Fortalecendo a Infraestrutura:

Dicas para Switches e OLTs

DATACOM

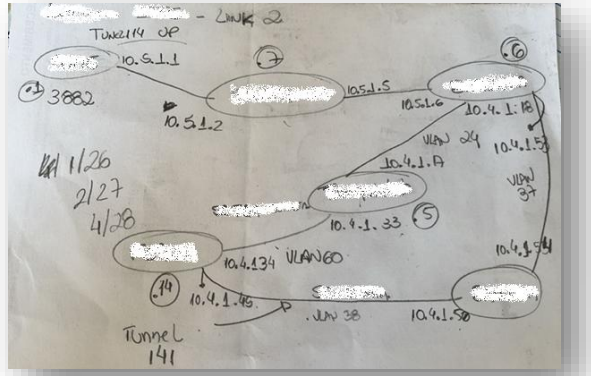
Planejamento

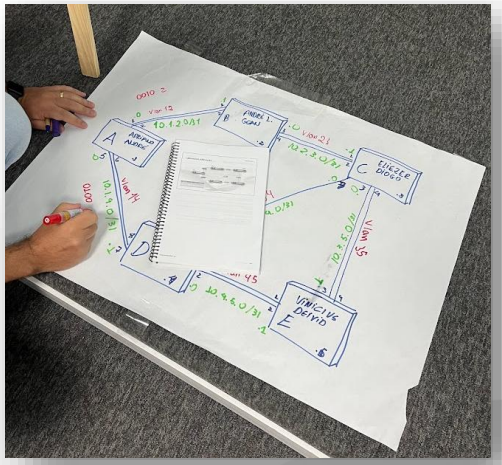
- Defina o seu processo: Qual o seu “produto final”? Quais são as suas “dores”?
  - Pensar
  - Esboçar/Elaborar - Rascunho
  - Organizar/Ordenar/Sistematizar
  - Executar

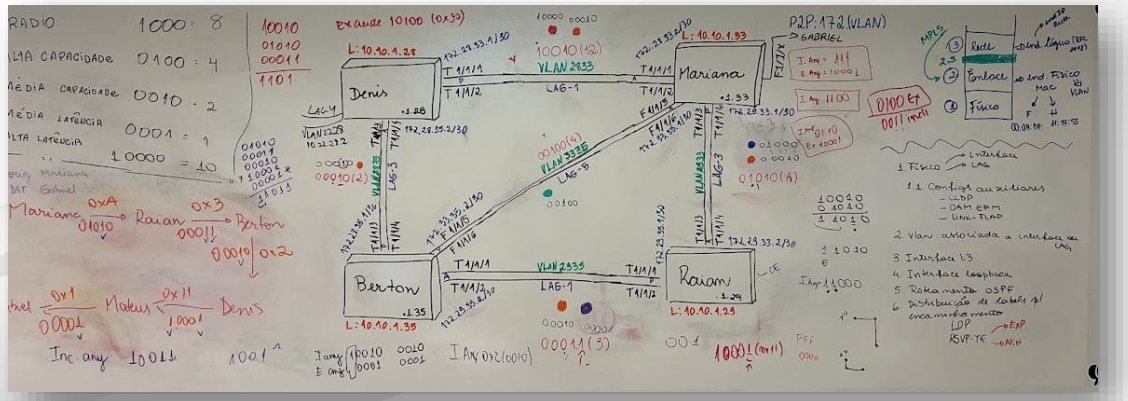
- Quais documentações serão necessárias para a sua rede, serviços/soluções ofertados?

- Tecnologias envolvidas: GPON, Ethernet, DWDM, Wireless?

- Indique nomes e defina funções

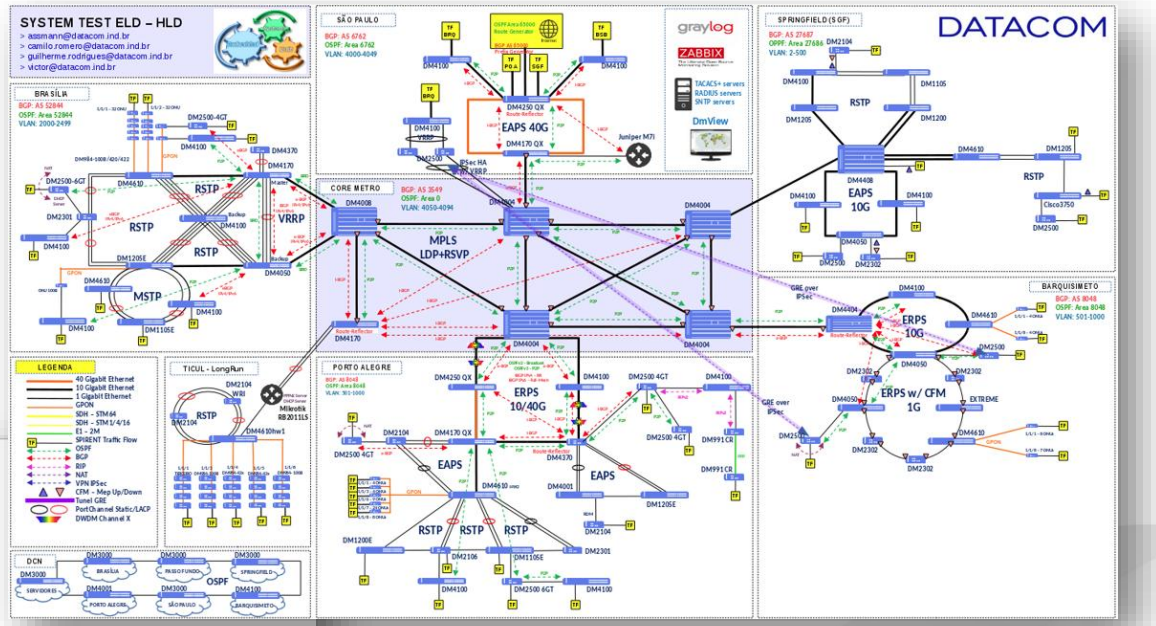


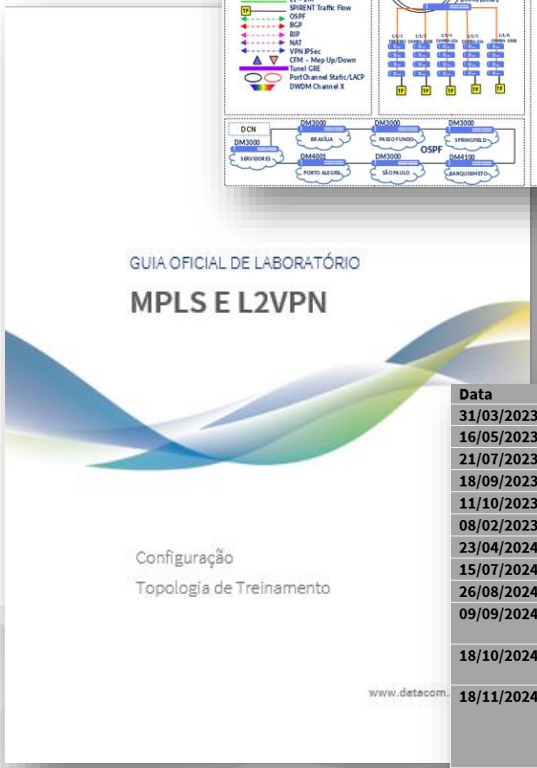




Documentação

- Mapeamento de toda a infraestrutura física e lógica
- Padrão de nomenclaturas e simbologias
- Alocação dos blocos de endereçamento IPv4 e IPv6, VLANs e Pseudowires
- Configurações e uma breve descrição do seu propósito
- Políticas de encaminhamento, roteamento, qualidade de serviços e outros
- Controle de inventário





Mantenha atualizado

Data	Revisão	Autores / revisores	Alterações de Revisão
31/03/2023	1.0	Tatiane Figueiredo	Criação da documentação
16/05/2023	1.1	Tatiane Figueiredo	Versão de firmware e melhorias no documento
21/07/2023	1.2	Tatiane Figueiredo	Versão de firmware
18/09/2023	1.3	Tatiane Figueiredo	Melhorias no documento
11/10/2023	1.4	Tatiane Figueiredo	Versão de firmware
08/02/2023	1.5	Tatiane Figueiredo	Versão de firmware
23/04/2024	1.6	Tatiane Figueiredo	Versão de firmware
15/07/2024	1.7	Tatiane Figueiredo	Versão de firmware
26/08/2024	1.8	Tatiane Figueiredo	Versão de firmware e melhorias no documento
09/09/2024	1.9	Tatiane Figueiredo	Adição de nova topologia de laboratório e melhorias no documento
18/10/2024	2.0	Tatiane Figueiredo	Versão de firmware, inserção de novas informações e correções de grafia
18/11/2024	2.1	Tatiane Figueiredo	Adição de modelo de equipamento, configuração de interface túnel para afinidade, atualização de firmware e melhorias no documento
28/04/2025	2.2	Tatiane Figueiredo	Versão de firmware, endereço IP do servidor SNTP e faixa de IPs dos switches com DmOS

DATACOM

Documentação nos Equipamentos

```
interface tunnel-te 1
 name T1-STRICT-DmOS_22-DmOS_24
 destination 24.24.24.24
 path-option 1 explicit name T1-STRICT-DmOS_22-DmOS_24-VIA-DmOS_21
!
interface gigabit-ethernet 1/1/4
 description CLIENTE-TEST_SET
 no shutdown
 negotiation
 duplex full
 speed 1G
 advertising-abilities 10Mfull 100Mfull 1Gfull
 mdix normal
 mtu 16338
!
interface ten-gigabit-ethernet 1/1/1
 description LAG-1_SW22_SW21
 no shutdown
 no negotiation
 duplex full
 speed 10G
 mdix normal
 mtu 16338
```

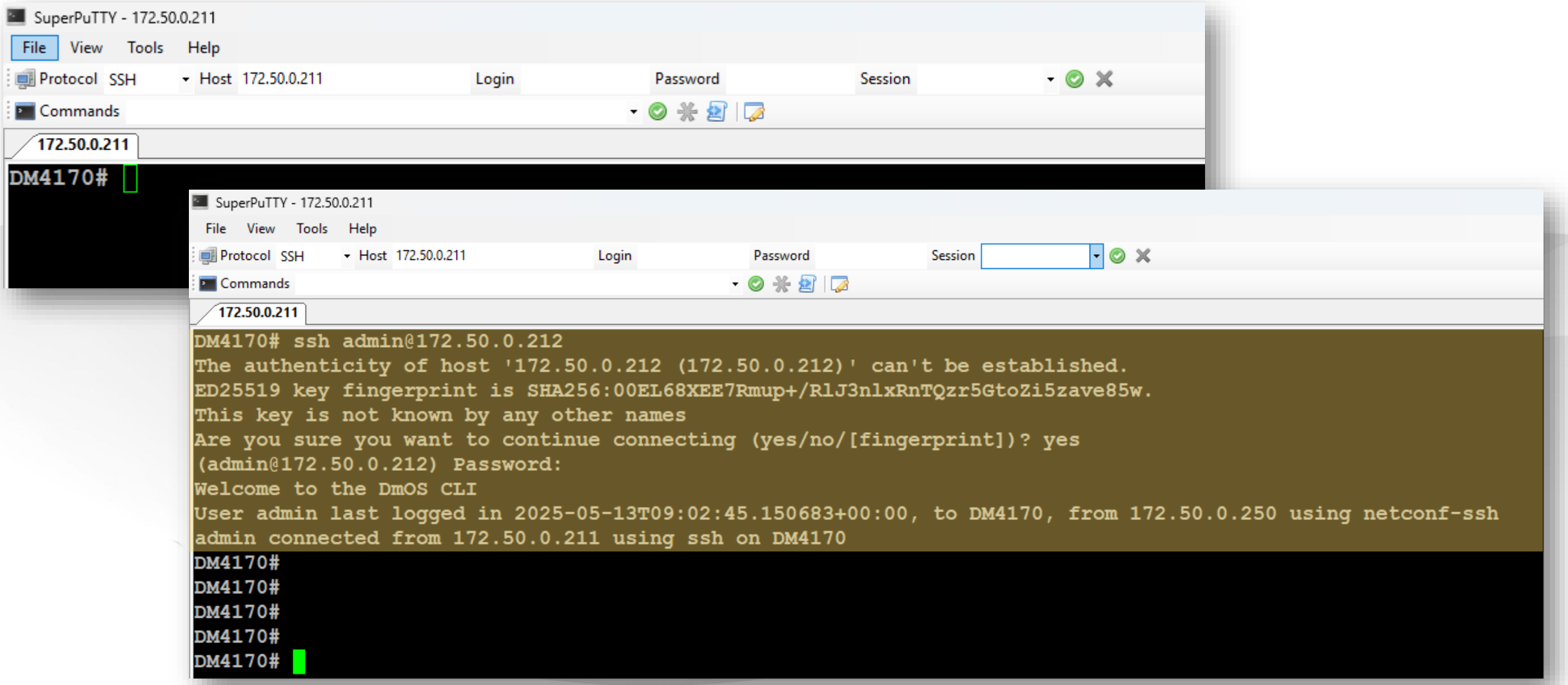
```
dot1q
 vlan 2122
  name Infra-OSPF-MPLS-SW22-SW21
  interface lag-1
  !
 !
!
link-aggregation
 interface lag 1
  description LAG-1_SW22-SW21
  mode passive
  interface ten-gigabit-ethernet-1/1/1
  !
  interface ten-gigabit-ethernet-1/1/2
```

```
hostname DmOS-22
```

```
mpls l2vpn
 logging pw-status
 vpws-group EAD-VPWS
  vpn 5
   neighbor 23.23.23.23
    pw-type vlan
    pw-id 5
   !
   access-interface gigabit-ethernet-1/1/5
    dot1q 30
```

DATACOM

Que equipamento é esse?

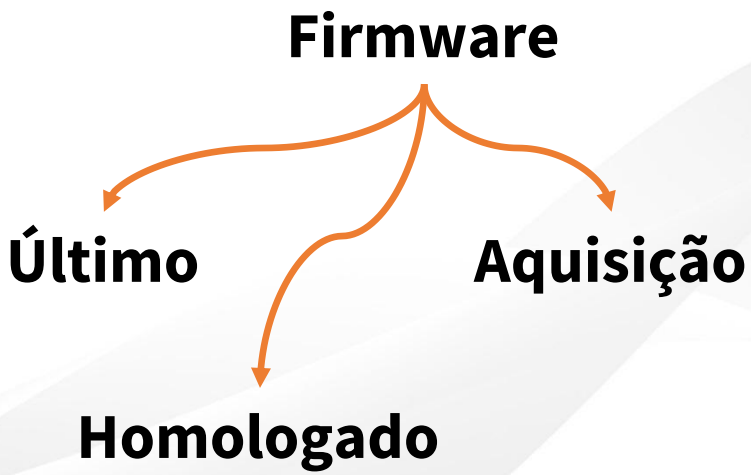


DATACOM

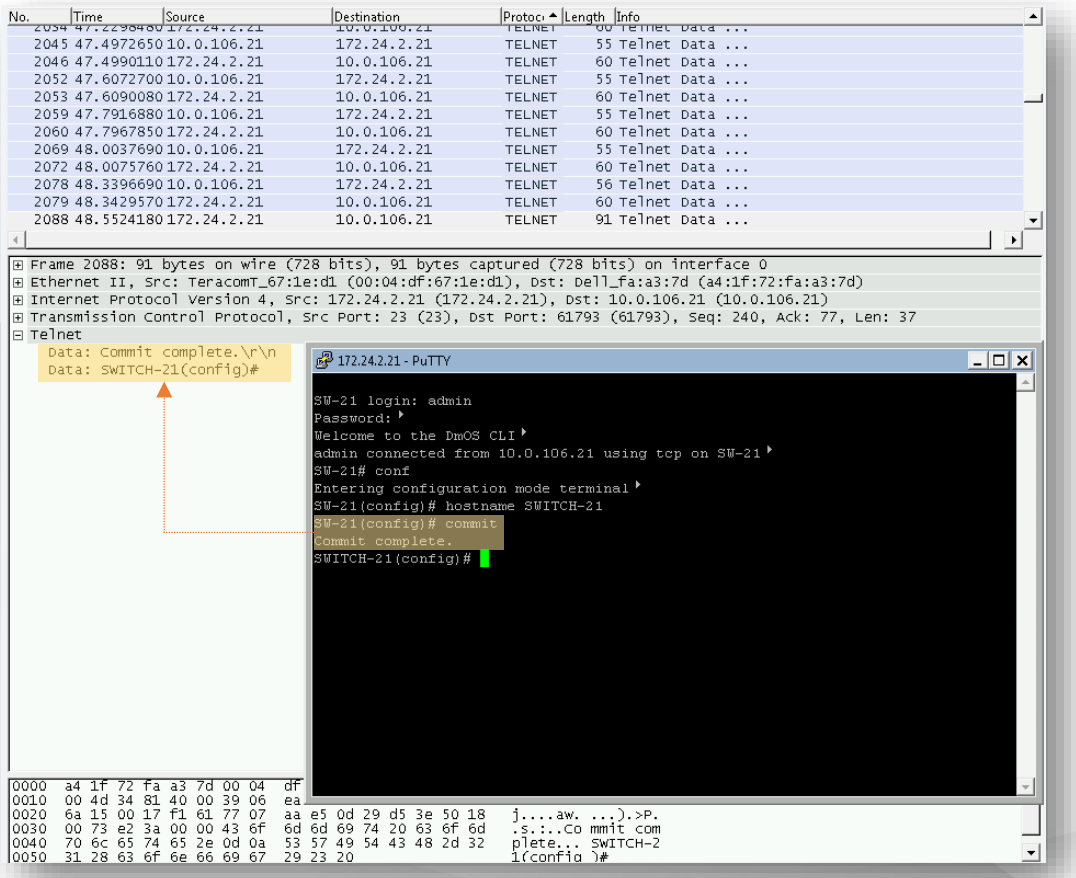
Atualização de Firmware

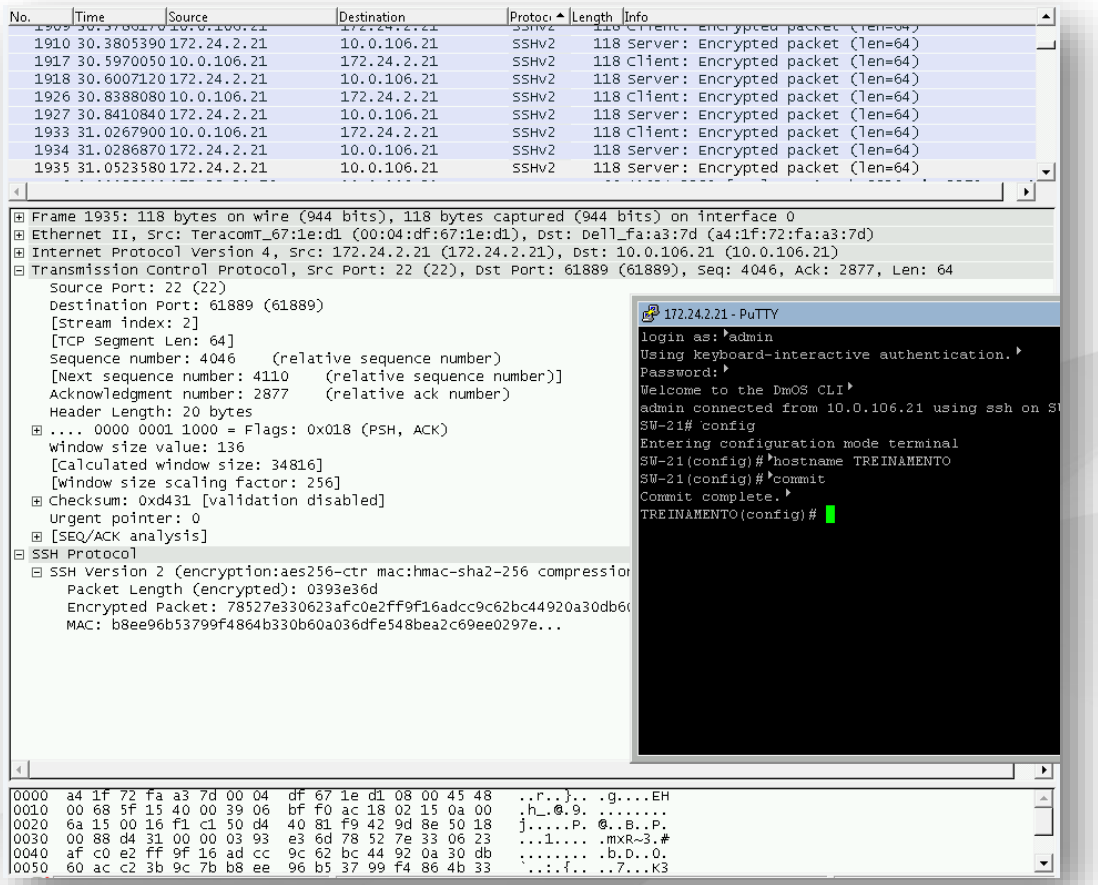
- Release notes - Novas funcionalidades, melhorias, correções, vulnerabilidades, problemas identificados, interoperabilidades e itens importantes no olhar do fabricante
- Programe atualizações periódicas

```
SW-ACC-IIR_C42_101#show uptime
Systema uptime: 3914 d, 21 h, 10 min, 0 s
Estimated startup tim: Mon Oct 8 18:22:01 2012

SW-ACC-IIR_C42_101#show system

Product
-------
Model:                  DmSwitch3224F2
Systema capabilities:   Bridge
OID:                    1.3.6.1.4.1.3709.1.2.17
```



Telnet x SSH


No. Time Source Destination Protoc Length Info
2045 47.4972650 10.0.106.21 172.24.2.21 TELNET 55 Telnet Data ...
2046 47.4990110 172.24.2.21 10.0.106.21 TELNET 60 Telnet Data ...
2052 47.6072700 10.0.106.21 172.24.2.21 TELNET 55 Telnet Data ...
2053 47.6090080 172.24.2.21 10.0.106.21 TELNET 60 Telnet Data ...
2059 47.7916880 10.0.106.21 172.24.2.21 TELNET 55 Telnet Data ...
2060 47.7967850 172.24.2.21 10.0.106.21 TELNET 60 Telnet Data ...
2069 48.0037690 10.0.106.21 172.24.2.21 TELNET 55 Telnet Data ...
2072 48.0075760 172.24.2.21 10.0.106.21 TELNET 60 Telnet Data ...
2078 48.3396690 10.0.106.21 172.24.2.21 TELNET 56 Telnet Data ...
2079 48.3429570 172.24.2.21 10.0.106.21 TELNET 60 Telnet Data ...
2088 48.5524180 172.24.2.21 10.0.106.21 TELNET 91 Telnet Data ...
Frame 2088: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
Ethernet II, Src: TeracomT_67:1e:d1 (00:04:df:67:1e:d1), Dst: Dell_fa:a3:7d (a4:1f:72:fa:a3:7d)
Internet Protocol Version 4, Src: 172.24.2.21 (172.24.2.21), Dst: 10.0.106.21 (10.0.106.21)
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 61793 (61793), Seq: 240, Ack: 77, Len: 37
Telnet
Data: Commit complete.\r\n
Data: SWITCH-21(config)#
172.24.2.21 - PuTTY
SW-21 login: admin
Password:
Welcome to the DmOS CLI
admin connected from 10.0.106.21 using tcp on SW-21
SW-21# conf
Entering configuration mode terminal
SW-21(config)# hostname SWITCH-21
SW-21(config)# commit
Commit complete.
SWITCH-21(config)#
0000 a4 1f 72 fa a3 7d 00 04 df
0010 00 4d 34 81 40 00 39 06 ea
0020 6a 15 00 17 f1 61 77 07 aa e5 0d 29 d5 3e 50 18 j....aw. ...).>P.
0030 00 73 e2 3a 00 00 43 6f 6d 6d 69 74 20 63 6f 6d .s.:..Co mmit com
0040 70 6c 65 74 65 2e 0d 0a 53 57 49 54 43 48 2d 32 plete... SWITCH-2
0050 31 28 63 6f 6e 66 69 67 29 23 20 1(config)#


No. Time Source Destination Protoc Length Info
1910 30.3805390 172.24.2.21 10.0.106.21 SSHv2 118 Server: Encrypted packet (len=64)
1917 30.5970050 10.0.106.21 172.24.2.21 SSHv2 118 Client: Encrypted packet (len=64)
1918 30.6007120 172.24.2.21 10.0.106.21 SSHv2 118 Server: Encrypted packet (len=64)
1926 30.8388080 10.0.106.21 172.24.2.21 SSHv2 118 Client: Encrypted packet (len=64)
1927 30.8410840 172.24.2.21 10.0.106.21 SSHv2 118 Server: Encrypted packet (len=64)
1933 31.0267900 10.0.106.21 172.24.2.21 SSHv2 118 Client: Encrypted packet (len=64)
1934 31.0286870 172.24.2.21 10.0.106.21 SSHv2 118 Server: Encrypted packet (len=64)
1935 31.0523580 172.24.2.21 10.0.106.21 SSHv2 118 Server: Encrypted packet (len=64)
Frame 1935: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
Ethernet II, Src: TeracomT_67:1e:d1 (00:04:df:67:1e:d1), Dst: Dell_fa:a3:7d (a4:1f:72:fa:a3:7d)
Internet Protocol Version 4, Src: 172.24.2.21 (172.24.2.21), Dst: 10.0.106.21 (10.0.106.21)
Transmission Control Protocol, Src Port: 22 (22), Dst Port: 61889 (61889), Seq: 4046, Ack: 2877, Len: 64
Source Port: 22 (22)
Destination Port: 61889 (61889)
[Stream index: 2]
[TCP Segment Len: 64]
Sequence number: 4046 (relative sequence number)
[Next sequence number: 4110 (relative sequence number)]
Acknowledgment number: 2877 (relative ack number)
Header Length: 20 bytes
.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
Window size value: 136
[Calculated window size: 34816]
[Window size scaling factor: 256]
Checksum: 0xd431 [validation disabled]
Urgent pointer: 0
[SEQ/ACK analysis]
SSH Protocol
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compressior
Packet Length (encrypted): 0393e36d
Encrypted Packet: 78527e330623afc0e2ff9f16adcc9c62bc44920a30db6(
MAC: b8ee96b53799f4864b330b60a036dfe548bea2c69ee0297e...
172.24.2.21 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Welcome to the DmOS CLI
admin connected from 10.0.106.21 using ssh on S
SW-21# config
Entering configuration mode terminal
SW-21(config)# hostname TREINAMENTO
SW-21(config)# commit
Commit complete.
TREINAMENTO(config)#
0000 a4 1f 72 fa a3 7d 00 04 df 67 1e d1 08 00 45 48 ..r..}.. .g....EH
0010 00 68 5f 15 40 00 39 06 bf f0 ac 18 02 15 0a 00 .h_.@.9. ....
0020 6a 15 00 16 f1 c1 50 d4 40 81 f9 42 9d 8e 50 18 j.....P. @..B..P.
0030 00 88 d4 31 00 00 03 93 e3 6d 78 52 7e 33 06 23 ...1.... .mxR~3.#
0040 af c0 e2 ff 9f 16 ad cc 9c 62 bc 44 92 0a 30 db .... .b.D..0.
0050 60 ac c2 3b 9c 7b b8 ee 96 b5 37 99 f4 86 4b 33 `..;.{.. ..7...K3

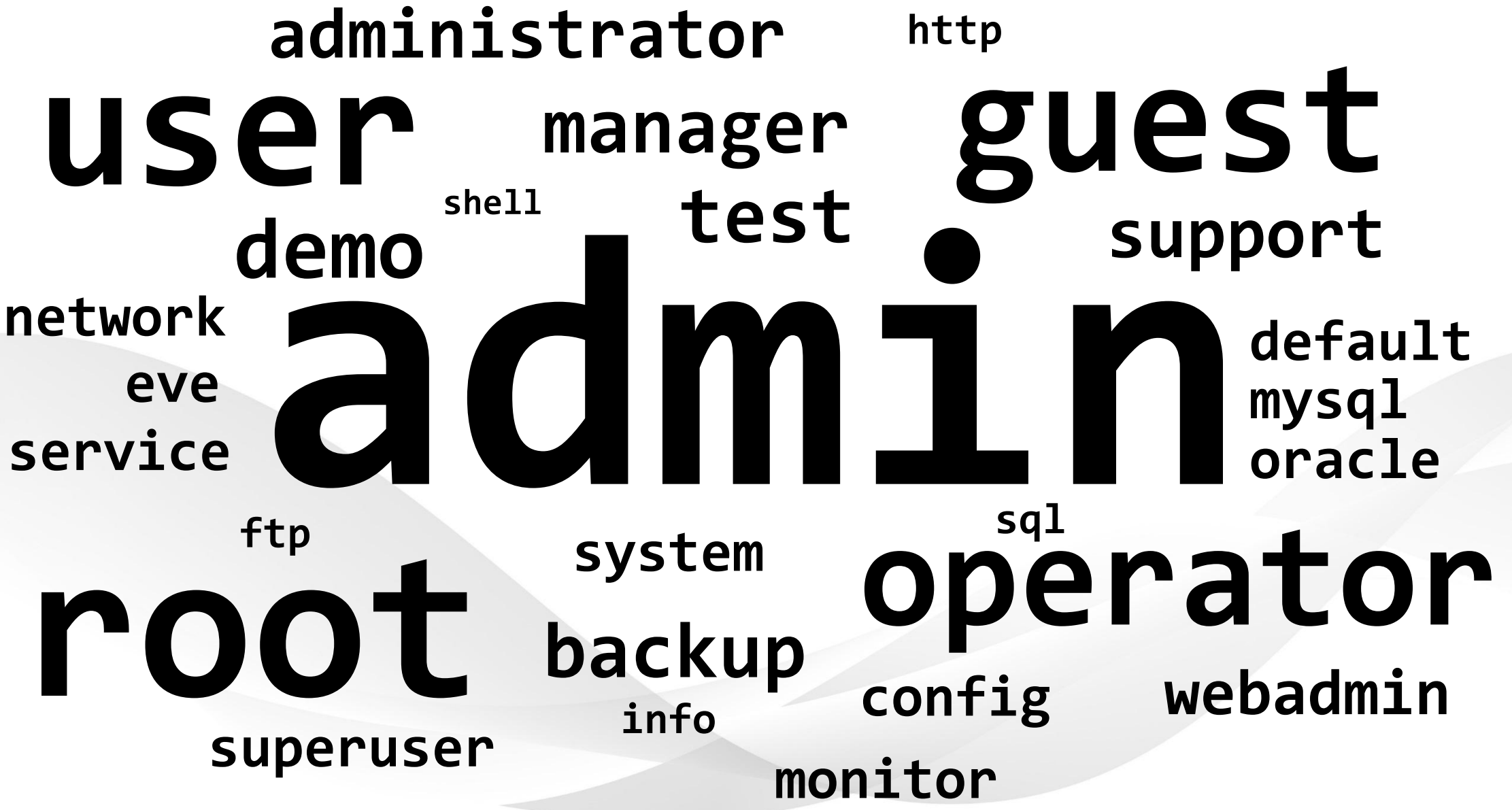
DATACOM

Credenciais de Acesso

- Alterar as credenciais originais antes de adicionar o equipamento a rede
- Usuários com acesso individual, exclusivo e de acordo com o seu perfil – privilégios mínimos
- Implementar servidores AAA como RADIUS e TACACS
- Utilizar senhas que atendam a requisitos como quantidade de caracteres, letras maiúsculas, minúsculas, números e caracteres especiais
- ATOS 77 e 2436 da Anatel

```
25/05/2020 16:46:24.875 : <Warn> %AAA-CONNECTION_FAILED : pam-
app[4279] : User [operator]: Connection from host 83.212.127.42
failed. Protocol ssh

25/05/2020 16:46:32.839 : <Warn> %AAA-CONNECTION_FAILED : pam-
app[4283] : User [user]: Connection from host 118.27.14.123 failed.
Protocol ssh

25/05/2020 16:47:39.219 : <Warn> %AAA-CONNECTION_FAILED : pam-
app[4304] : User [eve]: Connection from host 45.156.186.188 failed.
Protocol ssh

25/05/2020 16:48:48.511 : <Warn> %AAA-CONNECTION_FAILED : pam-
app[4972] : User [chocolat]: Connection from host 167.71.89.108
failed. Protocol ssh

25/05/2020 16:48:49.349 : <Warn> %AAA-CONNECTION_FAILED : pam-
app[4970] : User [openfiler]: Connection from host 103.92.24.240
failed. Protocol ssh
```

Em nenhuma circunstância um equipamento deve permanecer com as credenciais originais de fabrica!!


administrator
http
user
manager
guest
shell
test
demo
support
admin
network
default
eve
mysql
service
oracle
sql
ftp
system
operator
root
backup
config
webadmin
info
superuser
monitor

DATACOM

Gerência de Usuários via AAA

Authentication | Autenticação – Verifica e confirma a identidade do usuário

Quem é o usuário?

```
user = treinamento1 {
            pap = cleartext “suporte”
            login = cleartext “suporte”
            enable = cleartext “suporte”
            name = “Treinamento DATACOM”
            member = admin
```

Authorization | Autorização – Define os privilégios e restrições do usuário, ou seja, permite a execução ou não, de uma operação no equipamento

O que pode fazer?

```
group = admin {
        default service = permite
        service = exec {
            priv-levl = 15
        }
        cmd = config {
            permit .*
```

Accounting | Contabilização (Auditoria) – Coleta informações sobre o comportamento dos usuários e de que forma consomem os recursos da rede

O que, onde e quando fez?

```
Nov 11 17:19:53 172.24.2.70     tati    mgmt
172.31.208.93   stop    task_id=7901    timezone=UTC-3
service=shell   stop_time=947122509     cmd=CLI
'interface gigabit-ethernet-1/1/1' <cr>
```

DATACOM

Restrição de Acesso

- Definir quais redes/endereços IPs serão confiáveis e que acessarão os equipamentos
- Implementar listas de controle de acesso - SSH, SNMP, HTTP/HTTPS, SNTP/NTP, TFTP e outros
- Alterar portas padrão de serviço de acesso
- Bloquear de portas padrões e/ou não utilizadas
- Limitar quantidade de acessos simultâneos
- Permitir apenas protocolos configurados na sua estrutura
- Não utilize protocolo inseguros - Telnet e HTTP
- Serviços/protocolos/interfaces não utilizados devem ser desabilitados
- Restrição física de acesso aos equipamentos
- VLAN exclusiva para gerencia (L2) ou loopback (L3)
- Repensar a necessidade de IPs públicos em switches e OLTs

Banner Login

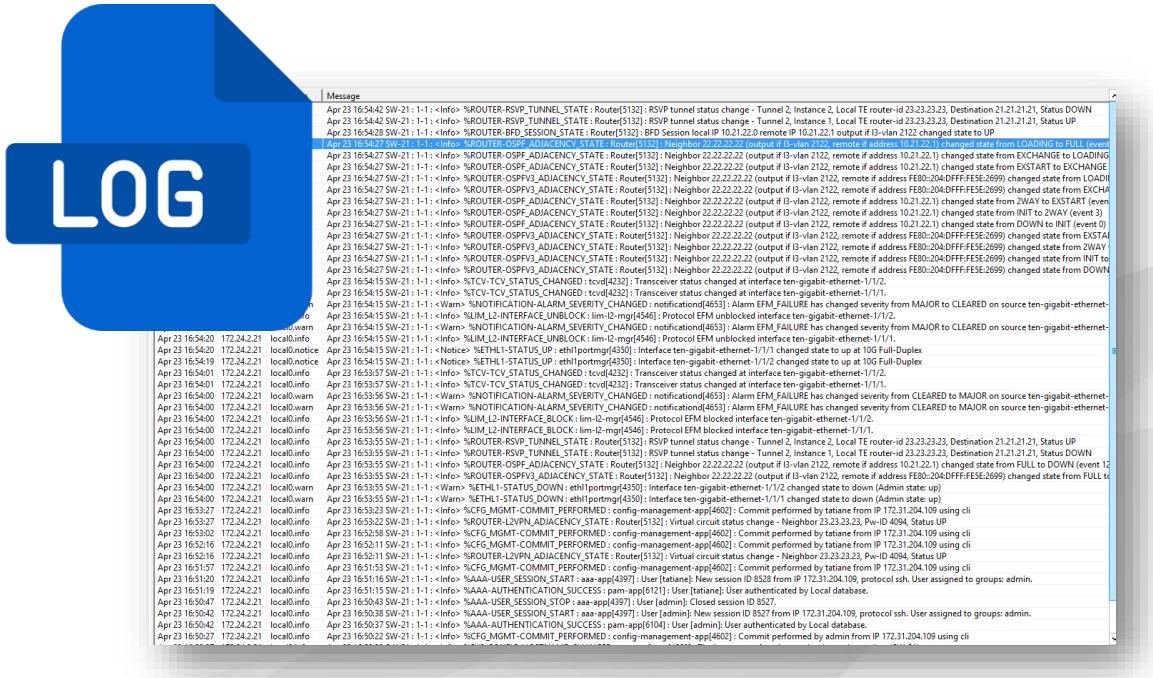
- Aviso de acesso restrito a usuários e de monitoramento do equipamento
- Auxiliar na identificação do dispositivo e localidade
- Reforço das políticas de segurança

```
*******************************************************
*                                                     *
*      ____    _  _____  _    ____ ___  __  __       *
*     |  _ \  / \|_   _|/ \  / ___/ _ \|  \/  |      *
*     | | | |/ _ \ | | / _ \| |  | | | | |\/| |      *
*     | |_| / ___ \| |/ ___ \ |__| |_| | |  | |      *
*     |____/_/   \_\_/_/   \_\____\___/|_|  |_|      *
*           https://www.datacom.com.br                *
*      Laboratorio Suporte - Eng. de Aplicacao        *
*******************************************************
sw03-rack03 login:
```

```
##############################################################################
##                                                                          ##
## Only authorized personnel are allowed to access this piece of equipament.##
##               Other are urged to log off IMMEDIATELY.                    ##
##                                                                          ##
##      Somente pessoal autorizado pode acessar este equipamento.           ##
##            Outros, por favor, desconectar IMEDIATAMENTE.                 ##
##                                                                          ##
##############################################################################
```

LOGs

- Mantenha a data e hora atualizados – NTP.BR
- Registre ações/comandos, tentativas de acesso
- Insira diferentes níveis de criticidade/severidade
- Tenha um servidor externo - Syslog
- Guarde os registros de forma segura – Processos judiciais e mandatos policiais

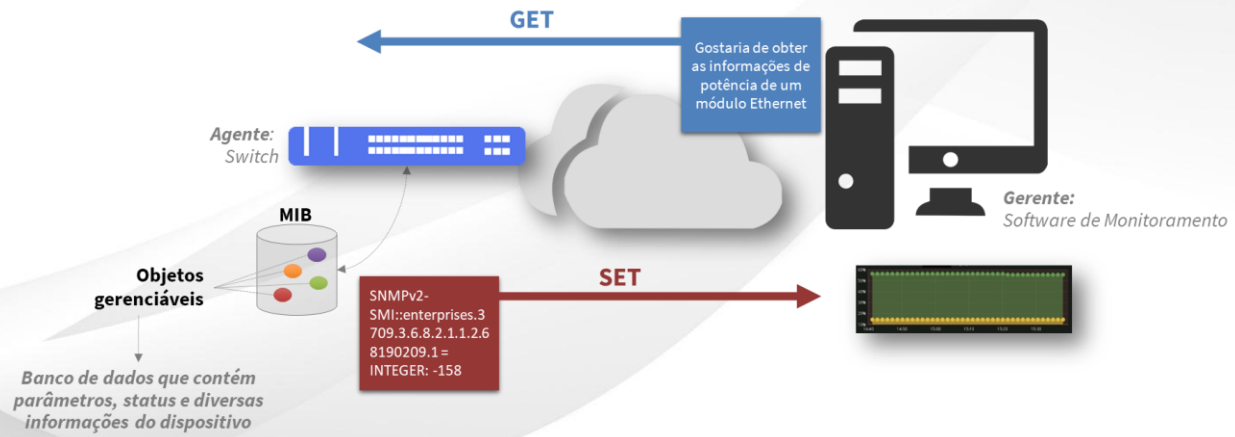


DATACOM

Monitoramento por SNMP

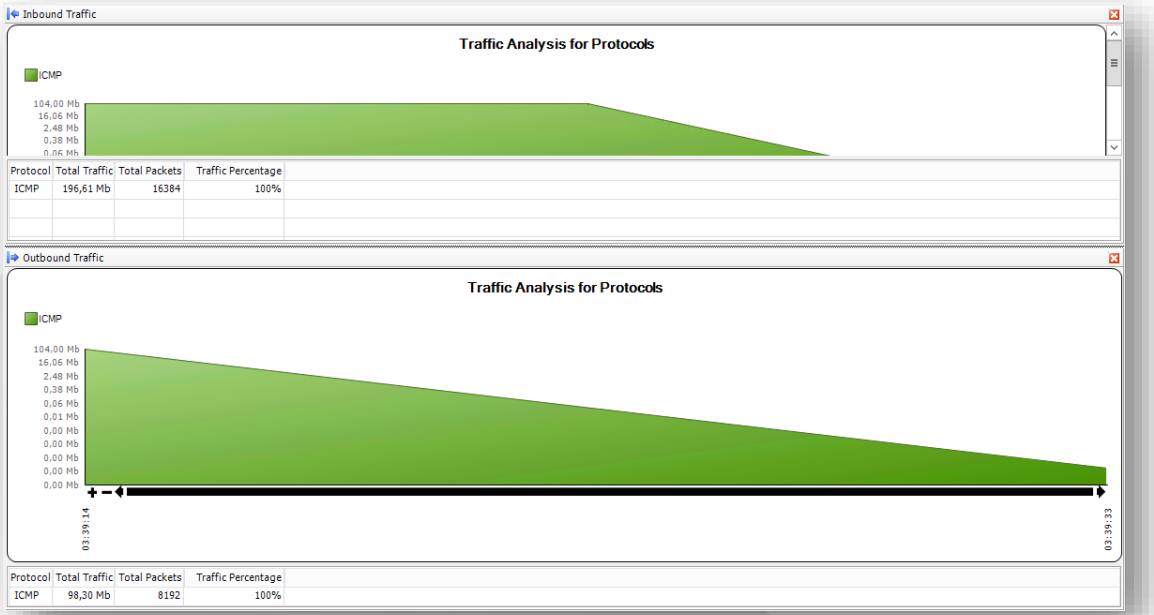
- Defina comunidades específicas
- Prefira o SNMPv3
- Retire a comunidade Public
- Especifique quais endereços IPs poderão realizar coletas
- Cuide com o intervalo de monitoramento para não sobrecarregar a CPU do seu equipamento

Versão	Descrição
SNMPv1	Versão original do SNMP, strings das comunidades enviadas em texto simples com segurança fraca
SNMPv2	A versão v2c é a versão mais usada e melhorou o tratamento do protocolo em relação a versão v1. A segurança ainda é um problema porque utiliza strings de comunidade em texto simples
SNMPv3	Versão mais recente do SNMP, suportando segurança e autenticação SHA e MD5 completas.

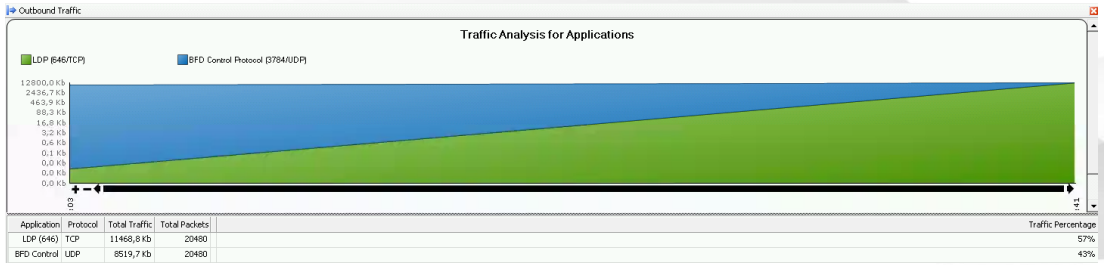


Monitoramento por sFlOW: Análise de Tráfego

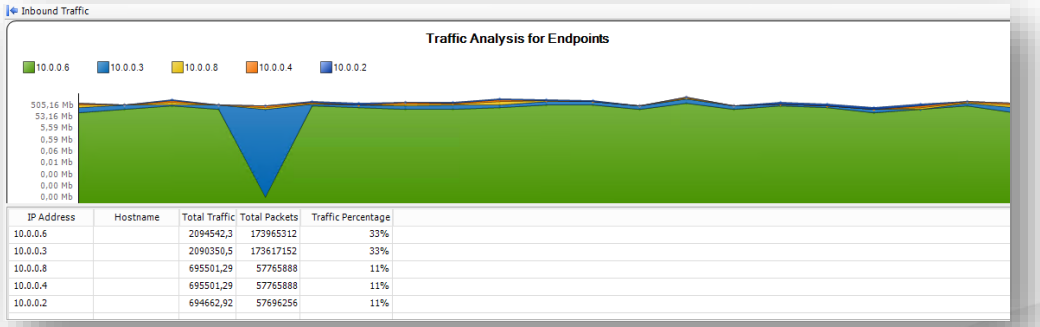
ICMP:



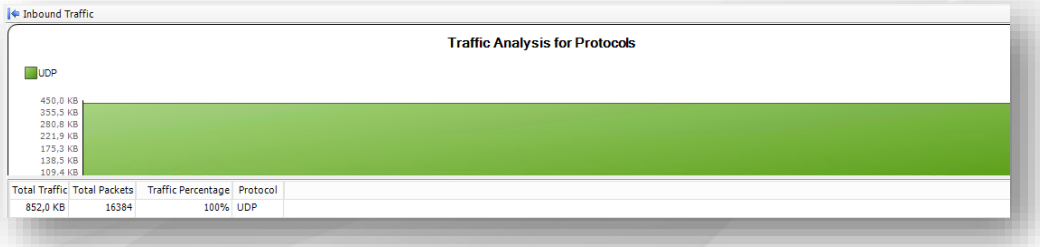
Protocolos:



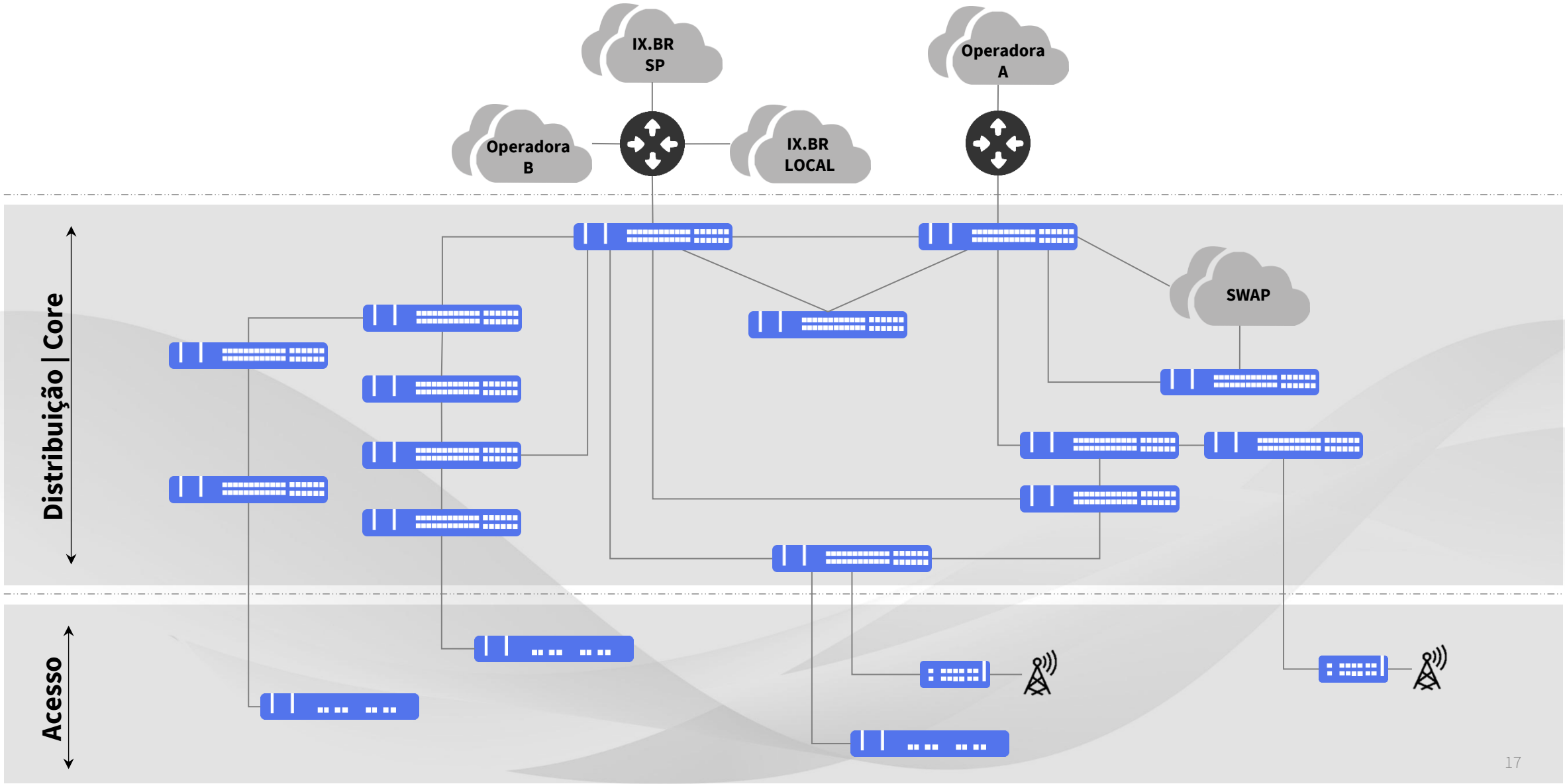
Tráfego de uma Interface:



Tráfego UDP:



Dicas por Camadas Hierárquicas


IX.BR
SP
Operadora
A
Operadora
B
IX.BR
LOCAL
SWAP
Distribuição | Core
Acesso

Acesso: Conexão para os Usuários Finais

L2 e GPON

- Segmentação do tráfego em VLANs e cuidado com a VLAN default!
- Controle de tempestade de pacotes – Storm Control
- Controle de banda – VLAN ou Interface
- Aplicações de QoS – Prioridades/Marcações
- Controle de MACs
- Controle e/ou troca de portas padrões
- OAM EFM – IEEE 802.3ah (mundo Ethernet)
- LLDP – use com moderação

GPON

- Gerência separada para as ONUs e com IP privado – RFC 1918 + ACL
- Controle de banda de upstream – Não deixar a OLT em bridge
- Option 82 – DHCP/IPoE

Distribuição | Core

Redes L2

- Protocolos de proteção de loop – xSTP, EAPS, ERPS para prover redundância
- Segmentação do tráfego em VLANs + QinQ + Tunelamento de protocolos de Camada 2
- Retirar a VLAN default (ID 1)
- Agregações e backups de links
- Balanceamento de tráfego
- OAM EFM e Link-Flap
- LLDP – use com moderação

Distribuição | Core

Redes MPLS

- Caminhos de redundância
- Agregações de links
- Roteamento dinâmico + Autenticação MD5
- BFD
- LDP e/ou RSVP-TE
- L2VPN + Autenticação MD5
- Segmentação por VPNs
- Balanceamento de tráfego - FAT
- Limitação do aprendizado de MAC
- OAM EFM e Link-Flap
- LLDP – use com moderação

DATACOM

Backup

- Criar uma rotina de backup das configurações de todos os equipamentos
- Armazene em um local “seguro”
- Execução manual, por script ou plataforma de NMS
- Mantenha o backup atualizado
- Teste o backup regularmente

DATACOM

Comece hoje ;)

1. Mantenha os equipamentos **atualizados** e com uma **rotina de backup**
2. **Má configuração** ou a realizada **sem conhecimento** podem gerar problemas – Pode parar uma rede!
3. **Utilize SSH** ao invés de Telnet e desabilite-o
4. Crie **usuários distintos** e com **privilégios mínimos** conforme a função. Sempre que possível, utilize **RADIUS** ou **TACACS**
5. **Altere o usuário default**!
6. **Desative** serviços/protocolos **não utilizados**
7. O **SNMPv3** tem o propósito de segurança, não esqueça de **retirar a comunidade "Public"**
8. Assegure que os equipamentos estão gerando **LOGs** que facilitem o monitoramento e a identificação de tentativas de ataque e acesso indevido
9. **Bloqueie portas** que são utilizadas para ataque
10. **Portas** ou **VLANs** destinadas para gerência **deverão** ser acessadas somente **internamente** ou por **endereços confiáveis**. **Evite o uso de IPs públicos**
11. Utilize **rate-limit** e **ACLs** nos equipamentos
12. **Controle** a tempestades de pacotes (**storm-control**)
13. Adote **IPv6**

Tatiane de Figueiredo

tatiane.figueiredo@datacom.com.br

@tati.fig.telecom

@datacomteracom

DATACOM

www.datacom.com.br

DATACOM EAD

https://ead.datacom.com.br