em <https://github.com/ohitz/dhcpcd-snmp>. Esta ferramenta permite integrar a coleta de informações sobre os empréstimos de endereços no agente SNMP do servidor. Desta forma, torna-se mais simples configurar em ferramentas de gerenciamento como Zabbix ou Nagios.

A configuração é feita no arquivo dhcpcd-snmp.conf onde são listados os pools de endereços que serão monitorados e o local do arquivo de log com os registros dos empréstimos (/var/lib/dhcp/dhcpd.leases). No exemplo 6.1 está listado o conteúdo de um arquivo dhcpcd-snmp.conf.

Exemplo 6.1

```
leases:/var/lib/dhcp/dhcpd.leases  
  
pool:1,ANDAR1,10.15.110.1-10.15.110.254,  
  
pool:2,ANDAR2,10.15.120.10-10.15.120.254,  
  
pool:3,ANDAR3,10.15.130.10-10.15.130.254,  
  
pool:4,ANDAR4, 10.15.140.10-10.15.140.254,
```

Para ativar a integração com o agente SNMP, editar o arquivo /etc/snmp/snmpd.conf onde está o servidor de DHCP e configurar a chamada de uma OID privada para executar a coleta dos dados dos empréstimos. No Exemplo 6.2 uma linha de comando para ativar um OID para execução do dhcpcd-snmp.

Exemplo 6.2



```
pass_persist      .1.3.6.1.4.1.21695.1.2      /usr/bin/perl      /usr/local/sbin/dhcpd-snmp  
/etc/dhcpd-snmp.conf
```

Para coletar os dados dos empréstimos, apontar o cliente de SNMP para o IP do servidor e para o número do OID configurado, no Exemplo 6.2 seria o OID .1.3.6.1.4.1.21695.1.2 . No Exemplo 6.3 está a saída da execução de uma coleta de empréstimos de endereços. As descrições dos OIDs são *dhcpdSnmpPoolIndex*, *dhcpdSnmpPoolDescription*, *dhcpdSnmpPoolSize*, *dhcpdSnmpPoolActiveLeases* e *dhcpdSnmpPoolExpiredLeases*. No pool do “ANDAR1” existem 254 endereços no total, com 71 endereços em uso e 183 endereços expirados (disponíveis).

Exemplo 6.3

Comando:

```
snmpwalk -v2c -c public localhost .1.3.6.1.4.1.21695.1.2
```

```
iso.3.6.1.4.1.21695.1.2.1 = INTEGER: 4 # Total de pools de endereços
```

```
iso.3.6.1.4.1.21695.1.2.2.1.1 = INTEGER: 1 # Índice do pool (dhcpdSnmpPoolIndex)
```

```
iso.3.6.1.4.1.21695.1.2.2.1.2 = INTEGER: 2
```

```
iso.3.6.1.4.1.21695.1.2.2.1.3 = INTEGER: 3
```

```
iso.3.6.1.4.1.21695.1.2.2.1.4 = INTEGER: 4
```

```
iso.3.6.1.4.1.21695.1.2.2.2.1 = STRING: "ANDAR1" # Descrição do pool  
(dhcpdSnmpPoolDescription)
```

```
iso.3.6.1.4.1.21695.1.2.2.2.2 = STRING: "ANDAR2"
```

```
iso.3.6.1.4.1.21695.1.2.2.2.3 = STRING: "ANDAR3"
```

```
iso.3.6.1.4.1.21695.1.2.2.2.4 = STRING: "ANDAR4"
```

```
iso.3.6.1.4.1.21695.1.2.2.3.1 = INTEGER: 254 # Total de endereços no pool  
(dhcpdSnmpPoolSize)
```

```
iso.3.6.1.4.1.21695.1.2.2.3.2 = INTEGER: 245
```



iso.3.6.1.4.1.21695.1.2.2.3.3 = INTEGER: 245

iso.3.6.1.4.1.21695.1.2.2.3.4 = INTEGER: 245

iso.3.6.1.4.1.21695.1.2.2.4.1 = INTEGER: 71 # Endereços em uso
(dhcpdSnmpPoolActiveLeases)

iso.3.6.1.4.1.21695.1.2.2.4.2 = INTEGER: 33

iso.3.6.1.4.1.21695.1.2.2.4.3 = INTEGER: 36

iso.3.6.1.4.1.21695.1.2.2.4.4 = INTEGER: 56

iso.3.6.1.4.1.21695.1.2.2.6.1 = INTEGER: 183 # Endereços com empréstimo expirado
(dhcpdSnmpPoolExpiredLeases)

iso.3.6.1.4.1.21695.1.2.2.6.2 = INTEGER: 212

iso.3.6.1.4.1.21695.1.2.2.6.3 = INTEGER: 209

iso.3.6.1.4.1.21695.1.2.2.6.4 = INTEGER: 189



O monitoramento dos pools de endereços mostram estatísticas interessantes do comportamento dos hosts em rede. Por exemplo, os horários com maior número de hosts ativos e horários de encerramento (caso os hosts sejam desligados ou suspensos). Outro caso é no uso de APs piratas em modo bridge. A quantidade de empréstimos de endereços aumenta muito e podem esgotar porque dispositivos móveis estão recebendo IPs da VLAN errada.

Para saber mais



Introdução ao protocolo DHCP -

<https://www.youtube.com/watch?v=lzwtJzw4SXM>



7) Backup de Banco de Dados: Dump x Cópia de arquivos

O backup de banco de dados é um procedimento de rotina na administração de redes e a garantia da integridade dos dados é fundamental. Um fator a ser avaliado é a duração do tempo para o término do backup. Enquanto está sendo feito o backup, o gerenciador de banco de dados estará com um consumo alto de recursos e fazendo *locks* nas tabelas para garantir a integridade dos dados. Durante este período, os acessos ao banco de dados poderão ficar indisponíveis. Portanto, reduzir o tempo do backup aumentará o tempo de disponibilidade de acesso aos dados.

Uma das soluções para reduzir o tempo de backup está na cópia dos arquivos binários do banco para um outro servidor e realizar o backup a partir deste servidor “replicado”. Para avaliar se este procedimento de cópia valerá a pena, pode-se somar o tempo da cópia dos arquivos do banco de dados para o outro servidor. Neste caso, o banco deverá ser parado, realizada a cópia na rede para outro servidor e reiniciar o banco. No servidor que recebeu a cópia dos arquivos, deverá haver a mesma versão do banco de dados do servidor original. Neste servidor, com os arquivos copiados, será disparado o backup do banco de dados. O tempo consumido pela ferramenta de backup para fazer o dump do banco de dados pode chegar a 6x que o tempo da cópia dos arquivos binários na rede de um servidor para outro (quanto mais rápida for a rede, menos tempo).

No Exemplo 7.1 está um caso de um banco de dados MySQL com 250 GB de dados, onde o tempo de cópia na rede resultou em um ganho considerável de tempo para o backup. O cuidado é que o banco ficará indisponível, foi parado, até o término da cópia dos arquivos entre os servidores. Após o término será disparado o backup no servidor replicado, onde não haverá conexões de usuários e o tempo para término do backup deixará de ser crítico.

Exemplo 7.1

Banco MySQL com 250 GB

- A) Servidor original - Tempo de backup: 8 hs
- B) Servidor Dedicado para Backup - Tempo de transferência dos arquivos entre servidores (rede 1 Gbit/s): por volta de 50min



Tempo para término do backup

- A) Servidor original: 8 horas (com consumo excessivo de recursos e possíveis intermitências no acesso dos usuários)
- B) Servidor Dedicado para Backup - 50min (mais 8 horas para terminar o procedimento de backup, sem afetar o banco de dados em produção)



O uso de bancos de dados em código-fonte aberto como MariaDB ou PostgreSQL são excelentes para cenários menos críticos. Quando há necessidade de sistemas com alto volume de dados e com tolerância a falhas, a administração destas soluções livres pode se tornar muito complexa ou inviável. Na minha experiência com banco de dados em código-fonte aberto, a primeira opção é o PostgreSQL, que ao longo dos anos é o que menos deu problemas em ambientes mais complexos.



8) Níveis de alertas e notificações

As ferramentas de monitoramento de redes são baseadas em notificações com níveis de alertas. Estes alertas são configuráveis de acordo com o nível de criticidade do recurso que está sendo monitorado. A quantidade de níveis de criticidade poderá variar de acordo com cada ferramenta. Na Figura 8.1 está um exemplo de níveis utilizados pela ferramenta Nagios Core (<http://www.nagios.org/>) para configuração de alertas. Para o monitoramento de Hosts existem os estados de *Up*, *Down*, *Unreachable* e *Pending* (significa que ainda não foi checado). No caso de Services (Serviços em execução em cada Host) os estados possíveis são *Ok*, *Critical*, *Warning*, *Unknown* e *Pending*.

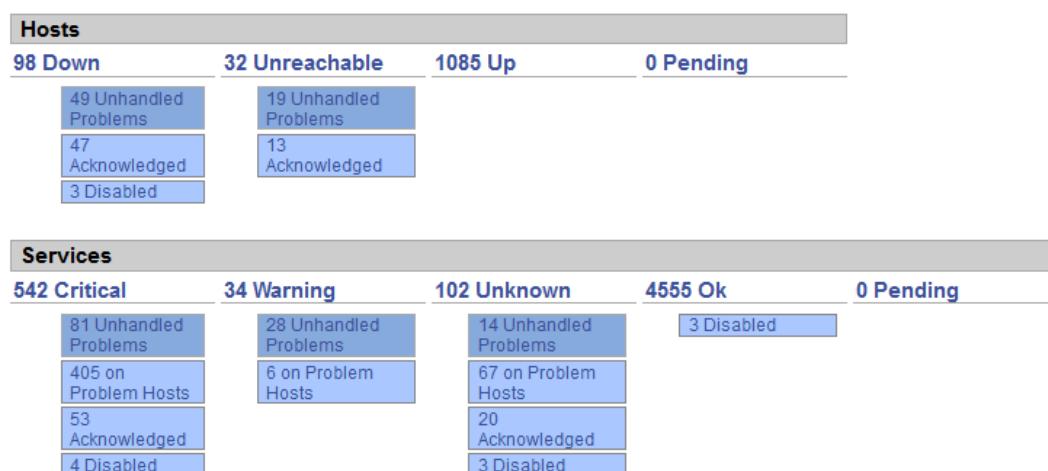


Figura 8.1. Níveis de criticidade da ferramenta Nagios.

A configuração das notificações de alertas deve obedecer a uma filtragem para os hosts e serviços realmente críticos e criar uma hierarquia de dependências. No caso de um host que está atrás de um roteador, quando o roteador ficar em estado de *Down* o host também será afetado podendo ficar em estado de *Down* ou *Unreachable*. Se a configuração não considerar esta hierarquia haverá duas notificações em vez de apenas uma informando a queda do roteador e o estado de *Down*.

Outra consideração sobre as notificações é qual estado realmente importa ser gerado um alerta. Existem mudanças de estado que ficam oscilando várias vezes durante o dia



causando um estado de *flapping*. Isto pode acontecer devido a uma configuração equivocada no limite de um serviço para mudar o estado de Ok para Warning. No Exemplo 8.1, está uma configuração para o serviço de checagem do número de processos em um servidor Linux com os limites para o estado de Ok, Warning e Critical. Para o estado de Ok seriam 149 processos ou menos, para o estado Warning de 150 até 159 processos e para o estado de Critical 160 ou mais processos. Com valores de limite muito próximos entre os estados haverá notificações de alertas de forma desnecessária. Em cada mudança de estado poderá haver a geração de uma notificação com um alerta. Estas notificações são enviadas por e-mail ou mensagens em aplicativos tais como Telegram ou Whatsapp (alguém ainda usa SMS para isto?).

Exemplo 8.1

```
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 160
```

Portanto, realizar uma análise dos Hosts e Serviços críticos resulta em uma quantidade reduzida de notificações e maior foco do administrador de redes para priorizar as ações de prevenção e correção. Os ajustes nos limites dos valores que serão considerados Ok, Critical ou Warning fazem toda a diferença para tornar a ferramenta de gerenciamento confiável. Avaliar se o recebimento de 100 notificações por hora é algo produtivo para a administração de servidores e serviços. Na prática poderá haver o descarte das notificações da mesma forma que mensagens de SPAM. Uma regra simples é monitorar o máximo possível, guardar o histórico dos monitoramentos e receber as notificações de alertas principais com níveis de criticidade alto.



Estabelecer perfis de monitoramento para hosts e serviços torna a atenção aos alertas melhor. Receber notificações de alertas na madrugada talvez não tenha efeito nenhum se o turno de trabalho do administrador não compreende este horário. Entretanto, deverão ficar registrados os alertas e as notificações para serem disparadas em horário em que a atenção do responsável estará focada.



9) Liberação de regras para DNS e navegação Web no firewall

As regras de firewall que devem ser liberadas, minimamente, para possibilitar a navegação Web em uma rede local tiveram algumas alterações devido a novos protocolos e o comportamento de protocolos clássicos. Uma das principais mudanças está no comportamento do protocolo DNS (*Domain Naming System*) que é o responsável pelo serviço de tradução de nomes de domínio para endereços IP. O DNS tem como base o protocolo UDP (*User Datagram Protocol*) na camada de transporte e o uso da porta 53. Entretanto, se a requisição ou a resposta de uma *query* DNS for maior do que 512 Bytes, o protocolo usado na camada de transporte será o TCP (*Transmission Control Protocol*). Com o uso de domínios em nuvem e o protocolo IPv6 a troca de UDP para TCP acontece nas *queries* com bastante frequência e poderá causar indisponibilidade no acesso a sites ou serviços.

Ainda em relação ao DNS, alguns navegadores como Firefox e sistemas operacionais como Android e iOS ativam como padrão o DoH (*DNS over HTTPS*). O DoH utiliza a porta TCP 443 para repassar as requisições e respostas de DNS de forma criptografada. Em situações onde o firewall deveria forçar o uso do serviço de DNS local realizando bloqueios para DNS externos nas portas UDP e TCP 53 não surtirá efeito. Para evitar o uso de serviços de DNS externos deverão ser feitos os bloqueios dos servidores de DoH pelo endereço IP.

Os protocolos QUIC e HTTP/2 utilizam na camada de transporte o protocolo UDP na porta 443. Desta forma, para liberar a navegação de forma plena serão necessárias as liberações das portas 443 para TCP e para UDP. O QUIC/HTTP/2 tem como objetivo a melhoria de desempenho em sites que foram desenvolvidos para aproveitar as conexões permanentes e o envio antecipado de objetos. Exemplos de sites e serviços que utilizam estes protocolos são Google, Youtube, Facebook, Instagram e TikTok. No Exemplo 9.1 a lista de portas mínima para liberação da rede interna para acesso à Internet.

Exemplo 9.1

Portas TCP: 443 (HTTPS), 53 (DNS), 80 (HTTP)

Portas UDP: 443 (QUIC), 53 (DNS), 123 (NTP)





O protocolo HTTPS é o mais utilizado nas redes atuais. Este protocolo é a base de todos os serviços e portais na Internet. E isto é um problema para identificar os tipos de serviços realizando análise de tráfego. Uma das formas para isto é verificando a troca de pacotes com os certificados, que ocorre em texto plano, para identificar pelo domínio qual o serviço que está sendo conectado. Para saber mais sobre classificação de rede tem este vídeo disponível em



https://www.youtube.com/watch?v=RSEaosSsd_0



10) Forçar o uso do endereço MAC como identificação no serviço de DHCP

O endereço MAC (*MAC Address*) é um identificador da interface de rede gerado pelo fabricante e é parte fundamental para o funcionamento de redes do padrão Ethernet. O endereço MAC é usado na camada de enlace de dados sendo usado pelo switch para encaminhar os pacotes aos destinos corretos. O protocolo ARP (*Address Resolution Protocol*) em IPv4 e o protocolo ICMPv6 em IPv6 realizam a descoberta do endereço MAC a partir do endereço IPv4 ou IPv6

O endereço MAC é usado como um identificador de dispositivos para acesso em serviços tais como portais de captura, ACLs (*Access Control List*) em switches ou autenticação no padrão IEEE 802.1x. É comum o uso do MAC para fixar endereços IP no servidor de DHCP. No Exemplo 10.1 um mapeamento de endereço MAC para um IPv4 do endereço físico 34:ea:e7:26:f2:5e para o endereço IP 172.16.128.1 em um servidor DHCP no sistema operacional Linux.

Exemplo 10.1

```
# Sensor1  
  
host sensor1 { hardware ethernet 34:ea:e7:26:f2:5e; fixed-address 172.16.128.1; }
```

Os sistemas operacionais Android, Windows, iOS e Linux possuem uma funcionalidade de geração de endereços MAC aleatórios. O objetivo é a privacidade do usuário e evitar que o dispositivo seja rastreado na rede. A principal motivação para esta funcionalidade está no uso em redes sem fios. No Exemplo 10.2 a descrição de como são gerados os endereços MAC aleatórios e como identificá-los nos logs.

Exemplo 10.2

```
Para cada SSID ou identificação de nova conexão de rede será gerado um endereço MAC  
  
O formato do endereço MAC é baseado em uso local  
  
2º bit menos significativo do 2 Byte do endereço fixado em “1”
```



00000010

3, 7, B, e F não são usados em unicast, somente em multicast

Identificação de endereços MAC de uso local, gerados de forma aleatória

X**2**-XX-XX-XX-XX-XX

X**6**-XX-XX-XX-XX-XX

X**A**-XX-XX-XX-XX-XX

X**E**-XX-XX-XX-XX-XX

Esta opção está ativada por padrão no Android e iOS. No Microsoft Windows 10 não está ativada por padrão, mas é provável que seja ativada nas próximas versões do sistema operacional. Este comportamento acontece em redes sem fios e a troca do MAC poderá acontecer por nome de rede ou por AP que o cliente faça à associação.

Outra forma de identificação de hosts na rede é com o uso de UID (*Unique Client Identifier*). O UID é usado pelo servidor de DHCP da mesma forma que o endereço físico. O objetivo seria que ao trocar o endereço MAC de um host não trocaria o UID. Com o uso de endereços MAC privados e aleatórios o uso de UID poderá fazer sentido. Porém tem um efeito colateral que é o servidor de DHCP emprestar mais de um IP para o mesmo host, considerando o endereço físico e o UID como identificações distintas. Ao fazer isto poderá exaurir os endereços IP disponíveis para empréstimo, além de causar problemas com sistemas de portais de capturas ou qualquer outro sistema que utiliza o endereço IP como parte da autenticação. O host que pegar 2 IPs, poderá usar um deles para autenticar e ao renovar o endereço pegar o outro IP que ficou emprestado para esse mesmo host.

Para evitar este comportamento, em servidores de DHCP é possível ignorar a identificação dos hosts por UID e deixar apenas por endereço físico. Em servidores Linux usando a versão mais recente do ISC DHCP Server, no arquivo **/etc/dhcp/dhcpd.conf** usar a diretivas do no Exemplo 10.3.

Exemplo 10.2

Para ignorar o UID e evitar empréstimos duplicados



```
deny duplicates;  
one-lease-per-client on;  
ignore-client-uids true;
```



O comportamento em rede dos sistemas operacionais tornam a administração de redes mais dinâmica do que o normal. No caso do comportamento do DHCP, um dos protocolos mais utilizados em rede, a alteração para uso de outra forma de identificação que não o endereço MAC pode causar sustos ao administrador. Desta forma, analisar os logs dos serviços e o tráfego de rede devem ser rotinas prioritárias.

Para saber mais



Random MAC Address - geração de MACs para privacidade dos usuários



- <https://www.youtube.com/watch?v=DHlowrr6wc4>



11) Ativar os logs de DNS para identificação de malware e domínios indesejados

Os registros em logs das requisições de DNS possibilitam ao administrador de redes o monitoramento de tráfego e de comportamento do usuário. Ao realizar o filtro dos registros pode-se encontrar informações importantes sobre clientes com comportamento anômalo ou com acesso a domínio reconhecidos como fontes de *malware*. Para ativar o log do servidor de DNS em serviços que implementam o ISC BIND pode-se utilizar a configuração do Exemplo 11.1.

Exemplo 11.1

```
logging {  
    channel queries_file {  
        file "/var/named/log/queries.log" versions 3 size 100m;  
        severity dynamic;  
        print-time yes;  
    };  
    category queries { queries_file; };  
};
```

Nos arquivos de logs serão registradas informações de cada requisição realizada para o servidor. A partir disto torna-se possível o uso de filtros para identificar domínios maliciosos ou indesejados e qual endereço IP está fazendo a requisição. No Exemplo 11.2 está o registro de uma requisição (*query*) para o servidor 10.15.130.1, feita a partir do cliente de IP 10.15.130.84 na porta UDP 54263, solicitando os endereços IPv4 do domínio www.youtube.com.

Exemplo 11.2



15-Dec-2024 20:35:44.926 client 10.15.130.84#54263 (www.youtube.com): query: www.youtube.com IN A + (10.15.130.1)



Os logs do serviço de DNS são importantes na administração de redes. Entretanto, com o uso de DoH (DNS over HTTPS) cada vez mais sendo usado, o controle sobre as requisições de DNS na rede interna está ficando mais complexo de se obter. Pode-se tentar bloquear os servidores de DoH externos, caso o cliente não consiga acesso a estes servidores, fará um fallback para o DNS configurado no sistema operacional do host. Este comportamento torna bem complicado para administrar serviços que dependem da resolução de DNS para funcionar corretamente, tais como portais de captura (captive portals).



12) DHCP Snooping

O serviço de DHCP (*Dynamic Host Control Protocol*) tem como objetivo facilitar a administração de endereços de rede e configurações. É um serviço fundamental e usado em praticamente todas as redes atuais. Entretanto, devido a ser um serviço simples e que consome baixos recursos computacionais está disponível em quase todos os dispositivos de rede, mesmos dispositivos que não seria para uso no gerenciamento de redes tais como impressoras ou câmeras de vídeo.

Em um ambiente de redes existe um servidor de DHCP legítimo, que fornece as configurações de endereços de acordo com a administração de redes. O problema está quando um servidor de DHCP pirata (*Rogue DHCP Server*) é ativado, distribuindo endereços e configurações diferentes. Esta ativação de um servidor DHCP pirata pode ser de forma involuntária ou maliciosa, de qualquer uma destas formas haverá intermitências e indisponibilidade para os usuários.

Para evitar os transtornos causados pelo DHCP pirata deve-se utilizar a funcionalidade disponível em switches gerenciáveis chamada *DHCP Snooping*. O *DHCP Snooping* ativa o monitoramento do tráfego de rede nas portas em busca de pacotes de DHCP originados por servidores. Para indicar qual a porta onde o servidor de DHCP legítimo está conectado, configura-se a porta no modo *Trust* (Confiável). Todas as outras portas deverão ficar como *Untrust* (Não confiável), ou seja, em caso de detecção de tráfego DHCP originado de um servidor na porta configurada como *Untrust* haverá um bloqueio e será gerada uma notificação no log do switch. As portas de uplink, onde o tráfego do servidor de DHCP legítimo tem que passar, devem ficar como *Trust*. Na Figura 12.1 um exemplo de configuração da funcionalidade de DHCP Snooping em switches HP modelo 1910. No Exemplo 12.1 um trecho de configuração em switches Huawei para ativação de DHCP Snooping, indicando quais portas são confiáveis (*Trust*) e quais seriam não confiáveis (*Unstrut*) para tráfego de servidor DHCP.



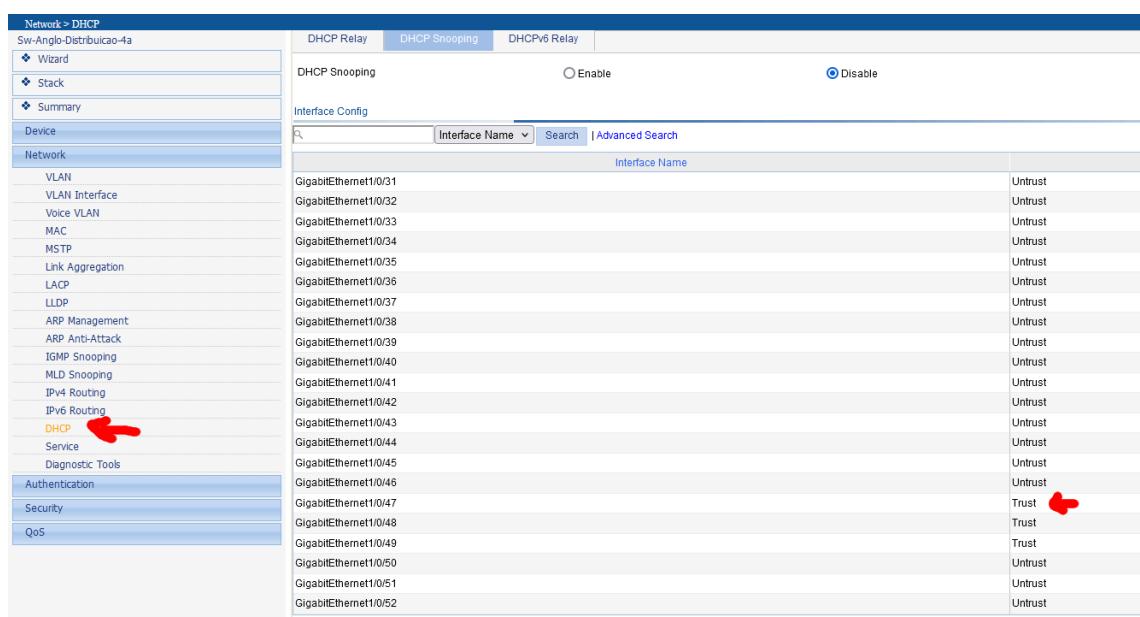


Figura 12.1 Configuração de DHCP Snooping em switches HP 1910

Exemplo 12.1

```

dhcp snooping enable ipv4
#
interface GigabitEthernet0/0/24
port link-type trunk
port trunk allow-pass vlan 10, 20, 30
dhcp snooping trusted
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 10

```



dhcp snooping enable

#

interface GigabitEthernet0/0/2

port link-type access

port default vlan 10

dhcp snooping enable

#

interface GigabitEthernet0/0/3

port link-type access

port default vlan 10

dhcp snooping enable

Quando não havia switches gerenciáveis ou ainda não havia a funcionalidade de *DHCP Snooping*, a forma de identificar a origem do DHCP pirata era na base do desliga porta/uplink até parar o tráfego indesejado. Atualmente, um switch gerenciável de acesso possui a funcionalidade de *DHCP Snooping* e basta ativá-la para evitar indisponibilidade na rede devido a um usuário desavisado conectar um AP ou qualquer outro dispositivo com um servidor de DHCP ativado.



Em uma época em que existiam poucos switches gerenciáveis e não havia a funcionalidade de DHCP Snooping o pesadelo do servidor de DHCP pirata assombrava o administrador de redes. A busca da origem do servidor pirata era na base do tira cabo de uplink, isolava um prédio ou uma área específica e verifica se parou de funcionar a distribuição de IPs diferentes dos corretos. Em uma rede pequena já era um problema complicado, em uma rede com dezenas de switches era tarefa demorada e chata, sem contar a necessidade de renovação de endereços IP das interfaces de rede dos hosts depois de achar o DHCP pirata.



Para saber mais



DHCP Snooping - evitando DHCP indesejado na rede -



<https://www.youtube.com/watch?v=WjutKkBziFI>



13) Limitar tráfego em broadcast e multicast

Os serviços de comunicação que se baseiam em descoberta de recursos ou envio de pacotes para endereços que representam **broadcast** (todos os hosts da rede diretamente conectados) ou que representam **multicast** (para hosts participantes de um grupo) são rotina em uma rede. Normalmente, este tipo de tráfego tem a função de controle e um volume alto destes pacotes não é algo desejável e pode indicar algum problema tal como um *loop* na rede. Quando há uma grande quantidade de pacotes em broadcast ou multicast denomina-se que são tempestades. Desta forma, levam o nome de **Broadcast Storm** e **Multicast Storm** para quantidade excessiva de pacotes em broadcast e multicast. O efeito no desempenho da rede será comprometido pelo consumo de recursos de CPU dos switches e pelo congestionamento do tráfego gerado pelos pacotes entrando em *loop* nas portas dos switches. Existem funcionalidades dos switches gerenciáveis que auxiliam a diminuir a quantidade de pacotes de broadcast e de multicast a um limite definido pelo administrador.

Por padrão não há limites de pacotes por segundo ou largura de banda que os pacotes de broadcast/multicast podem utilizar nas interfaces de rede. É uma boa prática limitar estes pacotes em portas de switch de acesso, nas quais estão conectados computadores de usuários, impressoras, telefones IP e dispositivos finais. Um valor razoável para o limite de pacotes por segundo (pps) para tráfego broadcast e multicast seria de 80 a 100 pps. Em alguns switches a limitação é feita por largura de banda em vez de pacotes por segundo. Nestes casos 50 a 100 Kbit/s seriam limites razoáveis para portas de acesso. Em portas do tipo *trunk* ou que sejam uplink os limites devem ser maiores ou nem haver limites. Em caso onde houver perdas de pacotes devido aos limites configurados poderá haver problemas com serviços de descobertas de dispositivos (ex.: impressoras) e não recebimento de endereços IP por DHCP, que é baseado em broadcast. No Exemplo 13.1 um trecho de configuração de limites de pacotes em broadcast e multicast da porta G0/0/21 em um switch Huawei modelo S5720. Nesta configuração se houver mais de 200 pps de broadcast ou multicast haverá o bloqueio da porta e registro em log.

Exemplo 13.1

```
interface GigabitEthernet0/0/21
```

```
description AirFiber
```



port link-type hybrid

port hybrid tagged vlan 2023 2200 3333 4079

port hybrid untagged vlan 142

stp loop-protection

storm-control broadcast min-rate 100 max-rate 200

storm-control multicast min-rate 100 max-rate 200

storm-control action block

storm-control enable log

Na Figura 13.1 um exemplo de configuração de limites de pacotes em um broadcast e multicast em 100 pps na porta 12 em um switch HP modelo 1910. Neste modelo as nomenclaturas das funcionalidades são *Broadcast Suppression* e *Multicast Suppression* e estão limitados em 100 pps.

The screenshot shows the 'Port Management' section of the HP Web Management Platform. On the left, a sidebar lists navigation options like Wizard, Stack, Summary, Device (selected), Basic, Device Maintenance, System Time, Syslog, Configuration, File Management, Port Management (selected), Port Mirroring, Users, and Loopback. The main area has tabs for Summary, Detail (selected), and Setup. Below the tabs is a 'Select a Port' section showing a 4x12 grid of ports numbered 1 to 48. Port 12 is highlighted in blue. To the right is a table with the following data:

Port State	Enabled [Active]	PVID	111
Flow Control	Disabled	Link Type	Hybrid
MDI	Auto	Speed	Auto [1000M]
Duplex	Auto [Full]	Max MAC Count	No Limit
Broadcast Suppression	100(pps)	Multicast Suppression	100(pps)
Multicast Suppression	100(pps)	Unicast Suppression	100%
Power Save	Enabled	Description	Hidrica3
EEE	Disabled		

A note at the bottom of the table states: "The table shows the configured values for the selected port, while those inside the square brackets are the actual values of the port."

Figura 13.1 Configuração de limites para Broadcast e Multicast Storm em switch HP modelo 1910

A configuração para limitação de pacotes em caso de tempestades de broadcast ou multicast originadas de *loops* são apenas paliativos e somente identificando e eliminando o *loop* será restaurado o comportamento normal da rede. Entretanto, se não estiverem ativados



os limites haverá indisponibilidade na rede e impossibilidade de acesso remoto a console do switch se um *loop* existir na rede.



Em episódios de loop físico na rede o volume de dados gerado pelos pacotes em broadcast e multicast tornarão a rede indisponível. Quando não havia switches gerenciáveis ou o switch gerenciável não possuía a funcionalidade de limitação de pacotes que não sejam em unicast, a solução era ir desconectando cabos nos racks até isolar o switch com o loop e desconectar os cabos das portas. Uma tarefa muito trabalhosa de descoberta e tentativa e erro. Vale lembrar que durante a busca a rede estava indisponível e a cada encontro com o usuário vinha aquela pergunta: “Que horas voltará à Internet?”

Para saber mais



Switches Gerenciáveis - <https://www.youtube.com/watch?v=37pqbjy2C6I>



14) Ativar agregação (Link Aggregation) em uplinks

As conexões de dispositivos em camada 2 em redes corporativas são realizadas por switches. Os switches possuem quantidades de portas disponíveis dentro de padrões tais como 8, 16, 24 e 48 portas, com portas adicionais com velocidades maiores para realização de conexões com o resto dos equipamentos de rede. Em modelos mais simples as portas adicionais possuem a mesma capacidade das demais portas, por exemplo 24 portas 10/100/1000, mas com tipo de interface diferente, por exemplo 4 portas do tipo SFP (*Small Form Factor*) com velocidade de 1 Gbit/s, usadas para conexão com interfaces mini GBIC e fibra ótica. Em switches de maior capacidade são comuns portas adicionais de 10 Gbit/s ou de maior capacidade e interfaces SFP+ para 10 Gbit/s.

Normalmente, as portas adicionais são usadas para cascamenteamento (uplinks) ou para conexão de equipamentos servidores (virtualização, storage, roteador/firewall). Portanto, a largura de banda que estará disponível entre a conexão de dois dispositivos será a menor velocidade entre as interfaces as quais estão conectados. Um dos casos mais comuns é a conexão entre dois switches, onde todas as portas são 10/100/1000. Ao realizar o cascamenteamento entre os switches haverá 1 Gbit/s disponíveis para todo o tráfego. Se houvesse portas de 10 Gbit/s em cada switch poderia ser realizado um cascamenteamento com capacidade 10x maior do que as portas comuns em cada switch. Nestes casos pode-se utilizar de uma funcionalidade disponível na maioria dos switches gerenciáveis atuais que é a agregação de portas (*Link Aggregation*). Esta funcionalidade permite agrregar portas físicas e criar uma porta lógica com capacidade de trafegar o total de cada porta física. A ideia é que ao se conectar N portas haverá tráfego de rede TxN (Tráfego de Redes x Número de Portas). Por exemplo, ao agrupar 4 portas de 1 Gbit/s haveria 4×1 Gbit/s disponíveis entre dois equipamentos (não será criado um link de 4 Gbit/s e sim um link de 4×1 Gbit/s). Na Figura 14.1 a funcionalidade de agregação de links em um switch HP modelo 1910. Basicamente, deve ser definida uma identificação de grupo e escolher quais interfaces farão parte da agregação. A partir disto será criada uma interface lógica que poderá ser configurada com VLANs, ACLs e demais configurações de uma porta física.



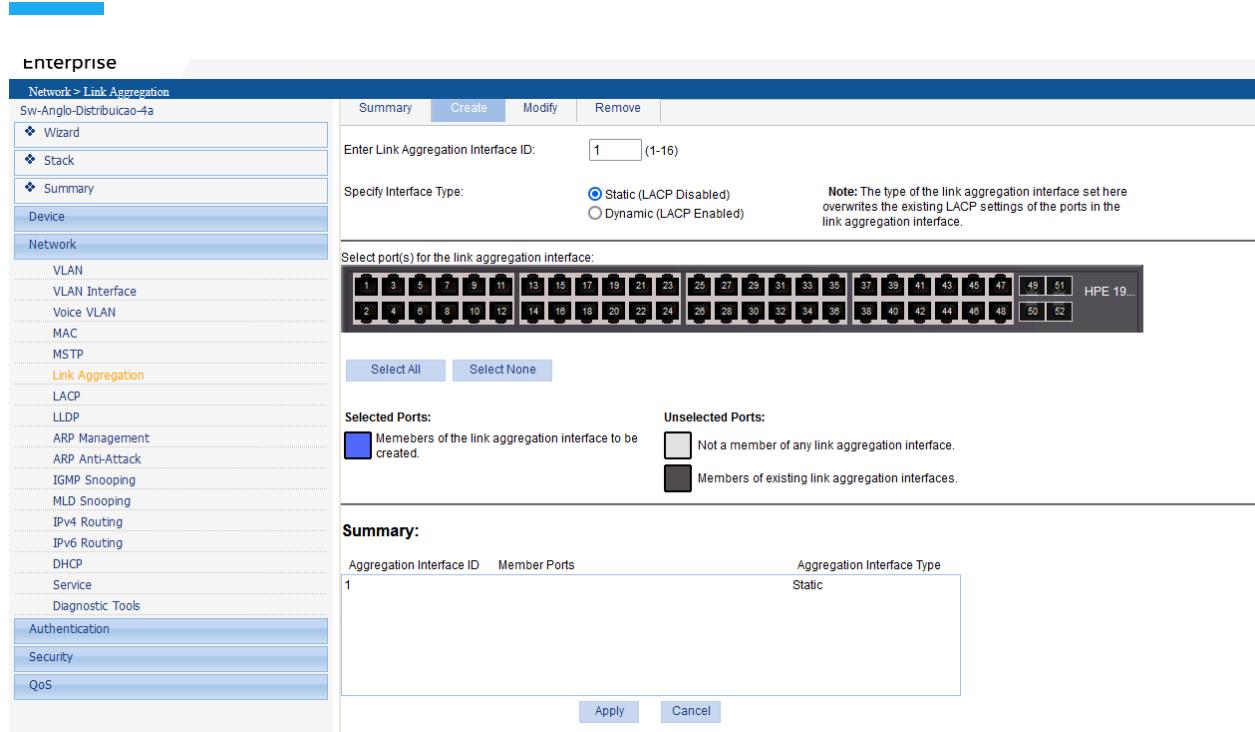


Figura 14.1 Funcionalidade de agregação de portas em um switch HP modelo 1910

A agregação pode ser realizada entre servidores e unidades de armazenamento. No caso dos servidores a agregação tem outro nome e se chama **bonding**. No **bonding** o objetivo é utilizar múltiplas interfaces de rede físicas e agrupar logicamente em uma única interface de rede com um endereço IP. Desta forma, a capacidade de conexão do servidor pode ser expandida facilmente. Vale lembrar que ao realizar qualquer um dos tipos de agregação as portas físicas dos switches serão ocupadas. Por exemplo, ao fazer o cascamente com um grupo de 4 portas agregadas haverá 8 portas consumidas, 4 portas em cada dispositivo conectado na agregação.



O uso de agregação de portas possui algumas limitações de acordo com cada dispositivo. As limitações são no número de portas máximo que podem ser agregadas, 4 portas é o limite mais comum, e quantos grupos de agregação podem ser configurados. O nome Etherchannel é proprietário da empresa Cisco, sendo o LACP (Link Aggregation Control Protocol) o nome usado no padrão IEEE 802.3ad. Outro fator é configurar como será feito o balanceamento nas portas da agregação, que pode ser feito por endereço MAC, endereço IP ou porta de



comunicação. Esta configuração definirá o desempenho da conexão.

Para saber mais



Etherchannel (Link Aggregation) -



<https://www.youtube.com/watch?v=rFWJB-1N99g>



15) Multihoming em servidores de arquivos

Uma forma simples de aumentar a vazão em servidores é usar o recurso de *multihoming*. O conceito de *multihoming* consiste em conectar um host em mais de uma rede simultaneamente. Em caso de uma rede com várias VLANs poderia haver uma conexão física do servidor em cada VLAN, em vez de utilizar uma porta tronco no switch ou realizar a comunicação por roteamento entre VLANs. Em servidores físicos é comum haver múltiplas interfaces físicas que poderiam ser usadas para conectar nas principais VLANs, as que possuem maior tráfego com o servidor. Do lado cliente, cada VLAN onde há uma conexão física com o servidor deverá usar um IP da mesma rede para não passar por roteamento. Na Figura 15.1 está um cenário onde o servidor de arquivos possui uma interface física de rede em cada VLAN e os clientes acessam com o IP diretamente conectado na mesma rede.

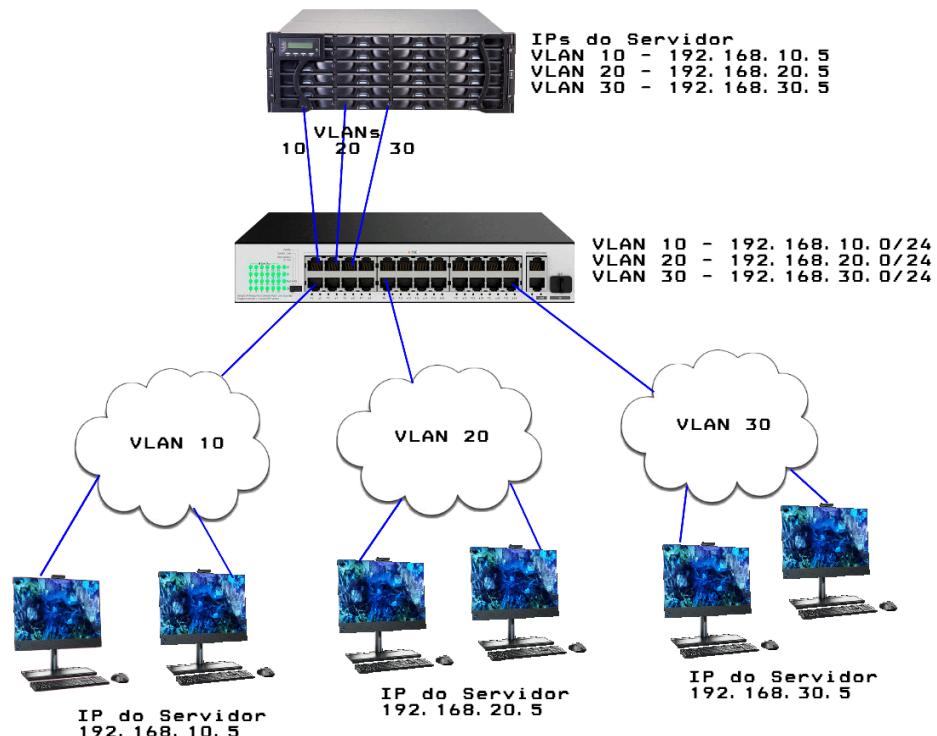


Figura 15.1 Cenário com um servidor de arquivos com três conexões físicas em VLANs diferentes

Outra forma de melhorar a vazão no acesso a um servidor de arquivos sem haver VLANs está em múltiplas conexões físicas na mesma rede, com IPs diferentes. A distribuição dos clientes pode ser realizada manualmente, 1/3 dos clientes para cada uma das 3 conexões, ou utilizar um registro de DNS com múltiplos IPs para o mesmo domínio, por exemplo `srv-arquivos.local` respondendo por 3 IPs diferentes. Neste caso do DNS, haverá uma fila circular (*round robin*) e a cada resolução de nome para IP será enviado um dos IPs que respondem pelo domínio. Na Figura 15.2 está um cenário com o uso de alocação manual de IPs e com uso de DNS para clientes na mesma rede. A VLAN 10 possui o endereço 192.168.10.0/24 e alguns clientes farão acesso de forma estática para o IP 192.168.10.3 e outros usarão a resolução de DNS para balancear em qual interface física a conexão será feita no servidor de arquivos.



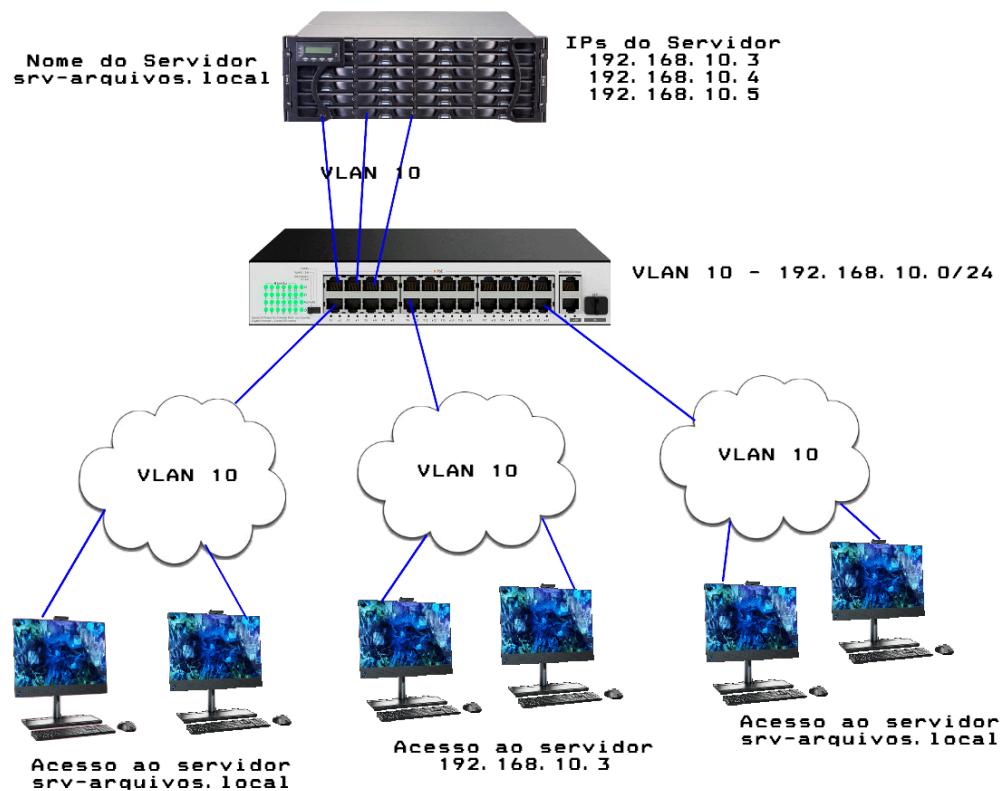


Figura 15.2 Alocação manual de IPs para distribuição no acesso ao servidor de arquivos

No Exemplo 15.1 está um trecho de configuração de uma zona de DNS para possibilitar a resolução de múltiplos IPs para um mesmo domínio. Quando o cliente fizer acesso ao domínio *srv-arquivos.local* será resolvido para qualquer um dos IPs disponíveis.

Exemplo 15.1

```
# Zona .local

srv-arquivos      IN      A      192.168.10.3
srv-arquivos      IN      A      192.168.10.4
srv-arquivos      IN      A      192.168.10.5
```





Utilizar interfaces físicas de rede em servidores para realização de backups ou transferências de grandes volumes melhoram o desempenho nas conexões de clientes. Entretanto, os recursos computacionais do servidor deverão suportar a carga. Caso isto não aconteça, o multihoming causará mais problemas do que solução.



16) Uso de VLANs

A configuração de VLANs possibilita uma melhor organização da rede. Separar os hosts por tipo de aplicação, acesso ou funcionalidade torna a execução das políticas de segurança mais simples. O isolamento para usuários convidados, câmeras de vigilância, impressoras, VOIP e da rede sem fios faz com que as regras de roteamento e firewall possam ser aplicadas para melhorias na segurança da rede com os domínios de broadcast separados. Com os domínios de broadcast separados os ataques que podem ser realizados em camada 2 tais como ARP spoofing, MAC spoofing e loops ficarão contidos na VLAN.

Outro fator é o acesso de compartilhamentos ativados em computadores de usuários que podem estar abertos e com possibilidade de descobertas e acessos indevidos. Ao usar um firewall para filtrar os acessos entre VLANs é possível reduzir bastante estas vulnerabilidades. Entretanto, se o compartilhamento estiver aberto na mesma rede do atacante o firewall entre as VLANs não terá efeito.

A relação da identificação de VLANs com o endereçamento IPv4 e IPv6 devem seguir uma organização. As identificações de VLANs, *VLAN ID*, compreendem uma faixa de 0 a 4095 (12 bits no cabeçalho). Algumas identificações de VLANs são reservadas, por exemplo a VLAN 1 que é a VLAN default dos dispositivos. Desta forma, ao montar o mapeamento de VLANs com endereçamento IP se deve considerar uma aproximação. No Exemplo 16.1 está um mapeamento de identificação de VLAN com endereçamentos IPv4 e IPv6.

Exemplo 16.1

VLAN	End.IPv4	End.IPv6
100	192.168.100.0/24	2804:0:AABB:100::/64
101	192.168.101.0/24	2804:0:AABB:101::/64
102	192.168.102.0/24	2804:0:AABB:102::/64
103	192.168.103.0/24	2804:0:AABB:103::/64
104	192.168.104.0/24	2804:0:AABB:104::/64





E como eram as redes sem as VLANs? Para isolar logicamente as redes eram usados endereçamentos IP distintos conectados na mesma rede física. Um host em uma rede só teria comunicação com outro em outra rede passando por um roteador. Entretanto, bastaria trocar o endereço IP do host para ele estar na outra rede. Outra forma de fazer era isolando as redes por meio físico, por exemplo, passando cabos separados, fazendo uma rede em paralelo. Esta foi a realidade em um momento em que as redes locais começaram a se expandir e os switches gerenciáveis possuíam altos valores de investimento.

Para saber mais



VLAN: Conceitos Básicos -

<https://www.youtube.com/watch?v=xZ-SOGYkafA>



17) Servidor de logs centralizado

A coleta automatizada e centralizada de logs deve ser organizada de forma cuidadosa. O registro de eventos em logs e a possibilidade de correlacionar com outras fontes de dados podem tornar a administração de redes mais simples. Os dispositivos com poucos recursos de armazenamento registram um número limitado de eventos em log e ao serem reiniciados perdem o conteúdo dos registros que ficam em memória volátil. Além deste caso, existem problemas relacionados à integridade dos logs quando há violações de segurança, por exemplo a remoção de logs ou comprometimento do host.

Manter um servidor de logs centralizado é algo simples de fazer e de manter, além de não consumir muitos recursos computacionais se for apenas armazenamento. Se houver uso de ferramentas para correlação de eventos e análise de logs, o consumo de recursos de processamento, memória e disco poderão ser muito grandes. O maior cuidado está na definição do que será logado e o tempo de retenção dos logs (dependerá da capacidade de armazenamento disponível). Um dos serviços mais usados e compatíveis é o que implementa o protocolo syslog. Em Linux, o syslog e suas atualizações é o padrão.

Em dispositivos tais como switches, APs, roteadores e impressoras quando há funcionalidade de log remoto a versão será compatível com o syslog. Portanto, não há necessidade de muitos recursos para ser disponibilizado um servidor de logs centralizado e que será bastante útil em casos em que os logs originais não estarão mais disponíveis. E a partir desta centralização podem ser usadas ferramentas de análise de logs e eventos para extraír informações relevantes para o administrador de redes. Exemplos de ferramentas para extração de informações são a tríade ELK (*Elastic Search, Logstash e Kibana*) e o Graylog. Na Figura 17.1 a configuração de log remoto em um switch HP modelo 1910.



Figura 17.1 Configuração de log remoto em um switch HP modelo 1910

No Exemplo 17.1 um trecho da configuração do arquivo /etc/rsyslog.conf em um servidor Linux com Rsyslog para possibilitar o recebimento de logs remotos

Exemplo 17.1

```
# Permite o recebimento de logs na porta UDP 514
$ModLoad imudp
$UDPServerRun 514
```

No Exemplo 17.2 um trecho da configuração do arquivo /etc/rsyslog.conf de um host linux para enviar os logs para um servidor de logs remoto com IP 102.168.10.9.

Exemplo 17.2

```
*.* @192.168.10.9
```



O armazenamento de logs é algo infinito e o tempo de retenção torna-se um problema a ser administrado com cuidado. Deve-se ficar atento às questões legais em relação a logs de conexões e endereços para possíveis identificações de usuários. Não é somente armazenar os logs, mas possuir uma forma de filtrar e relacionar os logs de diversos formatos em algo que possa gerar a informação necessária. Saber o caminho percorrido por um dispositivo móvel de um usuário dentro de uma área coberta por rede sem fios corporativa (WLAN) é trivial com os



logs ativados do AP e o conhecimento do MAC da interface do usuário. Entretanto, a geração de endereços MAC aleatórios nos sistemas operacionais Android, iOS e Microsoft Windows não vão tornar a vida do administrador de redes e a busca nos logs mais simples no futuro.

Para saber mais



Administração de Logs - https://www.youtube.com/watch?v=_OkxboqXfIY



18) Backup de banco de dados

A realização de backup de banco de dados é uma tarefa de rotina na administração de redes e uma das mais importantes. O backup tem como objetivos manter os dados íntegros e disponíveis para recuperação em caso de sinistros ou necessidade de registros históricos. Em sistemas de gerenciamento de banco de dados não somente os dados, registros armazenados em tabelas do banco, devem ser realizados backup. O banco de dados será acessado por um sistema e por usuários, que possuem permissões específicas, funções criadas no banco e as configurações do banco de dados (*tuning*) são fundamentais e devem estar incluídas na rotina de backup.

Quando houver a necessidade de uma restauração dos dados, sem haver a restauração também dos usuários, senhas, permissões e funções o sistema não ficará disponível, mesmo que todos os dados de registros estejam recuperados. Portanto, deve-se verificar a rotina de backup para incluir todo o necessário para a restauração do sistema de forma íntegra. Uma das formas para saber se está tudo correto é montar um ambiente de testes para simular a restauração do banco de dados e do sistema como um exercício periódico de validação do backup. No Exemplo 18.1 um trecho de script para backup de usuários e permissões em bancos de dados MySQL e PostgreSQL.

Exemplo 18.1

```
### MySQL

# Usuários

/usr/bin/mysqldump -u $MUSER --password=$MSENHA --no-create-info mysql user > usuarios.sql

# Grants

/usr/bin/mysql -u $MUSER --password=$MSENHA --skip-column-names -A -e"SELECT
CONCAT('SHOW GRANTS FOR "','"user','"@"','host','";') FROM mysql.user WHERE user<>'"

| mysql -u $MUSER --password=$MSENHA --skip-column-names -A | sed 's/$;/g' > grants.sql
```



```
### PostgreSQL  
# Backup de usuarios do Postgresql  
su - postgres -c "pg_dumpall --globals-only -S postgres > usuarios.sql"
```



O backup de banco de dados tem algumas particularidades importantes. No espaço de tempo entre os backups não haverá cobertura dos dados alterados. Um caso comum é realizar o backup na madrugada. Portanto, entre a madrugada do dia anterior e até o começo do próximo backup os dados não terão cópias. Caso algo dê errado neste espaço de tempo, causado por um disco com problemas ou uma alteração nos dados de forma errada, não haverá cobertura do backup. Isto deve ficar claro para todos os envolvidos com os dados e evitar uma surpresa desagradável com possíveis perdas de dados.

Para saber mais



Script para Backup de Bancos de Dados MySQL, MariaDB e Postgresql -



<https://www.youtube.com/watch?v=hpEFnmS9N6w>



19) Bloqueios por consumo de tráfego

Gerenciar de forma eficiente o consumo de largura de banda é um dos desafios na administração de redes. Usar procedimentos automatizados para detecção dos maiores consumidores de largura de banda deve ser realizado. Um uso fora do padrão no consumo de largura de banda poderá indicar um host com malware ou uso de aplicações para download ou upload de disseminação de conteúdo ilegal. O propósito do que está sendo feito para consumir a largura de banda acaba sendo algo secundário porque existirá o congestionamento no link de acesso à Internet. Uma das alternativas utilizadas para evitar este tipo de comportamento é restringir a largura de banda de todos os hosts, limitando cada endereço IP a um valor máximo de banda.

Entretanto, este tipo de estratégia prejudica o desempenho das aplicações que são baseadas em rajadas de pacotes e que consomem um grande volume de tráfego em poucos segundos. O problema do consumo de tráfego está em downloads e uploads que possuem volume de dados e duração maior. Portanto, não há sentido limitar a largura de banda de todos os usuários. Deve-se identificar os usuários que estão consumindo de forma excessiva os recursos de rede e realizar procedimentos para que não prejudiquem os demais. Uma das primeiras alternativas que surgem para o administrador de redes após identificar um endereço consumindo recursos é realizar o bloqueio do endereço IP do usuário.

Porém, pode estar sendo realizado um download ou upload legítimo e ao bloquear o endereço o usuário terá a conexão interrompida e terá que recomeçar a transferência ao ser desbloqueado. Em casos em que seja identificado um tráfego de malware deve-se bloquear de forma permanente até a resolução do problema. Nos casos onde não sejam identificados tráfegos maliciosos, apenas consumo de download ou upload, pode-se reduzir a largura de banda do endereço IP de forma temporária e não causar a interrupção da conexão. Ao identificar o endereço IP que está consumindo a largura de banda, por exemplo usando ferramentas tais como Iftop, Netflow, Tcpdump, pode-se associar o IP a uma classe de QoS (*Quality of Service*) com um limite de largura de banda definido pelo administrador de redes. Em Linux está disponível a ferramenta **tc** para criação de filas com limites de largura de banda e com recursos para associar um endereço IP a determinada fila. Ao reduzir a largura de banda por endereço IP o usuário poderá continuar o download ou upload, com vazão reduzida, e o consumo do link para o restante dos usuários poderá ser melhor gerenciado.



No Exemplo 19.1 está um script que cria duas filas com restrição de 1,5 Mbit/s cada uma e associa dois endereços IP, um em cada fila. A interface eth1 seria a interface do lado interno da rede, onde os endereços IP estão conectados diretamente.

Exemplo 19.1

```
# Exemplo de uso do CBQ para dois endereços IPs, com classes de 1500 kbit/s cada

# Remove o raiz

/sbin/tc qdisc del dev eth1 root

# Adiciona o raiz com o limite máximo de 1000Mbit com o handle 20:

/sbin/tc qdisc add dev eth1 root handle 20: cbq bandwidth 1000Mbit allot 1514 avpkt 1000

#Define uma classe com o ID 20:10 com 1500 kbit/s

/sbin/tc class add dev eth1 parent 20:0 classid 20:10 cbq bandwidth 1000Mbit rate 1500kbit
allot 1514 weight 1 prio 5 maxburst 21 avpkt 1000 bounded isolated

#Define a politica da classe

/sbin/tc qdisc add dev eth1 parent 20:10 sfq perturb 15

# Cria filtro para associar o IP 10.0.0.10/32 a classe 10

/sbin/tc filter add dev eth1 protocol ip parent 20:0 prio 10 u32 match ip src 10.0.0.10/32 flowid
20:10

/sbin/tc filter add dev eth1 protocol ip parent 20:0 prio 10 u32 match ip dst 10.0.0.10/32 flowid
20:10

#Define uma classe com o ID 20:11 com 1500 kbit/s

/sbin/tc class add dev eth1 parent 20:0 classid 20:11 cbq bandwidth 1000Mbit rate 1500kbit
allot 1514 weight 1 prio 5 maxburst 21 avpkt 1000 bounded isolated
```



```
#Define a politica da classe  
  
/sbin/tc qdisc add dev eth1 parent 20:11 sfq perturb 15  
  
# Cria filtro para associar o IP 10.0.0.11/32 a classe 10  
  
/sbin/tc filter add dev eth1 protocol ip parent 20:0 prio 11 u32 match ip src 10.0.0.11/32 flowid  
20:11  
  
/sbin/tc filter add dev eth1 protocol ip parent 20:0 prio 11 u32 match ip dst 10.0.0.11/32 flowid  
20:11
```



O consumo de largura de banda em ambientes corporativos para navegação e acesso a serviços básicos tais como DNS e e-mail não são um problema devido à capacidade dos links atuais. Entretanto, em redes sem fios o problema continua. A forma de compartilhamento em um AP é tal como em um hub, onde existem colisões, com o agravante das interferências externas ao canal de comunicação. Desta forma, mesmo com um link de grande capacidade para escoar o tráfego para a Internet, dentro de uma rede local sem fios ainda haverá a incidência de limitações de banda devido ao modo de operação de um equipamento sem fios.

Para saber mais



Gerenciamento de Largura de Banda -

<https://www.youtube.com/watch?v=z7vmkujLILc>



20) Janela de manutenção

As janelas de manutenção são usadas para realizar atualizações, migrações, correções e procedimentos que demandam indisponibilidades em sistemas, serviços e conexões. Estimar o tempo que será necessário para realizar os procedimentos deve considerar se as coisas não derem certo. Um dos erros mais comuns é realizar os procedimentos em um ambiente de testes e contabilizar somente o tempo de tudo der certo. Na minha experiência profissional foram diversos episódios que uma janela de manutenção prevista para um tempo determinado excedeu o esperado e causou indisponibilidade de sistemas, serviços e conexões. Portanto, ao estimar a janela de manutenção estabelecer com folga o tempo de parada e programar com todos os envolvidos (público interno e externo). O tempo para o término de algum procedimento deve ser avaliado em relação ao que pode dar errado. No Exemplo 20.1 estão alguns procedimentos que deveriam ser rápidos e acabaram não sendo.

Exemplo 20.1

Seria só um reboot “rápido”, mas não voltou ainda...

O backup termina em 10 minutos, já se passaram 40 minutos...

O switch será reiniciado e já voltará o acesso à Internet, (só que na volta, a porta do roteador negociou em 10 Mbit/s Half-Duplex e só foi percebido uma hora depois...)

Muitos fatores podem causar variações nos tempos considerados “normais”, por exemplo, uma atualização pendente que será aplicada ao reiniciar o servidor ou realizar um backup em horário fora da rotina. Deve-se avaliar os riscos dos procedimentos antes de estimar o tempo necessário para o término. Estabelecer um tempo de manutenção realista não é simples, envolve a experiência em outras manutenções similares. Em vários casos não é possível criar um ambiente de testes igual ao ambiente de produção para avaliar o tempo exato que demandará uma atualização ou uma troca de *firmware* em um storage. Portanto, deve-se estimar um tempo com uma tolerância razoável e evitar “promessas” tais como estão listadas no Exemplo 19.2

Exemplo 20.2



Em 30 minutos será feito a ativação do rack

A atualização dos 8 servidores Windows deverá durar, no máximo, 45 minutos

Se tudo der certo, tudo estará funcional em 2 horas (como garantir o “Se tudo der certo”?)

Realizar o maior número possível de testes e validações de forma antecipada a manutenção agendada. Se aplicável, começar a fazer os procedimentos mais complexos inicialmente e depois os mais simples. Criar um checklist para validar os procedimentos e ter planos para caso seja necessária alguma alteração no plano inicial, o quase sempre esquecido “Plano B”. Ao acelerar os procedimentos necessários para validação corre-se o risco de sair da janela de manutenção e ter surpresas desagradáveis.



Um dos episódios que tornam um administrador de redes mais experiente e em muitas vezes causam traumas está nas janelas de manutenção. Em um destes casos, uma janela de manutenção programada para durar 30 minutos, seria uma parada no servidor de arquivos Novell Netware 3.12 para clonar um HD com defeito, durou mais de 4 horas e criou o mito do “Teste do Meio-Metrinho”. A história completa está no vídeo disponível em

<https://www.youtube.com/watch?v=fOjPplBI-kg>



21) Remoção de regras de firewall no Linux

Em sistemas operacionais Linux o firewall é baseado no *framework* Netfilter. O Netfilter pode ser manipulado pelos utilitários Iptables ou Nftables para criação de regras de filtragem e alteração de pacotes. Estes dois utilitários são os de mais baixo nível e são usados como base para outras implementações de firewall tais como Shorewall, UFW e Firewallld. O Iptables é o utilitário mais popular e amplamente utilizado como base em soluções de firewall no sistema operacional Linux.

A estrutura do Iptables é baseada em *chains*, que seriam contextos de aplicação das regras. Por exemplo, a *chain* INPUT seria relacionada aos pacotes que são destinados a uma interface do host. Outro exemplo seria a *chain* FORWARD onde as regras criadas afetam os pacotes que passam entre interfaces de um roteador. Além das *chains* padrão podem ser criadas outras para uso em regras de acordo com a aplicação desejada.

Outro fator importante a se considerar em um firewall Iptables está relacionado às políticas das *chains*. As políticas basicamente podem ser todos os pacotes aceitos ou todos os pacotes bloqueados. Em caso de política de tudo aceito, qualquer pacote será permitido e apenas os pacotes que baterem em alguma regra serão bloqueados. Já no caso da política tudo bloqueado, somente os pacotes que baterem em uma regra da *chain* será permitido.

Quando é necessária a remoção do firewall, não basta apenas remover as regras de bloqueio ou liberação, deve-se alterar as políticas da *chain*. Em um cenário onde a política da *chain* é tudo bloqueado e as regras são de liberação, ao remover as regras de liberação o acesso poderá ficar indisponível porque os pacotes serão todos bloqueados. Portanto, a remoção das restrições de firewall deve ser feita com cuidado e validação do resultado para não ocorrer perda de acesso a um host remoto ou deixar um acesso à Internet indisponível em uma rede corporativa. No Exemplo 21.1 um trecho de script de firewall para limpar as regras de firewall, limpar *chains* não padrão e aplicar políticas de tudo permitido.

Exemplo 20.2

```
# Limpa tabelas e configura defaults  
iptables -F -t filter
```



```
iptables -F -t nat  
iptables -F -t mangle  
  
# Delete chains não defaults  
  
iptables -X  
  
iptables -X -t nat  
  
iptables -X -t mangle  
  
# Políticas em ACCEPT, chains INPUT, OUTPUT e FORWARD  
  
iptables -P INPUT ACCEPT -t filter  
  
iptables -P OUTPUT ACCEPT -t filter  
  
iptables -P FORWARD ACCEPT -t filter
```



Realizar procedimentos em firewall de forma remota deve ser feito com o máximo de cuidado. Ao aplicar uma regra errada poderá causar a perda de acesso remoto ao firewall e ao restante da rede protegida por este firewall. Mesmo não salvando a configuração, onde um reboot do firewall retornaria a versão antes da alteração, haveria alguém apto para isto no lado remoto?

Para saber mais



Iptables na Prática - <https://www.youtube.com/watch?v=6a-nJ3NQccs>



22) Temperatura de data center/sala de servidores

Existem recomendações sobre quais temperaturas seriam as necessárias para manter o tempo de vida útil dos equipamentos. A temperatura recomendada é dependente do tipo de equipamento, por exemplo HD, memória, processador ou GPU. Acima ou abaixo da temperatura recomendada os equipamentos sofrerão alterações no funcionamento e prováveis danos permanentes. A primeira ideia seria colocar na temperatura mais baixa configurável no aparelho de ar condicionado. Caso o projeto de climatização esteja correto, a temperatura configurada no aparelho será entregue no ambiente. Caso não tenha sido feito um projeto correto, o aparelho trabalhará de forma constante a plena capacidade para tentar entregar a temperatura. Em breve, é provável que este aparelho não esteja mais em funcionamento.

A ASHRAE (*American Society of Heating, Refrigerating and Air Conditioning Engineers*) publica guias de recomendações para climatização em data centers. Define 4 classes de equipamentos: A1, A2, A3 e A4. Sugere condições recomendadas (melhor caso) e permitidas (mínimo), sendo a última recomendação foi publicada em 2021, disponível em https://www.ashrae.org/file%20library/technical%20resources/bookstore/supplemental%20files/referencecard_2021thermalguidelines.pdf. No Exemplo 22.1 estão as recomendações, segundo a ASHRAE, as quais seriam as temperaturas recomendadas e permitidas.

Exemplo 22.1

Para data centers de alta densidade (classe H1)

Recomendado: de 18 a 22 °C

Permitidas: de 5 a 25 °C

Para os outros tipos de data center (classes A1 a A4)

Recomendado: de 15 a 32 °C

Permitidas: de 5 a 45 °C

Os níveis de umidade aceitos ficam entre 20% e 80%



Além da recomendação da ASHRAE, o relatório técnico “*Temperature management in data centers: Why some (might) like it hot*” de 2012 faz uma análise da relação de falhas de discos com as condições ambientais de data centers do Google. O trabalho apresenta considerações importantes sobre a relação temperatura versus falhas de componentes. Os autores apresentam testes onde a variação da temperatura influencia mais nas falhas do que na temperatura estável. O aumento de alguns graus na temperatura não afetou de forma considerável a confiabilidade dos componentes. A economia de energia com a climatização torna o risco da perda de algum componente de hardware aceitável.

A partir destas recomendações e análise, diferente do que é o senso comum, não há nenhuma necessidade de colocar a temperatura de um data center de uso comum no nível mais baixo possível. Os componentes dos servidores, tais como disco, CPU e memória possuem tolerância para suportar temperaturas consideradas altas em um data center sem prejuízo de desempenho ou danos aos componentes. Sistemas homologados para uso em data center podem utilizar as recomendações da ASHRAE. Sistemas de menor porte devem usar as orientações mínimas da ASHRAE, **22 ou 23 °C** seria uma boa opção. As vantagens para o uso de temperaturas mais altas está no aumento do tempo de vida útil dos aparelhos de ar condicionado, principalmente em aparelhos “domésticos” que não são dimensionados para uso em 24x7x365, e a redução do consumo de energia que gera um custo considerável. Em resumo, se o Google não utiliza temperaturas tão baixas no seus data centers, por que não poderemos fazer?



A climatização controlada para equipamentos que funcionam em regime de 24x7x365 torna a vida útil muito maior e é fundamental para a disponibilidade da rede. Porém, no mundo real, acontecem casos onde os 2 aparelhos de ar condicionado falham simultaneamente e a temperatura de 22 graus sobe rapidamente para 40 graus. O que fazer nestes casos? Colocar ventiladores para fazer a troca do ar quente da sala dos servidores com o ambiente externo. Como melhor prática em projetos de data center não há janelas para abrir. Portanto, realizar a manutenção dos aparelhos de ar condicionado é tão importante quanto monitorar o espaço em disco de um servidor de arquivos.

Para saber mais





Temperatura em Data Center -

<https://www.youtube.com/watch?v=Uw3r7T4odNk>



23) Emulador CORE

O emulador CORE (*Core Open Research Emulator*) é uma ferramenta de emulação de redes baseado em Linux. Derivado do projeto IMUNES, desenvolvido na universidade de Zagreb (Croácia), patrocinado pelas empresas Boeing e Ericsson em 2004. O projeto CORE utiliza a licença BSD e é liderado por Jeff Ahrenholz (Boeing). O projeto CORE, começou em 2008 e está atualmente na versão 9.10. O código está disponível em <https://github.com/coreemu/core>

Os emuladores de redes são apenas ferramentas e deve haver conhecimento por parte do usuário para obter resultados úteis dos cenários utilizados. O emulador CORE é uma ferramenta com diversas funcionalidades interessantes tais como o uso de aplicações reais em ambiente emulado, simplificação na montagem de cenários, possibilidade de ser adaptado e expandido (código-fonte aberto) e pouco consumo de recursos computacionais. Entretanto, o CORE possui algumas limitações no uso VLANs, limitações para execução de aplicações (customização), a documentação não é tão vasta e alguns bugs na interface.

A instalação do emulador CORE demanda diversos serviços e aplicações para funcionar de forma correta. Para facilitar o acesso à ferramenta foi disponibilizada uma versão em máquina virtual criada pelo autor para uso em laboratórios das disciplinas do curso de Redes de Computadores e está acessível em <https://mega.nz/file/r94wxKDL#dafvk3ukDY7v2ywiWXei4F-KVoxJd7Uvp5cDcZHosKU>



As versões mais atuais do emulador CORE são bem diferentes da versão disponibilizada em máquina virtual que é da série 4.x. A versão da máquina virtual possui diversos serviços e aplicações prontos para serem usados. Ao baixar uma versão mais atual deverá ser montado todo o ambiente com serviços instalados no hospedeiro do emulador CORE para os cenários funcionarem da forma correta.

Para saber mais





Emulador CORE- https://youtu.be/ELcZ1Vnwu-s?si=CMnN_AX8HN7fEK-o



Este trabalho está licenciado com uma Licença [Creative Commons - Atribuição-NãoComercial-Compartilhável 4.0 Internacional](#)

24) Snapshots antes de alterações em VMs

Em ambientes de virtualização existe a funcionalidade de snapshot. O snapshot possibilita criar um estado da máquina virtual que provê o retorno ao estado original em caso de alguma alteração posterior. É usado antes de testes com atualizações ou instalações em máquinas virtuais. Entretanto, snapshot não é backup porque o estado dos arquivos ou consistência de um banco de dados não serão garantidos. As conexões de rede que estiverem ativas no momento do snapshot não estarão ativas quando for realizada a restauração posteriormente. Isso vale para transações em andamento no banco de dados que ficarão inconsistentes ao ser restaurado o *snapshot*.

Ao realizar snapshots de máquinas virtuais haverá consumo de armazenamento no disco do hospedeiro. Se for realizado um snapshot com o estado da memória da VM, haverá um dump de igual tamanho da memória RAM no disco do hospedeiro. Portanto, deve-se manter organizado os snapshots para evitar consumo excessivo no disco do hospedeiro e causar indisponibilidades no ambiente.



O recurso de snapshot é usado para casos em que uma alteração no sistema operacional convidado ou na aplicação hospedada na VM poderá causar problemas. Em um ambiente virtualizado o snapshot deve estar no topo da lista de procedimentos que um administrador deverá executar antes de alterar o sistema operacional ou aplicação na máquina virtual.

Para saber mais



Backup - Myths & Legends in Computer Network Administration



#5 - <https://www.youtube.com/watch?v=3LV2CWh6rxM>



25) Descoberta de IPs em uso

Quando não há uma organização do endereçamento IP torna-se complexo a descoberta de IPs livres para uso. Em VLANs que não fazem uso de serviço de DHCP, onde todos os hosts possuem endereços IP estáticos, com servidores em uma DMZ, o problema de descobrir IPs livres é algo comum. Em VLANs com um grande número de hosts que provêm serviços a necessidade de descobrir um IP livre acontecerá quando da ativação de um novo servidor. Caso o administrador de redes seja organizado e possua uma ferramenta de gerenciamento de endereços, uma planilha simples já serviria, seria tudo mais simples. Entretanto, na prática, acaba acontecendo a necessidade de descobrir um IP não usado para usar no novo servidor.

Uma das formas mais simples é o uso da tabela ARP. Ao realizar testes de ping para todos os hosts ativos na rede haverá o registro na tabela ARP do MAC de cada um IP que respondeu. A ferramenta **arp-scan** pode ser usada para este tipo de verificação. No Exemplo 25.1 uma linha de comando para realizar a varredura da rede 10.10.16.0/24 em busca de hosts ativos e filtra pelo IP 10.10.16.71. Caso haja ocorrência do IP filtrado, ele está em uso.

Exemplo 25.1

```
#Realiza uma varredura na rede da interface eth1, 10.10.16.0/24 e filtra pelo IP 10.10.16.71  
arp-scan -l eth1 10.10.16.0/24 | grep 10.10.16.71
```

Outra forma é verificar nos registros de DNS por domínio que possuam IPs relacionados. Os testes com ARP só terão resultados para hosts ativos na rede. Caso o host esteja desligado, não será possível verificar se o IP está livre ou não. Só será possível saber quando o host for ligado e o endereço conflitar com o novo host conectado na mesma rede. Outro local possível de verificar se um endereço está sendo usado é na lista de hosts em ferramentas de monitoramento. Se houver algum registro do IP pode indicar que o host pode estar desligado temporariamente.





Manter a organização do endereçamento IP com uma equipe de pessoas não é uma tarefa das mais fáceis. O uso de IPs para testes temporários, que viram permanentes, a alocação de IPs reservados para uso futuro em uma máquina virtual criada de forma “urgente” e outros episódios similares causam transtorno e podem ser diminuídos com o uso de ferramentas de IPAM (IP Address Management) tais como phPIPAM (<https://phpipam.net/>) e netbox (<https://github.com/netbox-community/netbox>). Entretanto, se a ferramenta não for mantida e atualizada, haverá o mesmo problema de desorganização, só que agora com uma ferramenta para aumentar a bagunça.



26) Backup de configurações de serviços

Ao realizar alterações nas configurações de serviços e aplicações é importante preservar uma cópia do arquivo original. Em casos em que a alteração realizada não resulte em sucesso, ficará simples de voltar ao estado anterior. Quando são usados arquivos com as configurações dos serviços bastaria fazer uma cópia do arquivo original *arquivo.cfg*, renomear para algo como *arquivo.cfg-23122024v1* (usar a data corrente e algum indicativo de versão, no exemplo seria dia 23/12/2024 e versão 1) para retornar em caso de problemas.

Isso vale para os arquivos de configuração que são disponibilizados por padrão na instalação de um serviço ou sistema. É comum que nestes arquivos existam dicas de parâmetros e diretivas que ajudam a realizar configurações. Realizar a cópia destes arquivos para algo como *arquivo.cfg-default* poderá facilitar um acesso posterior ou retornar para o padrão da instalação.



Recuperar um arquivo de configuração em uma rotina de backup que acontece apenas uma vez por dia na madrugada não terá efeito. Durante a janela não coberta de backup haverá apenas o último arquivo alterado e não as versões deste arquivo com as alterações prévias. Portanto, realizar cópias antes de fazer as alterações é uma melhor prática na área de administração de redes.



27) Usar comentários nos arquivos de configuração

Quando são feitas alterações em arquivos de configuração de serviços, aplicações e sistemas deve-se registrar em formato de comentário quem, quando e qual o motivo da alteração. Isto torna o processo de análise em caso de problemas mais simples. Em um cenário onde um serviço parou de responder, por exemplo o serviço de banco de dados, ao verificar o arquivo de configuração com comentários ficará bem mais rápido identificar a causa do problema e quem realizou o procedimento.

Os comentários são fundamentais quando existe mais de um administrador de redes responsável pelo suporte ao sistema ou serviço. Criar uma armadilha para o colega não é algo incomum, onde uma mudança na configuração poderá causar uma indisponibilidade em um acesso não previsto no momento da alteração. Mesmo com um único administrador poderá haver o esquecimento do motivo da troca de um parâmetro, em caso de não haver documentação ou registro no próprio arquivo. Pensar em algum momento depois de 2 anos será necessário alterar o arquivo e será pouco provável que o administrador lembrará o motivo da alteração.

É uma boa prática deixar o valor original, anterior a modificação, comentado para referência futura. Normalmente, o valor original de algum parâmetro é genérico e representa um limite aceitável para funcionamento mínimo do sistema ou serviço. Desta forma, seria um valor para restaurar as condições de ativação de um serviço. Esta informação poderá resultar em algumas horas a menos em um serviço que fique indisponível. No Exemplo 27.1 um trecho do arquivo de configuração do serviço de SSH onde foi trocada a porta do serviço de 22 (padrão) para 6222.

Exemplo 27.1

```
# Porta alterada de 22 para 6222 para evitar rastreamentos externos  
# Alterado por emmonks; 23/12/2024 - 17h22min  
Port 6222  
# Valor original; 23/12/2024 - 17h22min
```



Port 22

Em dispositivos tais como switches e roteadores, usar a descrição das interfaces nas configurações ajudam muito na identificação e diagnóstico de problemas. A descrição poderá conter o que está ligado em cada interface de rede, por exemplo, *servidorA* ou *UplinkPredio33*. Outras condições a serem colocadas nas descrições poderiam ser relacionadas a bloqueios administrativos de uma interface ou problemas físicos na interface.



Os comentários guardam o histórico de alterações em serviços e ajudam o administrador iniciante a aplicar as diretrivas de configuração. Em épocas nas quais a documentação era muito menos disponível, havia casos em que a única dica era o comentário no arquivo de configuração deixado pelo último administrador de redes ou pelo desenvolvedor do serviço.



28) Revisar a sala dos servidores diariamente

A revisão diária da sala dos servidores é uma atividade que deve estar na rotina do administrador de redes. A referência para sala dos servidores, ao invés de data center, se dá devido à grande parte das áreas destinadas aos ativos mais importantes de TI de uma empresa estarem acomodados em instalações não ideais de climatização, fornecimento de energia, espaço físico e de acesso. Em muitos casos são salas de depósito compartilhadas com qualquer outro material, sem condições para garantir a disponibilidade adequada dos serviços ou até mesmo acesso aos equipamentos dentro da sala. Na Figura 28.1 uma sala de servidores inadequada, não há necessidade de mais comentários para este caso.



Figura 28.1 Sala de servidores inadequada.

A revisão diária é importante para verificação de casos em que as ferramentas/sensores de monitoramento não registram os possíveis problemas ou nem existem soluções de monitoramento. No Exemplo 28.1 alguns problemas comuns que são detectados facilmente na presença física e não são tão simples de monitorar remotamente.

Exemplo 28.1

Mensagens nas consoles dos servidores

Vazamentos de água

Janelas abertas

Temperatura errada (mensagens de erro nos aparelhos de ar condicionado não gerenciáveis)

Cabos soltos ou próximos a se soltarem

Leds de alerta em nobreaks não gerenciáveis

Ação de roedores

Sujeira acumulada em coolers ou em áreas de ventilação em equipamentos



Em projetos onde há previsão de salas para equipamentos de TI, costumeiramente, são alocadas salas de tamanho mínimo, onde muitas vezes a abertura da porta de um rack não se torna possível. E para os projetos onde nem há previsão de área para os equipamentos? A sala escolhida será o depósito ou onde ficam os materiais de limpeza. É uma situação que acaba se repetindo inúmeras vezes e causa surpresa para os criadores do projeto quando questionados. Em grande parte das vezes, os arquitetos nem sabiam desta necessidade ou achavam que um equipamento como um servidor de arquivos ou um servidor de câmeras ficaria no rack de parede no meio do corredor.



29) Ativar o gerenciamento SNMP em todos os dispositivos compatíveis

O protocolo SNMP (*Simple Network Management Protocol*) é a forma padronizada de agente para gerenciamento de dispositivos em rede. Quando se considera um dispositivo gerenciável está se tratando de um dispositivo compatível com SNMP. Entretanto, existem dispositivos com console de gerenciamento, por exemplo uma console web, sem compatibilidade com o SNMP e que o fabricante classifica como gerenciável. Trocar os dispositivos que não são gerenciáveis por gerenciáveis deve ser prioritário para obtenção de melhores resultados na disponibilidade da rede. Na Figura 29.1 está a configuração necessária para a ativação do agente SNMP em um switch HP modelo 1910.

The screenshot shows the configuration interface for an HP 1910 switch. On the left, there's a navigation tree under 'Device' with options like Basic, Device Maintenance, System Time, Syslog, Configuration, File Management, Port Management, Port Mirroring, Users, Loopback, VCT, Flow Interval, RMON, Energy Saving, and SNMP. The 'SNMP' option is highlighted. On the right, there's a 'View' tab selected in the top menu. Below it is a search bar with 'View Name' and 'Search' buttons. A table titled 'ViewDefault' lists rules for MIB subtrees. The table has columns for 'View Name', 'Rule', and 'MIB Subtree'. The data is as follows:

View Name	Rule	MIB Subtree
ViewDefault	Included	1
ViewDefault	Excluded	1.3.6.1.6.3.15
ViewDefault	Excluded	1.3.6.1.6.3.16
ViewDefault	Excluded	1.3.6.1.6.3.18
ViewDefault	Excluded	1.3.6.1.4.1.25506.2.111

An 'Add' button is located at the bottom right of the table area.

Figura 29.1 Ativação do agente SNMP em um switch HP modelo 1910.

Atualmente, os dispositivos gerenciáveis possuem em grande maioria compatibilidade com o protocolo SNMP por meio de um agente. O agente disponibiliza para coleta de um gerente SNMP informações sobre o dispositivo gerenciado. Existem diversos gerentes, também conhecidos como NMS (*Network Management System*), que coletam as informações dos dispositivos e geram *dashboards*, gráficos e alertas de acordo com as configurações estabelecidas pelo administrador de redes. Na Figura 29.2, os gráficos gerados pela ferramenta Observium a partir de coletas de um switch com o agente SNMP ativado.



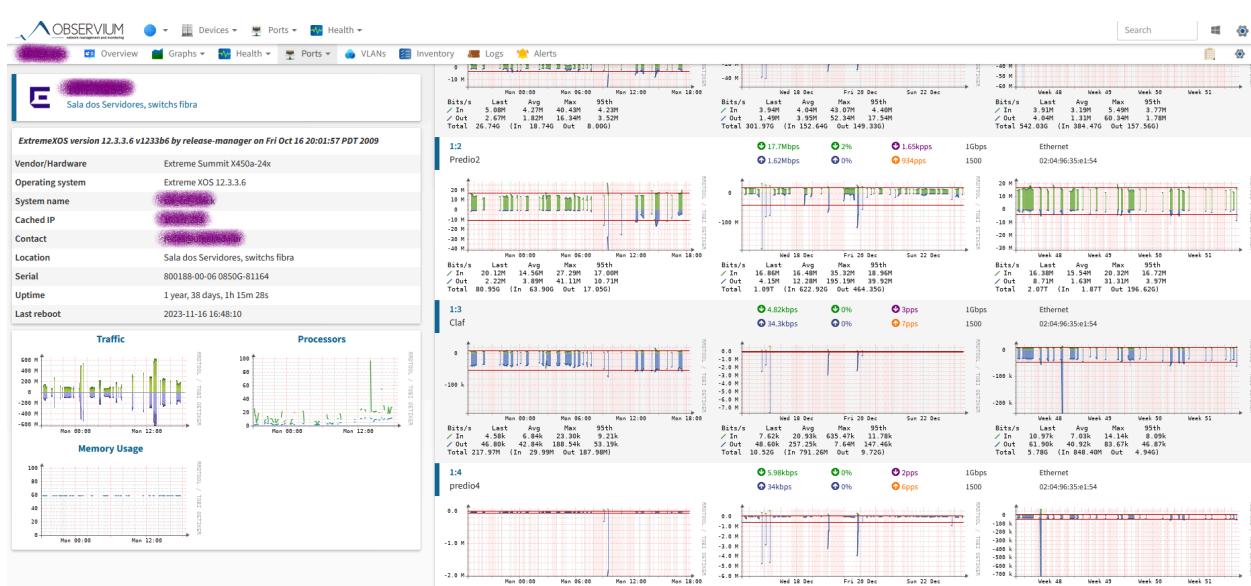


Figura 29.2 Gráficos da ferramenta Observium.

É provável que vários dispositivos que possuem gerenciamento não estejam configurados para ativar o SNMP. Este gerenciamento possibilita uma visão excelente do desempenho da rede, facilita no diagnóstico de problemas e possibilita ao administrador de redes ser pró-ativo e aumentar em muito a disponibilidade da rede. Portanto, ativar o gerenciamento SNMP nos dispositivos que sejam compatíveis é fundamental para a administração em redes.



O agente SNMP está disponível em sistemas operacionais Linux e Windows sendo um procedimento simples para ser ativado e configurado. O protocolo SNMP possui 3 versões que são 1, 2c e 3. Nas versões 1 e 2c existe uma comunidade, que funciona como uma senha e uma restrição por meio de endereços IP que podem acessar as informações. Na versão 3 a forma de autenticação é com usuário e senha, com views (visões parciais com as permissões de quais objetos podem ser acessados) e é a versão recomendada para uso. O agente SNMP pode ser configurado para ativar traps, que são mensagens enviadas para o gerente quando um evento é detectado no dispositivo, por exemplo a queda de uma interface em um switch.



Para saber mais



Observium - ferramenta de gerenciamento de redes (Parte 1) -



<https://www.youtube.com/watch?v=afxzOHzT1tQ>

Observium - ferramenta de gerenciamento de redes (Parte 2) -



<https://www.youtube.com/watch?v=PGExnrKkLcg>



30) Documentar os disjuntores de racks e demais equipamentos importantes

A disponibilidade da rede depende muito do fornecimento de energia com qualidade e dimensionado de forma correta. A utilização de UPS (*Uninterruptible Power System*), o popular *nobreak*, e geradores resolvem grande parte dos problemas de fornecimento de energia para data centers, salas de servidores e dispositivos de rede em geral. Entretanto, documentar onde estão os disjuntores elétricos principais e as indicações dos equipamentos que proveem a energia tais como cores de leds, avisos sonoros ou mensagens em *displays* podem ajudar muito na identificação da origem do problema. Avaliar que em caso de falta de energia, talvez não tenha mais acesso à Internet facilitado para buscar informações, fora o tempo necessário para encontrar a documentação correta.

Desta forma, documentar de forma *offline* os procedimentos de ligamento ou desligamento de geradores, *nobreaks* ou disjuntores é algo simples de fazer quando tudo está normalizado. Estas documentações farão o administrador de redes ganhar tempo para retorno da disponibilidade da rede na próxima queda de energia. Na Figura 30.1 uma caixa de distribuição elétrica com identificação de disjuntores relacionados a racks de comunicação.



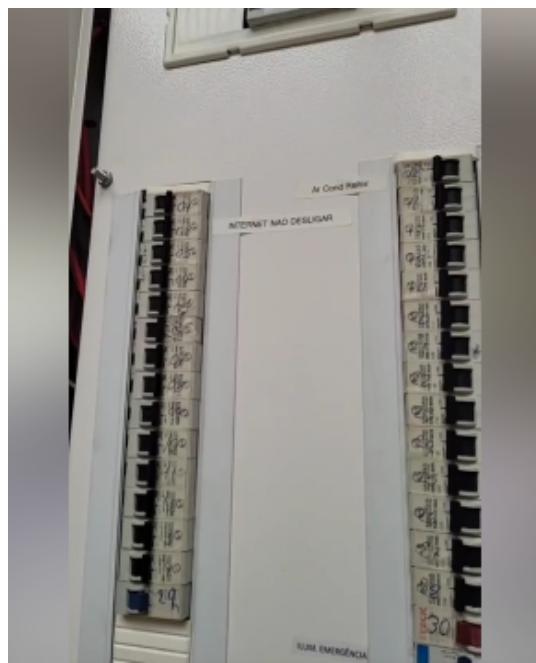


Figura 30.1 Caixa de distribuição elétrica com identificações de racks.



Em certos momentos críticos como uma falta de energia elétrica, onde as baterias do nobreak estão no final, saber onde ficam os disjuntores ou como se aciona um gerador de energia são as informações mais importantes. Não é responsabilidade do administrador de redes ser um especialista em rede elétrica, mas saber o básico, os contatos do pessoal responsável pela rede elétrica do local e onde estão conectadas as fontes de energia que alimentam os ativos de rede deve estar no bloco de anotações e bem disponível para quando necessário.



31) Criar um repositório para toda a documentação

A documentação na administração de redes pode ser considerada uma das principais diferenças entre um administrador de redes iniciante e de um sênior. É esperado que o administrador sênior possua uma biblioteca de anotações importantes em um repositório de forma organizada e mantido de forma atualizada. As experiências em diversas situações complexas, que podem se repetir com espaços de tempo longos, fazem com que o administrador mais experiente adote a documentação dos procedimentos como parte fundamental do trabalho. O principal motivo é que os problemas se repetem e as soluções também. Entretanto, se não houver o registro da solução aplicada na primeira vez que apareceu o problema, acontecerá um processo de repetição de tentativas e perda de tempo para chegar na resolução do problema. E quando o tempo para solucionar o problema aumenta, o tempo de indisponibilidade da rede aumenta também.

O formato da documentação deverá possuir uma organização onde seja rápido e simples a busca de tópicos e de dicas relacionados a um problema específico. Diversas ferramentas podem ser utilizadas tais como Wiki, Trello, Google Drive com um documento compartilhado, sistemas customizados, bases de conhecimento em sistemas de helpdesk ou até mesmo um bloco de anotações como o da Figura 31.1. Afinal, o fato de uma informação não ser em formato digital não faz diferença nenhuma para resolver um problema. Outro fator é que um bloco de anotações de 2015 ainda está disponível em 2024, um pendrive ou DVD de 2015 talvez não esteja mais.





Figura 31.1 Bloco de anotações, método antigo e eficaz.



Desde o começo da minha vida profissional mantive anotações sobre os procedimentos realizados, comandos executados, informações que foram úteis e que poderiam ser novamente úteis no futuro (e foram!) e eventos importantes. Todos em ordem cronológica, em um formato e com o nível de detalhamento que eu poderia entender no futuro o que foi realizado com clareza. Esta é uma das dicas mais importantes: manter anotações das experiências e procedimentos para não precisar somente buscar na memória em um momento crítico.



32) Monitorar o espaço em disco consumido por arquivos/pastas/tabelas temporárias

O monitoramento do consumo de espaço em disco em servidores e unidades de armazenamento requer o máximo de atenção do administrador de redes. Quando houver um alerta de nível crítico de consumo deverá haver uma ação do administrador. Entretanto, realizar a limpeza dos dados armazenados nem sempre é possível e poderá haver a necessidade de mover dados entre servidores e unidades de armazenamento causando degradação no desempenho da rede e dos dispositivos. Portanto, manter um ambiente enxuto e com planejamento de capacidade para o crescimento do volume de dados a serem armazenados é fundamental para evitar transtornos.

Uma das rotinas que ajudam em muito a manutenção e abertura do espaço de armazenamento é a remoção de arquivos de testes e temporários que consomem espaço de forma desnecessária. Estes arquivos são gerados em processos de instalação de aplicações, cache, logs, tabelas em banco de dados de uso temporário e outros arquivos que são gerados em sistemas de versionamento ou sessões PHP em servidores web. Além do consumo do espaço, podem afetar o tempo de realização de backups. Criar filtros para evitar que estes arquivos sejam incluídos no backup tem que ser realizado e validado por meio de monitoramento automatizado.



A quantidade de arquivos poderá aumentar muito o tempo de um backup diferencial. Este aumento de tempo não é somente pelo volume de dados e sim pelo tempo necessário para verificação se um arquivo foi alterado na origem e se deverá ser copiado para o repositório do backup. Normalmente, os arquivos temporários são de tamanhos pequenos e em grandes quantidades. Outro caso recorrente é o de logs em tabelas no banco de dados que entram no backup muitas vezes de forma desnecessária e tendem ao infinito armazenamento. Se há backup diário, ao terminar o processo de cópia, pode-se realizar um **truncate** na tabela de logs. Assim, caso seja necessário um log do dia anterior, estes dados poderão ser restaurados do backup e não precisam ficar consumindo o banco em produção.



33) Ativação do protocolo Netflow

O uso do protocolo Netflow é fundamental para o monitoramento do tráfego de rede. Este protocolo permite analisar dados dos fluxos de rede, informações sobre endereços IP, portas de comunicação, protocolos da camada de transporte e a vazão. Diferente do monitoramento de bytes que entram e saem de interfaces de rede, que resulta em saber que houve alteração do tráfego em determinado período, o Netflow permite saber quais hosts e em quais portas de comunicação houve alguma anomalia. Na Figura 33.1 o ambiente para verificação dos fluxos com o Netflow na ferramenta NFSen, onde podem ser identificados os volumes de tráfego dos protocolos TCP, UDP, ICMP e outros no decorrer do tempo. Com isto é possível identificar os endereços IP e portas e não somente o volume de tráfego em bytes que trafegam na rede.

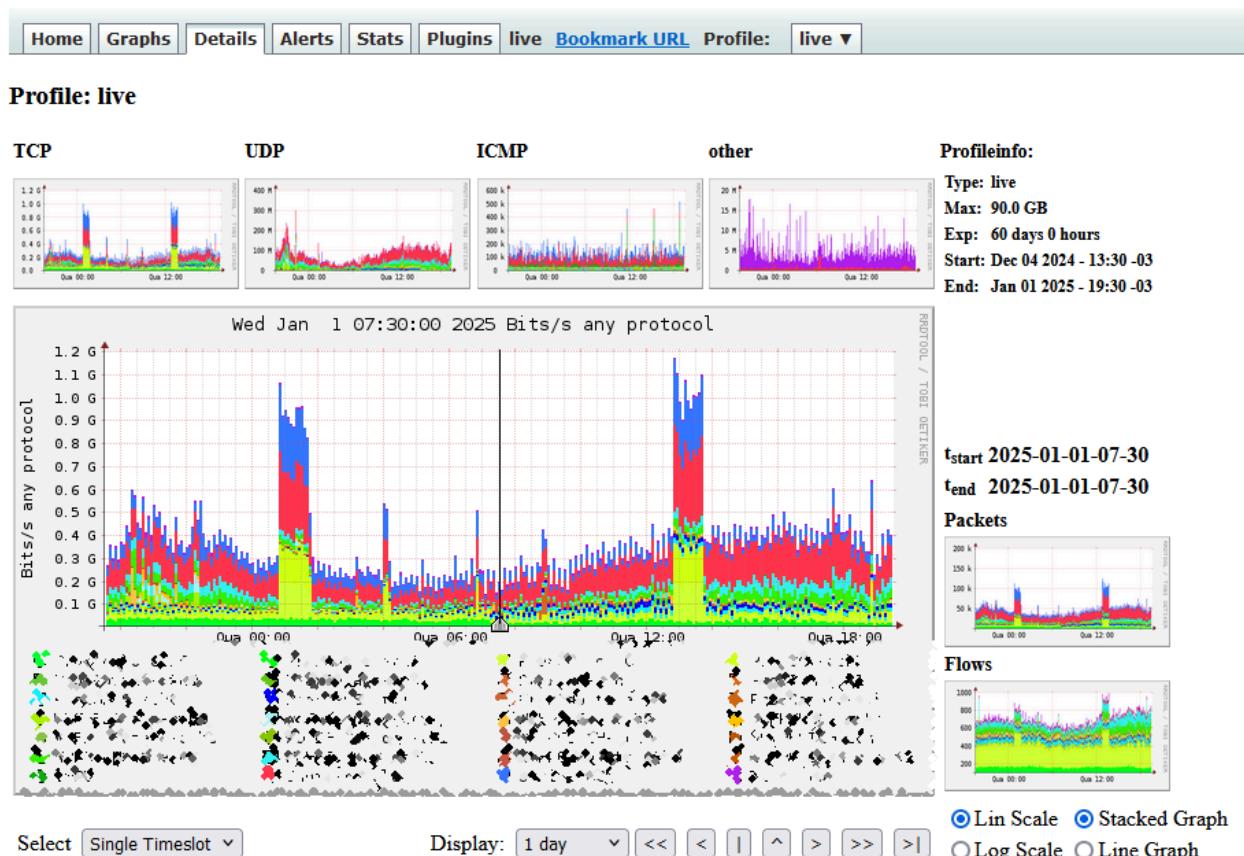


Figura 33.1 Ambiente da ferramenta NFSen.

Para obter informações sobre os fluxos com o Netflow existem *probes* que podem ser configurados nos dispositivos tais como switches e roteadores. A compatibilidade com o Netflow deve ser observada quando da aquisição dos equipamentos. Em Linux estão disponíveis pacotes como o fprobe ou o pmacct (<http://www.pmacct.net/>) para ativar os *probes* Netflow. Para uso de um coletor (*collector*) pode-se utilizar o NFSen (<https://github.com/phaaag/nfse>) ou o NFSen-NG (<https://github.com/mbolli/nfse-ng>). Estes coletores são baseados em código-fonte aberto e possuem as funcionalidades básicas para o monitoramento dos fluxos de rede.



A coleta de tráfego de rede em interfaces com o protocolo SNMP geram dados relacionados ao volume de tráfego e não identificam quais os hosts envolvidos. O Netflow permite identificar os fluxos de rede, com os endereços de origem, destino, portas de origem e destino e o volume de tráfego trocado no fluxo. Estas informações são muito úteis para analisar o comportamento da rede e realizar auditorias. Em casos em que um gráfico mostra o aumento de tráfego em uma porta de um switch ou roteador, quais hosts ou protocolos estariam envolvidos neste tráfego? O Netflow poderá responder esta pergunta que é recorrente na rotina do administrador de redes.

Para saber mais



Protocolo Netflow - <https://www.youtube.com/watch?v=H0SLzSbk4x0>



34) Evitar cabos soltos dentro de racks e em mesas de usuários

A organização do cabeamento de rede em racks e nos espaços dos usuários reduzem o risco de *loops* na rede. Basta haver um cabo desconectado que poderá haver um incidente. São inúmeras ocasiões em que um técnico faz uma manutenção em um rack e acaba conectando todos os cabos, mesmo que seja um *patch cord* solto dando voltas no meio do cabeamento. Como verificação básica em uma manutenção em rack, se ao conectar um cabo que não seja de uplink acenderem dois leds, haverá um problema. Para evitar esta situação a organização do rack e a documentação do cabeamento devem ser mantidas atualizadas.

No espaço físico dos usuários, basta haver um cabo desconectado que se torna uma tentação para conectar na primeira tomada de rede ou switch/AP em cima de uma mesa. Uma das medidas é coibir o uso de equipamento em cima de mesas por meio de orientação aos usuários ou medidas administrativas de notificação. Outra medida a ser tomada é ativar as proteções de loop nos switches (*loop protection*) e monitorar os logs para identificar anomalias. Em resumo, um cabo solto é um chamariz de problemas, portanto, evitar esta situação devido ao alto risco de loops e conexões em VLANs erradas.



Um caso de organização em racks que não acabou em final feliz. Um estagiário foi incumbido com a tarefa de arrumar o cabeamento de um rack. A orientação foi deixar os cabos acomodados e mexer o mínimo possível nos switches. Em pouco tempo, alertas de indisponibilidade na rede começaram a aparecer e o telefone a tocar. O estagiário fez o trabalho dele, organizou os cabos e ficou muito bonito o rack. Entretanto, ao recolocar os cabos no switch, o estagiário colocou em qualquer porta, sem saber que havia VLANs para a rede do prédio, câmeras de vigilância, impressoras e rede sem fios. Neste caso faltou orientação ao estagiário e excesso de proatividade por parte dele na resolução da tarefa.

Para saber mais





Combatendo Loops na Rede -



<https://www.youtube.com/watch?v=aprt2k4dVEE>



Este trabalho está licenciado com uma Licença [Creative Commons - Atribuição-NãoComercial-Compartilhável 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/)

35) Cuidados com sistemas legados

A área de TI está em constante mudança. São mudanças de tecnologias, ambientes de programação, sistemas operacionais e novos padrões. Entretanto, o que está funcionando não será trocado ou atualizado só porque existe uma nova linguagem de programação ou uma nova família de processadores. Em sistemas em produção as mudanças devem ser evitadas ao máximo. Em cada alteração, haverá o risco de um novo bug e indisponibilidade.

Desta forma, surge um problema complexo que é o de manter sistemas legados. Estes sistemas podem ser usados como a principal ferramenta de gestão dos dados de uma instituição e possuem um alto custo para atualização. Outra questão, talvez o sistema seja tão antigo que não seja possível realizar a atualização devido ao hardware específico, tal como uma arquitetura Risc, ou a linguagem na qual foi desenvolvido, por exemplo Cobol ou Delphi.

Nestes casos de sistemas legados, são geradas vulnerabilidades no ambiente devido a haver mais atualizações de segurança, de compatibilidade com novo hardware e novos protocolos tais como IPv6, SSHv2 e soluções de criptografia. No Exemplo 35.1 estão recomendações importantes para diminuir as vulnerabilidades destes sistemas.

Exemplo 28.1

Restringir ao máximo o acesso externo a rede local

Limitar somente para os usuários que realmente necessitam usar o sistema

Se possível, em caso de servidor físico, virtualizar antes que o pior aconteça com o hardware antigo

Realizar backup dos dados e das configurações, talvez não seja tão fácil encontrar documentação de como instalar um sistema com tecnologia de desenvolvimento de 20 anos ou mais

Exportar em texto, no pior dos casos, e importar em uma planilha os dados do banco de dados legado

Analizar a possibilidade de atualizar o ambiente do sistema operacional até a versão mais recente que seja compatível para o funcionamento do sistema legado





Um cenário para refletir o que seria um sistema legado: um sistema desenvolvido na linguagem e banco de dados Zim nos anos 90, sendo executado em um servidor IBM RS/6000 de 1997, com discos originais, com o sistema operacional AIX 4.3.3. Este ambiente estava em execução em 2024 até o hardware apresentar problemas na placa-mãe e nos discos. A primeira questão é: por que não foi atualizado? O custo de investimento no desenvolvimento de um sistema é muito alto. Além disso, não é tão simples sair de um sistema complexo e migrar para uma nova tecnologia. A solução foi virtualizar o ambiente, a partir do backup dos dados, o hardware de um IBM RS/6000 pode ser emulado pelo virtualizador Qemu com algumas restrições. Portanto, o sistema ainda continua ativo e funcional.



36) Criar um ambiente de testes

Realizar testes e validações de configurações e de dispositivos antes de colocar em produção é um procedimento indispensável para evitar surpresas desagradáveis na rede. Montar um ambiente para testes com equipamentos físicos, tais como switches, APs, roteadores, com infraestrutura de rede lógica e elétrica resultam em melhores níveis de disponibilidade na rede e da possibilidade de novas funcionalidades a serem aplicadas no ambiente de produção. Existem outras abordagens possíveis como ler a documentação, fóruns do fabricante, blogs, vídeos no Youtube ou consultar outros colegas. Entretanto, nada substituirá a experiência de realizar os testes pessoalmente, além de aumentar em muito a confiança do administrador de redes. Na Figura 36.1 um laboratório composto de bancada para realização de testes e validações dos mais diversos dispositivos e ferramentas de rede.

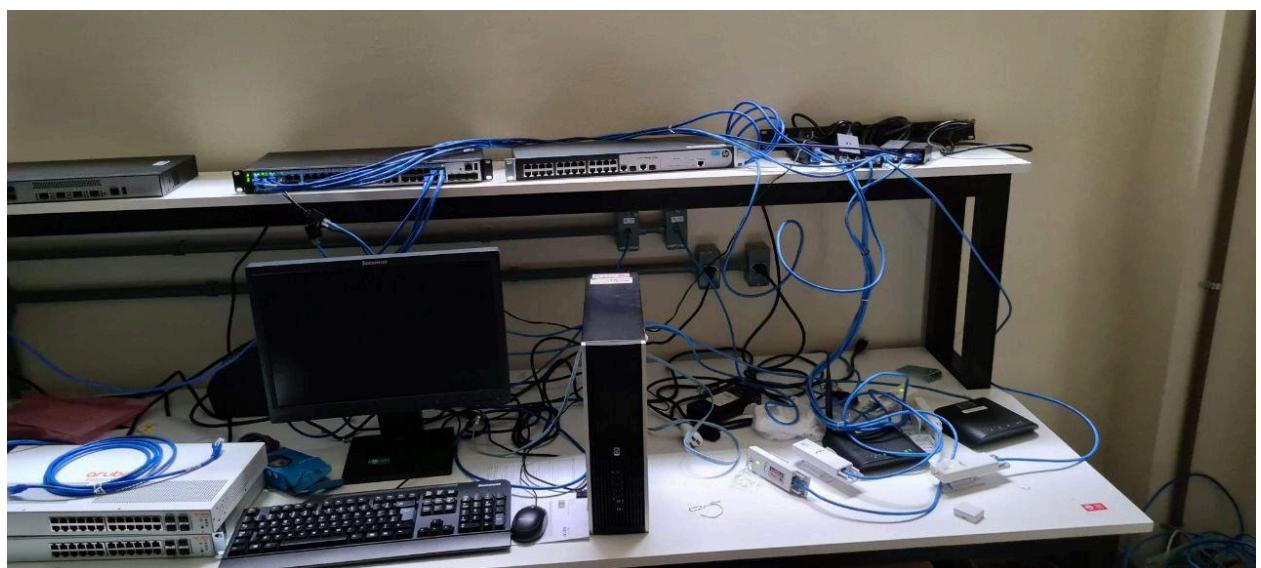


Figura 36.1 Laboratório para realização de testes de dispositivos e ferramentas.

Além do recurso de um laboratório físico, podem ser usados simuladores e emuladores de rede para montar os mais diversos cenários de testes. As ferramentas EVE-NG (<https://www.eve-ng.net/>), CORE Emulator (<https://coreemu.github.io/core>), Cisco Packet Tracer (<https://www.netacad.com/cisco-packet-tracer>), GNS3 (<https://www.gns3.com/>), entre outras possibilitam a montagem de cenários complexos para a validação de



configurações que envolvam protocolos e serviços com firmwares originais de fabricantes tais como Extreme, Cisco, HP e Huawei e sistemas operacionais Linux, Microsoft Windows e Mikrotik RouterOS. Os recursos computacionais utilizados pelos emuladores dependerá da complexidade dos cenários a serem montados e grande parte dos cenários reais necessários para emulação possuirá baixos recursos para serem emulados.



Existir uma bancada permanente para testes é muito raro em ambientes de trabalho. O tempo necessário para montar os cenários de testes sem um lugar adequado será muito maior. Fora os casos em que os testes necessitam ser realizados em um período maior. Na próxima vez que houver alguma alteração no ambiente de trabalho solicitar uma área para uma bancada de testes que fará bastante diferença na hora de realizar procedimentos e configurações com equipamentos. É um investimento importante para melhorias na administração de redes.



37) Revisar as ferramentas de gerenciamento

O uso de ferramentas de gerenciamento de hosts, dispositivos e serviços em rede é uma das principais atividades do administrador de redes. Em qualquer tamanho de rede, o monitoramento automatizado com alertas configuráveis deve ser usado. Existem diversas soluções disponíveis, em código-fonte aberto ou comerciais. As opções de ferramentas que possuem licenças comerciais, normalmente, possuem versões comunidade (*community*) que podem ser usadas sem diferenças da comercial para o uso básico. O uso básico é o monitoramento por meio de *ping* e conexões nas portas de comunicação dos hosts, por exemplo, verificar se a porta do MySQL TCP 3306 está aceitando conexões. Outra questão é o monitoramento de aplicações, por exemplo quantos usuários estão conectados no banco de dados, quantas transações por segundo estão sendo realizadas ou a quantidade de uso de memória RAM em um servidor web. As ferramentas de gerenciamento tais como Nagios (<https://www.nagios.org/>) ou Zabbix (<https://www.zabbix.com/>) possuem funcionalidades para automatizar grande parte das configurações necessárias e utilizam agentes nos hosts para obter dados por meio de *plugins* e/ou utilizam o protocolo SNMP para coletar informações.

O papel do administrador de redes é realizar a configuração da ferramenta de gerenciamento que representa todos os hosts e serviços que devem ser monitorados e ajustar os valores limites para os alertas e notificações. Em muitos casos, existe um volume excessivo de dados sendo coletados de hosts secundários na rede e falta de dados dos hosts principais. Estes ajustes são importantes para tornar confiável os alertas recebidos das ferramentas de gerenciamento. Em resumo, validar se realmente todos os hosts, dispositivos, sistemas, aplicações e serviços estão sendo monitorados corretamente, com limites configurados para representar o estado correto de funcionamento. Receber um “OK” de um monitoramento incorreto torna a vida do administrador bem mais difícil e resulta em indisponibilidade na rede. Como regra geral garantir que todos os hosts e serviços estejam sendo monitorados e retirar os que não são mais necessários. Esta limpeza deve ser uma das rotinas principais para o administrador de redes.



A primeira ferramenta de gerenciamento de redes que usei foi a Netsaint (<https://www.nagios.org/about/history/>), nome anterior da ferramenta Nagios. Em uma época em que não existiam muitas opções de ferramentas livres, havia soluções tais como IBM Tivoli, HP OpenView e CA Unicenter. Estas ferramentas comerciais eram complexas e possuíam diversos licenciamentos que exigiam um



investimento alto de aquisição e fora do alcance da maior parte das empresas pequenas e médias. Atualmente, existem muitas soluções com vários níveis de licenciamento e custos. A minha opção principal continua sendo com o Nagios.



38) Ativar um servidor de gerenciamento fora da infraestrutura principal

O uso de virtualização é bastante comum em redes corporativas, com serviços locais ou com serviços em nuvem. A infraestrutura de virtualização é composta de servidores físicos, switches e unidades de armazenamento. Esta infraestrutura provê os recursos para as máquinas virtuais serem executadas e é onde ficam os dados e sistemas corporativos. Quando do uso de serviços de nuvem, esta infraestrutura é provida por empresa terceira e apenas as máquinas virtuais são administradas.

Se as ferramentas de gerenciamento da rede estiverem hospedadas na infraestrutura virtualizada ou na nuvem, em caso de indisponibilidade da infraestrutura virtualizada, o administrador de redes ficará sem os monitoramentos necessários para diagnosticar o problema. Portanto, é recomendado que a ferramenta de gerenciamento seja colocada fora da infraestrutura principal, por exemplo em um servidor físico ou em outro serviço de nuvem diferente. Não há problema de manter uma máquina para a ferramenta de gerenciamento dentro da infraestrutura principal, mas deve-se manter sincronizadas as configurações com um ou mais servidores de fora da infraestrutura principal. Portanto, a estratégia de utilizar o monitoramento externo a infraestrutura principal será importante quando houver indisponibilidade nos serviços de virtualização ou de nuvem.



Quando não havia virtualização de servidores, as salas dos servidores tinham dezenas de computadores. Esta quantidade de computadores, muitos deles eram com configurações comuns de desktop fazendo o papel de servidor e geram muito trabalho de manutenção. Toda a semana tinha a fonte de um servidor com problemas ou um disco com falha. A confiabilidade dos equipamentos era baixa devido a serem computadores comuns e não realmente servidores. Normalmente, o computador menos robusto era usado para ser o servidor de gerenciamento. Portanto, era mais comum o servidor de gerenciamento estar indisponível do que ele monitorando alguma coisa. O servidor de gerenciamento tem papel fundamental para a administração de redes e deve ser um equipamento confiável e com os recursos computacionais necessários para suportar a carga, que será bem alta dependendo das ferramentas usadas para o gerenciamento. Além da confiabilidade do equipamento, deverá haver redundância para casos de



possíveis problemas ou manutenção no servidor de gerenciamento principal.



39) Revisar as baterias dos nobreaks e realizar trocas periódicas

O uso de sistemas de nobreaks ou UPS (*Uninterruptible Power Supply*) aumentam muito a disponibilidade da rede. A interrupção do fornecimento de energia causa problemas sérios em equipamentos e dispositivos, tais como perda de dados, danos em discos, queima de fontes de alimentação e indisponibilidade de acesso a sistemas e serviços. Idealmente, deve-se ter fornecimento alternativo de energia elétrica por meio de geradores para reduzir o tempo necessário de uso dos nobreaks.

Como é característica do próprio gerador depender de uma movimentação mecânica interna, o equipamento leva um tempo até atingir os indicadores de funcionamento ideal. Os aparelhos conectados à carga do gerador, mesmo que por poucos segundos, sofrem com a queda de fornecimento de energia. É neste momento que o nobreak entra em operação.

Os equipamentos UPS não precisam de um tempo maior para começar a operar. Assim que detectado a falta de energia pela rede, o nobreak é acionado instantaneamente. No curto intervalo de tempo entre a queda e o acionamento do gerador, o nobreak entra em operação e fornece a energia por meio das baterias internas.

Mesmo em um cenário onde exista gerador de energia, os nobreaks serão ativados na queda do fornecimento de energia externo até o acionamento do gerador. Normalmente, isto acontece em entre 10 e 15 segundos, da queda de energia externa até o acionamento do gerador. Neste intervalo serão usadas as baterias para sustentar a carga.

O estado das baterias é fundamental para que o fornecimento de energia seja mantido. Deve-se manter uma rotina de trocas de baterias, em média o tempo de vida útil máxima pode chegar a 5 anos (para autonomia mínima em minutos), sendo 3 anos o tempo recomendado para a troca. O tempo é relativo ao ambiente onde estão armazenadas as baterias. Em ambientes com umidade e temperatura controladas a tendência é que as baterias tenham vida útil maior. Em caso de baterias expostas às mudanças de temperaturas devem ser trocadas com menos tempo, um caso comum é o uso de nobreaks em racks de parede ou dentro de racks sem controle de climatização. Na Figura 39.1 um caso de nobreak



onde a bateria terá tempo de vida útil reduzido pela exposição às mudanças de temperatura e umidade do ambiente.



Figura 39.1 Nobreak de pequeno porte usado em rack de parede sem controle de climatização.

É uma boa prática manter um registro do histórico das baterias, realizando de forma preventiva testes de duração (autonomia) e o agendamento para a troca das baterias com janela de manutenção planejada.





É importante ter o contato de empresas que prestam manutenção em nobreaks de grande porte. Por mais confiabilidade que estes equipamentos possam apresentar e sejam raras as falhas, cada fabricante insere particularidades nos nobreaks e haver técnicos autorizados na região é um fator importante quando da aquisição de um equipamento. Outro fator crítico é ter redundância de nobreaks, possuir no mínimo dois nobreaks onde cada um isoladamente suporte a carga total. Em caso de falha em um dos nobreaks, o outro nobreak terá a capacidade de segurar toda a infraestrutura. Uma outra dica é adquirir nobreaks, mesmo de pequeno porte, com gerenciamento integrado com agente SNMP.



40) Criação de políticas de uso de recursos de TI e de segurança

A administração de redes é baseada na execução de políticas. As políticas de TI são o guia para as rotinas de backup, segurança, uso de serviços e sistemas. O papel do administrador de redes é garantir que as políticas sejam respeitadas. Para isto devem ser definidos termos de aceitação de uso para serviços específicos, tais como e-mail, uso de dispositivos móveis, BYOD (*Bring Your Own Device*), uso de senhas, duplo fator de autenticação e qualquer outro ativo de rede que tenha acesso por usuários.

A TI é executora de políticas, não deve criá-las de forma independente e sem o consentimento da alta gestão. Portanto, as políticas de TI devem ser elaboradas de forma colegiada, por meio de comitês, com a gestão administrativa e técnica da instituição para tornar exequível os termos definidos. Quando não há sincronização entre a parte administrativa e a parte técnica não haverá um ambiente saudável para a administração de redes. Um caso bastante comum é apontar a TI como responsável por determinada limitação, por exemplo acesso a sites ou uso de senhas fáceis. Entretanto, deve ficar formalizado que a TI está executando uma política que foi definida pela administração e não é uma aplicação arbitrária da parte técnica.

Esta batalha pode causar diversos transtornos e indisposições entre os usuários e o pessoal da TI. Tudo seria bem mais simples com a formalização e publicação de políticas e termos de uso nos quais os usuários devem dar ciência e são a principal resposta para aqueles episódios onde o usuário questiona o porquê não pode trazer de casa um roteador sem fios para colocar na mesa dele.



Em episódios onde o administrador de redes sofre questionamentos por usuários do motivo pelo qual não é possível acessar o Netflix no ambiente de trabalho, a resposta não deve ser do administrador e sim da política de TI e do termo de uso dos recursos computacionais na instituição. O ideal é não haver nenhuma restrição sem estar formalizada junto à gestão. Em caso contrário será algo pessoal, sem justificativa documentada, mesmo sendo óbvio que acessar um seriado durante o horário de trabalho não faz parte do rol de tarefas do usuário. Mesmo neste caso, o administrador de redes não é o supervisor do usuário, não seria ele o responsável pela produtividade do colaborador. Quantas vezes escutei algo como: "Por favor, tens como bloquear os sites X, Y ou Z para que o Fulano de



Tal possa trabalhar?“. A minha resposta era algo como: “Certo, e se o Fulano trouxer um livro e ficar lendo, devo apagar a luz para ele não ler?”. A TI não faz nenhuma pessoa trabalhar quando ela não o quer. Mas consegue fazer a pessoa não trabalhar quando ela quer!



41) Uso de sistemas de chamados para atendimento

Para manter uma melhor organização do trabalho deve-se ter um sistema formalizado para receber chamados de suporte. Sem um sistema de registro de chamados, a rotina de trabalho do administrador de redes será muito mais difícil. O uso de solicitações por e-mail, Whatsapp, telefone e atendimento presencial devem ser somente em casos de emergência e não o padrão.

Com vários canais possíveis de solicitação de chamados haverá perda do histórico da resolução dos problemas, dificultando a formação de uma base de conhecimento, além de grande chance de perder chamados no meio da confusão. A formalização da solicitação por parte do usuário possibilita que exista o acompanhamento por parte do requisitante e da equipe de atendimento.

Em muitas instituições será uma mudança complicada de cultura. O usuário poderá até se ofender ao ser solicitado que abra um chamado no sistema. Quase sempre, na visão do usuário, o chamado é urgente, prioritário e tem que ser atendido imediatamente. Entretanto, um sistema de chamados cria uma fila automática para que os pedidos possam ser priorizados pelo administrador de redes e o usuário poderá ficar ciente da quantidade de chamados em aberto ou em atendimento.

Esta mudança poderá levar um certo tempo, mas tem que ser apoiada pela alta gestão da instituição e ser embasada de forma objetiva com estatísticas de número de chamados que foram abertos, fechados e o tempo de atendimento médio. Estes dados poderão servir para solicitar melhores condições de trabalho e para o aumento de pessoal no atendimento.

Caso não exista um sistema formalizado, o trabalho será muito maior e ficará sem registro formalizado. Outro fator importante é a formação de uma base de conhecimento centralizada com os chamados e as soluções apresentadas. Estas informações são uma excelente fonte para reduzir o tempo de atendimento em chamados futuros e para capacitar novos colegas no ambiente de trabalho.





Não registrar as demandas e os chamados por parte dos usuários de forma organizada e sistematizada tornará a vida do administrador de redes bem difícil. Porém, ter um sistema e não mudar a cultura da instituição de que é necessário a abertura de um chamado para haver o atendimento poderá levar tempo, mas esta mudança tem que ser implantada. Quando houver uma cobrança sobre algum atraso no atendimento, basta questionar: “Qual o número do chamado? Foi aberto um chamado?”



42) Gerenciamento de backups

O gerenciamento de backups deve possuir uma política definida sobre os dados, que determine o tempo de retenção, quais os dados devem ser copiados, o tempo necessário para restauração em caso de solicitação de usuários, os termos para replicação dos dados em ambientes externos e quais são as responsabilidades para os administradores e para os usuários que geram e armazenam os dados. Infelizmente, sem um gerenciamento organizado de backups haverá falhas nas cópias de dados importantes que são armazenados em lugares incorretos, por exemplo em disco local em um computador de usuário ao invés do compartilhamento onde há backup.

Utilizar repositórios diversos e externos para armazenamento do backup é importante para haver redundância dos dados. Entretanto, ao distribuir os dados de backup em ambientes externos os cuidados com as permissões de acesso devem ser redobrados. O acesso aos dados de backup possibilita eliminar camadas de segurança. Um exemplo é com um dump de banco de dados. Em um sistema que faz uso do banco de dados, para se obter acesso deve-se realizar autenticação em duplo fator e existem permissões para usuários em módulos específicos do sistema. Se o dump do banco de dados não possuir criptografia, bastaria restaurar o dump e ter acesso irrestrito aos dados sem autenticação nenhuma. Portanto, deve-se adotar restrições das permissões de acesso aos repositórios de arquivos de backup.

Outro fator, que muitas vezes é deixado em segundo plano, está na validação dos backups com restaurações (restores) periódicos. Ao estabelecer uma rotina de backup, o administrador de redes deverá possuir rotinas de restauração em ambientes de testes. É uma temeridade contar com a sorte quando houver a necessidade de restaurar um backup. É uma das situações mais críticas enfrentadas pelo administrador de redes e deve ser gerenciada com o máximo de organização, documentação e validação.



Em casos de problemas, sempre aparece aquele questionamento: “E temos backup?”. Como uma forma de exercício para este tipo de situação, realizar simulações em ambientes de testes para estimar o tempo de restauração e se com o backup existente haverá a restauração de forma correta e esperada. Sobre o questionamento: ““E temos backup?”, se houver silêncio e troca de olhares, é



sinal que a coisa não terminará bem.

Para saber mais



Backup - Mitos & Lendas na Administração de Redes de Computadores



#5 - <https://www.youtube.com/watch?v=3LV2CWh6rxM>



43) Anotar os telefones importantes para caso de tudo dar errado

Quando o administrador de redes está atuando em campo alguns cuidados são importantes. Um deles é possuir as principais informações necessárias para realizar a tarefa em uma mídia *offline*. Por exemplo, endereços IP de dispositivos, senhas, usuários, números de salas e os contatos das pessoas interessadas ou necessárias para a realização da tarefa. Um bloco de anotações básico já seria o suficiente para registrar estas informações importantes. Avaliar que as baterias de celular podem te deixar na mão, os links de Internet também e a talvez a única forma de comunicação seja um telefone fixo ou o telefone de um terceiro, onde não estariam os contatos necessários.

Atualmente, são raros os números de telefone que estão memorizados, com o uso de contatos salvos nos telefones celulares. Porém, quando se atua fora da base podem ocorrer imprevistos e ter uma redundância poderá ajudar muito. Não haverá muita dificuldade em adicionar um bloco de anotações ou um papel com os números anotados dentro da mochila.



As baterias de notebook possuem uma duração razoável quando em perfeito estado. Quando passa a vida útil, a degradação vai tornando a confiabilidade baixa. Em vários episódios de atendimento em campo com notebooks, onde estavam todas as configurações e aplicações necessárias, faltou o carregador porque era para ser um atendimento rápido. Entretanto, levar um carregador do notebook e ter uma extensão elétrica para conectar em uma tomada não tão próxima poderão salvar a necessidade do retorno ao local ou a um retrabalho.



44) Montar um kit de ferramentas e acessórios

Um administrador de redes deverá possuir sempre um kit de ferramentas e acessórios disponível e organizado. Uma das coisas mais frustrantes é faltar determinada ferramenta ou material para terminar uma tarefa e com esta falta deixar a rede indisponível. E não são somente ferramentas, mas um celular ou notebook com bateria carregada para configurar um switch dentro do data center poderá fazer a diferença de vários minutos preciosos de indisponibilidade da rede. Outro fator que deve ser considerado está na qualidade das ferramentas. O investimento em ferramentas e material com qualidade valem a pena e possuem confiabilidade e durabilidade muito superior às versões de baixo custo. No Exemplo 44.1 estão alguns componentes que não podem faltar no kit de ferramentas e acessórios de um administrador de redes.

Exemplo 28.1

Cabos de console, patch cords confiáveis, chaves de fenda e philips de diversos tamanhos, alicates e luvas de proteção

Testadores de cabos e energia com carga na bateria

Chaves de racks e de portas de salas para acesso

Lista impressa dos principais IPs e portas de switches

Documentação atualizada



Possuir uma bolsa fácil de transportar e com as ferramentas básicas para atuação em campo fazem o administrador de redes ganhar tempo em um atendimento. O problema é definir o que seriam ferramentas básicas. Com a experiência talvez o que seria básico comece a ser melhor selecionado, mas usar um martelo ou um pé-de-cabra podem fazer parte do arsenal necessário. Em um episódio, foi necessário o uso de um pé-de-cabra para resgatar um switch em um prédio que seria desocupado e o rack estava dentro de uma sala com uma porta de grade de ferro. Deu bastante trabalho, mas o switch voltou para casa.

Para saber mais





Ferramentas de Trabalho para Redes de Computadores -



<https://www.youtube.com/watch?v=xHoQaPZQuzU>



Este trabalho está licenciado com uma Licença [Creative Commons - Atribuição-NãoComercial-Compartilhável 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/)

45) Utilizar um sistema de gerenciamento de senhas

Com a administração de dezenas, em alguns cenários de centenas, de dispositivos, sistemas, aplicações, serviços e servidores rapidamente, haverá dezenas de senhas diferentes para serem gerenciadas. No mundo ideal haveria um login único para todos os tipos de dispositivos e sistemas, mas com sistemas legados ou dispositivos incompatíveis ainda não há uma solução integrada para tornar isto possível. O mais próximo que se pode chegar é com o uso de LDAP, Radius e uma solução de IdP (*Identity Provider*) para habilitar na maior parte de sistemas, serviços e dispositivos uma base única de identificação.

Para gerenciar as senhas de forma centralizada, quando não há uma solução se SSO (*Single Sign On*) possível, pode-se utilizar um sistema de gerenciamento tal como o Passbolt (<https://www.passbolt.com/>). Um sistema possibilita organizar as senhas de acordo com os grupos de pessoas que podem ter acesso a determinados dispositivos ou sistemas. O compartilhamento de senhas únicas entre administradores não é algo desejável, mas em certos casos não há outra maneira devido à impossibilidade no próprio sistema ou dispositivo a ser gerenciado. E não está descartado manter uma cópia *offline* em lugar seguro das principais senhas e manter esta lista atualizada.

O acesso rápido às senhas e a organização da documentação tornam a vida do administrador de redes mais simples. Ao necessitar do usuário e da senha de um sistema legado, o qual é acessado raramente, pode se tornar uma grande perda de tempo e de paciência. Outro caso é a troca de uma senha sem informar o resto da equipe de trabalho, e poderá acontecer da resolução do problema ser simples, mas o tempo para descobrir ou resetar a senha poderá levar horas desnecessárias. Portanto, manter a lista atualizada das senhas, de forma segura e disponível deve ser rotina para um administrador de redes.



Em equipamentos mais antigos as senhas possuíam restrições de número de caracteres e quais símbolos poderiam ser usados. Esta restrição bagunçava a padronização das senhas em dispositivos tais como switches. Esta restrição é rara nos dispositivos atuais. Outro fator que deve ser documentado são os usuários e não somente as senhas. O usuário padrão em dispositivos é o “admin”, mas isto não é regra universal. Portanto, quando for realizada a documentação das senhas, na verdade, deve-se documentar a identificação necessária para acesso



ao dispositivo, inclusive de quais endereços IP são permitidos os acessos e qual a forma de acesso (Telnet, SSH, console Web).



46) Conhecimento básico da linguagem Python para scripts

A linguagem Python possibilita a automação de várias tarefas na administração de redes. Em Python existem bibliotecas prontas para realizar conexões em dispositivos por Telnet ou SSH e para a geração de scripts aplicados nas tarefas de gerenciamento em massa de configurações. Para a criação de scripts que tratam de arquivos ou que geram a execução de linhas de comandos e coleta dos resultados das execuções possibilitam ao administrador de redes resolver tarefas com muito maior rapidez e assertividade.

No Exemplo 46.1 um script em Python 3 com a biblioteca Telnetlib para realizar a conexão em um servidor Telnet em Linux e executar 3 comandos: uptime, df -h e who.

Exemplo 46.1

```
import telnetlib,time

host='10.0.1.991'

username='suporte'

password='Pass@123'

tn=telnetlib.Telnet(host)

tn.read_until(b'login:')

tn.write(username.encode('ascii')+b"\n")

tn.read_until(b>Password:')

tn.write(password.encode('ascii')+b"\n")

print(tn.read_until(b'~$').decode('ascii'))

tn.write(b"\n")
```



```
# Comandos

comando1='uptime'

comando2='df -h'

comando3='who'

tn.write(comando1.encode('ascii')+b"\n")

tn.write(comando2.encode('ascii')+b"\n")

tn.write(comando3.encode('ascii')+b"\n")

time.sleep(0.2)

all_result = tn.read_very_eager().decode('ascii')

print(all_result)

tn.close()
```

No Exemplo 46.2 um script em Python 3 com a ferramenta Paramiko (<https://www.paramiko.org/>) para realizar a conexão por SSH em um servidor Linux e executar 3 comandos: uptime, df -h e who.

Exemplo 46.2

```
import paramiko

command1 = "uptime"
```



```

command2 = "df -h"

command3 = "who"

host='10.0.1.991'

username='suporte'

password='Pass@123'

client = paramiko.client.SSHClient()

client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

client.connect(host, username=username, password=password)

_stdin, _stdout,_stderr = client.exec_command(command1)

print(_stdout.read().decode())

_stdin, _stdout,_stderr = client.exec_command(command2)

print(_stdout.read().decode())

_stdin, _stdout,_stderr = client.exec_command(command3)

print(_stdout.read().decode())

client.close()

```

No Exemplo 46.3 um script em Python 3 com a biblioteca Netmiko (<https://github.com/kbbyers/netmiko>) no qual é realizada uma conexão por SSH para executar em um switch Huawei comandos do arquivo “config_changes.txt”, salvar a nova configuração com o comando “save” e mostrar a configuração atual do switch com o comando “display current-configuration”. O conteúdo do arquivo “config_changes.txt”, no Exemplo 46.3, define a descrição da interface GigabitEthernet0/0/1 para “Predio33”.



Exemplo 46.2

```
from netmiko import ConnectHandler

huawei_device = {

    'device_type': 'huawei',

    'ip': '10.11.1.131',

    'username': 'admin',

    'password': 'Pass@2o25',

    'conn_timeout': 60,

}

net_connect = ConnectHandler(**huawei_device)

cfg_file = "config_changes.txt"

output = net_connect.send_config_from_file(cfg_file)

print(output)

net_connect.save_config('save')

output = net_connect.send_command("display current-configuration")

print(output)

net_connect.disconnect()
```

Exemplo 46.3

```
interface GigabitEthernet0/0/1

description Predio33

return
```



Observação: os scripts dos exemplos são simplificados para melhor entendimento do leitor. Para uso em produção devem ser criadas validações que não estão contidas nestes códigos.



O desenvolvimento de scripts em Python reduz o trabalho e abre possibilidades de automatizar as tarefas que tomam tempo ou são propensas a erros pelo usuário ou pelo administrador de redes. É um conhecimento que vale muito o estudo para obtê-lo e será sempre útil em quase todas as rotinas relacionadas à área de redes. O que recebo de resposta quando realizo esta observação é algo assim: “Mas eu não gosto de programar!”. Digo que é um script, com o mínimo de código e com uso de muitas bibliotecas prontas. É juntar os blocos e construir um código que seja funcional, não precisa ser um código para ser publicado em algum concurso de desenvolvimento de software. Não tenham medo de programar, na área de Redes é um grande diferencial aplicar este conhecimento.

47) Escaneamento de vulnerabilidades

A administração de redes envolve uma diversidade de sistemas operacionais, dispositivos, aplicações e serviços. Esta diversidade gera a necessidade de monitorar dezenas de alertas, mensagens de fóruns, grupos de conversação e sites especializados relacionados a vulnerabilidades de segurança. Uma das principais referências para buscar vulnerabilidades publicadas é a CVEdetails (<https://www.cvedetails.com/>). Mesmo com bases de dados unificadas de vulnerabilidades, a tarefa de monitorar e verificar se há algum sistema ou serviço vulnerável na rede consome um tempo considerável do administrador de redes e deve ser automatizada. Na Figura 47.1 o resultado de uma busca pelo fabricante Huawei e a escala de privilégios retornam dezenas de ocorrências, com o nível de criticidade e mais informações importantes de como corrigir a falha.



CVEdetails.com
powered by SecurityScorecard

- Vulnerabilities
 - By Date
 - By Type
 - Known Exploited
 - Assigners
 - CVSS Scores
 - EPSS Scores
 - Search
- Vulnerable Software
 - Vendors
 - Products
 - Version Search
- Vulnerability Intel.
 - Newsfeed
 - Open Source Vulns
 - Emerging CVES
 - Feeds
 - Exploits
 - Advisories

Huawei : Security Vulnerabilities, CVEs Published In 2024 (Gain Privilege)

Published in: 2024 January February March April May June July August September October November December
 CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog
 Sort Results By : Publish Date ↗ Update Date ↗ CVE Number ↗ CVE Number ↗ CVSS Score ↗ EPSS Score ↗

[Copy](#)

CVE-2024-39670	Max CVSS	6.2
Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability.	EPSS Score	0.04%
Source: Huawei Technologies	Published	2024-07-25
	Updated	2024-07-26
CVE-2024-36500	Max CVSS	7.8
Privilege escalation vulnerability in the AMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	EPSS Score	0.04%
Source: Huawei Technologies	Published	2024-06-14
	Updated	2024-07-16
CVE-2024-32996	Max CVSS	6.2
Privilege escalation vulnerability in the account module Impact: Successful exploitation of this vulnerability will affect availability.	EPSS Score	0.04%
Source: Huawei Technologies	Published	2024-05-11
	Updated	2024-12-09

Exemplo 47.1 Resultados de busca no site CVEdetails para dispositivos Huawei.

Para isto se deve utilizar ferramentas que fazem varreduras periódicas em busca de vulnerabilidades. Um exemplo de ferramenta em código-fonte aberto para realizar varreduras por vulnerabilidades é a Greenbone OpenVAS (<https://www.openvas.org/>). Os resultados destas buscas geram relatórios que devem ser tratados pelo administrador de redes, em redes maiores junto a equipe de segurança. Nos relatórios são indicados os níveis de criticidade das vulnerabilidades encontradas. Quanto mais crítica a vulnerabilidade, mais prioritário deverá ser a correção ou a remediação do problema. Nem sempre será possível eliminar a vulnerabilidade encontrada, devido a ser um sistema legado ou uma aplicação desenvolvida por terceiros que não tem mais suporte e manutenção. Para estes casos devem ser adotadas restrições rígidas nos acessos aos sistemas vulneráveis e montar um planejamento para desativação destes sistemas no menor tempo possível. Na Figura 47.2 um trecho de um relatório com uma alerta de vulnerabilidade crítico gerado pela ferramenta Greenbone OpenVAS.



2.1.1 High general/tcp

High (CVSS: 10.0) NVT: Operating System (OS) End of Life (EOL) Detection
Product detection result cpe:/o:debian:debian_linux:9 Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0 ↔.105937)
Summary The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The "Debian GNU/Linux" Operating System on the remote host has reached the end of life. CPE: cpe:/o:debian:debian_linux:9 Installed version, build or SP: 9 EOL date: 2022-06-30 EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table
Impact An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Solution: Solution type: Mitigation Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Figura 47.2 Trecho de relatório da ferramenta Greenbone OpenVAS.

O uso de ferramentas automatizadas para varredura de vulnerabilidades podem ser executadas a partir de um host interno da rede alvo ou de forma externa, tal como um atacante faria a tentativa de explorar uma vulnerabilidade. O foco nestas varreduras é em sistemas operacionais e serviços, tais como Microsoft Windows Server, Linux, MySQL Server ou servidores web. Entretanto, as versões de firmware de dispositivos, tais como switches e câmeras, possuem os mesmos problemas e quando encerra o tempo de vida útil do suporte do fabricante não haverá mais correções. É comum equipamentos como switches ficarem em produção por muito mais tempo que o suporte do fabricante. Portanto, este tipo de



equipamento não deve ser exposto a Internet pública ou a acessos que não sejam limitados apenas para a administração de redes responsável.



Ao descobrir vulnerabilidades em sistemas e dispositivos na rede deve-se atuar o mais rápido possível. No mínimo, avaliar quais os procedimentos serão necessários para aplicar a correção, se houver correção. Começar com os procedimentos mais simples e de baixo risco, por exemplo, ao restringir no firewall os acessos somente para endereços conhecidos ou limitar os usuários que podem conectar. A partir disso, montar um plano de correções e o executar com janelas de manutenção programadas. Em sistemas de terceiros deverá haver uma sincronização dos procedimentos entre o administrador de redes e o suporte de terceiros para não haver problemas adicionais e retrabalho. Após a realização das correções deverá haver a validação. Em alguns casos, as correções aplicadas podem adicionar novas vulnerabilidades e o ciclo de verificações deverá ser executado novamente.



48) Manter os sistemas e serviços atualizados

A atualização de sistemas e de serviços possui algumas observações importantes sobre os efeitos das novas versões no restante do ambiente. Deve haver cuidado para a atualização devido à possibilidade de inserção de problemas de compatibilidade. Uma boa prática é analisar o ambiente que terá impacto com a atualização e realizar testes em laboratório previamente. Em muitos cenários na administração de redes haverá sistemas e serviços com um longo tempo de produção e isto tornará o processo de atualização bem mais complexo. Nem sempre será possível atualizar, por exemplo, sistemas legados ou de terceiros. Utilizar nestes casos filtros, desabilitar funcionalidades e acessos que possam estar vulneráveis.

Um caso interessante para ser citado é o de servidores rodando o sistema operacional Microsoft Windows Server 2003 no ano de 2024. Devido ao hardware ser virtualizado não há problemas de compatibilidade neste sentido. Entretanto, o sistema é vulnerável e deve ter acesso restrito, mesmo para usuários dentro da rede interna. Este servidor roda um sistema desenvolvido em 2006 e que não possui mais atualizações ou correções. Está sendo mantido apenas para consultas e para um limitado escopo de usuários.

As atualizações de versões podem causar diversos problemas, talvez mais problemas do que não realizar as atualizações em algumas situações. No Exemplo 48.1 estão alguns casos de situações em que uma atualização poderia causar problemas no ambiente.

Exemplo 48.1

Fazer um “distro upgrade” da versão 6 para a 11

O script de backup não está sendo executado desde a atualização do Python do 2.7 para o 3.1

Não tem mais o driver da impressora do Windows 7 no Windows 11

A atualização para a versão PHP 7 causou a parada da geração do relatório do sistema

O novo firmware do sensor de temperatura aumentou o consumo da bateria em 40%



As atualizações devem ser realizadas de forma preventiva quando possível, mas devem ser realizados testes nas atualizações antes de fazer no sistema de produção. Outro fator é uma falha dormente no ambiente, a qual foi gerada no processo de atualização e se não se manifestará imediatamente. Pesquisar a documentação e o *changelog* do sistema, serviço ou aplicação deve ser rotina para avaliar a necessidade da atualização. Quando as coisas não dão certo, pior que fazer um *upgrade* é fazer um *downgrade*. Analisar o tempo de maturidade de uma versão do sistema ou serviço para evitar bugs sem correção por parte dos desenvolvedores é uma boa prática, evitar ao máximo as versões instáveis (*unstable*) ou beta em produção.



Em uma rede corporativa de médio porte, na época ter 250 computadores era considerado uma rede “grande”, era usado o antivírus OfficeScan da empresa TrendMicro. A instalação era baseada em um servidor que centralizava as atualizações e realizava a distribuição pela rede local, além de possuir vários recursos de administração e relatórios. Nesta rede era usado o sistema operacional Novell Netware 4.11 que precisava de um cliente para autenticação e para o uso dos recursos de compartilhamento de arquivos e impressoras. As atualizações dos antivírus eram baixadas na madrugada e quando os usuários ligavam os computadores no início do expediente havia a verificação e aplicação das atualizações do antivírus OfficeScan. Porém, em um belo dia, no início da manhã começaram as reclamações dos usuários que não havia mais como ingressar na rede, que a janela inicial para pedir usuário e senha da rede Novell Netware não aparecia. O que causou a remoção foi um bug no OfficeScan que detectou o cliente do Novell Netware como um vírus e removeu a aplicação dos sistemas operacionais Windows dos usuários. A empresa reportou o problema algumas horas depois, mas o estrago já estava feito. Foi uma linda semana reinstalando clientes do Novell Netware em mais de 200 computadores. Neste caso não havia muito o que o administrador de redes fazer a não ser detectar a origem do incidente e fazer contato com o fornecedor para solucionar o problema.



49) Certificações Profissionais

Os cursos e materiais preparatórios para as certificações profissionais são as capacitações mais relevantes para um administrador de redes. Nestes cursos preparatórios são abordados tópicos práticos e com foco em tecnologias, alguns casos tecnologias de fabricantes específicos. Ao se capacitar para realizar as provas de certificação e a posterior execução da prova, o administrador desenvolverá competências que são muito desejadas no mercado de trabalho. As certificações possuem tempo de validade variável, por exemplo de um ano ou 3 anos, mas existem casos que não expiram como as certificações para instrutores. Entretanto, ao se tornar um instrutor haverá cursos de atualização em caso de os cursos mudarem de versão, por exemplo, Cisco CCNA 6 para o Cisco CCNA 7.

Para quem está começando na área as certificações mais abertas tais como CCNA (*Cisco Certified Network Associate*), HCNA (*Huawei Certified Network Associate*), MTCNA (*MikroTik Certified Network Associate*) ou CompTIA Network+ são recomendadas. Nestas certificações são tratados assuntos fundamentais e que compõem a base da área de redes, além de estudos de casos nas soluções dos fabricantes que disponibilizam as certificações CCNA (Cisco), HCNA (Huawei), MTCNA (Mikrotik). A certificação CompTIA Network+ é mais generalista e não está atrelada a nenhum fabricante. Estas certificações possuem graduações em níveis de conhecimento e vão recebendo outros nomes tais como CCNP, CCIE e HCIP que tratam de tópicos mais avançados na área de redes.

Outras certificações importantes são sobre o sistema operacional Linux. As certificações da LPI (*Linux Professional Institute*) são as mais reconhecidas no mercado. No site da LPI (<https://www.lpi.org>) estão disponibilizados materiais excelentes para os estudos de preparação das provas. Outras certificações importantes em Linux são as fornecidas pela empresa RedHat.

A empresa Microsoft (<https://learn.microsoft.com/>) possui uma série de certificações de todos os níveis em dezenas de sistemas operacionais, serviços e aplicações, inclusive com as soluções de nuvem da empresa (Azure). Da mesma forma, a empresa Amazon disponibiliza cursos e certificações na solução AWS (*Amazon Web Services*) em diversos níveis de conhecimento. Como recomendação para estes cursos é realizar as versões gratuitas e depois realizar as versões pagas para melhor aproveitamento.



Após realizar as versões mais básicas dos cursos preparatórios para certificações e obter algumas dessas certificações, é interessante criar uma trilha de estudos de acordo com a afinidade desejada nas áreas de segurança, data center, nuvem, banco de dados ou roteamento. O ideal é começar com certificações mais abertas e depois ir focando nos assuntos que são mais interessantes ou necessários para obter conhecimento ou melhores oportunidades de trabalho.



A preparação para uma prova de certificação deve ser feita com o material oficial. Isto é necessário para se habituar no formato das questões que podem ser cobradas e no nível de dificuldade em cada tópico abordado na prova. Realizar provas simuladas e exercícios similares ao conteúdo da prova, com registro de tempo para cada questão, são atividades preparatórias fundamentais para obter sucesso na prova. É importante realizar os estudos com o material da versão correta da prova, mesmo que não existam grandes alterações. Se um novo tópico for adicionado haverá grandes chances de haver questões na prova sobre o assunto. Na minha experiência em provas de certificação, a opção pelo idioma em inglês poderá induzir em menos erros devido a tradução do idioma nem sempre ser perfeita.

Para saber mais



Redes para Iniciantes - Certificações -

<https://www.youtube.com/watch?v=Vk4Q4HSCElw>



50) Antes de tudo, o mais simples

A abordagem para a resolução de um problema deve seguir a ordem do mais simples e rápido primeiro. É algo que parece lógico, mas é muitas vezes esquecido em situações em que a busca pela solução de um problema acaba causando mais problemas.

Em um cenário onde um servidor em rede não está respondendo remotamente, o recomendado seria fazer um reboot no servidor? Ou verificar se o cabo de rede está conectado na interface correta, se a porta do switch está respondendo, se o firewall entre a rede do cliente e do servidor está com as regras corretas, se existe um firewall no servidor causando o bloqueio e outros testes simples e rápidos de realizar? Esta abordagem vale para qualquer problema que um administrador de redes poderá enfrentar e ajuda no descarte de hipóteses do que está causando a indisponibilidade de um sistema ou dispositivo.

Outra vantagem desta abordagem está no tempo da resolução do problema que poderá ser muitas vezes menor do que um procedimento como um reboot em um servidor em produção. Como regra a ser adotada, sempre realizar as verificações mais simples e rápidas por meio de checklist antes de buscar as origens mais complexas dos problemas.



Quando o administrador de redes é inexperiente a abordagem para diagnosticar um problema parte do mais complexo para o mais simples. Esta abordagem é normal e faz parte do aprendizado. Ao longo da carreira, ao experimentar diversos problemas e resoluções, o administrador de redes tende a simplificar a abordagem e ir do mais simples para o mais complexo. Em um episódio, onde o acesso à Internet estava indisponível, começaram as teorias tais como: o link com o provedor está fora, rompeu uma fibra óptica entre os prédios, o roteador está com erro, um malware parou a rede entre outros. Embora todas as teorias possam ser verdadeiras, a primeira coisa a fazer é analisar fisicamente o equipamento que conecta com o provedor de Internet. Verificar leds e conexões físicas. Neste caso, era o patch cord do conversor de fibra que conecta no roteador que estava com mau contato. Um toque no cabo fez voltar à Internet. Em resumo, antes de tudo, o mais simples.



51) Rotinas de Validação de Procedimentos

Na administração de redes é tão importante solucionar um problema quanto validar se os procedimentos foram realizados corretamente. O fato de não haver nenhuma mensagem de erro não significa que o procedimento foi realizado de forma completa. No Exemplo 51.1 estão alguns casos comuns de execução de procedimentos que podem não estar completos.

Exemplo 51.1

Backup: o dump do banco de dados está íntegro?

Firewall: foram validadas as regras com algum acesso externo?

Switches: o arquivo de configuração padrão foi validado depois de ter sido atualizado e aplicado por script em 40 switches?

Banco de dados: todas as permissões foram criadas na tabela, o usuário validou a conexão?

Automatizar as rotinas de validação de procedimentos deve ser considerado como uma melhor prática na administração de redes. Em casos em que não há validação dos procedimentos realizados haverá surpresas desagradáveis em momentos críticos. Se houver dúvida, conferir o mais rápido possível e validar com ferramentas automatizadas. Documentar todos os procedimentos realizados e validar cada etapa de forma isolada é uma abordagem que provê menos erros futuros.



Em casos de janela de manutenção deve ser incluído o tempo para validação das alterações realizadas. Por mais que seja trabalhoso validar os procedimentos no final de uma jornada de horas de manutenção, o problema poderá ser bem maior quando liberar o acesso aos usuários e as coisas não derem certo. É comum ao término de uma atualização de 4 horas, o teste de validação ser em minutos e com poucas variações de testes. Este tempo para mais validações antes de encerrar a janela de manutenção evitará o retrabalho. Verificar se o servidor responde um ping depois de atualizar um banco de dados não é uma validação correta!



52) Evitar a postergação de atividades

Postergar atividades importantes que possuam algum risco são um prato cheio para problemas na área de administração de redes. No Exemplo 52.1 alguns casos recorrentes de postergação de atividades que resultaram em indisponibilidade na rede e poderiam ter sido evitados.

Exemplo 52.1

Amanhã eu revisarei o script de backup

Depois eu reviso os acessos da VPN

Semana que vem reviso as baterias do nobreak

Assim que possível farei a troca do HD no storage

Mês que vem eu vou ver aquele ar-condicionado do data center

Era para ter avisado ontem sobre a janela de manutenção antes do fechamento da folha de pagamento

Não depender da sorte na administração de redes deve ser a regra, ou melhor, deveria ser. Possuir uma organização das atividades e priorizar aquelas que realmente são importantes são desafios na rotina do administrador de redes. A atuação de forma preventiva é a vantagem que deve ser utilizada para obter melhorias na disponibilidade da rede. Para isto deverá haver uma atenção ao planejamento e ao cumprimento das atividades prioritárias que possuem impacto alto na disponibilidade da rede. Não deixar para depois o que deve ser feito imediatamente evitará transtornos futuros.



Certa vez, um disco em um servidor alertou um erro físico. Em um caso como este deveria ser feito a troca o mais rápido possível porque a tendência é que mais erros físicos comecem a se manifestar o que causará a indisponibilidade do disco e dos dados. Entretanto, não havia um disco para substituição porque o setor de compras da empresa estava esperando um 3º orçamento para poder realizar a



compra. A solicitação para a compra do disco tinha sido efetuada pelo administrador de redes 2 meses antes, prevendo que pelo tempo de vida útil do disco no servidor haveria a necessidade da troca. E o que aconteceu? O disco não foi comprado a tempo de haver uma indisponibilidade no servidor e a necessidade da montagem de uma solução temporária e precária até a chegada do novo disco, que desta vez foi comprado no mesmo dia. Sensibilizar a gestão administrativa sobre o impacto da não aquisição de um dispositivo deve ser formalizada para evitar problemas para a área técnica quando houver uma indisponibilidade na rede.



53) O problema é na rede?

A complexidade na administração de redes resulta em uma máxima recorrente de que o problema está na “rede”. A definição do que seria a rede é muito abrangente. Se um sistema não está disponível e o acesso é por rede, em caso de o usuário não conectar ao sistema é um problema na rede, mesmo que o servidor esteja desligado.

Neste caso do servidor desligado, bastaria fazer um ping de um host na mesma rede para o endereço IP do servidor e verificar se o endereço físico estaria na tabela MAC. Caso não esteja, o servidor não está ativo. Outra forma seria verificar a porta do switch no qual o servidor está ligado, se o estado da porta é inativo, o servidor estaria sem energia. Portanto, é um problema na rede? Não, não é um problema de rede. Ao usar a abordagem correta o administrador poderia responder com evidências de que o problema não está na rede. Outra questão é que o servidor está desligado, agora começa a abordagem para analisar os motivos do problema. Neste caso, fica o registro que para o usuário não fará muita diferença porque a conexão dele com o servidor ficou indisponível, sendo rede ou a fonte de alimentação do servidor.

Baseado neste caso, negar se o problema é na rede sem antes verificar ou passar para outros prejudica a confiança do usuário no administrador de redes. No Exemplo 53.1 alguns casos em que necessitaria uma avaliação do administrador de redes primeiro, antes de encaminhar o usuário para um terceiro ou apontar um problema externo.

Exemplo 53.1

Não está acessando o Gmail; o problema deve ser no Google

O sistema não conecta no banco; ligar para a empresa do sistema

Depois que fizeram aquela manutenção de ontem, o prédio ficou sem acesso à Internet; o que foi feito não tem nada a ver...(ou tem?)

Realizar a verificação e a certificação de que o problema não está relacionado a rede também faz parte do trabalho do administrador de redes e muitas vezes é bastante



trabalhoso. Porém deve ser feito com a abordagem correta para identificação e encaminhamento correto da solução.



Um sistema com leitura biométrica era usado para controle de pessoas em um restaurante universitário. Este controle foi implementado com o uso de leitura das digitais. Após a leitura, a consulta era feita em um banco de dados de forma remota para validação. A reclamação dos desenvolvedores do sistema era que a rede estava muito lenta e causando filas para o ingresso no restaurante. Segundo os relatos, todos os testes haviam sido realizados com sucesso e agora a conexão remota estava muito lenta, levando quase 1 minuto para validar uma digital. Portanto, o problema era na rede? O administrador de redes foi acionado para verificar o problema. A primeira observação foi de que o ambiente de testes usado para homologação do sistema, o banco de dados estava no mesmo servidor do sistema, portanto uma conexão em localhost. Desta forma, não houve nenhum teste na rede. A segunda observação foi realizada no local onde estava sendo executado o sistema. Ao solicitar que fosse feita a leitura de uma digital, com uma analisar de tráfego de rede instalado no computador cliente do restaurante, foi percebido que os pacotes da requisição eram entregues imediatamente no servidor de banco de dados e vários segundos depois vinha a resposta com trocas de pacotes muito rapidamente (o cliente e o sistema estavam na mesma rede local). Sendo assim, onde era o tempo de atraso para a entrega da resposta do sistema? Os pacotes estavam “trancados” em algum lugar da rede? A query utilizada para validar as digitais dos usuários estava com erros que causavam a demora no processamento do banco de dados. O envio na rede era basicamente um pacote com a requisição e um pacote com a resposta. O administrador apresentou um relatório técnico com as observações e coletas realizadas e indicou onde era a causa do problema, que não era na rede.

Para saber mais



O problema é na rede? -

<https://www.youtube.com/watch?v=HrMcFvldpG4>



54) Entender os “milagres”

Em certos momentos podem acontecer soluções “milagrosas” para alguns problemas complexos, resultado de diversas tentativas e erros. Quando isto acontece, deverá haver uma documentação dos procedimentos realizados. Avaliar que este problema poderá se repetir no futuro e deverá ser possível replicar em outra situação similar. O problema é não documentar os procedimentos realizados e não saber se um único procedimento resolveu ou se foram combinações de vários deles. No Exemplo 54.1 algumas reflexões que ocorrem nestas situações em que a solução foi encontrada de forma inexplicável.

Exemplo 54.1

Tentamos de tudo, até que funcionou!

Foram aplicadas umas 20 ferramentas até uma dar certo (nem lembro qual delas...)

Usei todas as dicas que busquei no Google e em fóruns para que funcionasse (qual das dicas?)

Será que foi o reboot que resolveu o problema? (seria bom olhar os logs...)

Após a solução do problema, montar novamente o cenário em um ambiente de testes e validar se os procedimentos que foram aplicados são válidos para resolução do problema. Desta forma, haverá uma evolução na experiência do administrador de redes e a solidificação dos conhecimentos e da confiança para as próximas situações. Importante salientar que é provável que em 10, 90 ou 180 dias aconteça novamente o mesmo problema. Entender plenamente o problema e os procedimentos utilizados na solução são requisitos básicos para um administrador de redes.



A cultura do reboot, ou seja, se algo está com algum problema, basta resetar para resolver tem limites. Em último caso, onde todos os procedimentos conhecidos foram aplicados e não houve sucesso, a execução de um reboot passa a ser a única alternativa restante. Entretanto, realizar uma investigação mais aprofundada sobre as origens dos problemas fará com que os procedimentos aplicados possam ser úteis em algum outro evento similar. Um fator muito importante que deve ser considerado: ao realizar um reboot poderá haver mais problemas no retorno, se retornar o sistema ou dispositivo reiniciado. Avaliar o risco em executar este tipo de procedimento em ambiente de produção.



55) Conhecimentos dos fundamentos de Redes

A formação de um administrador de redes deve possuir o conhecimento dos fundamentos da área. Na área de Redes os fundamentos são bastante estáveis, por exemplo o protocolo IPv4 foi publicado na RFC 704 de 1981 (<https://datatracker.ietf.org/doc/html/rfc791>) e é utilizado com mínimas alterações até hoje. Esta lógica vale para toda a família de protocolos TCP/IP. Portanto, possuir um conhecimento avançado nestes protocolos é um investimento de longo prazo.

Para analisar o tráfego de rede o conhecimento dos protocolos da camada de transporte TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*) é fundamental, principalmente o protocolo TCP que é o mais utilizado pelas aplicações em rede. O entendimento do comportamento dos protocolos da camada de transporte é muito importante para analisar o tráfego de rede. A compreensão do comportamento dos protocolos em condições não ideais de rede e de recursos computacionais dos hosts é essencial para avaliar o desempenho das aplicações em rede.

Em relação às redes locais (LAN), o conhecimento de switching e das funcionalidades de VLANs, DHCP *Snooping*, Loop Protection, STP (*Spanning-Tree Protocol*), *mirroring* em equipamentos de diferentes fabricantes são experiências que criam uma base sólida. É comum que existam diversos dispositivos de diversos modelos e fabricantes conectados em uma rede local, dispositivos tais como impressoras, access points, câmeras, telefones IP, sensores, fechaduras, ar condicionados e todo o dia aparece algo novo. Obter conhecimento na configuração destes equipamentos diversos, que muitas vezes possuem similaridades, é uma forma de se preparar para os desafios futuros.

Um dos conhecimentos mais importantes está relacionado ao endereçamento de redes IPv4 e IPv6. Até mesmo administradores de redes mais experientes podem ter dificuldades em definir uma máscara de rede /19 ou qual o ID de rede do IP 10.170.15.97/22. No Exemplo 55.1 estão os procedimentos para realizar os cálculos da máscara e do ID de rede. Este cálculo tem papel fundamental para entender o processo de roteamento e de summarização de rotas. Em IPv6 a abordagem de agrupamentos de endereços é similar, somente usando a notação em prefixos e não mais em máscaras de rede no formato decimal. Um prefixo IPv6 tal como 2001:DB8:A100:1:/64 representa os primeiros 64 bits com



identificação da rede e o restante são endereços que podem ser usados em interfaces de rede por hosts.

Os serviços básicos de suporte de redes tais como DHCP, DNS, SSH, Telnet, TFTP, NTP e SNMP devem ser dominados pelo administrador de redes, ao menos a parte básica dos serviços. Estes serviços dão suporte ao funcionamento das aplicações em rede. São serviços baseados em protocolos com dezenas de anos em uso, portanto, é um conhecimento de longo prazo que vale a pena o administrador de redes investir um tempo para dominá-los.

Exemplo 55.1

Máscara de um /19 - os 19 primeiros bits assume o valor “1” e converter o valor do binário para decimal, elevado na potência de acordo com localização do bit (mais à esquerda 2^7 até o 2^0)

1111111.1111111.11100000.00000000 → 255.255.224.0

Para descobrir o ID da rede e o broadcast de um endereço com a máscara, usa-se um cálculo de AND (E lógico) entre a máscara e o endereço IP. Onde for 255 (todos os bits em 1) o valor será o mesmo do octeto. Quando for 0 (todos os bits em 0) o valor resultante será zero. No octeto que o valor for diferente de 0 ou 255, converter para binário e fazer o AND (similar a multiplicação, 0 com qualquer coisa é 0, 1 com qualquer coisa será qualquer coisa).

10.170.15.97/22

10.170.15.97

----- AND

255.255.252.0

10.170.?.0 → 3º octeto em binário **15**=0 0 0 1 1 1 1

Máscara em binário **252**=1 1 1 1 1 0 0

252 **12**=00001100 AND entre 15 e

ID da Rede: 10.170.**12**.0/22



O broadcast é o último valor do conjunto para calcular, converter para o binário o ID de rede e colocar todos os bits de endereçamento em 1 para saber o último endereço do conjunto. Contar os bits do prefixo, 22 neste caso, e os outros 10 (para fechar os 32 bits do endereço IP) serão para o endereçamento de hosts. O octeto onde está o “12” é convertido para binário e os 6 bits do prefixo são mantidos como estão. Agora, todos os outros bits são colocados em 1 e converte-se para decimal para achar o maior valor do conjunto que é usado como endereço de broadcast em IPv4 (em IPv6 não existe esta regra porque são grupos de multicast usados para comunicação não unicast).

ID da Rede: 10.170.12.0/22

10.170.00001100.00000000 → 10.170.00001111.11111111 → 10.170.15.255 (este é o endereço de broadcast)



O interesse pela história da área onde se atua ajuda muito a entender a evolução das tecnologias e as novidades, que talvez nem sejam tão novidades assim. Um caso clássico é o de VoIP (Voz sobre IP). Os primeiros trabalhos acadêmicos sobre o uso de redes de pacotes de dados para transmissão de voz, nem existia o protocolo IP ainda, datam dos anos 60. Devido às restrições tecnológicas da época, a aplicação de voz sobre redes de pacotes de dados começou nos anos 90. Na área de Redes os fundamentos são mais estáveis que em outras áreas da TI devido a fazerem parte da base para que as aplicações possam trocar dados remotamente e envolvem dispositivos que não são tão simples de ser atualizados ou trocados, principalmente, no núcleo da Internet. Outro caso interessante é o protocolo IPv6 que possui a RFC 2460 de 1998 e ainda está sendo adotado de forma gradativa nas redes corporativas em 2024.

Para saber mais



CIDR (Classless Inter-Domain Routing) - Técnica para Resolução de

Endereçamento - <https://www.youtube.com/watch?v=apMymtnC7bQ>



56) Conhecimentos Não Técnicos

Os conhecimentos não técnicos são tão importantes quanto os conhecimentos técnicos para um administrador de redes. Embora o foco do profissional na área de TI em geral seja em tecnologias, no mercado de trabalho, principalmente no trabalho em equipe, o relacionamento fará a diferença em ser reconhecido pelo trabalho técnico. Em minha carreira profissional já trabalhei com diversos profissionais que eram excelentes tecnicamente, mas não possuíam desenvolvidas as habilidades necessárias para atuar em um ambiente de trabalho com pessoas não técnicas, técnicas de outras áreas ou com o trabalho em equipe.

No Exemplo 56.1 algumas características importantes para serem desenvolvidas e que fazem total diferença nas rotinas de trabalho de um administrador de redes. São objetivos a serem alcançados, só fato de tentar realizá-los trará benefícios para exercer a profissão de administrador de redes com muito mais chances de sucesso.

Exemplo 56.1

Saber aprender

Saber ensinar

Gerenciar bem o tempo de trabalho

Ser pró-ativo e ético

Possuir as habilidade para automatizar tarefas e processos

Planejar as ações

Ter a consciência que os usuários e a chefia entendem muito menos que você sobre redes

Estar atualizado

Saber se relacionar com os usuários

Documentar tarefas de forma inteligível para você e outras pessoas

Saber se relacionar com a chefia



Entender o negócio da instituição (o administrador de redes deve ser capaz de dar suporte ao negócio da empresa)

Procurar saber os “porquês” das coisas!

Evitar a máxima: “está funcionando, mas não sei como!”

Não a gambiarra, só quando estritamente necessário e de forma temporária



A relação entre componentes de uma equipe deve ser, antes de tudo, profissional. Existe uma dependência em cada procedimento executado que poderá resultar em armadilhas para os demais componentes da equipe. Portanto, a comunicação e a documentação dos procedimentos deve estar muito bem organizada. Não é simples trabalhar em equipe e sem haver uma boa comunicação ficará insustentável para realizar um bom trabalho. Um dos piores casos de falta de comunicação é aparecer um problema, a equipe passar um bom tempo analisando e tentando resolver e descobrir que um colega resolveu realizar uma atualização sem comunicar os outros envolvidos. Nunca é fácil!!



57) Serviços em Nuvem

Os serviços em nuvem propiciaram diversos avanços na área de Redes. O uso dos serviços na modalidade de IaaS (*Infrastructure as a Service*) possibilitaram aliviar os custos das empresas em infraestrutura de TI. A administração da infraestrutura local envolve custos elevados e manutenção constante e nem sempre disponível, em muitas regiões é complexo obter serviço especializado tais como para geradores de energia, ar condicionado e nobreaks. As empresas analisam os custos de manter uma infraestrutura local e optam por migrar os serviços para a nuvem de terceiros.

A questão que surge é: “Se está tudo em nuvem, então não há necessidade de infraestrutura de TI local. Será mesmo?”. Para responder esta questão é interessante entender o que existia antes dos serviços em nuvem. Os serviços de hospedagem possibilitam o compartilhamento de servidores físicos usando *virtual hosts* nos servidores Web e painéis de gerenciamento, por exemplo, Plesk (<https://www.plesk.com/>), ISPConfig (<https://www.ispconfig.org/>) e Cpanel (<https://cpanel.net/>). Depois usando contêineres, antes do Docker (<https://www.docker.com/>) já existiam soluções como OpenVZ (<https://openvz.org/>) e outros similares. Os serviços de *colocation* fornecem a locação de servidores físicos ou a possibilidade de hospedar os próprios servidores físicos em data centers remotos. Em todas estas opções anteriores aos serviços de nuvem ainda existe a necessidade de infraestrutura de rede local. No Exemplo 54.1 estão listadas situações nas quais a infraestrutura de rede local deverá ser mantida.

Exemplo 57.1

A rede interna das corporações continuará existindo

Gerenciamento da largura de banda (links) para que os serviços que estão em nuvem possam ser acessados

Computadores e usuários na rede local (alguns usuários poderiam ir para a nuvem... ☺)

Impressoras (ou iremos buscar as impressões no data center da Amazon ou da Microsoft?)

Backup (será feito tudo na nuvem? E quando o volume de dados for muito grande? Tempo para restaurar?)



Questões legais: nem todos os dados podem ser hospedados fora do país ou até mesmo fora da rede de alguma instituição

Outra questão envolve os custos dos serviços em nuvem. Avaliar se todos os serviços em rede local seriam viáveis ao serem hospedados em nuvem. Um cenário onde um servidor de câmeras poderia gerar um custo extremamente alto pelo consumo de largura de banda e do grande volume de armazenamento. Em alguns cenários os custos de administração dos serviços em nuvem não são muito menores que os custos de administração em uma rede local. As dificuldades em encontrar profissionais especializados em serviços de nuvem são iguais ou maiores do que para encontrar qualquer outro na área de redes.

Deve ser considerado o efeito “susto” a partir da alta demanda imprevista de recursos que podem ser gerados nos serviços de nuvem que podem impactar nos valores pagos. Os serviços em nuvem são uma ótima alternativa para melhoria e redução de custos na infraestrutura de TI. Entretanto, deve-se avaliar quais serviços são viáveis e compensam financeiramente para serem migrados para a nuvem.

A infraestrutura de TI local continuará existindo e sem ela não se alcançará os serviços em nuvem. Um cenário clássico é o de um sistema de controle de entrada dos funcionários hospedados na nuvem. Se não houver acesso à Internet, não haverá o registro de entrada de funcionários. A rede local e os serviços em nuvem são muito mais disponíveis que o link do provedor de Internet, mesmo redundante. Uma dica final é analisar de forma criteriosa os riscos de realizar a migração para serviços em nuvem e se há viabilidade técnica para isto em sistemas legados.



Uma das maiores dificuldades na migração de serviços para nuvem é a eventual necessidade de retornar da nuvem para uma infraestrutura local. Um dos serviços que passam por isto é o e-mail. Migrar as caixas postais dos usuários para a nuvem já é uma tarefa trabalhosa. Porém, migrar de volta para uma infraestrutura local demandará um investimento alto em recursos de armazenamento e procedimentos para retornar os dados sem perdas. Outro fato importante a ser observado está na mudança das políticas e termos de uso nos serviços de nuvem. Durante a pandemia do COVID19, o uso de educação à distância foi a solução possível para a continuidade das aulas. Muitas instituições de ensino migraram para serviços de nuvem que eram gratuitos. Entretanto, estes serviços mudaram as políticas de armazenamento de gravações das sessões de webconferência e



modificaram a forma de licenciamento com alterações nos valores a serem pagos. Estas mudanças fizeram com que os administradores de redes tivessem que achar alternativas para dar continuidade aos serviços, por exemplo, baixando e salvando as aulas gravadas para disponibilizar em outros serviços como o Youtube.

Para saber mais



Serviços em nuvem resolvem tudo? Mitos & Lendas na Administração de Redes de Computadores: #3 -



<https://www.youtube.com/watch?v=SWU3tgCgOm8>



58) Conhecimentos de outras áreas

A área de TI possui diversas linhas de atuação profissional, sendo as principais: Desenvolvimento de Sistemas e Aplicações, Redes, Governança e Segurança. Dentro destas linhas de atuação existem um grande número de especialidades e aqui não está sendo levado em conta as áreas que têm a TI como apoio crítico tais como Economia, Meteorologia, Física e outras. Desta forma, o administrador de redes deve ficar atento às outras áreas para, pelo menos, saber o básico e qual o uso da rede na qual está administrando. Em diversos episódios haverá a necessidade de descartar uma falha no sistema ou banco de dados em caso de indisponibilidade de algum serviço. Para isto, o administrador deverá conhecer o cenário nos quais os dados são transmitidos na rede.

Ao possuir um conhecimento básico sobre o negócio da empresa e as tecnologias de desenvolvimento de sistemas utilizadas poderá ajudar muito no diagnóstico de um problema na rede. Na parte administrativa é algo importante saber a interação entre cada setor ou unidade, quais sistemas ou aplicações são utilizados, os procedimentos para pagamentos ou emissão de notas com sistemas terceiros e demais processos que utilizem a rede para serem executados. Isto fará com que as soluções para os problemas sejam resolvidos de forma mais rápida e com menos correrias para o administrador de redes.



A área de redes provê o suporte para outras áreas de uma instituição. Portanto, entender o negócio da instituição deverá ser considerado em todos os procedimentos executados pelo administrador de redes e pela área de TI. A área de TI não deve estar contida nela mesma, deverá prover o suporte para que os sistemas e aplicações realizem a atividade-fim das instituições.



59) Padrões e Melhores Práticas

Na área de redes de computadores os padrões são fundamentais para prover a comunicação de dados. As aplicações e os dispositivos devem respeitar os padrões e em muitos casos existem homologações que atestam que foram implementados todos os requisitos necessários. Um dos exemplos atuais é a aliança entre fabricantes, denominada de *Wi-Fi Alliance*, para os padrões IEEE 802.11 de redes sem fios que leva o nome de *Wifi (Wireless Fidelity)*. Somente os dispositivos que são homologados possuem garantia de compatibilidade.

As RFCs (*Request for Comments*) são outro exemplo de padrões que devem ser seguidos de forma completa. Estes documentos são abertos e públicos e definem os protocolos, recomendações, melhores práticas e propostas para a comunicação de dados na Internet. Nem todos os padrões são abertos, alguns necessitam de permissão para uso e são pagos. Por exemplo, o Skype da Microsoft e o Facetime da Apple são protocolos proprietários e fechados, ou seja, não estão disponíveis ao público para uso em qualquer condição de licenciamento.

Outros padrões em formato de normas são muito importantes na área de infraestrutura de redes. Os padrões EIA/TIA para cabeamento estruturado, instalações elétricas, cabeamento entre outras. No Brasil estes padrões foram nacionalizados por meio das NBRs da ABNT tal como a NBR 14565 de Cabeamento Estruturado que tem como base o padrão EIA/TIA 568B. Em um projeto devem ser seguidas as normas e os padrões vigentes. Em muitos casos parece não fazer sentido o que diz a norma, mas pensar que são documentos baseados em experiências de dezenas de profissionais em projetos ao longo dos anos deve-se respeitar e aplicar nos projetos.

Portanto, o conhecimento sobre normas, padrões, recomendações e melhores práticas não são perda de tempo, muito pelo contrário, são a garantia de que não haverá surpresas quando houver alguma expansão ou alteração do projeto inicial e descobrir que não será possível devido a não obediência de alguma norma.





Não respeitar as normas, padrões e melhores práticas podem causar problemas sem uma solução simples. Por exemplo, em cabeamento estruturado, existe uma recomendação a qual determina uma sobra de 40% do espaço livre em racks e em eletrocalhas. Parece ser algo exagerado, até haver a necessidade de passar mais cabos em eletrocalhas ou de acomodar mais um switch em um rack e não ter como realizar devido à falta de espaço. A experiência ajudará nas adequações às normas, mas na dúvida deve-se seguir as normas e os padrões de forma íntegra.



60) Metodologia para diagnosticar problemas

Existem diversas metodologias para diagnóstico de problemas em rede. O principal objetivo do uso de uma metodologia é diminuir o tempo de resolução do problema e aumentar o tempo de disponibilidade da rede, registrando os procedimentos de forma organizada para criar uma base de conhecimento. As ferramentas de rede são fundamentais para auxiliar no diagnóstico e na validação da resolução de um problema. O descarte de hipóteses da origem do problema passa por uma abordagem onde as verificações mais simples acontecem primeiro. Desta forma, haverá uma aceleração para encontrar o problema e começar a etapa de investigação do motivo que originou a falha ou parada em algum serviço de rede.

Na Figura 60.1 um exemplo de metodologia baseada no livro “Diagnosticando Redes - Cisco Internetwork Troubleshooting” de Laura Chappell e Dan Farkas para diagnóstico de problemas em rede. A origem do problema poderá ser alertada por meio de ferramentas de gerenciamento de rede, informada por meio de sistema de tickets ou comunicada por telefone por usuários. Raramente haverá uma informação completa vindo dos usuários. Por exemplo, um relato tal como "Nada funciona!" ou "Não consigo acessar o site XYZ" ajudará o suporte em TI na definição do problema. Portanto, a primeira etapa é "Definir o problema", se é algo localizado ou se algo generalizado.



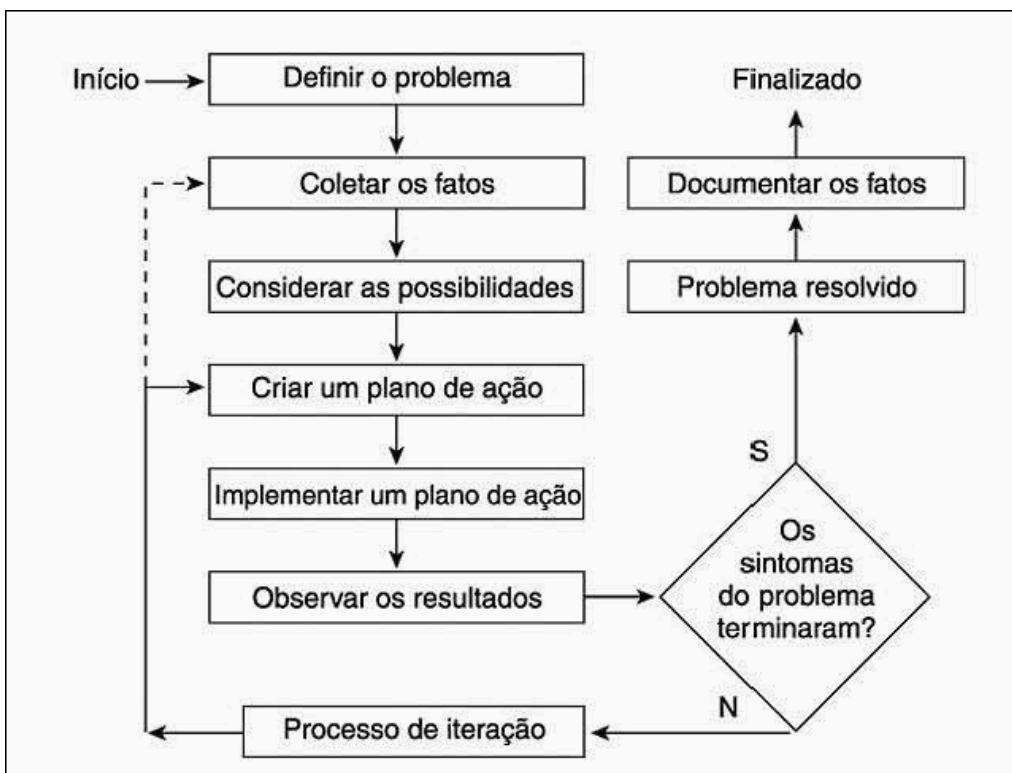


Figura 60.1 Metodologia do livro “Diagnosticando Redes - Cisco Internetwork Troubleshooting”

A próxima etapa "Coletar os fatos" passa por analisar os sensores e monitoramentos disponíveis (*logs, dashboards, consoles de equipamentos*), entrevistar os usuários que relataram o problema, validar se houve alguma atualização de versão em sistemas operacionais, *firmwares* de dispositivos ou ativação de algum novo serviço. A partir disto, na etapa de "Considerar as possibilidades" haverá o descarte, por meio de validações, do que não está causando o problema. Nesta etapa deve-se considerar o uso das ferramentas corretas para auxílio no diagnóstico. Por exemplo, utilizar a ferramenta *ping* para validar se o acesso a um banco de dados está disponível não é um teste completo. Para um caso como este, deve-se utilizar um cliente do banco de dados para validar a conexão, autenticação e permissões de acesso do usuário ao banco de dados.

Na etapa de "Criar um plano de ação" o responsável pelo suporte ao problema deverá fazer um checklist dos procedimentos a serem realizados e analisar as alternativas para cada resultado dos procedimentos. Após isto, em "Implementar um plano de ação"



serão executados os procedimentos planejados e serão observados os resultados que estão na etapa "Observar os resultados".

Se em algum dos procedimentos executados houver a resolução do problema, deve-se validar com o usuário e com ferramentas que possibilitem coletar evidências do funcionamento correto (tcpdump, logs das aplicações, clientes de acesso ao serviço, acesso à Internet). Encerrada a validação, considera-se o problema resolvido e antes do encerramento haverá a etapa "Documentar os fatos", a etapa mais importante que serve como registro na base de conhecimento do suporte para que em outros casos similares a resolução seja mais rápida e assertiva.

Recomenda-se uma metodologia flexível e adaptável, capaz de auxiliar o administrador de redes na descoberta e resolução de problemas específicos de cada ambiente.



Aplicar uma metodologia para diagnosticar problemas resultará em resultados melhores e em menos trabalho para o administrador de redes. Este é um exercício que deve ser praticado e será melhorado a cada nova situação. Em casos onde a origem do problema é desconhecida, o descarte de hipóteses deverá ser realizado e validado de forma mais rápida possível. Em um episódio em que o descarte foi fundamental aconteceu com um link com o provedor onde os acessos web não estavam disponíveis, mas ping e traceroute funcionavam perfeitamente. Segundo o provedor, nenhuma alteração havia sido feita na infraestrutura deles. A partir disto foram realizadas interações no fluxo da metodologia para descartar e validar possíveis causas do problema. Após descartar todas as possíveis causas na rede interna, novamente retornou-se ao provedor. Desta vez, foi reportado que houve uma atualização em um switch na noite anterior na infraestrutura do provedor. Com este fato novo, foi detectado que houve uma alteração no MTU (Maximum Transfer Unit) que causou fragmentação de pacotes maiores e os fragmentos estavam sendo descartados no firewall da empresa. Isto explicava o sucesso do ping e traceroute por serem pacotes pequenos. Em acessos web os pacotes eram maiores que a conexão era descartada. Esta indisponibilidade nos acessos durou cerca de 12 horas até o provedor aplicar uma correção e voltar à normalidade nas conexões. Sem uma metodologia para identificar que a causa do problema não era um problema interno, o tempo de indisponibilidade poderia ter sido muito maior.



61) Analisar as condições de licenciamento e garantia em aquisições

Quando são necessárias aquisições de sistemas, aplicações e dispositivos devem ser consideradas as condições de licenciamento e a garantia/suporte. Estas condições muitas vezes não ficam claras no momento da aquisição e podem acontecer casos em que o dispositivo não possui as funcionalidades necessárias pelo valor da licença adquirida ou que o suporte não cobre a integração da solução com o restante do ambiente da empresa.

A etapa de aquisição deve ser muito bem planejada para não haver surpresas desagradáveis. O custo da aquisição pode ser irrisório perto do valor da manutenção e da administração de uma solução. Na minha experiência um caso interessante aconteceu na aquisição de um storage. O storage foi adquirido com 5 anos de garantia e suporte. Um alto investimento que serviu como principal unidade de armazenamento por 5 anos, com raros problemas. Os problemas foram relacionados a HDs que precisaram ser trocados. A troca foi realizada em 3 dias úteis pela empresa, prazo que estava formalizado no contrato do serviço dentro da validade da garantia. Portanto, é um serviço excelente de suporte no período da garantia.

Após o período de garantia, foi realizada uma cotação para estender o prazo da garantia por mais 2 anos, algo que era previsto no contrato. Entretanto, o valor para mais 2 anos de garantia e suporte era superior ao valor de um storage novo com maior capacidade. Este é um caso em que o dispositivo serviu com excelência no período de cobertura da garantia. Porém, ao terminar os 5 anos da garantia, o valor se torna inviável para estender a garantia. Coincidência ou não, depois do tempo da garantia e suporte terem terminado houve problemas em mais 4 HDs que resultaram na necessidade de refazer os arranjos dos discos sobreviventes no storage.

Um outro caso interessante de garantias que possuem armadilhas nas letras miúdas do contrato aconteceu com APs. Foram adquiridos 122 APs de um modelo com 1 ano de garantia. Ao passar alguns meses do final da garantia, os problemas começaram a aparecer. No total, 30 APs (e ainda contando) pararam de funcionar, provavelmente por superaquecimento. Tudo leva a indicar um problema no lote do produto ou na construção do dispositivo. Ao fazer contato com a empresa e explicar o ocorrido, a empresa se colocou à



disposição para analisar os dispositivos. Até este momento tudo certo, o problema foi a necessidade de envio dos 30 APs para os EUA. O custo de envio dos APs para os EUA e o possível retorno com a troca por um novo, o que configura um novo dispositivo e incidência de impostos de importação, tornou-se inviável. Desta forma, é muito importante saber onde será feita a garantia e se haverá custos adicionais para isto.

O modelo de venda com serviço incluído, comum em soluções de segurança como firewalls, pode ter efeitos indesejados. Sempre perguntar o que acontecerá com as funcionalidades dos dispositivos em casos de não renovação do pagamento do serviço. O dispositivo ficará indisponível ou com recursos limitados? E se renovar depois do prazo, haverá alguma multa? A aquisição de equipamentos com funcionalidades proprietárias e vinculadas a um fornecedor específico demanda uma análise minuciosa do contrato, a fim de evitar a criação de uma dependência tecnológica (*vendor lock-in*).



A dependência em um único fabricante foi por muito tempo o padrão na área de TI. Nos anos 60 até os anos 90, a empresa IBM usava um modelo de negócios onde provia soluções proprietárias e incompatíveis com os demais fabricantes que eram compostas de hardware, sistema operacional, plataforma de desenvolvimento de sistemas e comunicação de dados. Com a publicação de forma aberta de padrões e protocolos houve o ingresso de novos fabricantes no mercado com soluções compatíveis e de valor reduzido. Este novo modelo propiciou a expansão das redes locais e dos primeiros provedores de acesso à Internet com escopo regional. Portanto, a mudança na forma de licenciamento das tecnologias teve papel fundamental no desenvolvimento e expansão das redes de computadores.



62) Verificar a conexão no servidor correto

Na administração de servidores é rotina haver diversas janelas com consoles de gerenciamento abertas. Em alguns casos chegam a dezenas de janelas com acesso por SSH em sistema Linux ou com o acesso por área de trabalho remota em servidores Microsoft Windows. Na Figura 62.1 um cenário onde se sessões de SSH o comando certo foi feito na janela errada e a partir disto poderá haver problemas devido a ter sido realizado um “shutdown -h now”.



Figura 62.1 Comando certo na janela errada em sessões de SSH

Nestes cenários deve-se ter o máximo de cuidado para não ocorrer o comando certo na janela errada ou o comando errado na janela certa e causar indisponibilidade em serviços. Uma das formas fáceis de diminuir o risco seria colocar nomes nas janelas dos terminais, cores de fonte e fundo para diferenciar cada servidor. No caso de servidores Windows, usar um papel de parede diferente ou um tema de janelas diferente poderá ajudar.

No acesso por SSH existem diversos gerenciadores de conexões que são muito úteis para organizar a administração de janelas, tais como MTPutty para Windows (<https://ttypplus.com/multi-tabbed-putty/>) ou Àsbrú Connection Manager para Linux (<https://www.asbru-cm.net/>).



Em mais de um episódio, aconteceu de um comando certo na janela errada ser aplicado e começarem os alertas e o telefone a tocar. Por exemplo, um comando com uma query SQL para realizar um update ou um delete no banco de testes ser aplicado no banco de produção. Ou em casos piores, onde um delete ou um update sem a cláusula where, para limitar quais registros deveriam ser atualizados ou apagados, ser aplicado em um banco de produção. Considerar que em certos momentos a certificação de estar na console certa para aplicação de comandos poderá ser a diferença entre terminar uma tarefa com sucesso ou criar o caos com sucesso!



63) Testes com ferramentas em ambiente de produção

Em alguns cenários se torna bastante complexo realizar testes em procedimentos e configurações antes de aplicar em ambiente de produção. Isto ocorre devido a não ser possível replicar exatamente o ambiente de produção porque não há dispositivos iguais reservas ou não há como realizar a interação de aplicações externas que necessitam de validação. Um teste realizado em um ambiente similar ao ambiente de produção não é um teste completo e nem todas as condições serão tratadas. Nestes casos de execução direta no ambiente de produção deve-se realizar backup de configurações, snapshots de máquinas virtuais, checklists para validação dos resultados e, principalmente, publicar uma janela de manutenção para todos os interessados.

Por mais simples que seja um procedimento em um ambiente de produção, deve-se avaliar o impacto e montar um plano de *fallback* (retorno) se as coisas derem errado. Um exemplo comum é com procedimentos em unidades de armazenamento ou no ambiente de virtualização. Pouco provável que exista um ambiente de testes reserva devido ao alto custo dos dispositivos. Portanto, uma atualização ou alteração de configuração deverá passar por uma pesquisa completa na documentação disponibilizada pelo fabricante e realizar uma boa varredura nos fóruns de usuários para se preparar para possíveis problemas. Na Figura 63.1 um pensamento tentador para realizar aquele procedimento que era simples e depois causou um efeito em cascata de indisponibilidade, é a formação da *unavailability storm* (tempestade de indisponibilidade).





Figura 63.1 Momento no qual as coisas podem começar a dar errado.

Nestes momentos de alterações em ambiente de produção podem ocorrer problemas “inéditos” onde somente o contato com o suporte do fabricante poderá ajudar na resolução, afinal há um contrato de suporte vigente com o fabricante, certo?



Nos anos 90 e começo dos anos 2000, em um cenário onde não existiam recursos de virtualização, basicamente os procedimentos eram feitos no ambiente de produção. Não havia recursos de snapshots e era um investimento alto ter redundância ou até mesmo um dispositivo similar para usar como ambiente de testes. Para aumentar a complexidade, os hardwares dos servidores possuíam particularidades tais como as controladoras de disco ou as interfaces de rede que necessitavam de drivers específicos para serem detectadas no sistema operacional. Uma instalação de um servidor não era apenas instalar o sistema operacional a partir de uma mídia, tinha uma etapa anterior que era o sistema operacional reconhecer o hardware. Bons tempos, bons porque ficaram no passado!



64) Viabilidade técnica

Em um projeto na área de redes um dos maiores dilemas está na viabilidade técnica versus o orçamento disponível. Na verdade, este é o problema de grande parte dos projetos na área de TI. A necessidade do cliente acaba sendo bem diferente do que ele tem de recursos para investir. Esse cenário, comum no mundo da TI, coloca o administrador de redes em um desafio: como entregar a melhor solução possível dentro das restrições financeiras? A demanda por soluções cada vez mais sofisticadas e a pressão por custos mais baixos criam uma dificuldade constante. A comunicação aberta e transparente com o cliente é fundamental para entender suas necessidades e expectativas, e para apresentar as opções disponíveis de forma clara e objetiva.

O tipo de demanda que chega até a área técnica em um projeto é que a rede não pode parar, que tenha mínimo de manutenção, que o armazenamento deve ser infinito, que a segurança máxima e que os equipamentos devam ter baixo custo, alto desempenho e que tenham o mínimo prazo para entrega. A primeira coisa é analisar a viabilidade técnica para isto. Existe infraestrutura na região com provedores de acesso à Internet que atendam com redundância em dupla abordagem, a área do data center comporta fisicamente os equipamentos, a rede elétrica está dimensionada de acordo e outros pré-requisitos. É importante que o administrador de redes priorize as necessidades mais críticas do cliente e identifique as funcionalidades que agregam mais valor ao negócio. A partir dessa análise, é possível propor soluções escaláveis que atendam às necessidades atuais e permitam futuras expansões.

A busca pela solução ideal muitas vezes envolve um processo de negociação. É preciso encontrar um equilíbrio entre as expectativas do cliente, as possibilidades técnicas e as restrições orçamentárias. Ao apresentar as diferentes opções, o administrador de redes deve ser transparente quanto aos benefícios e às limitações de cada solução. O proponente do projeto pode possuir 0,1 % do valor da solução ideal e querer o mesmo desempenho. Nestes casos deve-se deixar claro que com o valor para investimento não serão atingidos os requisitos solicitados e que a solução não será a ideal.

A melhor solução não é necessariamente a com o maior custo, mas sim aquela que atende às necessidades mínimas do cliente de forma confiável, dentro das restrições



orçamentárias. Sempre indicar a melhor solução técnica, independente do orçamento disponível e não realizar falsas promessas apenas para garantir um cliente devido ao custo da administração ser muito maior do que o custo da implementação.



Em um determinado projeto de rede lógica, o cliente solicitou cobertura total da área de um prédio com rede sem fios e pontos de rede em todas as salas. A partir disso foram realizados os estudos e a análise do local para montar os itens necessários. Um ponto de rede lógica envolve uma série de custos: cabos, conectores, eletrocalhas, eletrodutos, patch panel, porta do switch para conexão, serviços de passagem e conectorização dos cabos, rack, configuração do switch, caso o enlace seja com fibra óptica, fusão da fibra, fiber cords, patch cords e ferragens para dar suporte aos dutos e passagens. Outro fator a considerar é que um dispositivo sem fios possui um cabo de rede para conectar ao restante da rede, salvo se utilizar uma tecnologia em mesh que não é adequada a um ambiente corporativo. Se forem contabilizados os custos dos dispositivos e possíveis custos de licenças para gerenciamento em caso de controladores de redes sem fios, a conta só aumenta. Ao realizar a totalização dos custos necessários para executar os requisitos pedidos pelo cliente, os requisitos solicitados foram bastante reduzidos porque o orçamento previsto para o projeto não chegava em 10% do valor necessário para a cobertura total do prédio. Neste caso, a questão técnica ideal foi apresentada para realizar toda a cobertura do prédio. Entretanto, por restrições financeiras, apenas as áreas de uso comum como saguão e auditório foram cobertos pela rede sem fios. E esta condição ficou formalizada no contrato para execução do projeto.



Considerações Finais

As dicas que foram apresentadas neste livro não são regras a serem seguidas como uma norma. Cada profissional possui a sua trajetória e os ambientes de rede não são idênticos. Para quem atua em um provedor de Internet e para quem atua em uma rede de pequeno porte, as atividades e as tecnologias envolvidas podem ser bem diferentes. Entretanto, o propósito do livro foi fazer uma compilação da minha experiência na área de redes que acredito serem relevantes, principalmente para iniciantes na área.

Eu espero ter conseguido atingir o meu objetivo e que estas dicas sejam úteis nas rotinas dos administradores de redes. Experimente, erre e aprenda com seus erros. A experiência prática é a melhor forma de se tornar um excelente administrador de redes. Desde os meus primeiros “pings” na área em 1995 até os dias de hoje, ainda sigo na trilha do conhecimento e com desejo de novos desafios. Seguimos em frente para novos aprendizados!

“People think of education as something they can finish.”

ISAAC ASIMOV



Referências bibliográficas

Estas referências bibliográficas aqui listadas foram importantes na minha formação. Os livros foram a principal fonte de conhecimento nos anos 90 e começo dos anos 2000. Com a Internet comercial e o surgimento de fóruns, blogs e sites especializados em Linux, segurança em redes, cursos preparatórios para certificações e depois com canais do Youtube e redes sociais, houve uma ampliação exponencial de fontes de aprendizagem. Entretanto, a recomendação é que se faça uma boa revisão bibliográfica em livros clássicos que são uma fonte revisada e de boa qualidade.

Livros

- ABNT. NBR 14565: procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada. Rio de Janeiro: ABNT, 2000.
- BRITO, Samuel Henrique Bucke. Laboratórios de Tecnologias Cisco em Infraestrutura de Redes. 2. ed. São Paulo: Novatec, 2014.
- BURGESS, Mark. Princípios de Administração de Redes e Sistemas. 2. ed. LTC, 2006.
- BURTCHE, Ken O. Scripts de Shell Linux com Bash. São Paulo: Ciência Moderna, 2005.
- CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. Redes de computadores. Pelotas: Bookman, 2009.
- CHESWICK, William R. Firewalls e segurança na Internet: repelindo o hacker ardiloso. 2. ed. Rio de Janeiro: Bookman, 2004.
- COLCHER, Sergio; GOMES, Antonio Tadeu Azevedo; SILVA, Anderson Oliveira da. VoIP: Voz Sobre IP. Rio de Janeiro: Campus, 2005.
- COMER, Douglas E. Interligação de redes com TCP/IP: Vol. I. 5. ed. Rio de Janeiro: Campus, 2006.
- ENGEBRETSON, Patrick. Introdução ao Hacking e aos Testes de Invasão - Facilitando o hacking ético e os testes de invasão. São Paulo: Novatec, 2014.
- ENGST, Adam Engst; FLEISHMAN, Glenn. Kit do Iniciante em Redes sem Fio - O Guia prático sobre redes Wi-Fi. 2. ed. São Paulo: Pearson, 2005.
- EQUIPE IPv6.br. Laboratório de IPv6 - Aprenda na prática usando um emulador de redes. São Paulo: Novatec, 2015.
- FERREIRA, Rubem E. Linux: guia do administrador do sistema. 2. ed. rev. ampl. São Paulo: Novatec, 2008.
- FILIPPETTI, Marco Aurélio. CCNA 4.1: guia completo de estudo. Rio de Janeiro: Visual Books, 2008.



- FYODOR, G. Exame de Redes com NMAP. São Paulo. Ciência Moderna, 2009.
- HORST, Adail Spínola; PIRES, Aécio dos Santos; DÉO, André Luis Boni. De A a Zabbix - Aprenda a monitorar e gerenciar aplicações e equipamentos de redes com o Zabbix. São Paulo: Novatec, 2015.
- KUROSE, James; ROSS, Keith. Redes de computadores e a Internet: uma abordagem top-down. 3. ed. São Paulo: Pearson Education, 2007.
- LIMONCELLI, Thomas A. The Practice of System and Network Administration. 2. ed. EUA: Addison-Wesley Professional, 2007.
- LUTZ, M.; ASCHER, D. Aprendendo Python. 2. ed. São Paulo: Bookman, 2007.
- MATTHEWS, J. Rede de Computadores: protocolos de Internet em Ação. Rio de Janeiro: LTC, 2006.
- MORENO, Daniel. Introdução ao Pentes. São Paulo: Novatec, 2015.
- MORIMOTO, Carlos E. Redes e servidores Linux: guia prático. 2. ed. Porto Alegre: Sulina, 2006.
- MORIMOTO, Carlos E. Servidores Linux, Guia Prático. Porto Alegre. GDH Press e Sul Editores, 2008.
- MOTA FILHO, João Eriberto. Análise de Tráfego em Redes TCP/IP - Utilize tcpdump na análise de tráfegos em qualquer sistema operacional. São Paulo: Novatec, 2013.
- NEMETH, Evi . Manual Completo do Linux: guia do Administrador. 2. ed. São Paulo. Pearson Prentice Hall, 2007.
- NEMETH, Evi. Manual completo do Linux: guia do Administrador. 2. ed. São Paulo: Pearson – Prentice Hall, 2007.
- NORTHUP, Tony; MACKIN, J.C. Configuração do Windows Server 2008: infraestrutura de rede: kit de Treinamento MCTS(Exame 70-642). Porto Alegre: Artmed, 2008.
- ODOM, Wendell. CCNA ICND 2 Guia Oficial de Exame. 2. ed. Rio de Janeiro: Alta Books, 2008.
- OLIVEIRA, R.; CARISSIMI, A.; TOSCANI, S. Sistemas Operacionais. 3. ed. Porto Alegre: Sagra Luzzato, 2004.
- OPPENHEIMER, Priscilla. Top-Down Network Design. 2. ed. EUA: Cisco Press, 2004.
- PETERSON, Larry; DAVIE, Bruce. Redes de Computadores. 3. ed. Rio de Janeiro: Campus, 2004.
- PINHEIRO, José Maurício S. Cabeamento óptico. Rio de Janeiro: Campus, 2003.
- PINHEIRO, José Maurício S. Guia completo de cabeamento de redes. Rio de Janeiro: Campus, 2003.
- PRITCHARD, Steven. Certificação Linux LPI – nível 2 exames 201 e 202. 2. ed. Rio de Janeiro: Alta Books, 2007.
- PRITCHARD, Steven. Certificação Linux Lpi - Nível 1 Exames 101 e 102. 2. ed. Rio de Janeiro: Alta Books, 2007.



- PURDY, Grecor N. Linux Iptables: Guia de Bolso. Rio de Janeiro. Alta Books, 2006.
- RHODES, Brandon. Programação de redes em Python. São Paulo: Novatec, 2015.
- RUFINO, Nelson Murilo de O. Segurança em Redes sem Fio. 4. ed. São Paulo: Novatec, 2014.
- SANDERS, Chris. Análise de pacotes na prática. São Paulo: Novatec, 2017.
- SEITZ, Justin. Black Hat Python - Programação Python para hackers e pentesters. São Paulo: Novatec, 2015.
- SHIMONSKI, Robert. Wireshark Guia Prático - Análise e resolução de problemas de tráfego em rede. São Paulo: Novatec, 2013.
- SILBERSCHATZ, A.; GALVIN, P. B. Fundamentos de Sistemas Operacionais. 6. ed. São Paulo: LTC, 2004.
- SOARES, L. F. Gomes. Redes de computadores das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.
- STALLINGS, William. Criptografia e segurança de redes: princípios e Práticas. 4. ed. São Paulo: Pearson, 2008.
- STANEK, William R. Microsoft Windows Server - Guia de Bolso do Administrador. São Paulo: Bookman, 2006.
- STEVENS, W. Richard; FENNER, Bill; RUDOFF, Andrew. Programação de rede UNIX, Vol. I - API para sockets de rede. 3. ed. Porto Alegre: Bookman, 2005.
- TANENBAUM, Andrew S. Redes de computadores. Rio de Janeiro: Campus, 2003.
- TANENBAUM, Andrew. Organização estruturada de computadores. 5. ed. Rio de Janeiro: Prentice-Hall, 2007.
- TRULOVE, James. LAN Wiring. 3. ed. EUA: McGraw-Hill, 2005.
- WARD, Brian. Como o Linux funciona - O que todo superusuário deveria saber. São Paulo: Novatec, 2015.

Sites

- Canal Emmonks - <https://www.youtube.com/@emmonks>
- Top 100 Network Security Tools - <http://www.sectools.org/>
- Command-line Fu - <http://www.commandlinefu.com/commands/browse>
- LPI – <http://www.lpi.org/>
- Slashdot = <https://slashdot.org/>
- StackOverflow - <https://stackoverflow.com/>
- HowtoForge - <http://www.howtoforge.com/>
- GTER (Grupo de Trabalho de Engenharia e Operação de Redes) - <http://qter.nic.br/>
- GTS (Grupo de Trabalho em Segurança de Redes) - <http://gts.nic.br/>
- Open Web Application Security Project (OWASP) - <http://www.owasp.org/>
- OWASP Top 10 - http://www.owasp.org/index.php/OWASP_Top_10



- Cert.Br – <http://www.cert.br>
- Práticas de Segurança para Administradores de Redes Internet - <http://www.cert.br/docs/seg-adm-redes/>
- Help Net Security - <http://www.net-security.org/>
- Sans.org – <http://www.sans.org>
- Top 25 Software Errors - <http://www.sans.org/top25-software-errors/>
- ISPTools - <http://www.isp.tools/>
- MXToolBox - <https://mxtoolbox.com/NetworkTools.aspx>
- DNS Checker - <https://dnschecker.org/>

