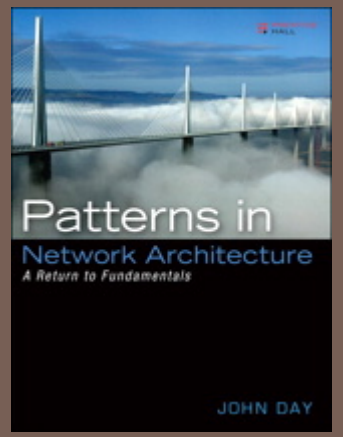


O MODELO IPC DE REDE

Capítulo 7

Patterns in Network Architecture

- *Não estou pensando que nomenclatura seja um remédio para todo defeito em arte ou ciência: mesmo assim não posso deixar de sentir que a confusão de termos geralmente brotam de, e sempre levam a uma confusão de ideias.*

  - John Louis Petit, 1854

- *Um problema bem formulado está meio resolvido.*

  - Charles Kettering

Introdução

Preâmbulo

- Neste capítulo iremos montar os elementos do modelo e descrever a sua operação em um único lugar.
- Os componentes apresentados aqui não devem ser tomados como uma estratégia de implementação e sim como um modelo lógico.
- Apesar do modelo ser descrito em termos de uma única camada, o leitor deve ser alertado de que esta provavelmente não é a melhor estratégia de implementação.

Preâmbulo

- Por enquanto, devemos concentrar as nossas atenções em mudar o nosso modo de pensar do modelo de redes tradicional de camadas estáticas para pensar em termos de aplicações distribuídas que proveem IPC recursivamente
  - Isto não é tão fácil como parece.
- Começamos introduzindo a terminologia para os diversos elementos comuns, depois uma descrição dos componentes e depois como as camadas são montadas.

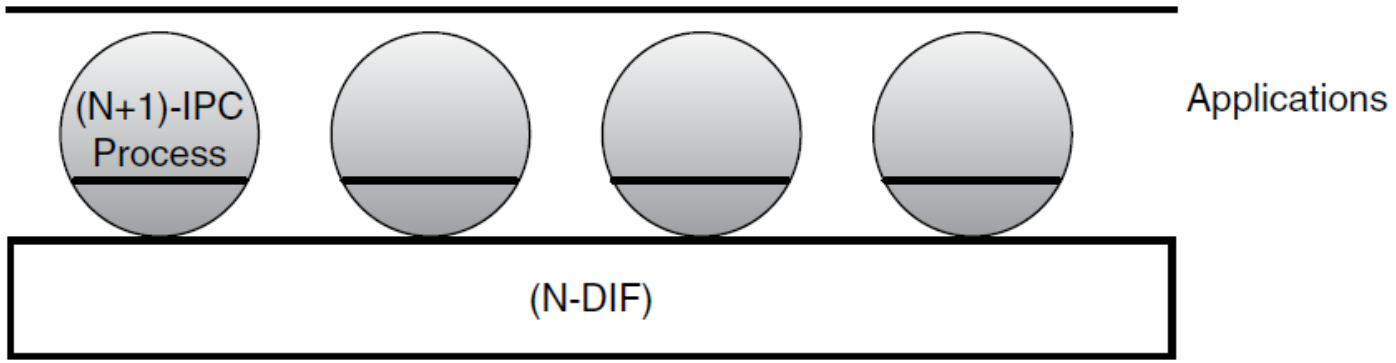
Estrutura Básica

Definições

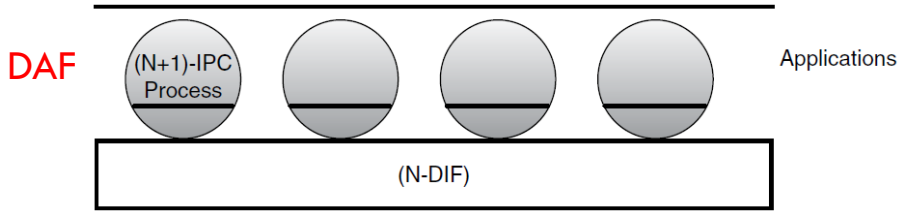
- Sistema de processamento.
  - O hardware e software capazes de dar suporte a tarefas que podem ser coordenadas com uma instrução “teste e aloque” (i.e., todas as tarefas podem referenciar de forma atômica a mesma memória).
- Sistema de computação.
  - A coleção de todos os sistemas de processamento (alguns especializados) sob o mesmo domínio de gerenciamento (sem restrições à conectividade dos mesmos, mas reconhecendo que para uma porção significativa desta população os elementos do domínio de gerenciamento estão diretamente conectados).

Definições

- Camada-(N):
  - Coleção de processos de aplicação cooperando como uma aplicação distribuída para prover uma comunicação entre processos (IPC).

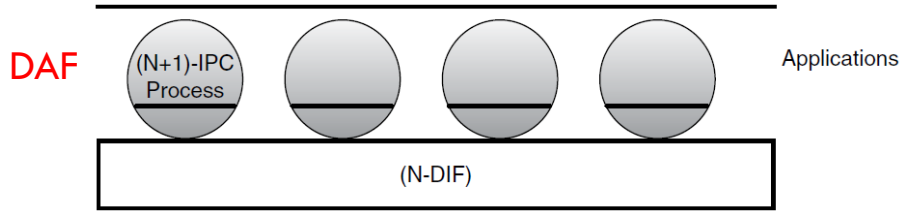


Definições



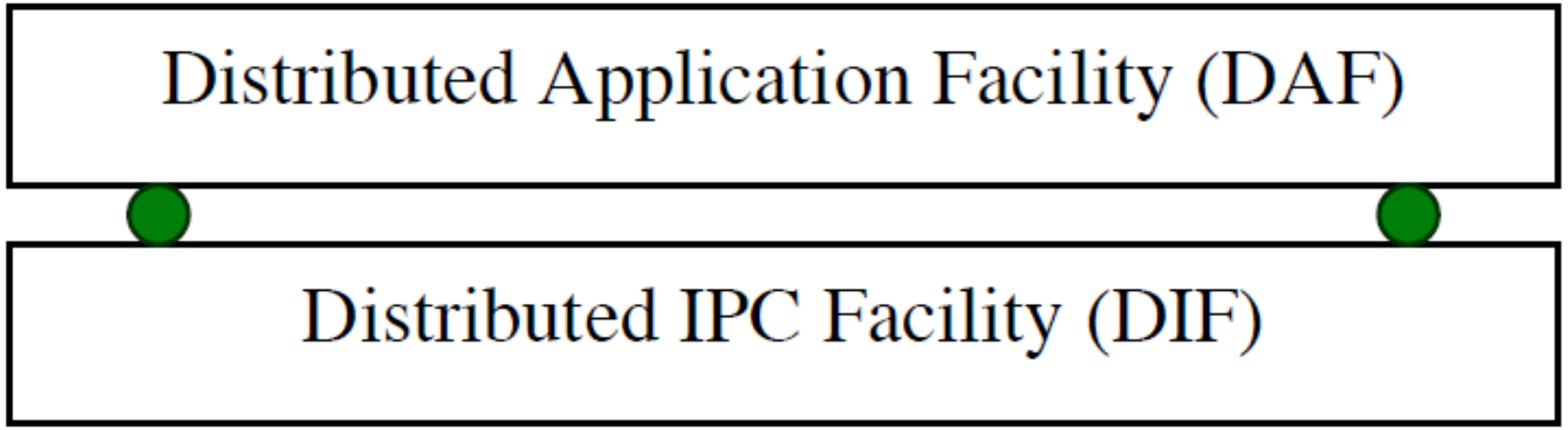
- Recurso de Aplicação Distribuída (DAF):
  - uma coleção de dois ou mais APs cooperantes em um ou mais sistemas de processamento, que trocam informações usando IPC e mantêm o estado compartilhado.
  - Em algumas aplicações distribuídas, todos os membros serão do mesmo tipo, i.e., um DAF homogêneo, ou podem ser diferentes, um DAF heterogêneo.
  - Possui:
    - Um nome de aplicação distribuída (DAN)
    - Um id da instância de aplicação distribuída (DANII)

Definições



- Recurso-IPC-Distribuído-(N) (DIF):
  - Uma aplicação distribuída que consiste de pelo menos uma aplicação IPC em cada sistema de processamento participante.
  - Um DIF é um DAF que faz IPC.
  - O (N)-DIF provê serviços IPC a processos de aplicação ou processos IPC de outros DIFs através de um conjunto de primitivas (N)-API que são usadas para trocar informações com o parceiro da aplicação.
  - Os processos de aplicação correspondentes podem estar em outros sistemas de processamento.

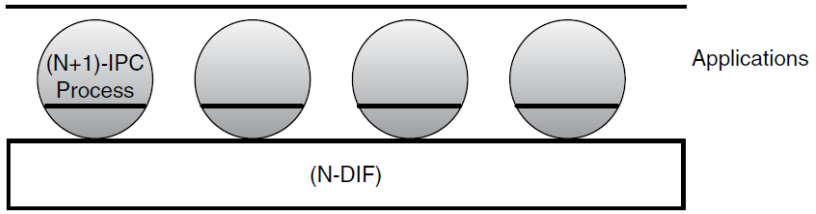
Relacionamento DAF e DIF



Definições

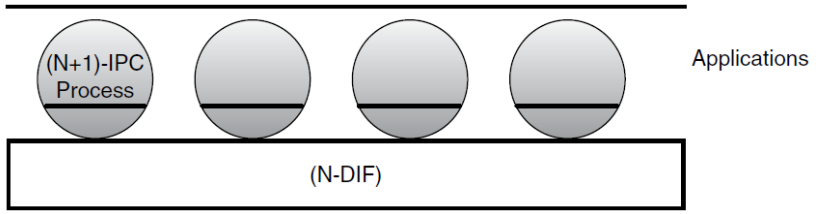
- Processo de Aplicação, AP
  - A instanciação de um programa executando em um sistema de processamento com a intenção de realizar alguma tarefa. Uma aplicação contém uma ou mais máquinas de protocolo.
- Aplicação distribuída
  - Uma coleção de APs cooperantes que trocam informações usando IPC e mantêm um estado compartilhado.

Definições



- Processo-IPC-(N):
  - Uma AP que é um membro da (N)-DIF e implementa localmente a funcionalidade para suportar IPC usando múltiplas subtarefas.
- Protocolo-(N)
  - A sintaxe das PDUs e o conjunto associado de procedimentos que especificam o comportamento entre duas (N)-PMs com a finalidade de manter coordenado um estado compartilhado.

Definições



- Máquina-de-Protocolo-(N), (N)-PM
  - Uma máquina de estados finitos que implementa um protocolo-(N), que troca PDUs com um parceiro para manter um estado compartilhado com uma (N)-PM correspondente, normalmente em outro sistema de processamento.
- Primitiva-API-(N)
  - Uma biblioteca ou chamada de sistema usada por uma aplicação ou um protocolo de aplicação para invocar funções do sistema, em particular funções de IPC, tais como solicitar a alocação de recursos IPC.

Definições

- Unidade-Dados-Serviço-(N), (N)-SDU
  - Uma unidade de dados contígua passada por uma APM em uma primitiva da API da IPC cuja integridade deve ser mantida ao ser entregue à APM correspondente.
- Unidade-Dados-Protocolo-(N), (N)-PDU
  - A unidade da troca de dados entre (N)-PMs que consiste de um (N)-PCI e Dados-usuário-(N).
- Informação-Controle-Protocolo-(N), (N)-PCI
  - A porção de uma (N)-PDU que é interpretada pela (N)-PM para manter o estado compartilhado do protocolo.

Definições

- Dados-usuário-(N)
  - A porção de uma (N)-PDU que não é interpretada e nem é interpretável pela (N)-PM e entregue de forma transparente ao seu cliente, como uma (N)-SDU.
  - Uma Dados-usuário-(N) pode consistir de uma parte de, exatamente uma, ou mais do que uma (N)-SDU.
  - Se houver mais do que uma (N)-SDU, então as SDUs nos Dados-usuário-(N) devem ser delimitados pela (N)-PCI.

Definições

- Protocolo de aplicação
  - Um protocolo que é um componente de uma AP, caracterizado por modificar o estado externo ao protocolo.
- Máquina de protocolo da aplicação, APM
  - A instanciação de um protocolo de aplicação dentro de uma aplicação. Apesar das aplicações de comunicação poderem ser diferentes, as PMs das aplicações comunicantes devem suportar o mesmo protocolo de aplicação.

Definições

- Protocolo-transferência-dados-(N)
  - Um protocolo-(N) usado por um (N)-DIF para entregar transparentemente Dados-usuário-(N) com características específicas; à exceção do envio e recepção transparentes das (N)-SDUs, todas as operações do protocolo são internas ao estado do protocolo.

Estruturas Básicas e Seus Princípios

- Uma camada é um recurso IPC distribuído, DIF.
- Um recurso IPC distribuído é uma aplicação distribuída que consiste de pelo menos um processo IPC em cada sistema de processamento que participa do DIF.
- O escopo de uma camada-(N) é o conjunto de processos IPC cooperantes que formam um (N)-DIF.
- Normalmente o escopo das camadas cresce com o valor de N.
  - No entanto, há configurações onde um (N+1)-DIF tem um escopo menor.

Estruturas Básicas e Seus Princípios

- Um (N+1)-DIF com menor escopo deve envolver um subconjunto próprio dos sistemas de processamento (N)-DIF.
- Se um (N+1)-DIF com menor escopo envolver sistemas e processamento de mais do que um (N)-DIF, há um potencial para comprometimento da segurança potencialmente permitindo que dados corrompidos (vírus, etc.) de um DIF menos seguro sejam introduzidos em um DIF mais seguro.

Estruturas Básicas e Seus Princípios

- Podem haver mais do que um DIF de mesmo nível.
- Frequentemente os conjuntos de sistemas de processamento que participam em diferentes DIFs são mutuamente exclusivos.
  - Quando este for o caso, sistemas em diferentes (N)-DIF não podem se comunicar sem fazer um repasse no (N+1)-DIF.

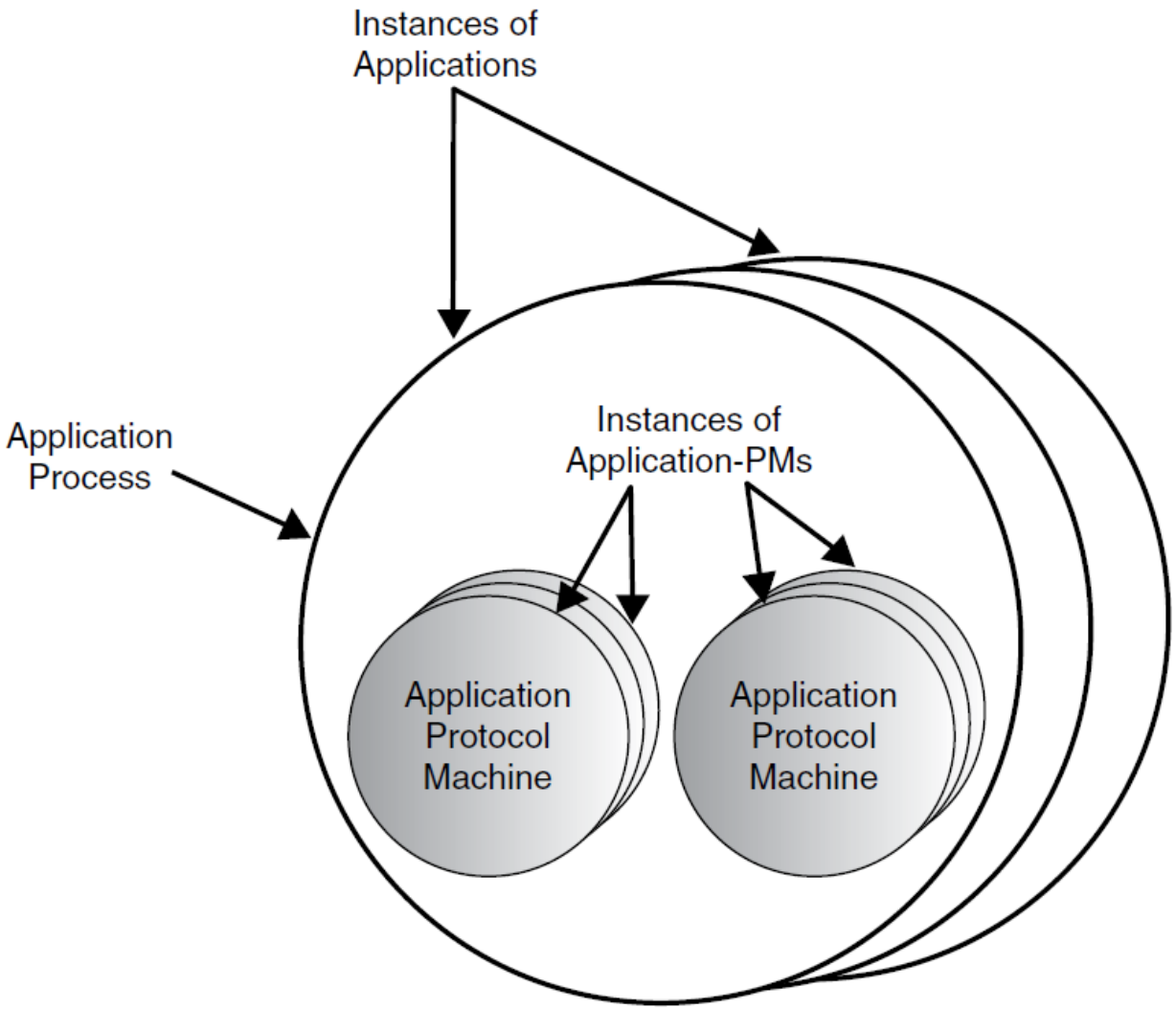
Estruturas Básicas e Seus Princípios

- Uma aplicação pode se comunicar com mais de um DIF ao mesmo tempo.
- No entanto, isto cria um potencial para comprometimento de segurança.
- Quando a segurança for uma preocupação, os únicos APs capazes de comunicar com dois ou mais DIFs deveria ser um processo (N+1)-IPC (i.e., um membro de um (N+1)-DIF).
- O sistema operacional deveria garantir esta restrição.

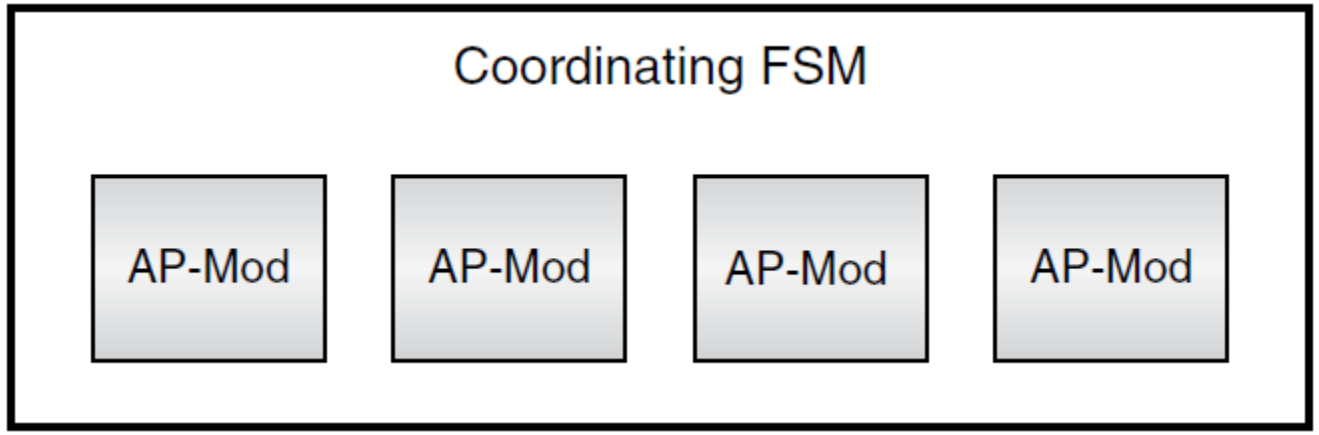
A Estrutura de Aplicações e Protocolos

- (...)
- *Conjectura*: qualquer estado associado com o correspondente em um protocolo de aplicação é parte da aplicação e não está associado com o protocolo de aplicação.
  - Qualquer estado que deva ser mantido durante a comunicação está associado com IPC.
  - Todos os protocolos de aplicação não possuem estados, enquanto que os protocolos de transferência de dados podem ou não ser sem estados.
  - Arquiteturalmente há apenas um protocolo de aplicação e ele é sem estado.

Máquinas de Protocolos de Aplicação



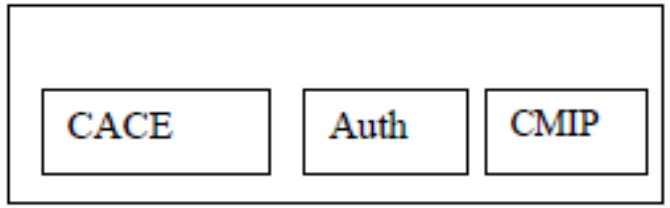
Construção de APs



- AP-Mod: módulos de protocolo de aplicação alguns dos quais implementam funções comuns.
- Uma FSM de coordenação governa a interação entre estes módulos (não é uma PM porque não gera PDUs).

CDAP

- Common Distributed Application Protocol:
  - Plataforma para a construção de aplicações distribuídas.
- Módulos:
  - CACE – Common Application Connection Establishment
  - CMIP – Common Management Information Protocol
  - Auth



Conjectura

- Todos os protocolos envolvem dois e apenas dois correspondentes.
- Estado compartilhado envolvendo múltiplos correspondentes (i.e., mais do que dois) é uma propriedade do AP, e não da APM.
  - Ou seja, todos os protocolos "multi parceiros" são aplicações distribuídas.

Conceitos de Nomes para (N)-DIFs e Aplicações

Definições

- Espaço de nomes do processo de aplicação
  - Conjunto de *strings* que podem ser atribuídos aos APs e usados para serem referenciados por outras aplicações no mesmo domínio de nomes.
- Nome do processo de aplicação, nome do AP.
  - Uma *string* alocado a um AP a partir de um espaço de nomes de AP e que não é alocado a nenhum outro AP enquanto estiver associado àquele a que foi alocado.
- Instância do processo de aplicação
  - A instanciação de um AP em um sistema operacional.

Definições

- Estas definições proveem múltiplas instâncias da mesma aplicação e permite que sejam acessadas separadamente:
  - Identificação da instância do processo de aplicação
    - Este é um identificador associado a uma instância do AP que quando combinado ao nome do AP é não ambíguo dentro do espaço de nomes de AP.
  - Espaço de nomes da PM de aplicação
    - Conjunto de *strings* que podem ser alocados a PMs de aplicações e usados para serem referenciados por outras aplicações no mesmo domínio de nomes.
  - Identificação da PM de aplicação
    - Identificador não ambíguo dentro do escopo do AP. Um PM-id quando concatenado como nome do AP é também não ambíguo no espaço de nomes dos APs.

Definições

- Estas definições permitem que uma AP tenha múltiplos protocolos de aplicação:
  - Instância da PM de aplicação
    - A instanciação de uma PM de aplicação dentro de um AP.
  - Identificação da instância da PM de aplicação
    - Este é um identificador não ambíguo no espaço de nomes do AP quando qualificado pelo nome do AP, id-instância do AP e a id da MP de aplicação.

Definições

- Estas definições permitem nomear múltiplas instâncias de protocolos de aplicação dentro de uma instância de um AP:
  - Nome do processo IPC
    - Um nome de AP que é alocado a um processo IPC. Este é o nome externo de um processo IPC.
  - Nome da aplicação distribuída, DAN
    - Um nome normalmente extraído do mesmo espaço de nomes dos APs para identificar uma aplicação distribuída.
    - Um tipo importante de aplicação distribuída é um DIF.
    - Um DAN age como um nome anycast ou multicast para o conjunto de Aps que inclui esta aplicação distribuída a depender da operação.
  - (N)-port-id
    - Um identificador não ambíguo dentro do escopo do sistema de processamento usado para distinguir uma alocação particular de um (N)-IPC.

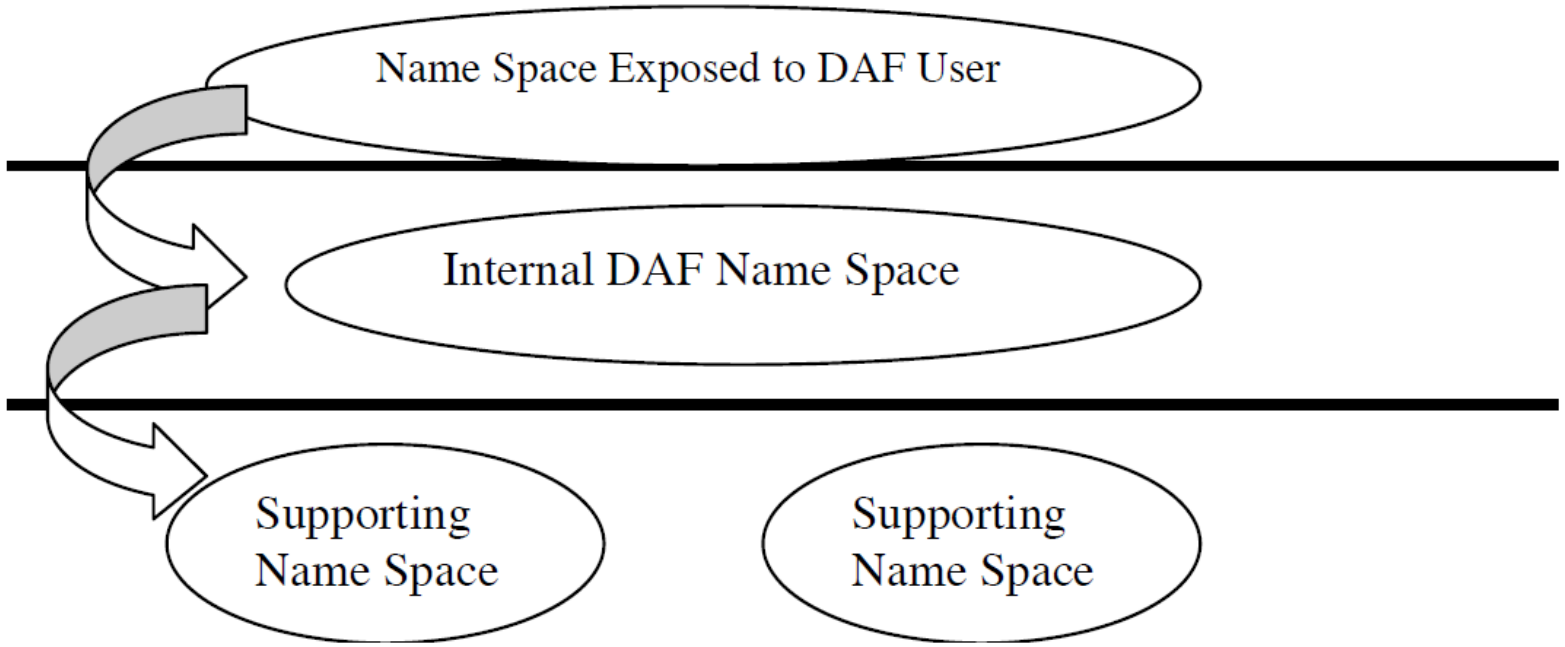
Nomeando a Aplicação

- Dado um DIF, A.
- Considere os sistemas de processamento de todos os processos IPC que compõem A.
- O espaço de nomes do AP deve cobrir todas as aplicações alcançáveis por este DIF.
- Adicionalmente, se qualquer destes sistemas de processamento possuir DIFs distintos além de A, o escopo do espaço de nomes da aplicação deve também incluir todas as aplicações alcançáveis por estes DIFs.
- O conjunto então formado representa o escopo do espaço de nomes do AP.

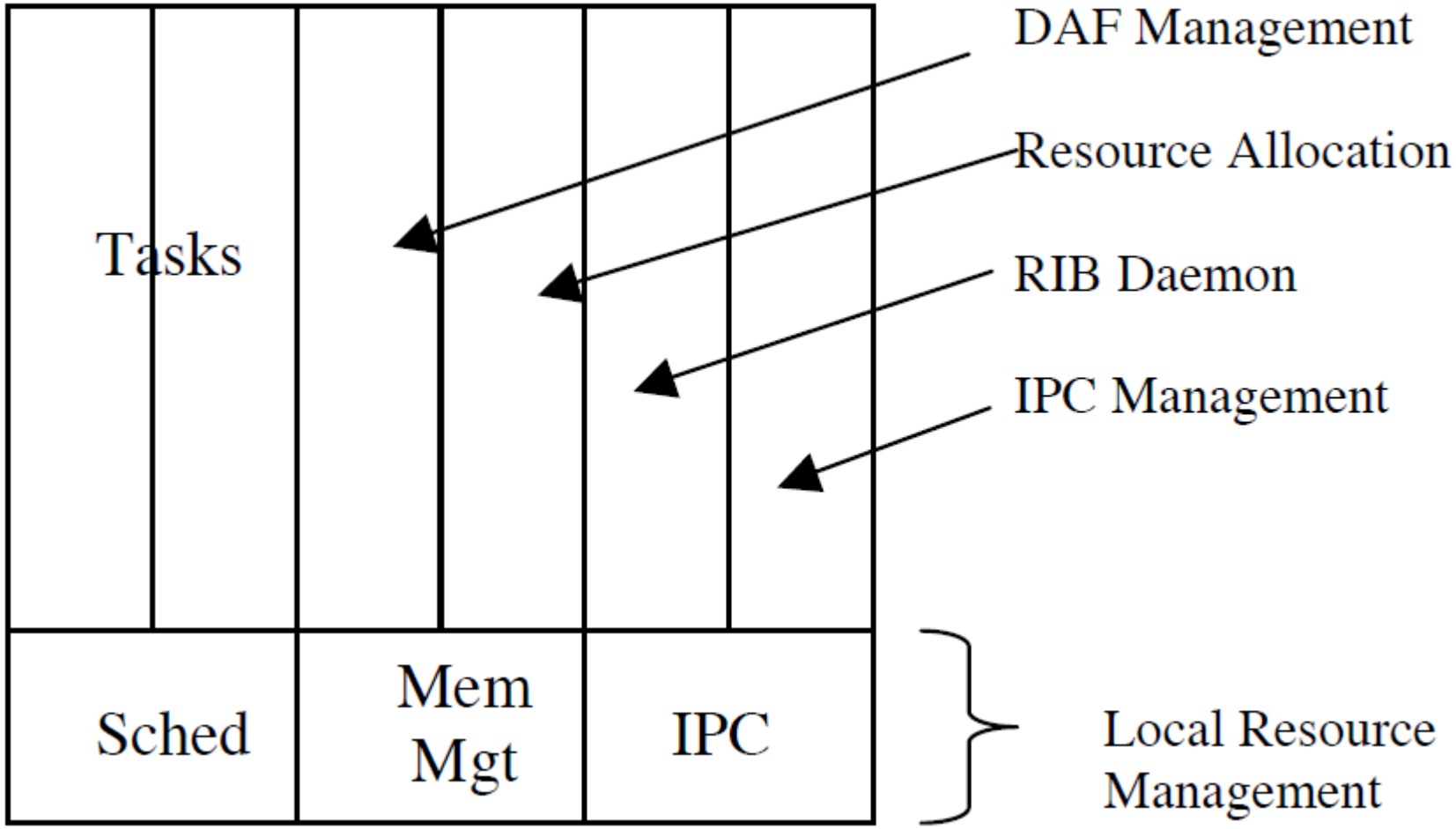
A Estrutura dos Espaços de Nomes

- A estrutura do espaço de nomes depende do seu escopo:
  - Em domínios com pouco escopo, eles podem ser simples e plano.
  - Para domínios com escopos mais abrangentes, eles podem ser hierárquicos.

Espaços de Nomes dos DAFs



Um Processo de Aplicação Distribuída (DAP)



O Recurso IPC Distribuído-(N)

Definições

- Protocolo-controle-erro-e-fluxo-(N) (EFCP)
  - O protocolo de transferência de dados necessário para manter uma instância de IPC dentro de um DIF entre port-ids correspondentes.
  - As funções deste protocolo garantem confiabilidade, ordem, e controle de fluxo, na medida da necessidade.
- Tarefa-repasse/multiplexação-(N) (RMT)
  - A tarefa dentro do processo IPC que realiza a multiplexação/repasse de (N)-PDUs e insere a PCI de repasse em todas as PDUs por questões de endereçamento.

Definições

- Identificador-conexão-(N)
  - Um identificador interno a um DIF e não ambíguo dentro do escopo de duas EFCPMs comunicantes daquele DIF que identifica esta conexão.
  - O identificador da conexão é comumente formado pela concatenação dos port-ids associados a este fluxo pelas EFCPMs origem e destino.
- Endereço-(N)
  - Um identificador dependente de localização *interno* a um DIF e não ambíguo dentro do DIF. Este identificador é usado na coordenação e manutenção do estado do DIF.

Definições

- EFCPM-(N)
  - Uma tarefa dentro do processo IPC que é uma instância do EFCP que cria uma única instância de estado compartilhado representado um canal, conexão, associação, fluxo, etc. full-duplex.
- Delimitação-(N):
  - Primeira operação executada pelo DIF, usualmente através de primitivas da API, para delimitar uma SDU de modo que o DIF possa garantir que seja capaz de entregar a SDU até o seu destinatário

Definições

- PCI-Repasse-(N)
  - A designação da PCI de repasse usado pela RMT de um processo IPC. Este é o PCI da fase de transferência de dados da aplicação IPC distribuída
- Proteção-SDU-(N):
  - A última operação (opcional) executada pela RMT para garantir que a SDU não tenha sido corrompida enquanto em trânsito.

Definições

- Protocolo de Troca de Informações de Recursos (RIEP)
  - Um protocolo de aplicação interno ao DIF usados para a troca de informações de recursos entre os processos IPC de um DIF. Informações enviadas via CDAP.
  - Logicamente o RIEP atualiza a Base de Informações de Recursos (RIB) distribuída.
- Protocolo de acesso IPC (IAP) – CACEP usando o CDAP
  - Uma aplicação do RIEP que encontra o endereço de um processo de aplicação e determina se aplicação solicitante tem acesso ao mesmo e comunica as políticas a serem usadas.

O Processo-IPC-(N)

- O processo IPC é um AP, um componente de um recurso IPC distribuído, formado por dois componentes principais:
  - A tarefa IPC e
  - A tarefa de gerenciamento IPC.
- A tarefa IPC é formada por uma RMT e uma EFCPM para cada conexão/fluxo que inicia neste processo IPC. E o CDAP para transporte de informações de controle de acesso e de gerência.
- Há uma tarefa de gerenciamento IPC em cada processo IPC.

Funções da Tarefa IPC

- Delimitação e proteção da PDU
  - Que consiste de funções razoavelmente diretas adequadas ao *pipelining*
- Repasse e multiplexação
  - Que se preocupa com o gerenciamento da utilização da camada abaixo
- Transferência de dados
  - Que distingue fluxos e sequenciamento caso necessário
- Funções de controle de transferência de dados
  - Responsável por mecanismos de realimentação e sua sincronização, que controlam as filas de transferência de dados e retransmissões.

A Tarefa de Gerenciamento da IPC

- A tarefa de gerenciamento da IPC usa o RIEP.
- O RIEP é usado para trocar informações entre os processos IPC necessárias para o gerenciamento do DIF.
- Eventos, incluindo estouros de temporização, podem fazer com que o RIEP emita atualizações (no modo publique/assine), ou um processo IPC ou sistema de gerenciamento de rede pode solicitar informações de um processo IPC (modelo cliente/servidor).
- Corresponde ao que tem sido referenciado como *plano de controle*.

A (N)-IPC-APM

- A IPC APM consiste de seis subtarefas distintas :
  - IPC API
  - Delimitação da SDU
  - PM de transferência de dados do EFCP
    - Que lida com mecanismos fortemente acoplados e transporta os dados do usuário
  - PM de controle EFCP
    - Que provê suporte a mecanismos fracamente acoplados
  - A tarefa de repasse e multiplexação
    - Que acrescenta a PCI comum de transferência de dados
  - Proteção da PDU
    - Consiste do CRC e funções de criptografia.

Primitivas da API da IPC

- Reason <- Allocate_Request (Destination, Source, QoS Parameters, Port-id)
- Reason <- Allocate_Response (Destination, QoS Parameters, Port-id)
- Reason <- Send (Port-id, buffer)
- Reason <- Receive (Port-id, buffer)
- Reason <- De-allocate (Port-id)

O Protocolo EFCP

- Este protocolo provê a conexão/fluxo IPC associado com cada pedido de alocação.
- Ele provê à transferência de dados entre APs.
- A ligação entre uma conexão APM a uma conexão IPC é realizada após uma resposta com sucesso pelo IAP e não pelo EFCP como é comum hoje.
- A função IPC requer um protocolo para manter a sincronização e prover controle de erro e de fluxo.
- O EFCP é dividido em dois protocolos separados que são implementados por duas máquinas distintas de protocolos, que compartilham um vetor de estados.

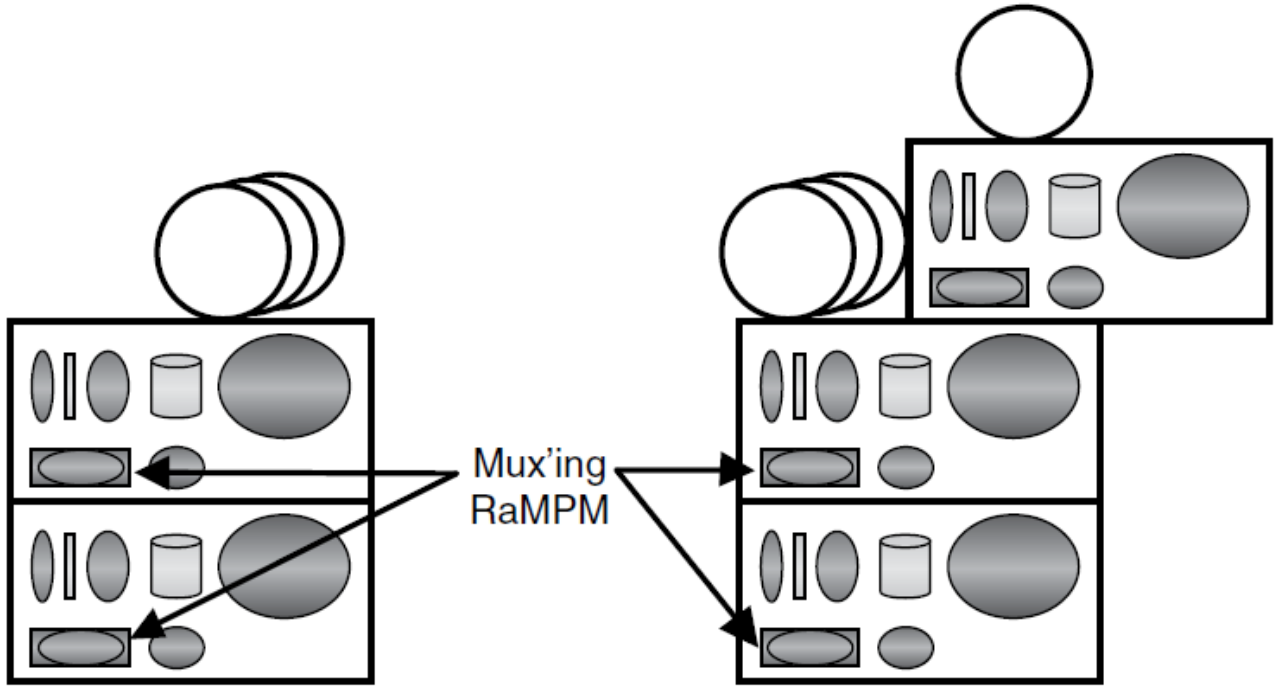
Protocolo EFCP

- Delimitação
- A PM de Transferência de Dados IPC
- O Protocolo de Controle IPC
  - Possui três modos de operação em função da QoS solicitada e da QoS provida pela (N-1)-DIF:
    - Sem sincronização
    - Sincronização fraca
    - Sincronização forte

A Tarefa de Repasse e Multiplexação (RMT)

- Três formas dependendo de onde aparecem na arquitetura:
  - Uma aplicação de multiplexação encontrada principalmente em *hosts* e nas camadas mais baixas de roteadores
  - Uma aplicação de repasse encontrada principalmente na camada mais "alta" de roteadores internos.
  - Uma aplicação de repasse e agregação encontrada principalmente na camada mais "alta" de roteadores de borda.

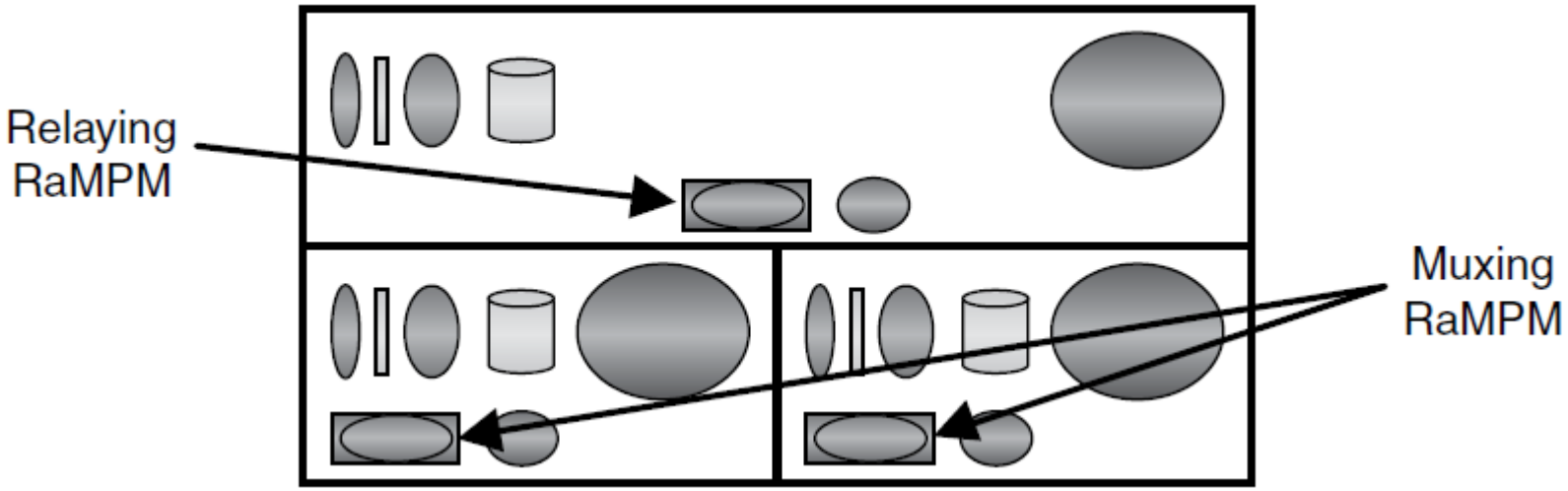
Multiplexação



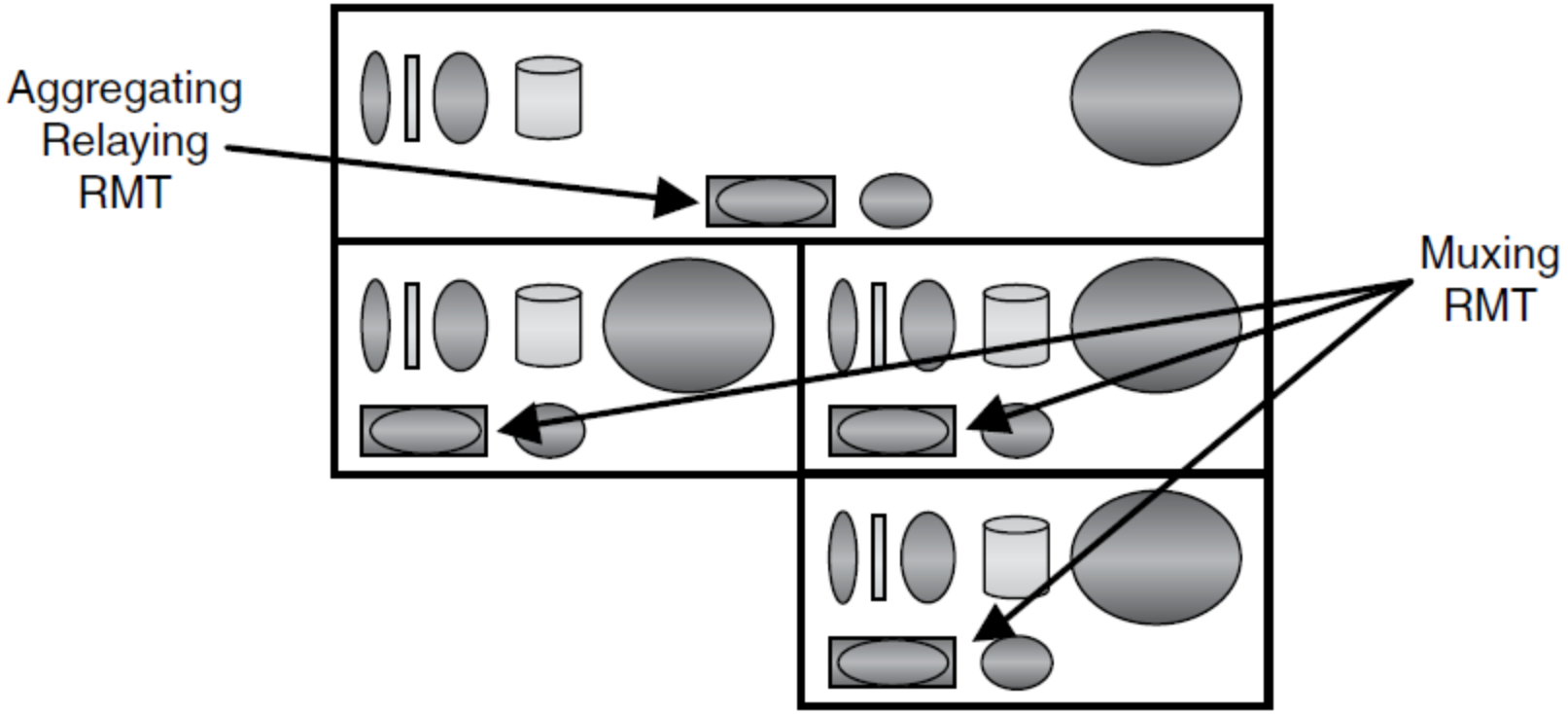
Host típico suportando aplicações.

Host suportando aplicações de repasse de correio e uma aplicação de correio.

RMT de um Roteador Interno



RMT de um Roteador de Borda

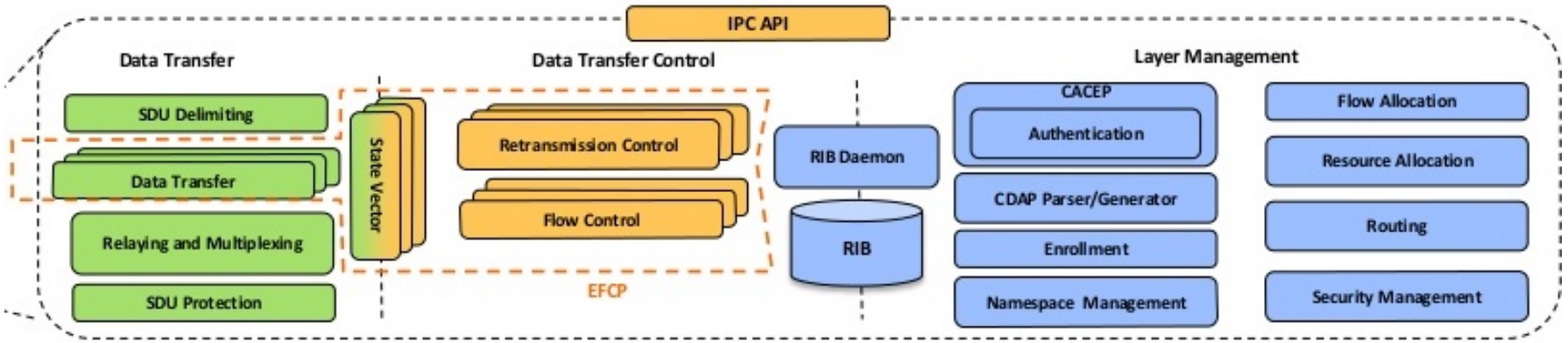


Proteção da PDU

- Última função executada nas PDUs antes que sejam entregues à camada abaixo. E a primeira função a ser executada nas PDUs que chegam.
- A delimitação e a proteção da PDU são componentes do DIF e não dos protocolos usados pelo DIF.
  - Não é possível ter mais do que uma função de delimitação ou de proteção da PDU operando num DIF porque ele não teria como determinar qual delas deveria ser aplicada.

A Tarefa de Gerenciamento da IPC

- Roteiro:
  - Protocolo-Acesso-IPC-(N) (IAP)
  - Protocolo de Troca de Informações de Recursos (RIEP)
  - Base de Informações de Recursos (RIB)
  - Funções de Gerenciamento da IPC



Protocolo-Acesso-IPC-(N) (IAP)

- Funções:
  - Encontrar o endereço do processo IPC destino com acesso ao AP solicitado.
  - Determinar se o AP solicitado está realmente naquele destino e se o AP solicitante tem permissão para acessar o AP solicitado.
  - Transportar informação para o processo IPC destino sobre as políticas a serem usadas para a comunicação solicitada e retornar a resposta do destino até a fonte.

Protocolo de Troca de Informações de Recursos (RIEP)

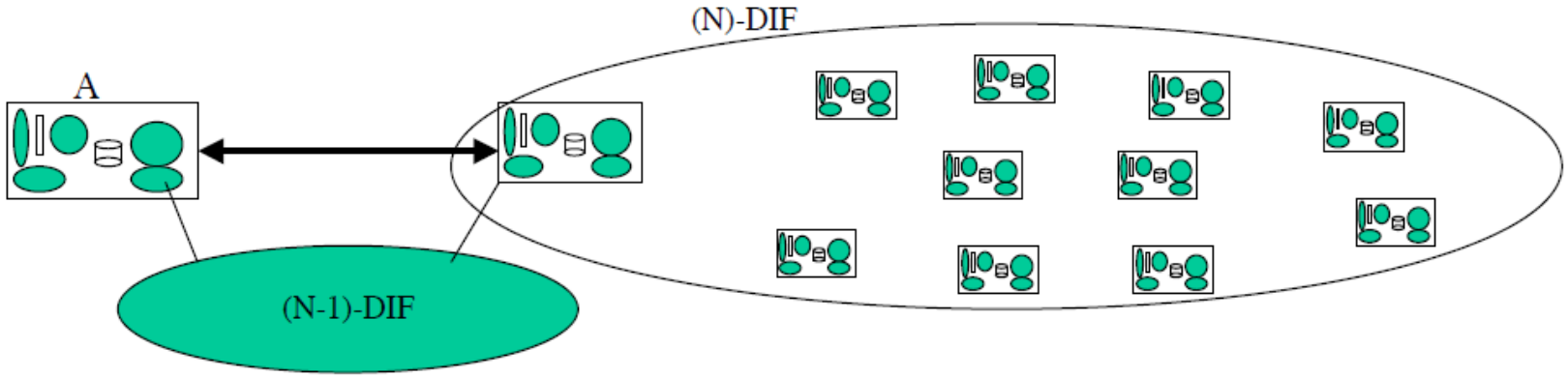
- Tradicionalmente este seria o protocolo de atualização de roteamento e era associado apenas com roteamento.
- Nós o vemos como uma ferramenta geral para o compartilhamento de informações entre os membros de um DIF.
  - Ex.: conectividade, tamanho de fila, carga de processamento, alocação de recursos, etc.

Base de Informação de Recursos

- A RIB é o depósito lógico para informações locais sobre o estado de um DIF.
- Cada processo IPC mantém uma RIB.
- Ela é bem semelhante a uma MIB
  - Aqui foi usado outro termo para indicar que pode incluir informações adicionais às de gerenciamento de rede.

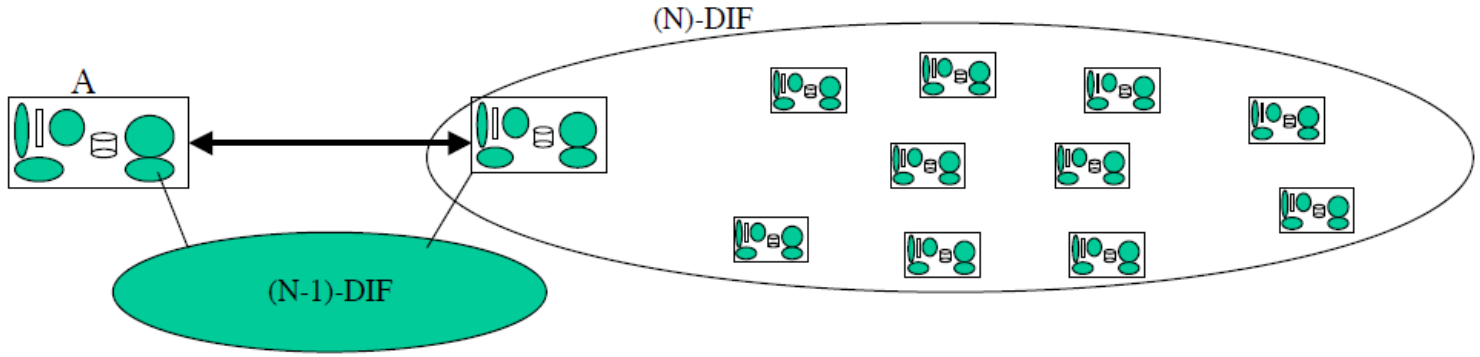
Funções de Gerenciamento da IPC

- Registro:
  - Ocorre quando um processo IPC estabelece uma conexão de aplicação (usando um (N-1)-DIF) com um outro processo IPC, que já é um membro de um DIF existente, para se unir ao DIF.



Funções de Gerenciamento da IPC

- Registro (cont.):
  - Quando isto ocorre, o processo IPC pode autenticar o novato, usando o RIEP para inicializar diversos objetos gerenciados e seus atributos, incluindo a alocação de um endereço.
    - Estes parâmetros caracterizam a operação deste DIF. Ex.: tamanho máximo da PDU, faixas de temporizadores, faixas de políticas, atualização de informações de roteamento e de alocação de recursos.



Funções de Gerenciamento da IPC

- Roteamento:
  - Esta tarefa realiza a análise da RIB para prover dados de conectividade para a criação da tabela de repasse.
  - A escolha de algoritmos de roteamento em um DIF em particular é uma questão de política.

Funções de Gerenciamento da IPC

- Diretório:
  - Cada DIF deve manter o mapeamento de (N)- para (N-1)-nomes e endereços dos vizinhos mais próximos para as suas fronteiras superior e inferior.
    - Fronteira superior: nome para endereço (função de diretório)
    - Fronteira inferior: endereço para ponto de conexão (para selecionar o caminho até a próxima etapa)
  - Uso principal para IAP e roteamento.

Funções de Gerenciamento da IPC

- Alocação de Recursos:
  - Classes de fluxos:
    - Fluxos solicitados por um AP, normalmente em um *host*
    - Fluxos criados pelo gerenciamento IPC para classes distintas de QoS para agregar tráfego e melhorar a eficiência, geralmente em roteadores de borda e entre eles.
    - Fluxos que atravessam um sistema (i.e., roteamento tradicional).

Funções de Gerenciamento da IPC

- Gerenciamento de segurança:
  - **Autenticação** para garantir que um processo IPC que deseja se unir a um DIF é quem se diz ser e é um membro admissível ao DIF.
  - Proteção contra modificação ou escuta por um (N-1)-DIF
  - **Controle de acesso** para determinar se os APs que requisitam um fluxo IPC com uma aplicação remota tem as permissões necessárias para estabelecer a comunicação.
    - Os procedimentos de segurança específicos usados para estas funções são uma questão de política.

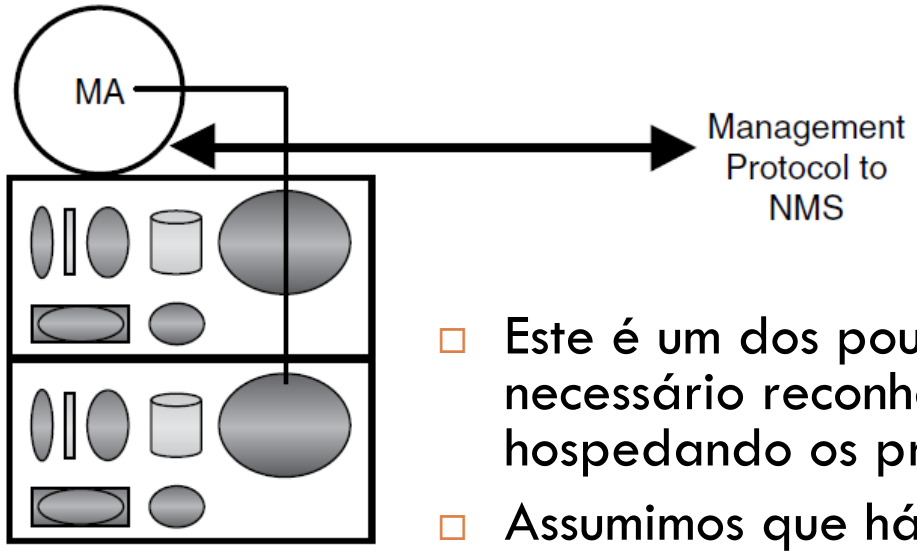
Protocolo de Gerenciamento de Rede e Arquitetura de Gerenciamento

- Normalmente é necessário ter uma visão externa na operação dos DIFs que formam a rede.
  - Isto requer o monitoramento dos múltiplos DIFs que constituem a rede (i.e., o domínio de gerenciamento)
- A função do gerenciamento da rede é *monitorar* e *reparar* e *não controlar*.
- Cada sistema de processamento na rede (que pode incluir os *hosts*) contém um agente de gerenciamento responsável por coletar informações de processos IPC em todos os DIFs do sistema e comunicá-las a um *sistema de gerenciamento de rede* (NMS)

Protocolo de Gerenciamento de Rede e Arquitetura de Gerenciamento

- O NMS exerce uma forte influência no registro.
  - As tarefas de registro agem pelo NMS
  - O NMS determina quando uma camada deve ser criada e inicia a atividade, mas são as tarefas de registro que as executa.
    - Isto inclui criar a habilidade para os agentes de registro sensoriar as condições corretas e tomar a decisão automaticamente.

Protocolo de Gerenciamento de Rede e Arquitetura de Gerenciamento



- Este é um dos poucos lugares nesta arquitetura onde é necessário reconhecer os sistemas que estão hospedando os processos IPC.
- Assumimos que há um *agente de gerenciamento* (MA) que é um AP.
- Um MA tem acesso a todos os DIFs no sistema.
- Ele se comunica com um NMS, exatamente como qualquer outra aplicação, usando um DIF.
- Um MA pode se comunicar usando um DIF mais baixo e ainda assim coletar informações de DIFs mais altos.

A Natureza das Camadas

Camadas

- Uma estrutura de elementos comuns que se repetem torna mais fácil caracterizar a natureza de uma “camada”.
- Uma camada é um recurso IPC distribuído ou DIF.
- A hierarquia (empilhamento) dos DIFs é simplesmente uma relação entre DIFs e, portanto, é aplicável apenas aos DIFs.

Aplicações e Camadas

- As aplicações não pertencem a nenhuma camada, a não ser que sejam processos IPC e um membro de um DIF.
- A divisão em camadas baseada em conceitos do *kernel* ou aplicações do usuário é uma propriedade do SO e não de comunicações.
- Potencialmente qualquer aplicação pode usar um DIF de qualquer nível desde que este tenha escopo suficiente para acessar as aplicações remotas necessárias e controles de acesso apropriados.

Fronteira entre Camadas

- Em outras arquiteturas sempre houve conflitos sobre o que pertence a cada camada.
  - Estes conflitos desaparecem quando nos apercebemos que todas as camadas/DIFs fazem apenas uma coisa: IPC.
  - A finalidade principal das camadas é a finalidade principal da IPC: o aspecto da transferência de dados.

Gerenciamento

- O gerenciamento é “extradimensional”.
- O gerenciamento do IPC deve ter a habilidade de compartilhar informações entre *camadas adjacentes* (e não todas as camadas).
- Apenas o NMS tem potencialmente a habilidade de ver as informações sobre a operação do DIF para todos os DIFs numa rede.
- Se o controle de acesso for apropriado entre camadas adjacentes, de modo que os endereços estejam disponíveis, mapeamentos efetivos entre endereços-(N) e endereços-(N-1) podem tornar o roteamento muito mais efetivo.

Estrutura

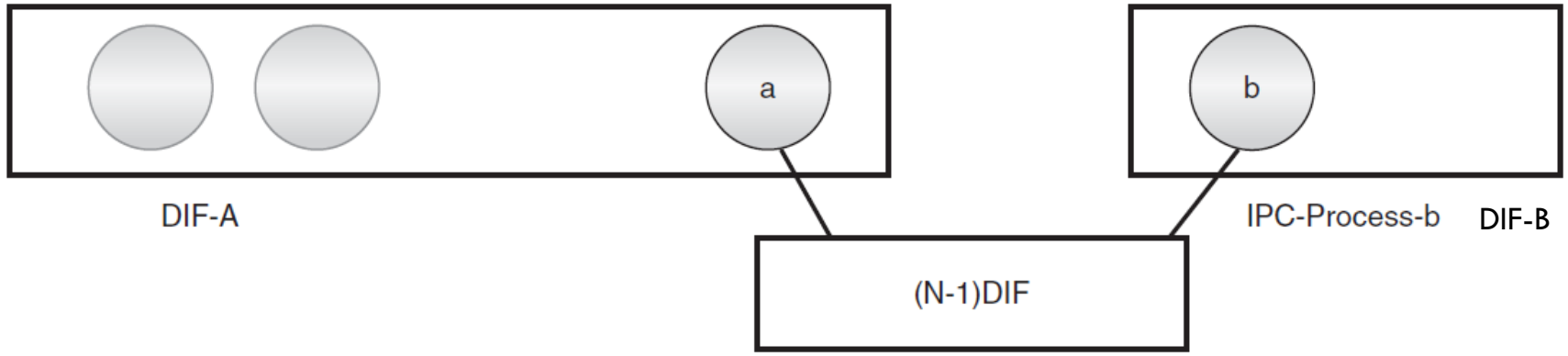
- Isto nos dá uma estrutura em camadas como os locais necessários pelo estado compartilhado,
  - mas que é ao mesmo tempo mais estruturado e mais flexível do que as nossas tentativas anteriores e
  - também se traduz em uma implementação simples.

Operação do DIF

Operação do DIF

- Nesta seção consideramos brevemente a operação de um DIF.
- Olhamos, em particular, a três operações fundamentais:
  - Como um processo IPC se junta a um DIF [registro]
  - Como um novo DIF é criado [registro]
  - Como uma aplicação solicita serviços IPC.
- A operação do DIF é conduzida pela ação dos APs.
- Os processos IPC devem coordenar suas ações com os outros membros de um DIF.

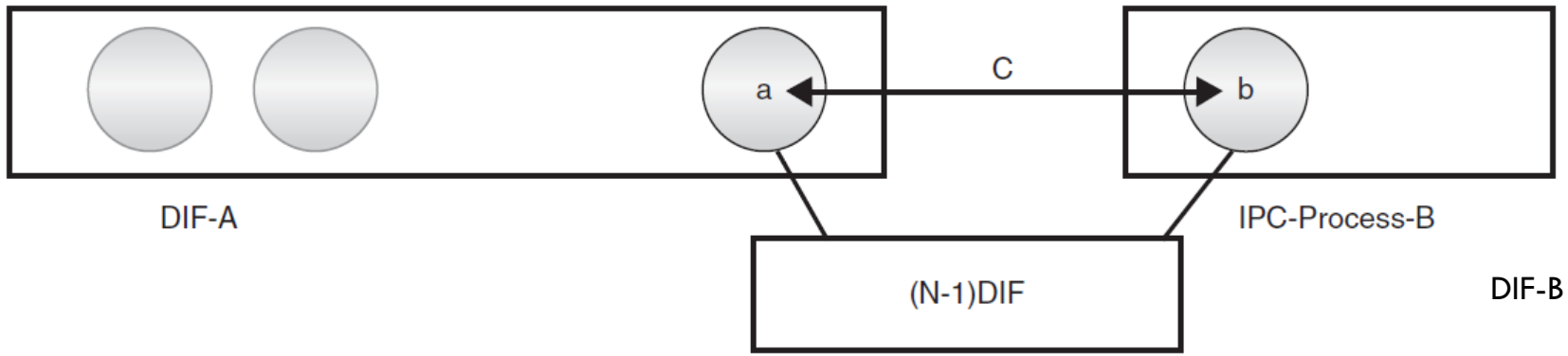
Adicionando um Novo Membro a um (N)-DIF



- Suponha que o DIF B queira se juntar ao DIF A
- O DIF B representa um único processo IPC.
- O processo IPC, **b**, em B possui o nome AP de um processo IPC, **a**, em A, mas não seu endereço.
- B não tem como conhecer os endereços de qualquer elemento de A.
- A e B estão conectados através do (N-1)-DIF, que em último caso seria o meio físico.

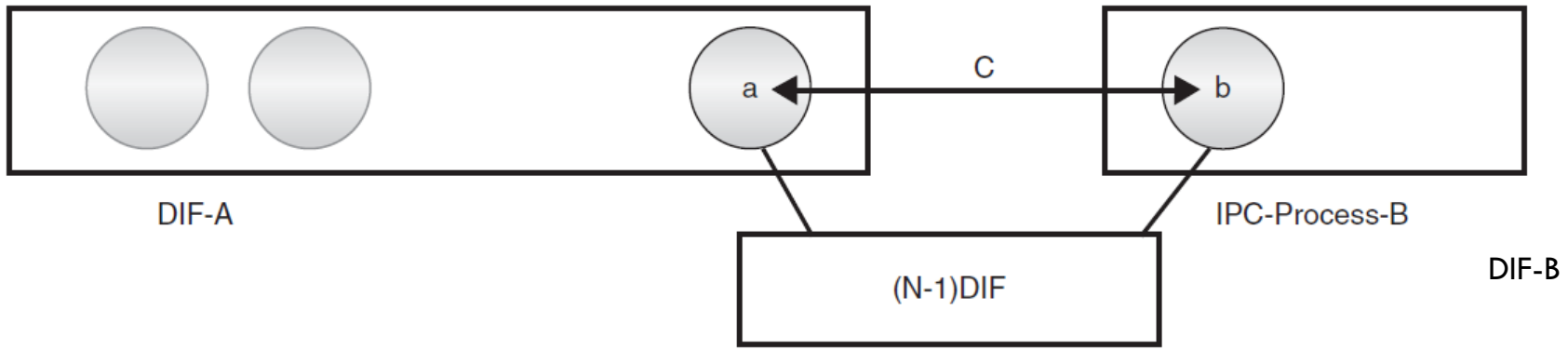
Adicionando um Novo Membro a um (N)-DIF

- Usando o (N-1)-DIF, **b** pede ao (N-1)-DIF que estabeleça um canal IPC com **a** da mesma forma que o faria com qualquer outra aplicação usando o nome AP de **a**.
- O (N-1)-DIF determina se **a** existe e se **b** tem acesso a **a**.
- Depois que a conexão da aplicação tiver sido estabelecida, **a** autentica **b** e determina se ele pode ser um membro de A.
- Se o resultado for positivo, **a** atribui um endereço-(N) a **b**.

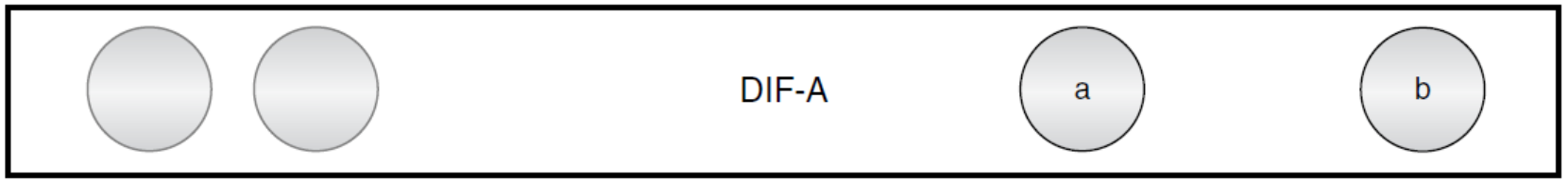


Adicionando um Novo Membro a um (N)-DIF

- **b** usa o endereço-(N) para se identificar perante outros membros do DIF A.
- Este endereço-(N) é usado no PCI de transferência de dados do protocolo de aplicação de registro, também chamado de PCI de repasse.
- Outros parâmetros de inicialização associados com o DIF A são trocados com **b**.



Adicionando um Novo Membro a um (N)-DIF



- O processo IPC, **b,** é agora um membro do DIF A.
- Logo após, **b** também estabelece comunicação semelhante com todos os membros de A que são vizinhos próximos.
- Estes fluxos são usados para trocar informações RIEP para manter o estado compartilhado do (N)-DIF.
- **b** agora está pronto para participar no (N)-DIF e agora pode aceitar pedidos das aplicações por IPC.

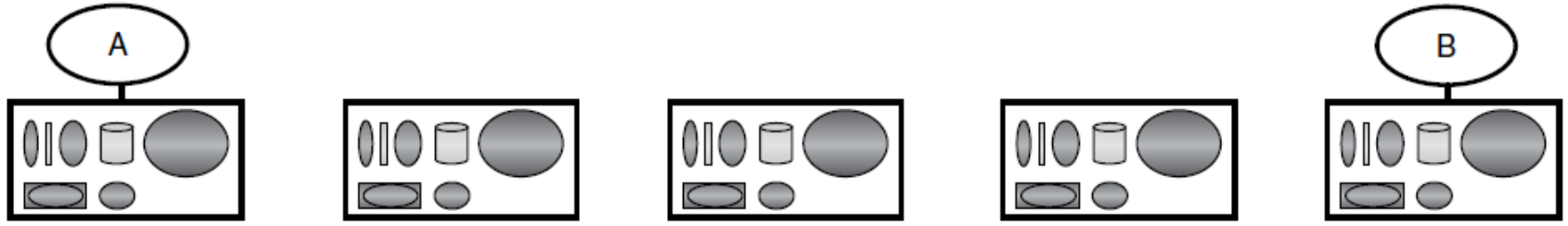
Criando um Novo DIF

- Um NMS ou uma aplicação semelhante com as permissões apropriadas provocam a criação e inicialização de um processo IPC
  - Incluindo a sua ligação com um ou mais (N-1)-DIFs.
- Como parte da sua inicialização são dados ao processo IPC os meios para reconhecer membros legítimos do DIF (ex. lista dos nomes de processos de aplicação, uma assinatura digital, etc.)
  - Ou pode ser direcionado a efetuar um registro com eles ou simplesmente esperar que ele encontre este processo IPC inicial

Transferência de Dados

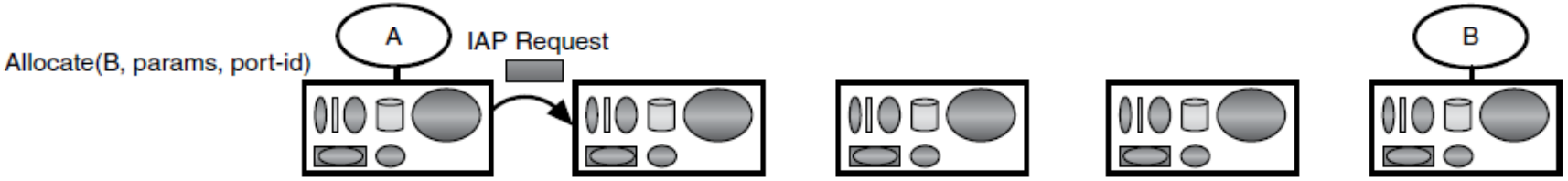
- Quando a inicialização do registro tiver se completado, o DIF estará disponível para prover IPC para os APs que residam no seu sistema de processamento ou para agir como um intermediário.
- Os APs solicitam a alocação de recursos IPC através de chamadas de biblioteca.

Solicitação da Comunicação



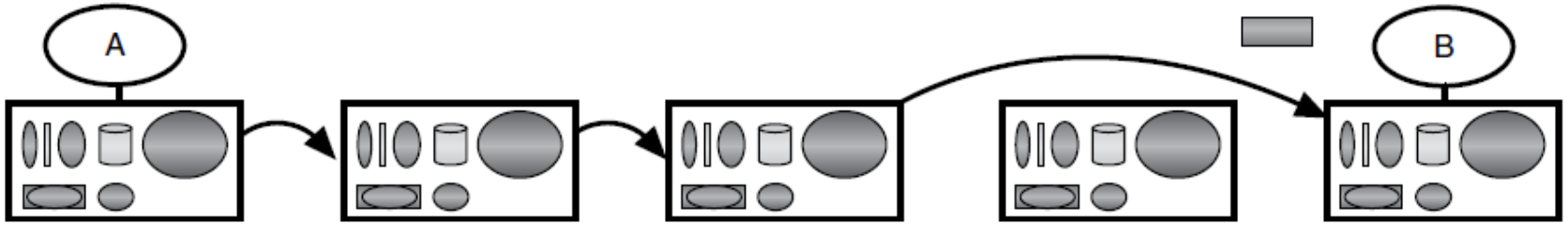
- Suponhamos que o AP, **A**, queria estabelecer uma conexão IPC com o AP **B**,
  - e que **A** resida em um sistema de processamento que use um DIF representado pelo processo IPC, **a**.
- **A** gera um pedido de Alocação que levará o gerenciamento do IPC de **a** a avaliar o pedido de acordo com as suas políticas de alocação.

Solicitação da Comunicação



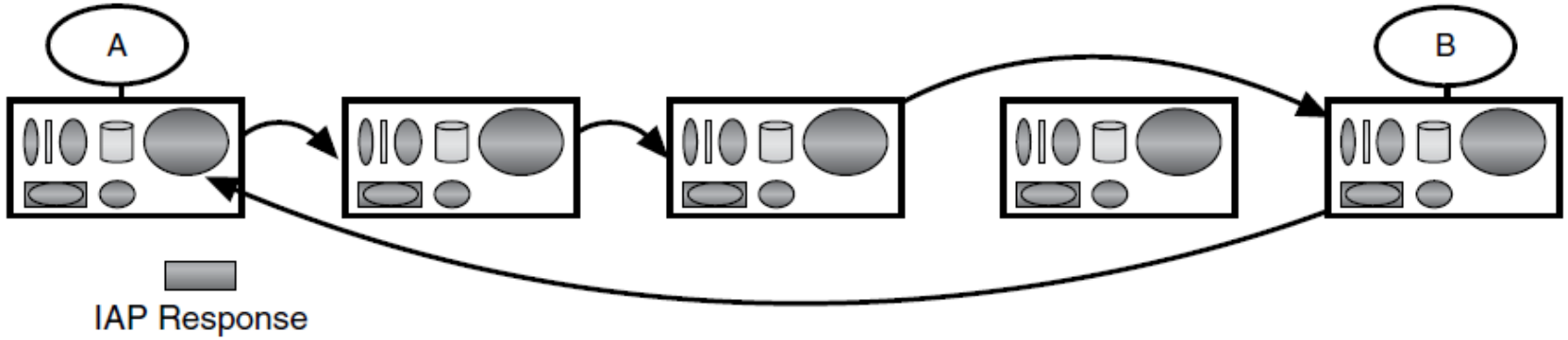
- A solicitação do IAP conterá:
  - Nome do processo de aplicação de **A**
  - Endereço de **a**, **a-addr**
  - A identificação da porta local, **a_i-port**
  - O nome do processo de aplicação **B**
  - Informações de controle e de capacitações para **A**
  - Políticas propostas para a conexão

Estabelecimento da Comunicação



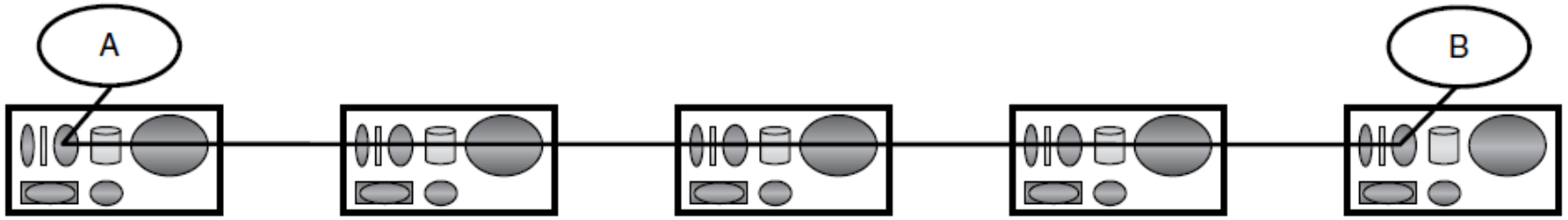
- Quando uma entrada na cache é encontrada, a solicitação IAP é encaminhada para **b** para confirmar se ele tem acesso a **B** e para determinar se **A** tem acesso a ele.

Estabelecimento da Comunicação



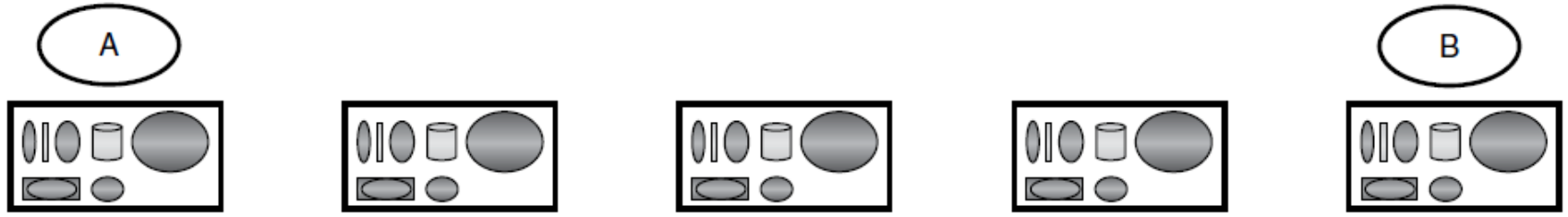
- Envio da resposta do IAP indicando sucesso e a identificação da porta alocada à comunicação com **b**.
- Os processos IPC **a** e **b** possuem agora as informações necessárias para criar um fluxo apropriado EFCP entre **a** e **b** para a sua comunicação.

Comunicação entre A e B



- É criado o fluxo/conexão EFCP e associado aos identificadores de porta retornados a **A** e **B.**
- As aplicações agora estão livres para trocar as SDUs.

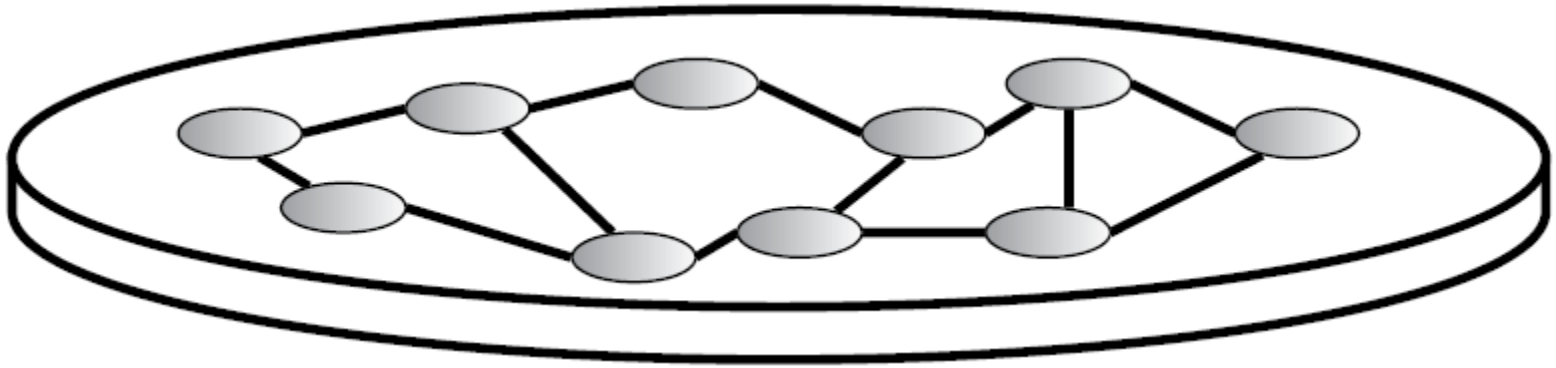
Dissociação



- Quando as aplicações tiverem terminado, as associações serão também terminadas.
- A terminação também do fluxo EFCP é uma questão de política
  - Com um protocolo EFCP baseado em temporização, esta questão se torna irrelevante.

Identificadores em um (N)-DIF

(N)-DIF



- Trocando informações sobre conectividade e uso e alocação de recursos, os processos IPC que constituem a camada criam uma aplicação distribuída.
- Os endereços-(N) precisam apenas ser conhecidos entre os processos IPC.
- Os nomes das aplicações são externamente visíveis à camada, enquanto que os endereços-(N) não.

Identificadores

- Identificadores Externos:
  1. Os nomes de aplicações distribuídas que designam um conjunto de APs que cooperam para executar uma tarefa particular.
  2. Nomes de APs para identificar os APs
  3. Os nomes das APMs que identificam as máquinas de protocolos (PMs) de aplicação, que são não ambíguos dentro do AP.
- Identificador interno ao sistema de processamento: port-id
- Identificadores Internos ao DIF:
  1. Os endereços-(N) alocados para os processos IPC
  2. A identificação de conexão usada no EFCP para distinguir as conexões.

O (N)-Port-ID

- O DIF requer identificadores para distinguir entre múltiplos fluxos IPC.
- Os APs precisa deles para a mesma finalidade.
- Quando a conexão é estabelecida, o APM e o DIF usa o port-id ao se referir à comunicação.
  - Os port-ids são distintos para cada sistema de processamento.
- Quando o protocolo IPC cria um estado compartilhado com o seu correspondente, a conexão é identificada por um conexão-id.
  - O conexão-id é geralmente formado pela concatenação dos port-ids da origem e do destino.

O (N)-Port-ID

- Os port-ids desempenham um papel crucial na ligação entre endereços-(N) e endereços-(N-1) em camadas adjacentes
  - Isolando ao mesmo tempo os endereços-(N) tanto dos nomes dos APs como dos endereços-(N+1).
- O único identificador que um AP tem associado com um fluxo é o port-id e o nome da aplicação de destino.
  - Ele não tem conhecimento do port-id do destino ou dos endereços-(N).

Nomes de Processos de Aplicação

- Os nomes dos processos de aplicação são usados por um novo sistema para estabelecer a comunicação inicial ao se unir ao DIF.
- É possível (e até útil) ter mais do que um DIF nos mesmos sistemas ou conjunto de sistemas.
  - Quando há mais do que um DIF em um sistema e um novo sistema quer se unir à camada ele deve conhecer a qual DIF está se unindo (ou seja, ele deve ter o seu nome de aplicação distribuída, ou DAN).
  - O DAN é usado para estabelecer a comunicação com o DIF usando o (N-1)-DIF.

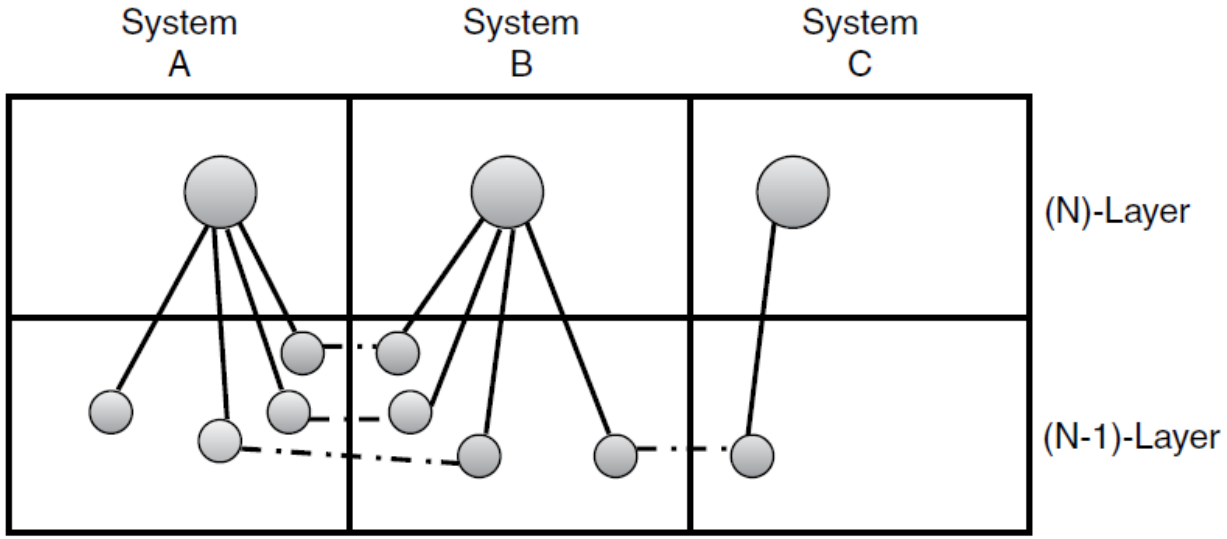
IDD – *Inter-DIF-Directory*

- Provê o mapeamento entre nomes de processos de aplicação e DIF(s) que suportam o processo de aplicação solicitado.
- Usado quando o IRM falha em encontrar a aplicação solicitada em qualquer dos DIFs disponíveis a ela.
  - Encontra um DIF que suporte a aplicação desejada.

Endereços-(N)

- Os nomes usados para o roteamento de PDUs não são apenas os nomes dos processos IPC mas são identificadores *internos* ao DIF formado pela coleção de processos IPC.
- A função de roteamento do IPC requer dois tipos de informação:
  1. Informação sobre o grafo dos RMTs (endereços dos nós nos termos de Saltzer) formado pela conexão direta pelos (N-1)-DIFs
  2. O mapeamento de endereços-(N) para os nomes dos processos IPC-(N-1) para todos os vizinhos mais próximos no (N-1)-DIF.

Rotas



- Rotas são sequências de endereços-(N)
- A próxima etapa é um endereço-(N).
- Mas cada processo IPC deve também conhecer os mapeamentos de endereços-(N) para (nome)endereço-(N-1) do vizinho mais próximo de camada-(N) para determinar o caminho para a próxima etapa.

Comparação com a Internet

- Na Internet o que temos mais próximo de um nome de processo de aplicação é a URL.
  - A sintaxe da URL permite especificar um protocolo de aplicação e o host no qual ela reside.
  - A parte do host se tornou essencialmente o nome da aplicação.
  - Não está claro como alguém poderia construir uma aplicação com múltiplos protocolos de aplicação.
- Se houver um protocolo especial para o meu projeto, deveria ser registrado com a IANA.
- Não há suporte para conectar a múltiplas instâncias específicas nem de APs nem de protocolos de aplicação associados com APs específicos.

Comparação com a Internet

- Há apenas um equivalente parcial do protocolo de acesso IPC:
  - O DNS permite que a *aplicação* determine o endereço da aplicação de destino.
  - Isto coloca mais peso na aplicação e também representa um problema de segurança:
    - Não há controle de acesso e
    - A aplicação tem conhecimento do endereço

Comparação com a Internet

- A Internet é baseada em um modelo de "tamanho único" ou talvez dois tamanhos: UDP e TCP.
  - No entanto, isto parece estar se ampliando com a adição de RTP, SCTP, DCCP e outros.
    - Isto contribui consideravelmente com a complexidade da arquitetura.
    - E a impossibilidade de casar estes EFCPs com a alocação de recursos associada ao IP aumenta os problemas.

Comparação com a Internet

- Na arquitetura Internet atual, há apenas endereços de pontos de conexão.
  - Portanto, as rotas são calculadas como uma sequência de endereços-(N-1)
  - É, portanto, difícil acomodar múltiplos caminhos entre nós adjacentes
  - Multihoming e Mobilidade não podem ser suportados sem a inclusão de mecanismos caros e complicados.

Recursos IPC

Estruturas IPC

- Um DIF sempre interfaceia um (N-1)-DIF ou o meio físico.
- Em geral cada DIF interfaceia m (N-1)-DIFs, porque o escopo do IPC tende a crescer em níveis mais altos.
- Para um DIF, uma solicitação pode conter um nome AP ou um endereço-(N+1).
- O DIF é responsável por conhecer que aplicações estão disponíveis para quem, no seu sistema.

Estruturas IPC

- No registro, um DIF pode ser autenticado junto ao (N-1)-DIF.
  - É assim que o (N-1)-DIF sabe que o AP que está solicitando serviço é também parte de um recurso IPC.
- O (N-1)-DIF encontra-se numa posição privilegiada para proteger-se porque ele pode sempre recusar solicitações do DIF.

Múltiplos (N)-DIFs do mesmo Nível

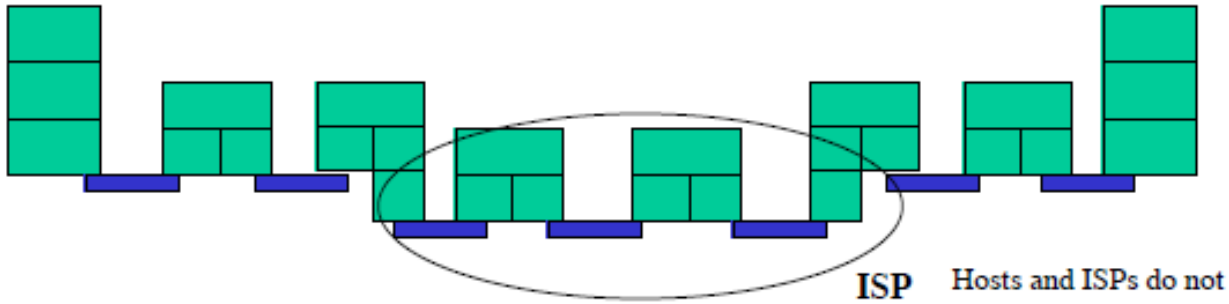
- No caso de um meio físico TDM, poderíamos ter um processo IPC separado para cada um dos canais.
  - Portanto, o número de processos IPC possíveis neste caso estaria entre um e o número de canais.
- Há duas formas que o DIF mais baixo pode assumir:
  - Um meio ponto a ponto, que terá um EFCP, mas não terá uma RMT
  - Um meio multiacesso, que precisará de políticas para a RMT e para o EFCP determinadas pelos erros.

Múltiplos (N)-DIFs do mesmo Nível

- Nas camadas acima, o mesmo princípio se aplica e podem haver um ou mais DIFs.
  - Acima da primeira camada, a criação de DIFs irá basicamente criar redes distintas e separadas.
- Em configurações comuns teríamos:
  - Um (N-1)-DIF por interface e um (N)-DIF por sistema.
  - Acima destes, (N+1)-DIFs podem ser criados como redes fechadas.

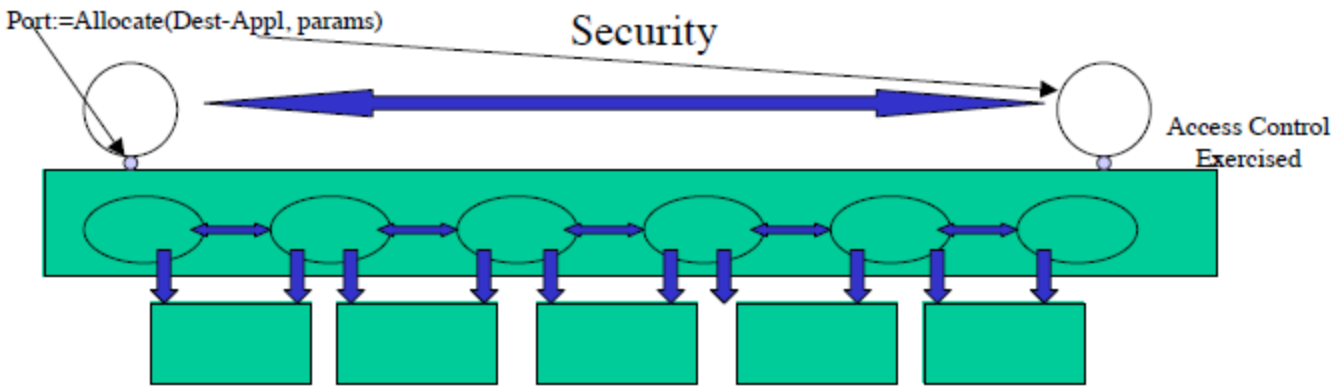
Implicações para Segurança

- Segurança através de isolamento
- Os hosts não podem endereçar nenhum elemento do ISP
- Nenhum hacker pode comprometer os ativos dos ISPs
  - A menos que o ISP esteja fisicamente comprometido.



Implicações para a Segurança

- Vamos assumir inicialmente que as únicas aplicações existentes sejam ameaças e não outros processos IPC.
- A única informação relacionada ao IPC a que a aplicação tem acesso é o nome da aplicação destino e a port-id local.
- A aplicação não tem acesso aos endereços ou port-ids do destino.



Implicações para a Segurança

- Os mecanismos de controle de acesso do IAP têm limitações:
  - O máximo que pode ser garantido é que o DIF está fornecendo acesso a uma aplicação que ele acredita ser a aplicação que está sendo solicitada.
  - É então responsabilidade da aplicação solicitante determinar se esta é mesmo a aplicação solicitada.

Implicações para a Segurança

- O grau de confiança que um (N)-DIF pode colocar em um (N-1)-DIF pode ser caracterizado da seguinte forma:
  - Um (N)-DIF pode apenas assumir que o (N-1)-DIF tentará entregar PDUs a algo e poderá copiá-las ou modificá-las no processo.
  - Se o (N)-DIF não confia no (N-1)-DIF, deve invocar a proteção apropriada de PDU e mecanismos de autenticação.
  - Se as aplicações que usam o (N)-DIF confiam no (N-1)-DIF menos do que o (N)-DIF, isto é sua responsabilidade.

Implicações para a Segurança

- Vamos assumir que um processo IPC comprometido entrou em um DIF
  - Passou informações de autenticação e se tornou um membro do DIF.
- Qual o dano que ele pode causar? Algum
  - A menos que as políticas do DIF sejam muito frouxas, sempre será possível encontrar o ofensor e terminar a sua participação.
  - Se for usado um EFCP baseado em temporização, não serão possíveis ataques de SYN.
  - Não há soquetes bem conhecidos para serem atacados.
  - Muitos nomes de aplicações podem não ser registrados em nenhum RIB.
  - Em geral, as ameaças são no máximo iguais às das arquiteturas atuais.

Implicações para a Segurança

- A natureza da recursão dos DIFs é tal que qualquer sistema terá acesso a informações de gerenciamento apenas nos DIFs (N+1), (N) e (N-1) que ele implementa.
- O (N-1)-DIF terá um escopo menor, e portanto a informação disponível para o sistema terá menos utilidade.
- A única informação-(N+1) disponível serão os nomes das aplicações disponíveis para o (N)-DIF.
- A maior ameaça que um sistema comprometido poderá fazer é distribuir más informações de alocação de recursos e informação de roteamento com seus parceiros.

Implicações para a Segurança

- Um aspecto sobre o qual este modelo não tem nenhum efeito é sobre os ataques de vírus perpetrada por aplicações de comunicação.
- Comprometimentos baseados em fragilidades no software de aplicação ou no sistema operacional local não podem ser resolvidos por este modelo.
- Apesar de que autenticações mais fortes de IPC possam ajudar, não irão prevenir estes comprometimentos.