

Eldorado do Sul, junho de 2016

A DATACOM comunica o lançamento da versão 14.10 de *firmware* para a linha de produtos DM4000 e DM4100. Alterações em relação à versão de *firmware* 14.8.

Procedimento de Atualização

- A atualização de *firmware em equipamentos chassis ou stacking*, deve ser realizado em todas as placas simultaneamente, respeitando as versões suportadas, evitando inconsistências indesejadas.
- Para atualizações de *firmware* de versões 12.x (ou inferiores) para 14.x, é necessário realizar o procedimento em duas etapas, ou seja, deve-se primeiramente realizar o *upgrade* para a versão 13.8.6 (versão intermediária recomendada) e depois para a versão final 14.x.

Etapas 1: atualização de *firmware* da versão 12.x para a 13.8.6 com posterior *reboot*.

Etapas 2: atualização de *firmware* da versão 13.8.6 para a 14.x com posterior *reboot*.

- As interfaces de acesso MPLS não devem ser configuradas com a funcionalidade QinQ external - mode. A exceção é o caso que combina acesso *untagged* com parâmetro *vc-type* vlan na VPN. Verificar as configurações ao fazer upgrade de versões anteriores à 14.2, pois pode ocorrer interrupções de tráfego.
- Os *meters* com modo *srTcm* e *trTcm* devem ser reconfigurados e associados aos respectivos filtros ao término da atualização de *firmware* com versões 12.x e 13.x para versões 14.x.

Em caso de dúvidas sobre o procedimento acima, consultar o Suporte Técnico DATACOM.

- Versões anteriores a 14.2 não possuem suporte a VPN TE (*mplstype te*). No caso de downgrade de *firmware* a config da vpn, apesar de sinalizar como VPN TE, funcionará como non-te, necessitando ajuste via reconfiguração do neighbor.
- Configurações de autenticação OSPFv3 não são mais compatíveis com versões anteriores a 13.0. Durante procedimento de upgrade/downgrade, a configuração de autenticação deve ser removida antes do procedimento e refeita após o novo FW estar ativo.
- Antes de realizar o downgrade do FW14.10, é necessário garantir que não existem IDs de túneis RSVP maiores do que 100 (cem) e que o número de portas de acesso em uma VPN VPLS seja limitado em 8 portas.

Novas Funcionalidades e Melhorias

- Modo unicast negociado para IEEE 1588v2 (PTP - Precision Time Protocol).
- Com o objetivo de facilitar o troubleshooting, novos logs para as VPNs MPLS foram disponibilizados: *mpls rsvp logging path-status*: quando há mudança de estado de túneis RSVP; *mpls l2vpn logging pw-status*: quando há mudança de estado de PWs; *mpls l2vpn logging redundancy*: quando há comutação de PWs para uma determinada VPN.
- Permitir dar nomes aos tunnels/path RSVP, e não somente id. Para os IDs, permitir números maiores do que 100.
- Permitir adicionar e remover interfaces a um port-channel que está sendo usado como acesso de L2VPNs, sem a necessidade de desabilitar a VPN. Esta ação provoca uma pequena indisponibilidade de tráfego, devido a uma transição de estados da VPN (down/up), sendo registrada em log apenas a mudança para o estado up.
- Permitir adicionar até 16 portas de acesso em uma VPN VPLS. Antes do FW14.10, o limite máximo era de 8 portas.

- Novo comando: *clear mpls ldp*, reinicializa as sessões LDP de todo o equipamento. Deve ser utilizado em horários de baixo tráfego, preferencialmente em janelas de manutenção, pois causa uma pequena indisponibilidade de tráfego nas VPNs, devido ao aprendizado de novos labels LDP. Após utilizar este comando, deve ser verificado se todas as VPNs voltaram a operar normalmente. Caso contrário, executar *disable* e *enable* na VPN que não se tornou operacional.
- Comando *cpu protocol priority hardware* faz com que os pacotes tunelados através da funcionalidade *l2protocol-tunnel* (L2TP), tenham a marcação do QoS (802.1p) igual a configuração da interface *switchport priority default x*. Também possibilita uma marcação das BPDUs tuneladas através de filtros (tendo prioridade em relação a marcação da interface).
- A Funcionalidade *cpu protocol priority tunnel <packet priority>* faz com que a marcação de todos os pacotes de controle tunelados pela funcionalidade *l2protocol-tunnel*(L2TP), utilize o valor configurado global, *packet priority*. Esta configuração fica sem efeito caso a funcionalidade *cpu protocol priority hardware* esteja sendo utilizada.
- A funcionalidade VRF-Lite foi habilitada para os modelos DM4100+L3.
- Possibilidade de configuração da feature *sflow* em interfaces *port-channel*.
- Incluído OID 28 na MIB DATACOM, *Dmswitch.mib* (.1.3.6.1.4.1.3709.3.5.201.1.28), permitindo consultar informações de Digital Diagnostic dos transceivers suportados.
- Filtros com mesmos parâmetros de *match* e prioridades diferentes, não poderiam ser criados.
- Correção do problema causado pela configuração *no ip igmp snooping flood-unknown*, que modificava o modo de operação padrão das VLANs, fazendo com que alguns pacotes multicast fossem descartados, prejudicando o funcionamento do protocolo OSPF.
- Correção da funcionalidade Adaptive Clock Recovery-ACR, em placas DM4000-PWE3 H Series. Recupera o clock através dos bundles, utilizando a configuração de interface *G704/E1C* com *sync-source adaptive bundle*.
- Mensagens de log originadas por endereço de origem broadcast eram mostradas sem a indicação do MAC de origem.
- Correção do bloqueio lógico (por exemplo OAM) em *port-channel*, quando interfaces que estavam originalmente bloqueada eram adicionadas a um *port-channel*.
- Correção no comando *show interfaces table utilization bandwidth* que apresentava lentidão na sua exibição.
- Correção do help do comando de *filter egress*, no cli.
- Correção do help do comando *show interfaces status sdh*, no cli.

Correções

- *Meters* não eram aplicados e acabavam sendo removidos da configuração após *reboot* de *unit*.

Compatibilidade e Restrições

- O uso da configuração *no ipv6 mld snooping flood-unknown* causa a queda das sessões OSPFv3.
- Esta versão de *firmware* suporta equipamentos das linhas DM4000 e DM4100. A matriz de compatibilidade entre MPU e placas de unidades para DM4000 em chassis está disponível no Anexo 1.
- A versão mínima de *Dmview* recomendada

para uso da funcionalidade CESoP é a 8.2.

- Recomenda-se que os equipamentos DM4100, operando em modo stacking, possuam a mesma licença de software instalada. As licenças de software disponíveis atualmente são: Bridge (L2), Router (L3) e MPLS.
- Não é recomendada a utilização da VLAN 1 (default) do equipamento em aplicações L2 e L3.
- Downgrade de firmware com a configuração de vc-type distintos na mesma interface física não é suportado.
- MPLS não é suportado em stacking pizza box.
- Uso de MPLS com memória externa habilitada para rotas L3 exige a configuração do comando *memory external-resource vlan*.
- Existem algumas restrições no uso de RSVP com MPLS (MPLS-TE). Consultar Suporte Técnico DATACOM.
- Não é garantida a comutação de túneis RSVP abaixo de 50ms na linha DM4100.
- Possibilidade de comportamento indesejado em VPNs, se existir a feature que suporta vc-type distintos na mesma interface ethernet ou com tuneis RSVP, após *switchover*.
- Local Tunnel e RFC3107 não são suportados para a família DM4100.
- Local Tunnel não é suportado pelo módulo DM4000 PWE3 H Series 32E1.
- Mais de uma sessão de RFC3107 (BGP address-family IPv4 com send-label) é suportada no mesmo PE somente quando os neighbors anunciam prefixos distintos em cada sessão.
- Manipulação de custo de métrica e metric type em rotas redistribuídas da RFC3107 para OSPF não são suportadas.
- Selective QinQ não é suportado em portas de acesso da VPN para toda família DM4000.
- Pode ocorrer perda momentânea de tráfego

durante período de graceful-restart em cenários LDP.

- Evitar o uso de balance *src-dst-ip* ou *enhanced* em port-channel de loop externo, relacionado a MPLS L2VPN – QinQ.
- VRF-Lite não permite sobreposição de endereços IP.
- Melhorias realizadas na funcionalidade CPU-Protect podem exigir reconfiguração da funcionalidade após a atualização de *firmware* para a versão 14.2 ou superior. Consultar Suporte Técnico DATACOM.
- Não há suporte a proteção de múltiplas redes IPv6 utilizando VRRP.
- BGP IPv6 Peer-groups não é suportado.
- Removidos os parâmetros de bloqueio para *broadcast*, *multicast* e *arp request* da funcionalidade *block* do CPU-DoS-Protect. A partir da versão FW14.2, um controle mais seletivo e flexível foi incluído para realizar o bloqueio e ou a limitação de pacotes para a CPU, incluindo *broadcast*, *multicast*, *ARP* e outros protocolos, totalizando 48 filas de controle (comando: *cpu-dos-protect queue*).
- Default originate do OSPF, quando utilizando VLAN link-detect, não garante tempos de convergência adequados e pode causar indisponibilidade momentânea do tráfego, durante convergência em ambiente BGP full routing.
- O comando *auto-cost reference-bandwidth* não deve ser utilizado na configuração do OSPFv3.
- Deve-se evitar a configuração de RIP com IP de VLAN /31.
- Para interfaces 1GB e 10GB (multicast / broadcast / unicast), os valores default para storm-control foram mudados no FW14.6.2. Interfaces 1GB mudaram de 1000pps para 10000pps e as 10GB de 10000pps para

100000pps.

- Existem algumas restrições no uso de 8k hosts em equipamentos DM4100 L3 24P. Consultar Suporte Técnico DATACOM.
- MPU384, do código de produto 800.0442.10, passou a ter *firmware* mínimo 14.6.
- Após operações de troca de master em Stacking, o banco de dados do DHCP Snooping apresenta registros inconsistentes após liberações de IPs de alguns clientes (mensagens release).
- DHCP Snooping não pode ser usado simultaneamente com as funcionalidades DHCP Server e DHCP client.
- Incompatibilidade de configuração da funcionalidade LDP-IGP Sync em interfaces que possuem apenas endereço IPv6.
- A utilização de ECMP em conjunto com BFD ou BGP pode causar a queda destes protocolos, ao cair o caminho principal. Ocorre se o intervalo de detecção de erro para uma sessão BFD, habilitada no neighbor BGP, for menor que 7 segundos, ou se o holdtime do BGP, for menor que 21 segundos para uma

sessão sem BFD.

- Para mudança do estado *shutdown* para *no shutdown* em *port-channel* com LACP, é necessário também realizar as configurações nas interfaces que formam o port-channel.
- Em switch DM4100 - ETH44GT+4GC+2XX+S é recomendado o uso de no máximo 7 instâncias xSTP.
- Devido à introdução de novos modos de *meters* que permitem a associação de *meters* hierárquicos aos filtros, há quebra de compatibilidade de *Meters* com modo *srTcm* e *trTcm* entre *firmwares* com versões 12.x e 13.x para versões 14.x, sendo estes removidos da configuração durante o *upgrade* de *firmware*. É necessário reconfigurá-los e reassociá-los aos filtros ao término da atualização.
- Para VRRPv3 não é reportado a ocorrência de IPv6 duplicado.
- A funcionalidade *ipfix* não está liberada para equipamentos DM4100-24p.
- Não é possível realizar ping para endereços broadcast.

Contate o Suporte DATACOM enviando um e-mail para suporte@datacom.ind.br ou pelo telefone +55 51 3933 3122 e obtenha informações adicionais sobre funcionalidades suportadas, procedimentos de atualização e compatibilidade entre versões de firmware, módulos e acessórios DATACOM.

Anexo 1: Matriz de Compatibilidade para DM4000 em Chassis

A seguinte tabela mostra a compatibilidade entre MPU e placas de unidade para DM4000 em chassis, na versão 14.10.

PLACAS	MPU384	MPU512
ETH24GX H Series	✓	✓
ETH24GX E Series	✓	✓
ETH24GX L Series ^(*)	--	--
ETH24GT H Series	✓	✓
ETH48GX H Series	✓	✓
ETH48GT H Series	✓	✓
ETH24GX+2x10GX H Series	✓	✓
ETH24GX+2x10GX E Series	✓	✓
ETH2x10GX H Series	✓	✓
ETH4x10GX H Series	✓	✓
ETH4x10GX E Series	✓	✓
PWE3 ETH20GX+32E1 H Series	✓	✓
PWE3 ETH20GX+2x10GX+32E1 H Series	✓	✓
PWE3 ETH16GX+4STM1 H Series	✓	✓
PWE3 ETH16GX+2x10GX+4STM1 H Series	✓	✓

^(*) - Equipamento L Series é compatível apenas em operação standalone através do uso de chassis DM4001 ou DM4001 L.