WHITEPAPER

LACP E LINK AGGREGATION: COMO FUNCIONAM, REDUNDÂNCIA, BALANCEAMENTO E ETHERCHANNEL

Entenda como LACP e Link Aggregation formam port-channels, distribuem tráfego, aumentam capacidade e redundância e devem ser projetados e testados.

A3A® Engenharia de Sistemas

SUMÁRIO

LACP é o protocolo usado para negociar e manter a agregação de múltiplos enlaces Ethernet em uma única interface lógica. Essa agregação é conhecida como **Link Aggregation Group (LAG)**, port-channel, bonding ou, no ecossistema Cisco, EtherChannel.

A técnica permite utilizar vários cabos ou portas como um único enlace lógico, aumentando a capacidade agregada e mantendo a comunicação quando um dos membros falha. Entretanto, LACP não soma a velocidade para cada fluxo individual, não substitui uma arquitetura redundante entre equipamentos e não corrige caminhos físicos que compartilham o mesmo ponto de falha.

Este artigo explica como LACP e Link Aggregation funcionam, as diferenças entre agregação estática e dinâmica, os modos active e passive, a distribuição de tráfego, a interação com Spanning Tree, os requisitos de projeto e os testes necessários para validar uma implementação.

1. O QUE É LINK AGGREGATION?

Link Aggregation é a combinação de duas ou mais interfaces Ethernet físicas em uma interface lógica. Para os protocolos superiores, o grupo é apresentado como um único enlace, com um endereço lógico, uma configuração comum e capacidade agregada formada pelos membros ativos.

O grupo pode conectar dois switches, um switch e um servidor, um switch e um appliance, ou outros equipamentos compatíveis. Os enlaces físicos que compõem o grupo são chamados de membros. A interface lógica pode ser chamada de LAG, port-channel, bond, team ou trunk, dependendo do fabricante e do sistema operacional.

A padronização atual está na família IEEE 802.1AX. A expressão IEEE 802.3ad ainda aparece em documentação e interfaces legadas porque a agregação de enlaces foi originalmente tratada naquele contexto antes de migrar para o padrão específico de Link Aggregation.

1.1. O QUE É LACP?

LACP significa **Link Aggregation Control Protocol**. O protocolo permite que os equipamentos nas duas extremidades troquem informações sobre as interfaces candidatas, identifiquem incompatibilidades e selecionem os membros que podem participar do grupo.

Sem LACP, a agregação pode ser configurada de forma estática. Nesse caso, o equipamento pressupõe que as portas remotas estão configuradas corretamente. Uma

ligação incorreta pode produzir loop, perda de tráfego ou comportamento assimétrico. Com LACP, existe negociação e estado operacional para cada membro, reduzindo o risco de incluir uma interface que não pertence ao mesmo grupo lógico.

1.2. LAG, LACP, ETHERCHANNEL E PORT-CHANNEL

Esses termos são relacionados, mas não idênticos:

Um EtherChannel pode utilizar LACP ou, em plataformas legadas, mecanismos proprietários. Um LAG também pode ser configurado estaticamente, sem protocolo de negociação.

2. POR QUE AGREGAR ENLACES?

A agregação é adotada principalmente por capacidade, disponibilidade e simplificação lógica. Em vez de configurar protocolos e políticas em cada porta física, o projeto trata o port-channel como a interface principal.

2.1. CAPACIDADE AGREGADA

Dois enlaces de 10 Gbit/s podem formar um grupo com capacidade agregada de até 20 Gbit/s entre múltiplos fluxos. Isso não significa que uma única sessão TCP passará automaticamente a 20 Gbit/s. Normalmente, cada fluxo é associado a um membro por um algoritmo de distribuição, permanecendo limitado à capacidade daquele enlace físico.

O ganho real depende da quantidade de fluxos, da diversidade dos endereços e portas utilizados no cálculo de hash e do equilíbrio entre as conversações. Poucos fluxos de grande volume podem concentrar-se no mesmo membro, enquanto milhares de fluxos tendem a produzir distribuição mais uniforme.

2.2. TOLERÂNCIA À FALHA DE PORTA OU CABO

Quando um membro deixa de operar, o grupo pode permanecer ativo com capacidade reduzida. Os fluxos são redistribuídos entre os membros restantes. A continuidade depende do tempo de detecção, da aplicação, do equipamento e da existência de capacidade suficiente após a falha.

A agregação protege contra a perda de uma interface ou enlace membro. Ela não protege, por si só, contra falha do switch, perda de energia, rompimento de uma rota comum, erro de configuração do port-channel ou indisponibilidade do equipamento remoto.

2.3. SIMPLIFICAÇÃO DA TOPOLOGIA LÓGICA

Para Spanning Tree, roteamento, VLANs e políticas, o grupo é normalmente tratado como uma única interface lógica. Isso evita que enlaces paralelos independentes sejam bloqueados pelo Spanning Tree e permite utilizar a capacidade de vários membros simultaneamente.

A simplificação lógica exige consistência. VLANs, modo trunk ou access, MTU, parâmetros Layer 3 e demais atributos precisam ser aplicados de forma compatível ao port-channel e aos membros.

3. AGREGAÇÃO ESTÁTICA VERSUS LACP

Na agregação estática, as interfaces são forçadas a participar do grupo. Não existe negociação padronizada para verificar se a extremidade remota reconhece os mesmos membros. Essa modalidade pode ser adequada em cenários muito controlados, mas aumenta o risco operacional durante implantação, manutenção e mudanças.

Com LACP, cada extremidade anuncia informações do sistema, porta, chave de agregação, prioridade e estado. Apenas interfaces compatíveis são selecionadas para encaminhamento. Portas que recebem informações inconsistentes podem permanecer fora do grupo, evitando que um enlace inadequado seja tratado como membro válido.

3.1. QUANDO PREFERIR LACP

LACP é geralmente preferível quando os dois equipamentos oferecem suporte e interoperabilidade adequada. Ele facilita diagnóstico, monitora a relação entre as extremidades e torna falhas de configuração mais visíveis.

A agregação estática pode existir por limitação de plataforma, interoperabilidade específica ou requisito legado. Nesses casos, os testes de implantação e mudança precisam ser ainda mais rigorosos.

4. MODOS ACTIVE E PASSIVE

Uma interface LACP em modo **active** inicia a transmissão de mensagens do protocolo e tenta formar o grupo. Em modo **passive**, responde quando recebe mensagens LACP, mas não inicia a negociação por conta própria.

As combinações usuais são:

O modo active em ambas as extremidades facilita a detecção e reduz dependências de configuração. A escolha deve seguir o padrão operacional da organização e as recomendações dos equipamentos utilizados.

5. COMO O LACP IDENTIFICA UM GRUPO

Cada participante possui um identificador de sistema, normalmente composto por prioridade e endereço do sistema. As portas também possuem identificadores, prioridades, chaves e estados. Essas informações permitem que as duas extremidades determinem quais interfaces pertencem ao mesmo agregador.

5.1. ACTOR E PARTNER

Em uma mensagem LACP, o equipamento local é chamado de **actor** e a extremidade remota é chamada de **partner**. Cada lado anuncia sua própria visão do grupo e a visão aprendida do parceiro.

Quando os estados são consistentes, a interface pode entrar em coleta e distribuição. Quando existe divergência de chave, sistema, configuração ou conectividade, a porta pode permanecer individual, suspensa ou fora do encaminhamento, conforme a plataforma.

5.2. CHAVE DE AGREGAÇÃO

A chave identifica interfaces compatíveis para o mesmo grupo. Em implementações comerciais, essa compatibilidade está relacionada a atributos como velocidade, duplex, modo de operação e associação ao port-channel.

Portas conectadas a equipamentos remotos diferentes não devem formar um grupo convencional, exceto quando a extremidade remota opera como um único sistema lógico por empilhamento, MLAG, vPC ou tecnologia equivalente.

5.3. PRIORIDADE DO SISTEMA E DA PORTA

A prioridade do sistema ajuda a selecionar qual identificador prevalece em cenários de decisão. A prioridade da porta pode influenciar quais interfaces permanecem ativas quando existem mais membros candidatos do que o número suportado pelo grupo.

Esses parâmetros raramente precisam ser alterados em redes simples, mas tornam-se relevantes em projetos com links sobressalentes, limites de membros e requisitos determinísticos.

6. ESTADOS DE UM MEMBRO LACP

Uma interface candidata pode passar por diferentes estados até encaminhar tráfego. A nomenclatura exibida varia por fabricante, mas os conceitos centrais incluem:

Uma porta fisicamente ativa não está necessariamente apta a encaminhar tráfego no LAG. O diagnóstico precisa verificar o estado lógico, o parceiro identificado, a chave, a sincronização e as flags de collecting e distributing.

7. REQUISITOS DE CONSISTÊNCIA DOS MEMBROS

As interfaces de um grupo precisam apresentar características compatíveis. Dependendo da plataforma, inconsistências podem impedir a formação do grupo, suspender o membro ou gerar comportamento inadequado.

Devem ser verificados:

A configuração deve ser aplicada preferencialmente na interface lógica, seguindo o modelo da plataforma, para reduzir divergências entre os membros.

8. PORT-CHANNEL LAYER 2 E LAYER 3

Um port-channel Layer 2 transporta VLANs como interface access ou trunk. Ele participa do domínio de comutação e interage com Spanning Tree. É comum em uplinks entre switches, conexões de servidores e agregação de switches de acesso.

Um port-channel Layer 3 opera como interface roteada. O endereço IP e os protocolos de roteamento são associados à interface lógica. Esse modelo reduz o domínio Layer 2 e pode ser utilizado entre distribuição, core, data center e outros módulos roteados.

A decisão entre Layer 2 e Layer 3 deve fazer parte da arquitetura de rede, considerando mobilidade, convergência, segmentação, operação e alcance das falhas.

Link Aggregation deve ser dimensionado como parte da arquitetura, não apenas configurado no switch.

A A3A Engenharia define capacidade, redundância, rotas físicas, interfaces, transceptores, protocolos, monitoramento e critérios de validação em projetos corporativos e industriais.

Conhecer o serviço de Projeto de Telecomunicações

9. COMO O TRÁFEGO É DISTRIBUÍDO ENTRE OS MEMBROS?

O balanceamento de um LAG normalmente é baseado em hash. O equipamento calcula um valor a partir de campos do quadro ou pacote e associa o fluxo a um dos membros ativos. Essa decisão preserva a ordem dos pacotes de uma mesma conversação, evitando que quadros do mesmo fluxo cheguem por caminhos com atrasos diferentes.

9.1. CAMPOS USADOS NO HASH

As plataformas podem utilizar combinações de:

Um hash baseado apenas em MAC pode produzir distribuição ruim quando muitas conversações utilizam o mesmo roteador ou servidor. A inclusão de IP e portas tende a aumentar a diversidade, mas precisa ser compatível com a plataforma, o tipo de tráfego e a necessidade de manter simetria.

9.2. POR QUE UM ÚNICO FLUXO NÃO UTILIZA TODOS OS ENLACES?

Distribuir pacotes individuais do mesmo fluxo por membros diferentes pode causar reordenação. Como consequência, uma única sessão normalmente é mantida em um membro. Um LAG de quatro portas de 10 Gbit/s pode oferecer 40 Gbit/s agregados para vários fluxos, mas uma sessão isolada continuará limitada, em condições normais, a 10 Gbit/s.

Aplicações com múltiplas sessões paralelas podem aproveitar mais membros. Testes com um único fluxo não comprovam a capacidade agregada do grupo; para isso, devem ser usados fluxos simultâneos com combinações distintas de endereços e portas.

9.3. DISTRIBUIÇÃO DESIGUAL NÃO SIGNIFICA NECESSARIAMENTE FALHA

O hash não mede continuamente a ocupação de cada membro como um balanceador de carga de aplicações. Dois fluxos muito grandes podem cair na mesma interface enquanto outros membros transportam pouco tráfego. A análise deve considerar quantidade e perfil das conversações, não apenas a soma dos contadores.

10. TEMPORIZADORES E DETECÇÃO DE FALHAS

O LACP pode operar com periodicidade lenta ou rápida para transmissão das mensagens de controle. A terminologia e os comandos variam, mas é comum encontrar intervalos associados a aproximadamente 30 segundos no modo lento e 1 segundo no modo rápido.

O timer rápido melhora a detecção de perda do parceiro, mas gera mais mensagens e não substitui mecanismos de detecção física. Uma falha elétrica ou perda de sinal pode ser detectada imediatamente pela interface, enquanto falhas unidirecionais, caminhos intermediários ou problemas do equipamento remoto podem depender de LACP, UDLD, BFD ou outros mecanismos.

10.1. TIMEOUT E ESTADO DEFAULTED

Quando as mensagens esperadas deixam de chegar, a informação do parceiro expira. A porta pode sair do estado sincronizado, deixar de coletar e distribuir tráfego e assumir valores padrão. O tempo exato depende da periodicidade negociada e da implementação.

10.2. MIN-LINKS

Algumas plataformas permitem definir uma quantidade mínima de membros ativos para manter o port-channel operacional. O recurso evita que um grupo planejado para determinada capacidade permaneça ativo com banda insuficiente.

Por exemplo, um grupo de quatro interfaces pode ser configurado para ficar indisponível quando restar somente um membro. Essa decisão deve considerar o impacto de derrubar toda a interface lógica versus continuar com desempenho degradado. Em ambientes críticos, o comportamento precisa ser alinhado ao failover de rotas, aplicações e serviços.

11. LACP E SPANNING TREE

Em um port-channel Layer 2, o Spanning Tree normalmente enxerga o grupo como uma única porta lógica. Isso permite que todos os membros selecionados encaminhem tráfego sem que cada enlace paralelo seja tratado como caminho independente e bloqueado.

O Spanning Tree continua necessário quando existem outros caminhos Layer 2. A prioridade, o custo, o papel da interface e as proteções são aplicados ao port-channel. Uma inconsistência entre membros pode fazer com que interfaces sejam suspensas ou tratadas fora do grupo, alterando a topologia esperada.

11.1. LOOP CAUSADO POR AGREGAÇÃO INCORRETA

Se uma extremidade agrupa duas portas e a outra as trata como enlaces separados, pode ocorrer loop ou encaminhamento assimétrico. O LACP reduz esse risco porque exige concordância lógica antes de selecionar os membros, mas não elimina erros de cabeamento, configuração ou interoperabilidade.

12. LACP NÃO É REDUNDÂNCIA ENTRE SWITCHES POR SI SÓ

Um LAG convencional conecta duas extremidades lógicas. Se todos os membros terminam no mesmo switch físico, a falha desse equipamento derruba o grupo completo. Para distribuir os enlaces por dois switches, os equipamentos remotos precisam operar como uma única extremidade lógica para o LACP.

12.1. STACK E CHASSI VIRTUAL

Em empilhamento ou chassi virtual, vários equipamentos podem compartilhar plano de controle e identificador lógico. Um port-channel pode então possuir membros em unidades diferentes, aumentando tolerância à falha de porta, cabo e, dependendo da tecnologia, de uma unidade do conjunto.

12.2. MLAG, VPC E TECNOLOGIAS EQUIVALENTES

Multi-Chassis Link Aggregation permite que dois equipamentos independentes apresentem uma única identidade lógica ao dispositivo conectado. Fabricantes utilizam denominações e arquiteturas diferentes, como MLAG, vPC ou MC-LAG.

Essas soluções exigem sincronização de estado, peer-link, keepalive, regras de consistência e tratamento de cenários de split-brain. Não devem ser consideradas equivalentes a um LAG simples. O projeto precisa avaliar comportamento durante falhas do peer-link, perda de keepalive, reinicialização e inconsistência de configuração.

12.3. INDEPENDÊNCIA FÍSICA

Mesmo com dois switches, os enlaces podem compartilhar eletrocalha, DIO, cabo tronco, sala, alimentação ou UPS. Redundância lógica precisa ser acompanhada por diversidade física compatível com a criticidade do sistema.

A A3A projeta redes Cisco com redundância coerente entre switching, fibra, energia, segmentação e operação.

O escopo pode abranger arquitetura, seleção de plataformas, LACP, EtherChannel, empilhamento, ISE, hardening, monitoramento, migração e documentação.

Conhecer a solução de Redes Cisco

13. LACP EM SERVIDORES, VIRTUALIZAÇÃO E APPLIANCES

Servidores podem utilizar bonding ou NIC teaming para agregar interfaces. No modo compatível com IEEE 802.1AX, o switch também precisa configurar o grupo correspondente. Velocidade, duplex, VLANs, MTU, hash e políticas devem ser coerentes entre sistema operacional, hipervisor e rede.

13.1. LINUX BONDING EM MODO 802.3AD

No Linux, o modo 802.3ad utiliza LACP e exige que os membros compartilhem características compatíveis. Parâmetros como lacp_rate, política de hash e quantidade mínima de links influenciam detecção, distribuição e disponibilidade.

13.2. HIPERVISORES E SWITCHES VIRTUAIS

Em virtualização, a agregação pode ocorrer entre interfaces físicas do host e switches físicos, mas o comportamento depende do switch virtual, do hipervisor e do modo de balanceamento. Algumas soluções utilizam LACP; outras distribuem máquinas virtuais ou portas virtuais sem negociar um LAG convencional.

13.3. FIREWALLS, STORAGE E OUTROS APPLIANCES

Firewalls, controladoras, sistemas de armazenamento e appliances podem oferecer interfaces agregadas. É necessário verificar se o grupo opera em Layer 2 ou Layer 3, como lida com alta disponibilidade, quais algoritmos são suportados e se o tráfego de controle ou sincronismo utiliza interfaces separadas.

14. CRITÉRIOS DE PROJETO PARA UM LAG

A decisão de agregar enlaces deve partir de requisitos de capacidade e disponibilidade. Adicionar interfaces sem conhecer o tráfego pode aumentar custo e complexidade sem resolver o gargalo real.

14.1. CAPACIDADE ATUAL E CRESCIMENTO

O dimensionamento deve considerar utilização média, picos, rajadas, quantidade de fluxos, crescimento e capacidade necessária durante manutenção ou falha. Se um grupo de dois enlaces opera próximo de 50% em condições normais, a perda de um membro pode saturar imediatamente o enlace restante.

14.2. PERFIL DOS FLUXOS

O número de conversações e a distribuição entre endereços e portas influenciam o aproveitamento do LAG. Tráfego entre poucos pares, como replicação entre dois servidores, pode exigir múltiplas sessões, links de maior velocidade ou tecnologia diferente para superar o limite de um único membro.

14.3. NÚMERO DE MEMBROS

A plataforma pode limitar a quantidade total de membros, membros ativos e interfaces em standby. Também é necessário verificar se o hardware distribui tráfego por todos os membros e se existem restrições entre portas, módulos ou velocidades.

14.4. TRANSCEPTORES, FIBRAS E CAMINHOS

Os membros devem utilizar interfaces e meios compatíveis. Em fibra óptica, o projeto precisa verificar tipo de fibra, comprimento de onda, alcance, orçamento óptico, conectores, polaridade e compatibilidade dos transceptores. Para redundância física, os enlaces devem utilizar rotas independentes sempre que o risco justificar.

14.5. LICENCIAMENTO E RECURSOS DE PLATAFORMA

Alguns recursos de agregação, MLAG, chassi virtual ou roteamento podem depender de licença, versão de software ou módulo específico. O projeto deve verificar limites e ciclo de suporte antes da aquisição.

14.6. COMPORTAMENTO DURANTE MANUTENÇÃO

A remoção planejada de um membro deve ser testada para evitar perda desnecessária de tráfego. Procedimentos podem incluir retirada controlada, verificação de capacidade remanescente, manutenção, reintegração e confirmação da distribuição após o retorno.

15. APLICAÇÕES EM REDES CORPORATIVAS E INDUSTRIAIS

15.1. UPLINKS DE SWITCHES DE ACESSO

Switches de acesso podem utilizar port-channels para a distribuição, aumentando capacidade e tolerância à falha de uplink. A arquitetura deve decidir se os enlaces terminam no mesmo equipamento, em uma pilha ou em um par multi-chassis.

15.2. INTERLIGAÇÃO DE DISTRIBUIÇÃO E CORE

Port-channels Layer 2 ou Layer 3 podem ser usados entre camadas. Em projetos modernos, interfaces roteadas e ECMP podem oferecer alternativa à agregação tradicional, dependendo da plataforma e do desenho. A escolha deve considerar domínio de falha, convergência, operação e necessidade de extensão de VLANs.

15.3. SERVIDORES E DATA CENTERS

Servidores, hipervisores e storage utilizam agregação para disponibilidade de interfaces e capacidade entre múltiplos fluxos. Em data centers, MLAG ou arquiteturas leaf-spine podem distribuir conexões por dois switches e reduzir dependência de um único equipamento.

15.4. REDES INDUSTRIAIS

Em redes industriais, LACP pode ser utilizado em uplinks, servidores, firewalls e pontos de concentração, mas não substitui protocolos e topologias específicos de redundância industrial. Anéis com RSTP, MRP, DLR ou ERPS e redes PRP/HSR possuem objetivos e comportamentos próprios.

A compatibilidade com protocolos industriais, multicast, sincronismo e janelas de manutenção deve ser verificada. Em equipamentos de campo, o suporte a LACP pode ser limitado ou inexistente.

16. MONITORAMENTO DE UM PORT-CHANNEL

Monitorar somente o estado da interface lógica pode ocultar a perda de um membro. A operação deve acompanhar o grupo e cada interface física individualmente.

16.1. SNMP, SYSLOG E TELEMETRIA

SNMP pode coletar estado, contadores e utilização; syslog registra entrada e saída de membros, suspensões e inconsistências; telemetria pode fornecer séries temporais mais detalhadas. O artigo sobre SNMP e SNMPv3 aprofunda a gestão segura dos equipamentos.

16.2. ALARMES DE DEGRADAÇÃO

O grupo pode continuar up após perder um membro. Por isso, deve existir alarme para redução da quantidade de interfaces, aumento de utilização, perda de capacidade e mudança do parceiro. Sem essa monitoração, a rede pode permanecer degradada até a ocorrência de uma segunda falha.

17. DIAGNÓSTICO DE FALHAS EM LACP

17.1. O GRUPO NÃO É FORMADO

Verifique se pelo menos uma extremidade está em active, se as interfaces pertencem ao mesmo grupo, se velocidade e duplex são compatíveis e se o equipamento remoto é o parceiro esperado. Passive–passive é uma causa comum de grupo inativo.

17.2. UM MEMBRO FICA SUSPENSO

Compare VLANs, trunk, MTU, modo Layer 2 ou Layer 3, chave, transceptores e limites da plataforma. Uma porta pode ter link físico e ainda assim não estar sincronizada ou autorizada a coletar e distribuir.

17.3. O TRÁFEGO UTILIZA SOMENTE UMA INTERFACE

Confirme se o teste utiliza múltiplos fluxos e se o algoritmo de hash inclui campos com diversidade suficiente. Um único fluxo permanecer em um membro é comportamento esperado em grande parte das implementações.

17.4. HÁ PERDA DURANTE A FALHA DE UM MEMBRO

Alguma perda transitória pode ocorrer enquanto tabelas e hashes são atualizados. Perdas prolongadas exigem análise de timer, detecção física, parceiro, Spanning Tree, MLAG, capacidade remanescente e comportamento da aplicação.

17.5. O TRÁFEGO É ASSIMÉTRICO

Cada extremidade calcula seu próprio hash. O caminho de ida pode usar um membro e o retorno outro sem que exista erro. O problema surge quando políticas, firewalls, captura de tráfego ou requisitos de simetria pressupõem o mesmo enlace físico.

18. SEGURANÇA E HARDENING

LACP é um protocolo de controle de enlace local. O projeto deve limitar acesso físico, proteger interfaces não utilizadas, registrar mudanças e evitar conexões não autorizadas. Configurações inconsistentes podem criar caminhos inesperados, ampliar VLANs ou contornar controles planejados.

19. TESTES DE COMISSIONAMENTO E ACEITE

O aceite de um port-channel precisa demonstrar funcionamento normal, distribuição, degradação controlada e recuperação. Apenas verificar o estado up não comprova redundância nem capacidade.

19.1. CHECKLIST DE VALIDAÇÃO

19.2. TESTE DE CAPACIDADE

O teste deve utilizar múltiplas sessões e pares de origem e destino suficientes para exercitar o hash. A metodologia precisa registrar tamanho de pacote, protocolo, quantidade de fluxos, duração, perdas, throughput por membro e throughput total.

19.3. TESTE DE FAILOVER

Durante tráfego contínuo, cada membro deve ser removido de forma controlada. Devem ser medidos tempo de detecção, perda, recuperação e utilização dos membros restantes. Em MLAG, também devem ser testadas falhas de equipamento, peer-link e keepalive conforme o projeto.

Redundância declarada precisa ser comprovada por testes.

A A3A estrutura roteiros, critérios, evidências e matrizes de pendências para validar port-channels, redundância, capacidade, monitoramento e recuperação.

Conhecer o serviço de Comissionamento e Aceite Técnico

20. ERROS COMUNS

21. CONCLUSÃO

LACP e Link Aggregation permitem combinar enlaces Ethernet em uma interface lógica, proporcionando capacidade agregada, tolerância à falha de membros e simplificação da topologia. O resultado, porém, depende de consistência, distribuição de fluxos,

independência física, capacidade após falhas e testes de aceite.

Uma implementação correta precisa ser tratada como decisão de arquitetura e não apenas como um comando de configuração. O projeto deve definir objetivos, membros, modo de negociação, hash, requisitos de disponibilidade, monitoramento, documentação e critérios de validação.

[1] IEEE. IEEE Std 802.1AX-2020 — IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation.

[2] LINUX KERNEL DOCUMENTATION. Linux Ethernet Bonding Driver HOWTO.

[3] OPPENHEIMER, Priscilla. Top-Down Network Design. 3. ed. Indianapolis: Cisco Press, 2011.

[4] IEEE. IEEE Std 802.1Q — Bridges and Bridged Networks.

[5] IEEE. IEEE Std 802.3 — Ethernet.

[6] CISCO SYSTEMS. EtherChannel and Link Aggregation configuration guidance.

[7] ABNT. ABNT NBR 14565:2019 — Cabeamento estruturado para edifícios comerciais.

[8] CISA; NSA. Network Infrastructure Security Guidance. 2022.

O que é LACP? LACP é o protocolo padronizado que negocia e monitora a agregação de múltiplas interfaces Ethernet em um único grupo lógico.**Qual é a diferença entre LACP e Link Aggregation?** Link Aggregation é a técnica e o grupo lógico de enlaces. LACP é o protocolo utilizado para negociar e manter esse grupo dinamicamente.**LACP soma a velocidade dos links?** A capacidade é agregada entre múltiplos fluxos, mas um único fluxo normalmente permanece associado a um membro e fica limitado à velocidade desse enlace físico.**Qual é a diferença entre active e passive no LACP?** Active inicia a negociação LACP. Passive apenas responde. Active–active e active–passive podem formar o grupo; passive–passive não inicia a negociação.**EtherChannel e LACP são a mesma coisa?** EtherChannel é a denominação Cisco para agregação de enlaces. Um EtherChannel pode utilizar LACP ou outro modo suportado pela plataforma.**LACP elimina a necessidade de Spanning Tree?** Não. O Spanning Tree continua protegendo a topologia Layer 2, mas normalmente trata o port-channel como uma única interface lógica.**LACP protege contra falha de switch?** Um LAG convencional protege contra falha de portas ou enlaces membros. Para tolerar falha de switch, é necessário empilhamento, MLAG, vPC ou arquitetura equivalente.**Quais testes devem ser feitos em um port-channel?** Devem ser verificados formação do grupo, membros ativos, distribuição de tráfego, falha de cada

enlace, capacidade remanescente, convergência, VLANs, MTU, contadores, logs e documentação.

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas