Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

WAAS Design and Deployment

BRKARC-2661

TOMORROW starts here.

Abstract

This session will show how to deploy WAAS into the network, covering design topologies and network interception techniques from the traditional Inline and WCCP to vPath and the latest award winning AppNav technology .

Updates on the latest application optimisers for secure protocols and VDI display protocols will also be covered to provide attendees with a comprehensive view of how WAAS can successfully be deployed in their own environments.

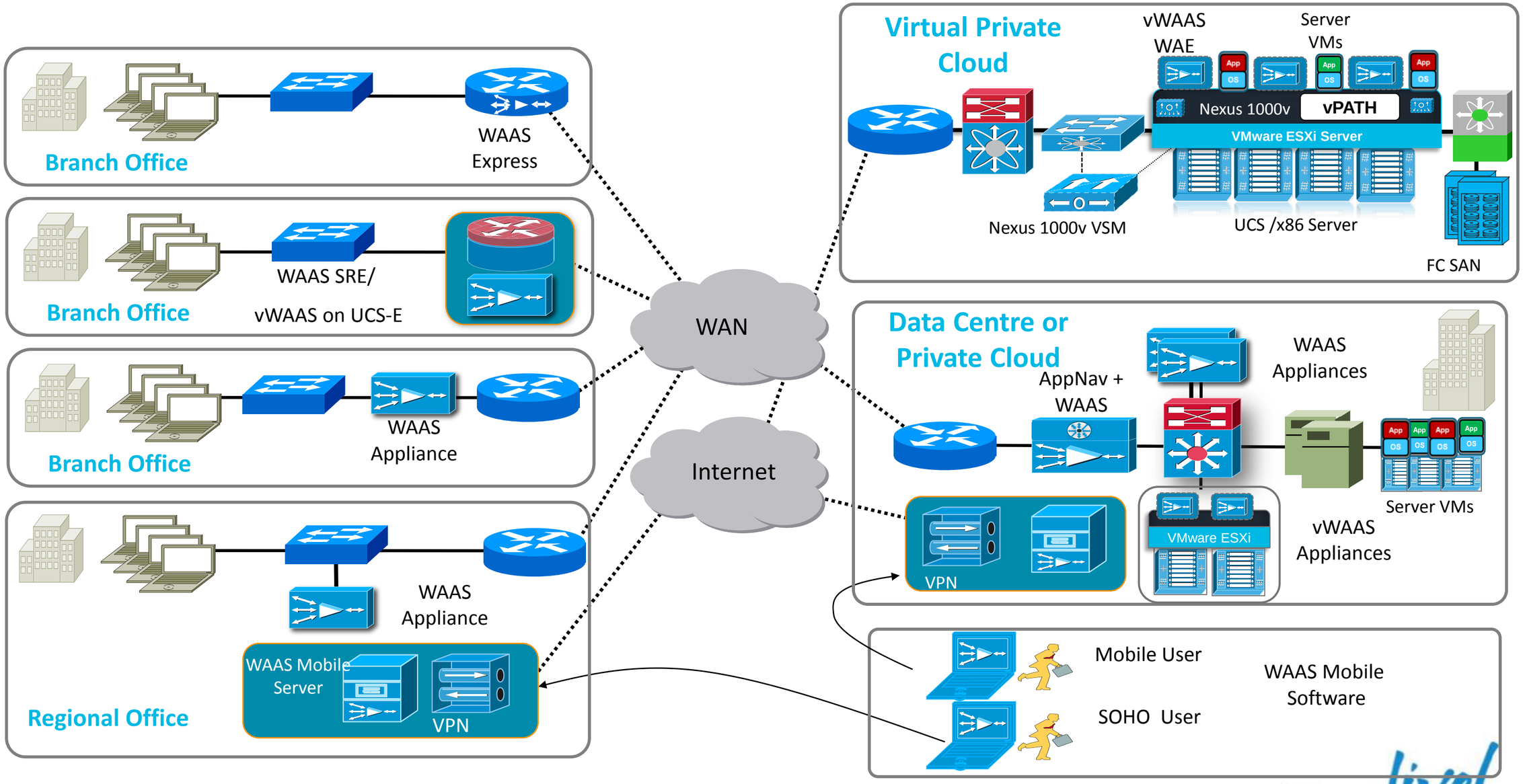
Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & complete the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions
- Please remember this is a 'non-smoking' venue!
- Please switch off your mobile phones
- Please make use of the recycling bins provided
- Please remember to wear your badge at all times

Agenda

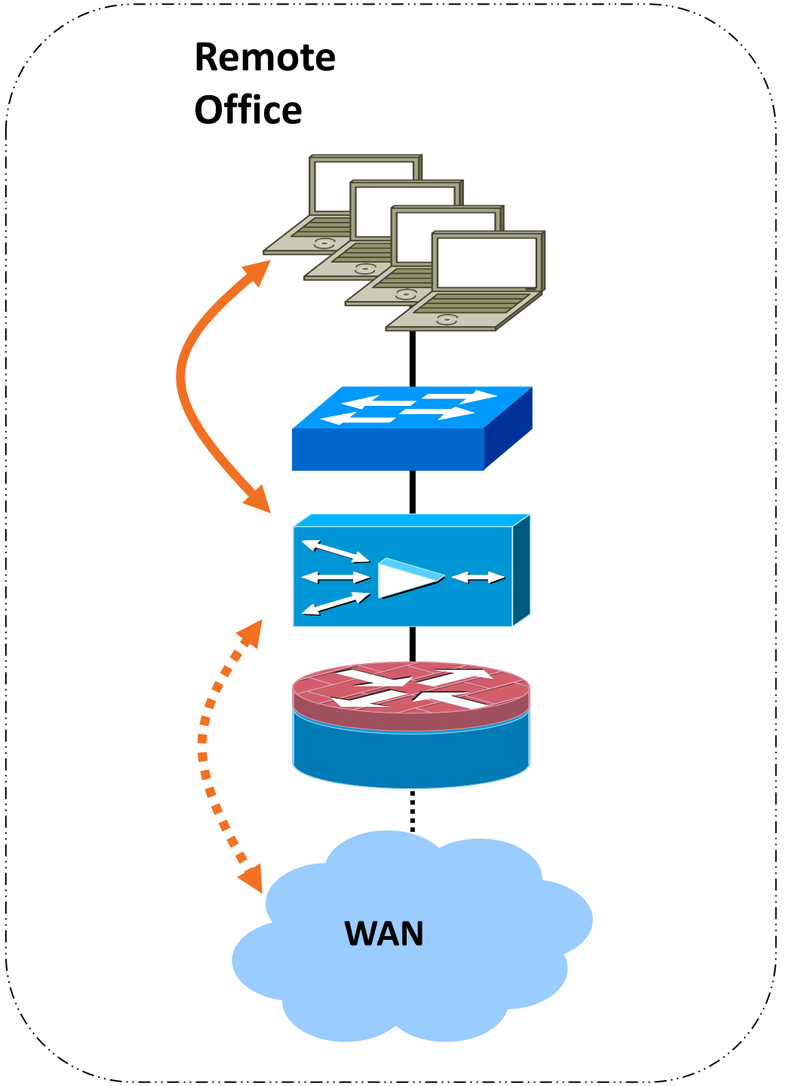
- WAAS Deployments Overview
  - In-Path, WCCP, vPath, AppNav
- Product Update
  - WAAS 5.1
  - Auto Deployments
  - Citrix Optimisation
- Citrix Optimisation Deployments Best Practices
- AppNav Overview
- AppNav Design Considerations

Cisco WAAS: WAN optimisation deployment



Simple Transparent In-path Deployment

- ✓Plug-and-Play
  - No network changes
  - Mechanical fail-to-wire
- ✓Scalability and High Availability
  - Up to 2
  - Redundant network paths & asymmetry
  - Load-sharing and fail-over
- ✓Transparent Integration
  - Transparency and auto discovery
  - 802.1q VLAN trunking
  - All WAE appliances
  - Interception access list



Network-Integrated Off-path Interception

WCCPv2

- Active/active clustering
- Load redistribution
- Fail-over
- Fail-through operation
- Near-linear scalability & performance

WCCP variable timer

✓ Configurable timeout (9,15,30 Sec)

✓ default = 30 Sec (same as pre WAAS 4.4)

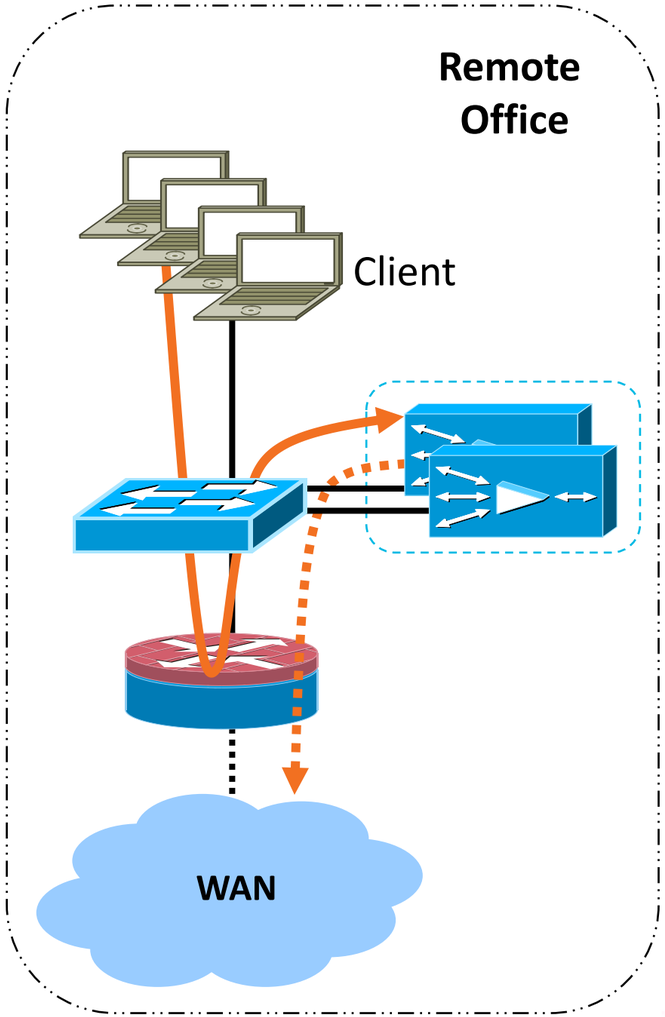
WCCP L2 Egress

✓ L2 Egress, WAAS remembers the source Router for every flow

✓ WAAS **ensures** as traffic leaves, it returns to the original router.

Policy Based Routing

- Cisco WAE as a next-hop router
- Active/passive clustering

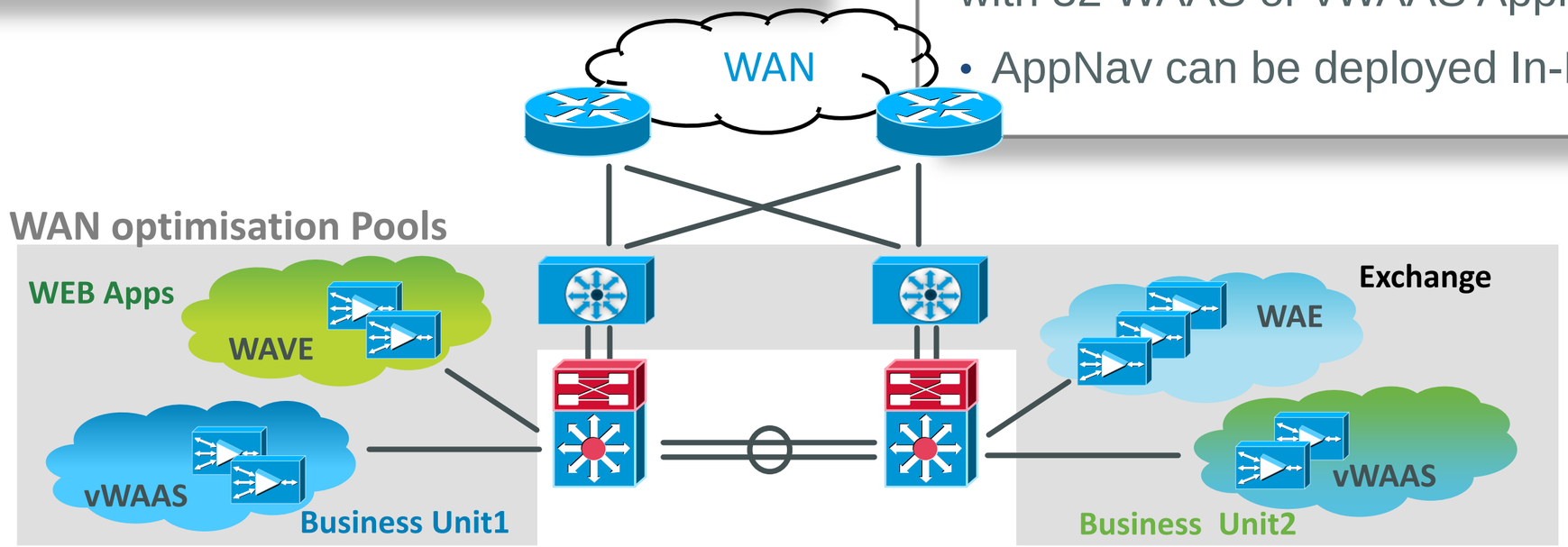


Cisco AppNav

AppNav gives the ability to ***Virtualise*** WAN optimisation resources into ***pools of elastic resources*** with ***business driven bindings***

Benefit

- AppNav IOM contains it's own network hardware, processing data independent of the WAVE Appliance.
- The host appliance for a AppNav module can still be used to optimise traffic.
- AppNav can scale up to 8 AppNav modules, along with 32 WAAS or vWAAS Appliances.
- AppNav can be deployed In-Path and Out-of-Path



AppNav Simplifies Service Insertion Easily Solve Deployment and Scalability Headaches

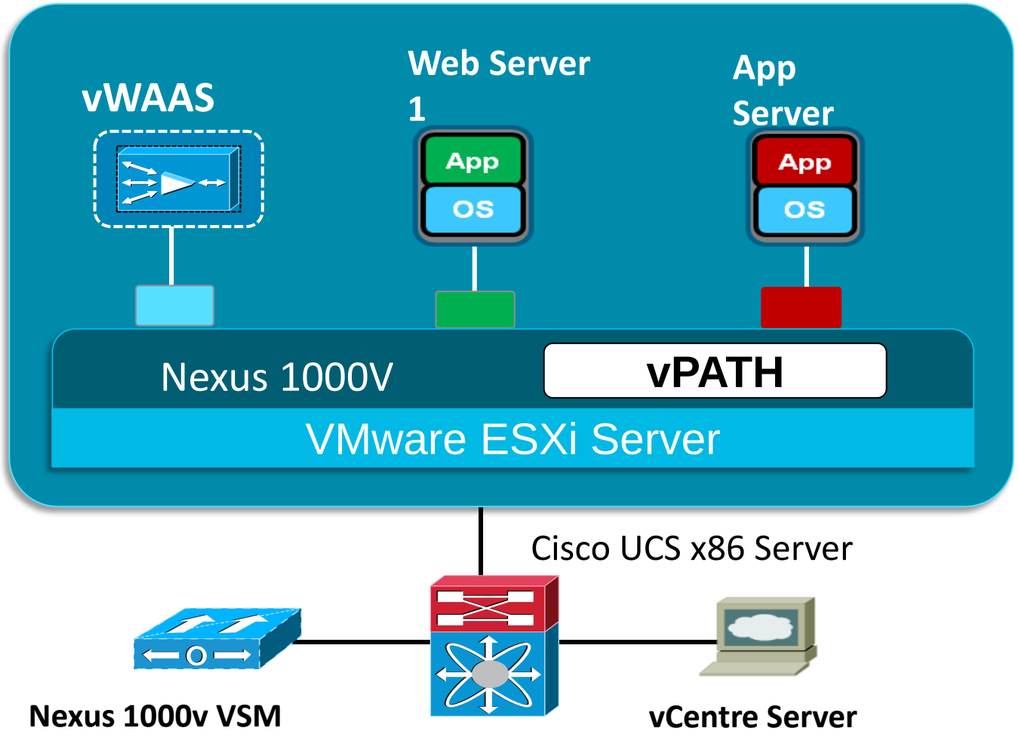
Deployment Consideration	In Path	Off Path	AppNav (In Path)	AppNav (Off Path)
No Cable Insertion Outage	✗	✓	✗	✓
No Router / Switch Code Dependency	✓	✗	✓	✓
No Router / TCAM Impact	✓	✗	✓	✓
Load and performance aware flow distribution	✗	✗	✓	✓
Asymmetric flow support	✓	✓	✓	✓
Inline Modes	Parallel and Serial	N/A	Only Parallel Required	N/A
Ability to scale out / add capacity	Constrained by Inline Device	Constrained by Router TCAM	Constrained by Inline Device	10's of Gbps / Millions of Connections

What is vPATH ?

- Intelligence build into Virtual Ethernet Module (VEM) of N1000V
- vPath has following main functions:
  - Intelligent Traffic interception for vWAAS, VSG & other services
  - Offload the processing of Pass-through traffic from vWAAS
  - ARP based health check
  - Maintain Flow entry table
- vPATH use Mac-in-Mac redirection (L-2 adjacent to vWAAS always)
- VPATH Redirection/Return traffic is sent in N1000V service VLAN
- Management packets will not be VPATH encapsulated.
- TCP MSS Adjusted in vWAAS to account for this overhead

Virtual WAAS: vPATH Interception (Nexus 1000V)

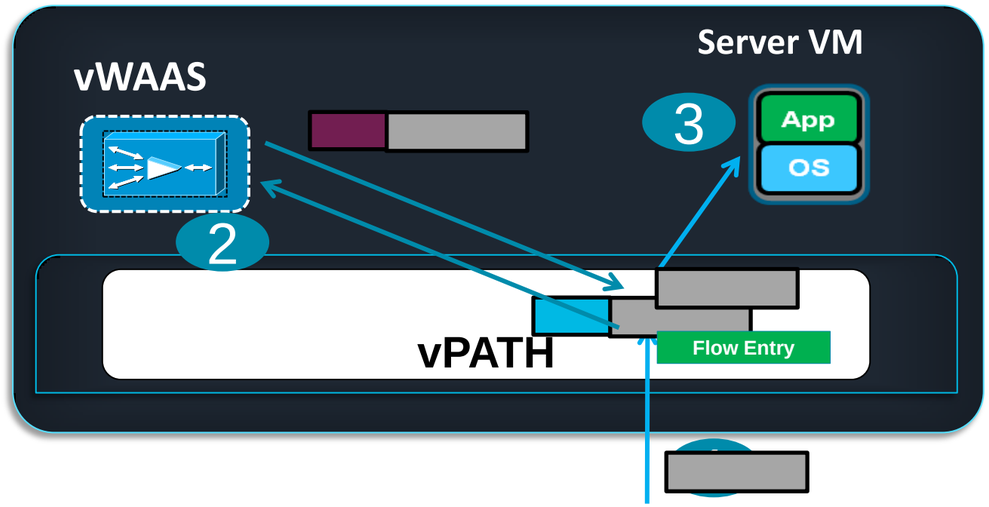
- Interception based on port-profile policy configured in Nexus 1000v
- **Bidirectional Interception** - (no IN/OUT configuration)
- **Pass-through traffic automatic bypass**

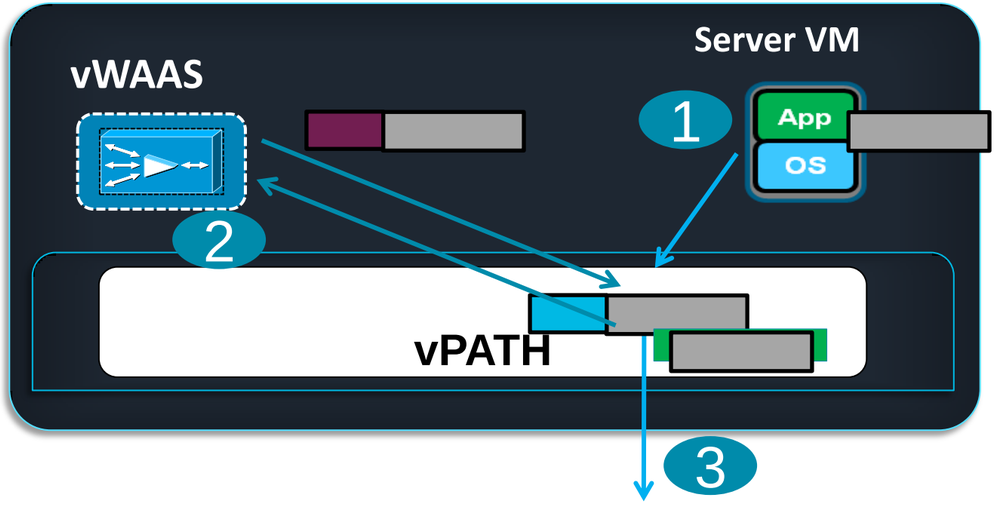


Life of a Packet (with vPATH Interception)

vWAAS's MAC

VEM's MAC





1. When vPATH received first packet from the WAN for optimised port-profile, it will lookup for any flow-entry relevant to the packet
2. vPath doesn't find any flow-entry for the packet. It encapsulated with vWAAS MAC, the packet is forwarded to vWAAS though a MAC-MAC tunnel
3. Upon received the packet from vWAAS, vPath will create a flow-entry (including reverse flow) for the packet and forwards the packet to the normal L2 to Server VM
4. For pass-through traffic vPATH create PT flow entry and don't send subsequent packet to vWAAS after initial TCP SYN/SYN-ACK

Virtual WAAS: On-demand orchestration using policy-based configuration

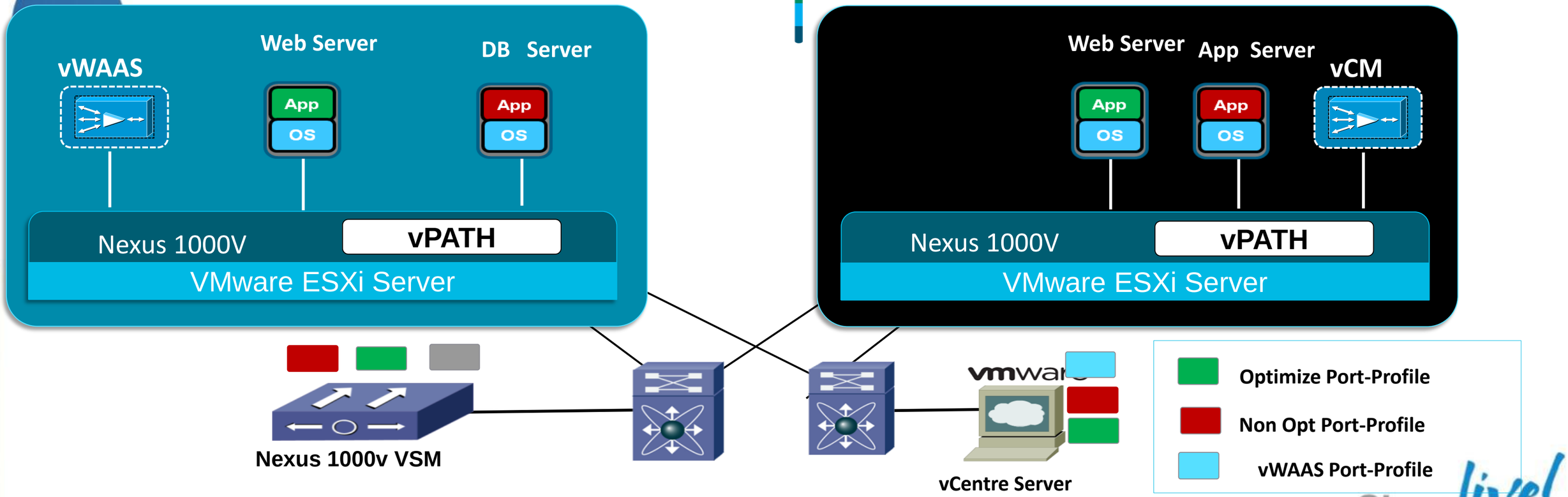
Feature

1. Optimisation based on policy configured in Nexus 1000V

2. Policy gets propagated to vCentre automatically

Benefit

1. Provide on-demand service orchestration in the cloud without network disruption



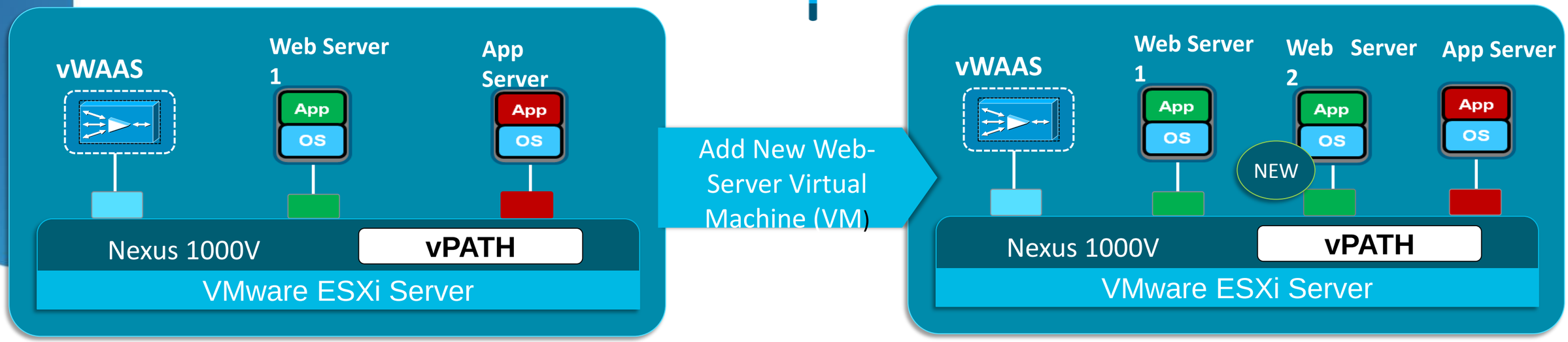
Virtual WAAS: Elastic WAN Optimisation Service

Feature

1. Automatic application of vWAAS service when a new ‘Web Server’ VM gets provisioned
2. vWAAS services associated with ‘Web server’ VMs using Nexus 1000V policies.

Benefit

1. Elastic vWAAS deployment
2. Scale-out Virtual Web Server farm by provisioning additional VMs while applying WAN optimisation



Virtual WAAS: Transparent to server-VM mobility

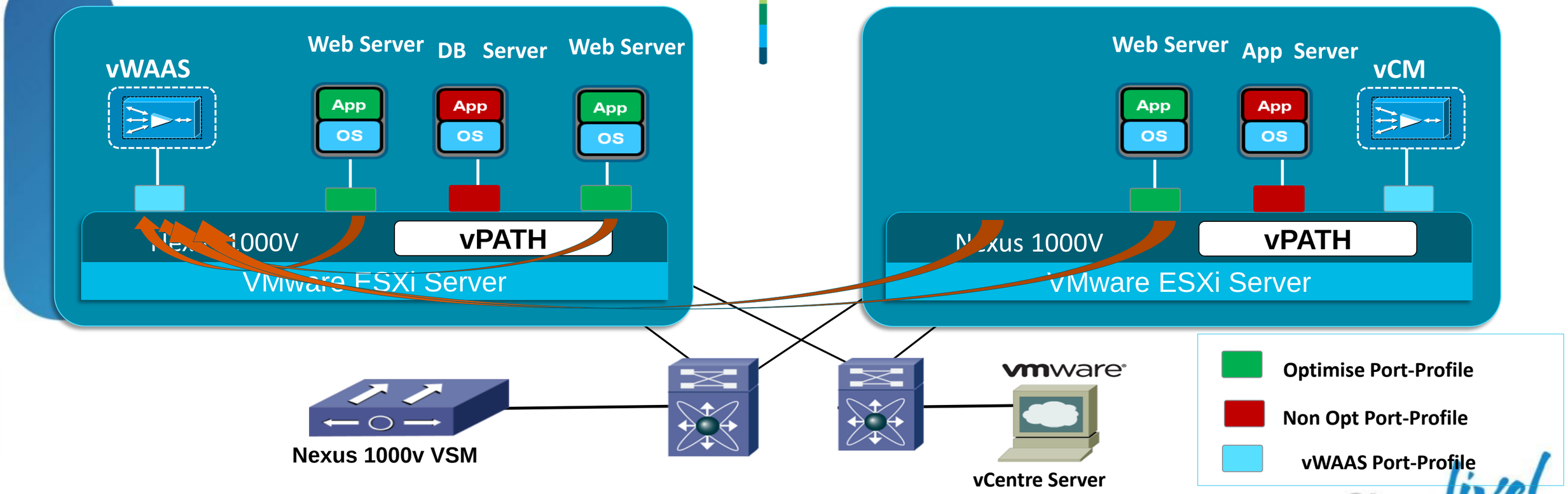
Feature

1. vPATH aware of movement of VM from one host to another.

2. Traffic interception continue to work as-is without any disruption or changes required.

Benefit

1. No disruption in WAN optimisation service if VM moves from one host to another.
2. Support VMware resources scheduling (DRS) and provides High availability



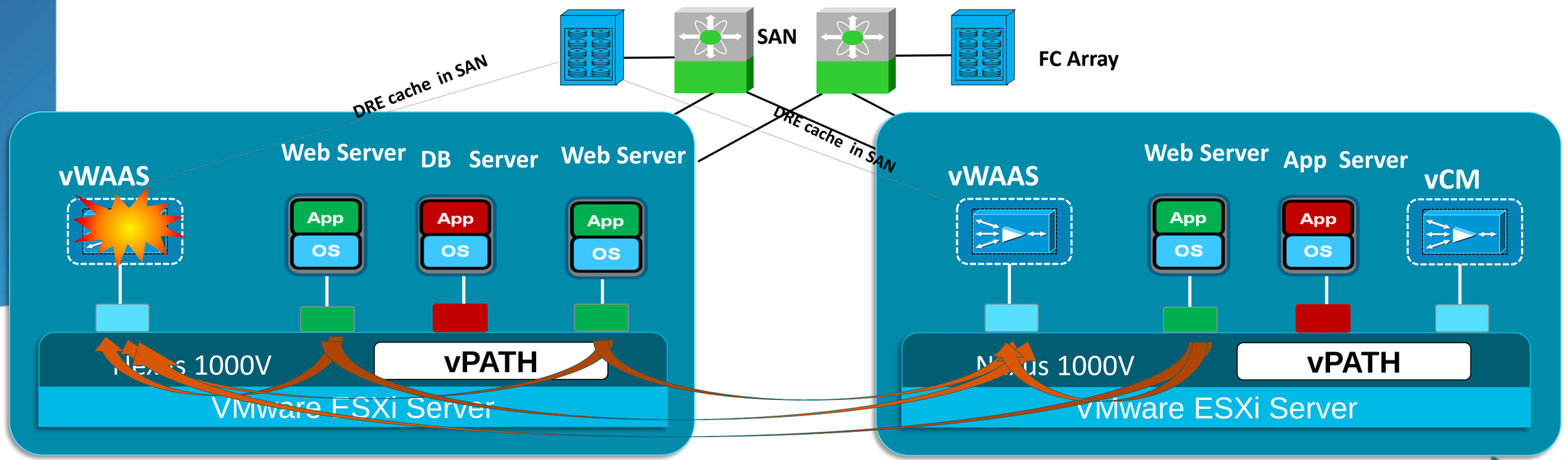
Virtual WAAS: Fault tolerant persistent performance

Feature

1. vWAAS DRE cache can be deployed in SAN
2. VMware HA creates new VM upon failure of vWAAS using same DRE cache storage.

Benefit

1. Ensures cache preservation and high persistent performance in the event of failure
2. Provide uninterrupted compression benefit of WAN optimisation



Agenda

- WAAS Deployments Overview
  - In-Path, WCCP, vPath, AppNav
- Product Update
  - WAAS 5.1
  - Auto Deployments
  - Citrix Optimisation
- Citrix Optimisation Deployments Best Pactices
- AppNav Overview
- AppNav Design Considerations

WAAS 5.1 – New Features

Enhanced Citrix

- MSI Support
- QoS
- Dynamic DSCP Marking
- Improved VDI Performance

Enhanced SharePoint

- Enhanced Acceleration
- Improved User Experience

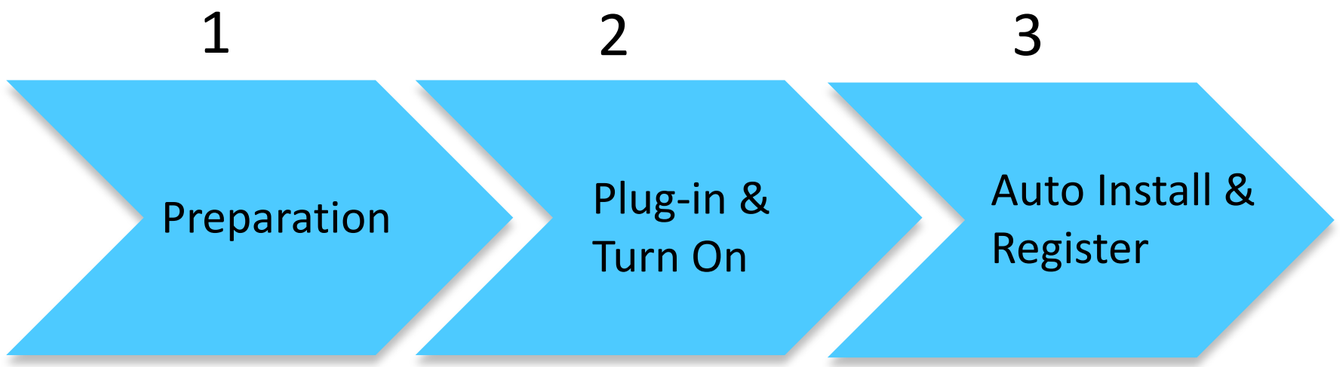
vWAAS

- VM Hypervisor 5.0
- UCS-E Half Slot and Full Slot

Enhanced Auto-Deploy

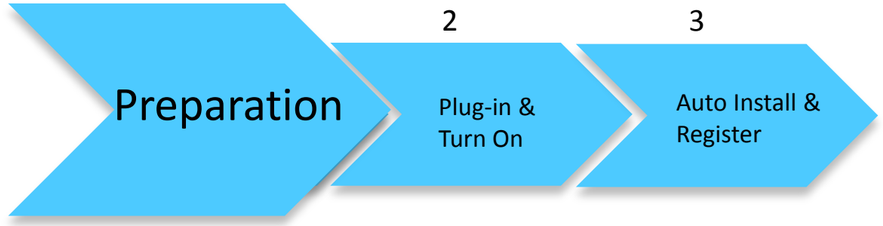
- Automate WAAS installation
- Simplified device configuration

Simple as 1, 2, 3 with Auto Deploy

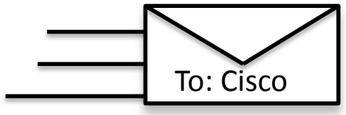


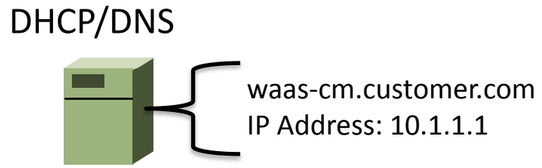
- Auto Deploy is a simple process designed to:
  - Significantly reduce time and OPEX spent at remote sites
  - Enable rapid deployment of WAN Optimisation system

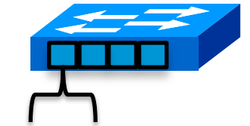
Simple as 1, 2, 3 with Auto Deploy



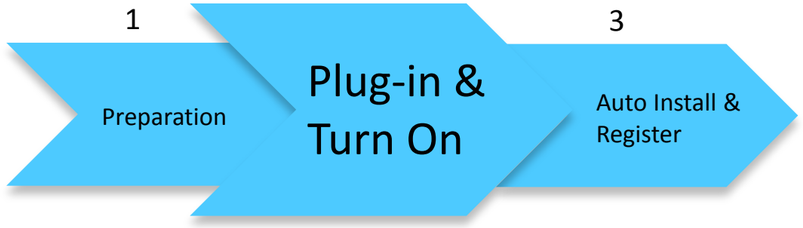
- Order WAAS for remote site
  - Update DHCP & DNS for central manager name
  - Configure switch/router for WAAS device



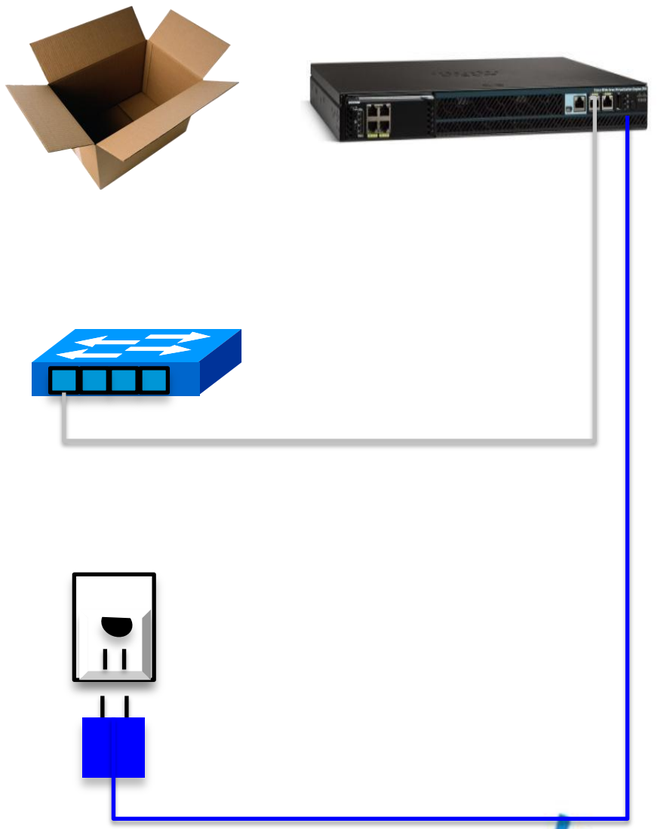




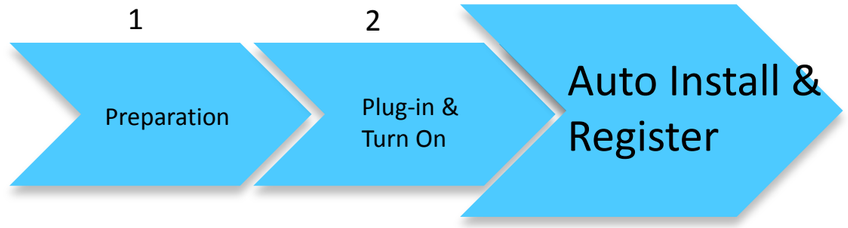
Simple as 1, 2, 3 with Auto Deploy



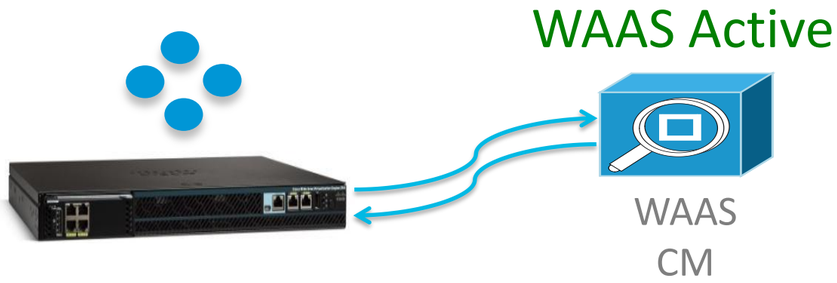
- Unpack the WAAS device and mount
  - Connect WAAS to the network
  - Plug it in and push “ON”



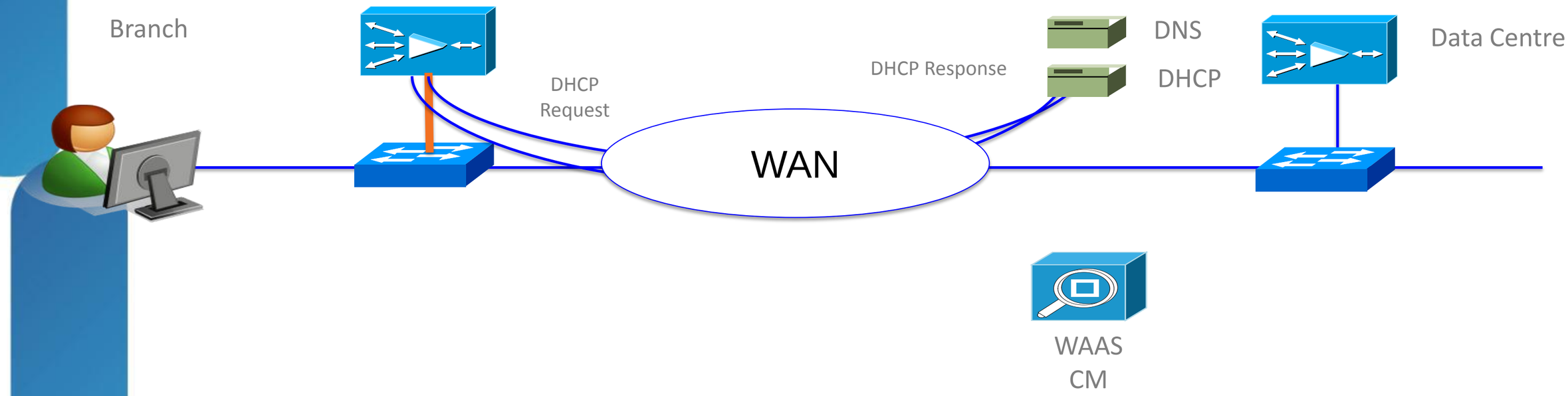
Simple as 1, 2, 3 with Auto Deploy



- WAAS begins auto installation
- Installation process completes
- WAAS registers to the Central Manager

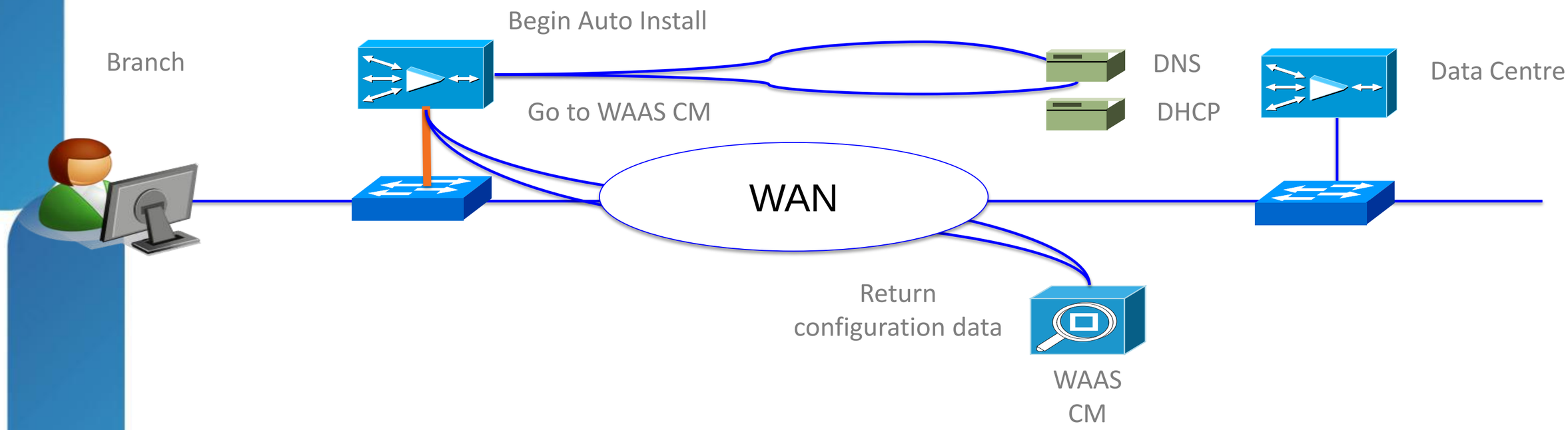


Fast Setup with Auto Deploy



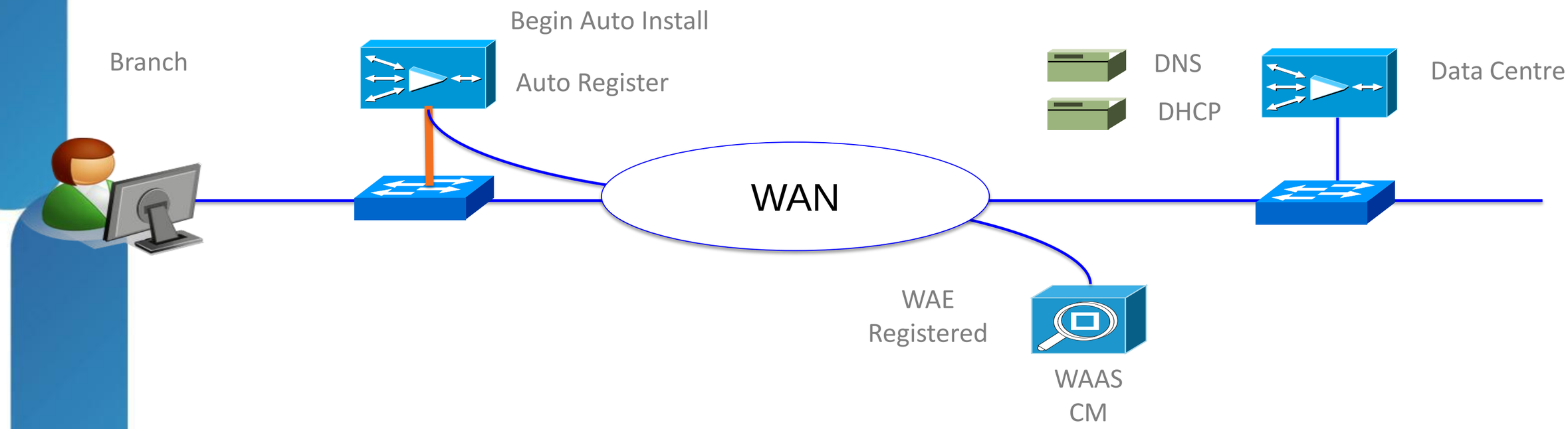
- WAAS Device Shipped to Branch and plugged in
- WAAS Obtains DHCP address upon boot up

Fast Setup with Auto Deploy



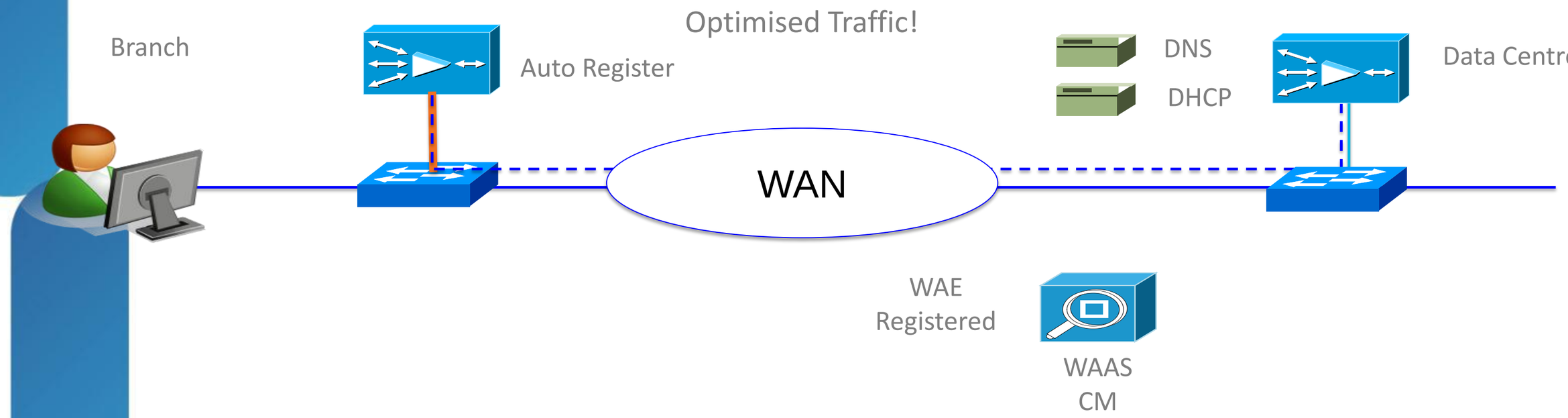
- IP address of CM obtained by DNS
- WAAS device pulls data from CM
- WAAS Auto Installation starts

Fast Setup with Auto Deploy



- WAAS Auto Registers to the WAAS CM

Fast Setup with Auto Deploy



- WAAS auto-discovers other devices and begins optimising traffic

Cisco WAAS Now Optimised for Citrix XenDesktop

Accelerates Citrix HDX Over the WAN

High Quality User Experience

- LAN-like experience
- Improved Application Performance
- HD Quality Video
- Faster Print Jobs

Most Cost-effective

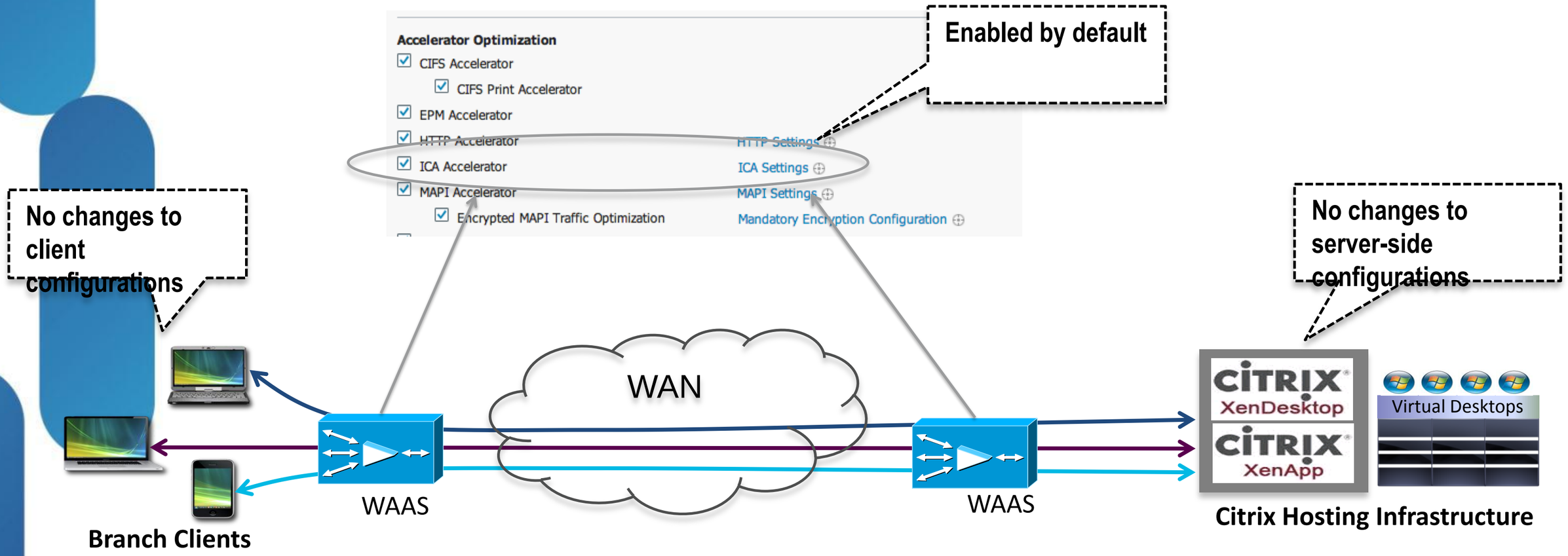
- 2X more users without costly WAN upgrades
- Single solution for virtual and physical desktops
- Industry's most flexible WAN optimisation portfolio

Jointly Supported

- First networking vendor to license ICA/HDX protocol
- Validated & supported by Citrix
- Zero-touch deployment
- Transparent interop with encryption, compression

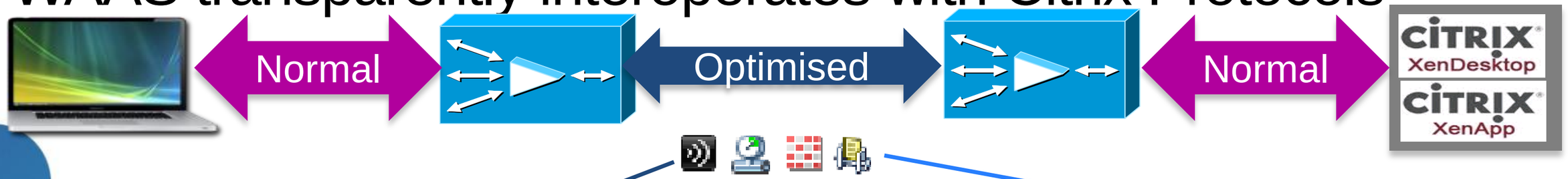
Configuring WAAS for Citrix ICA

Works Out of the Box. No Citrix Modification Required



Understanding the Citrix ICA Handshake with WAAS

WAAS transparently interoperates with Citrix Protocols



WAAS transparently inserts itself into the Citrix communication.

WAAS applies inline compression algorithm over the optimised data, maximising savings

WAAS applies TCP flow optimisation to maximise bandwidth usage and mitigate packet loss.

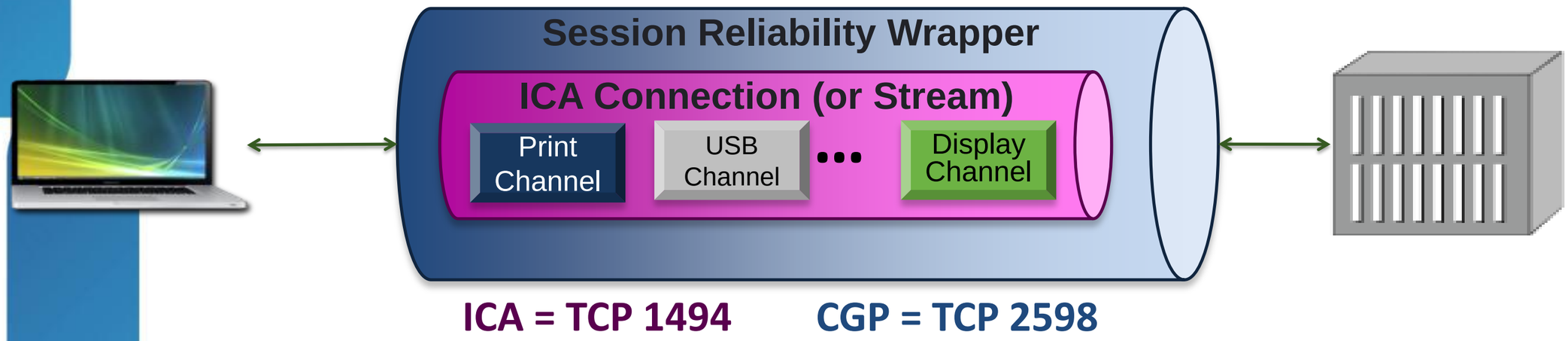
WAAS delivers Citrix Aware Redundancy Elimination that removes redundant data from across **all** end user connections.

Citrix – 5.1 New Feature

- Multi-stream ICA (MSI) Support
- QoS Support for ICA MSI and non-MSI Streams
- Enhanced ICA/CGP Optimisation
- ICA Implemented Admission Control

Session Reliability (aka CGP)

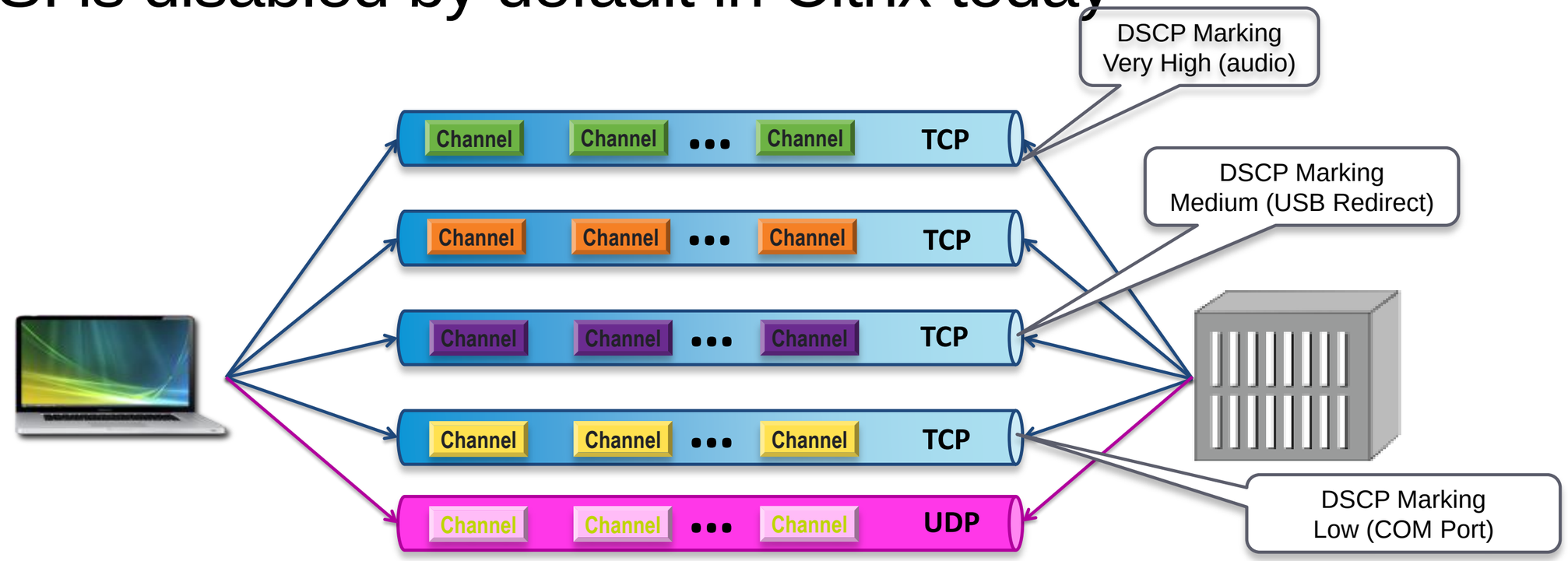
Improves session persistence over the WAN



- Session Reliability encapsulates ICA inside another Citrix protocol called CGP
- This is a “Default” Citrix Setting, Required for Multi-Stream ICA
- WAAS improves CGP over the WAN.

Multi-stream ICA (MSI) Splits a User into 5 Streams

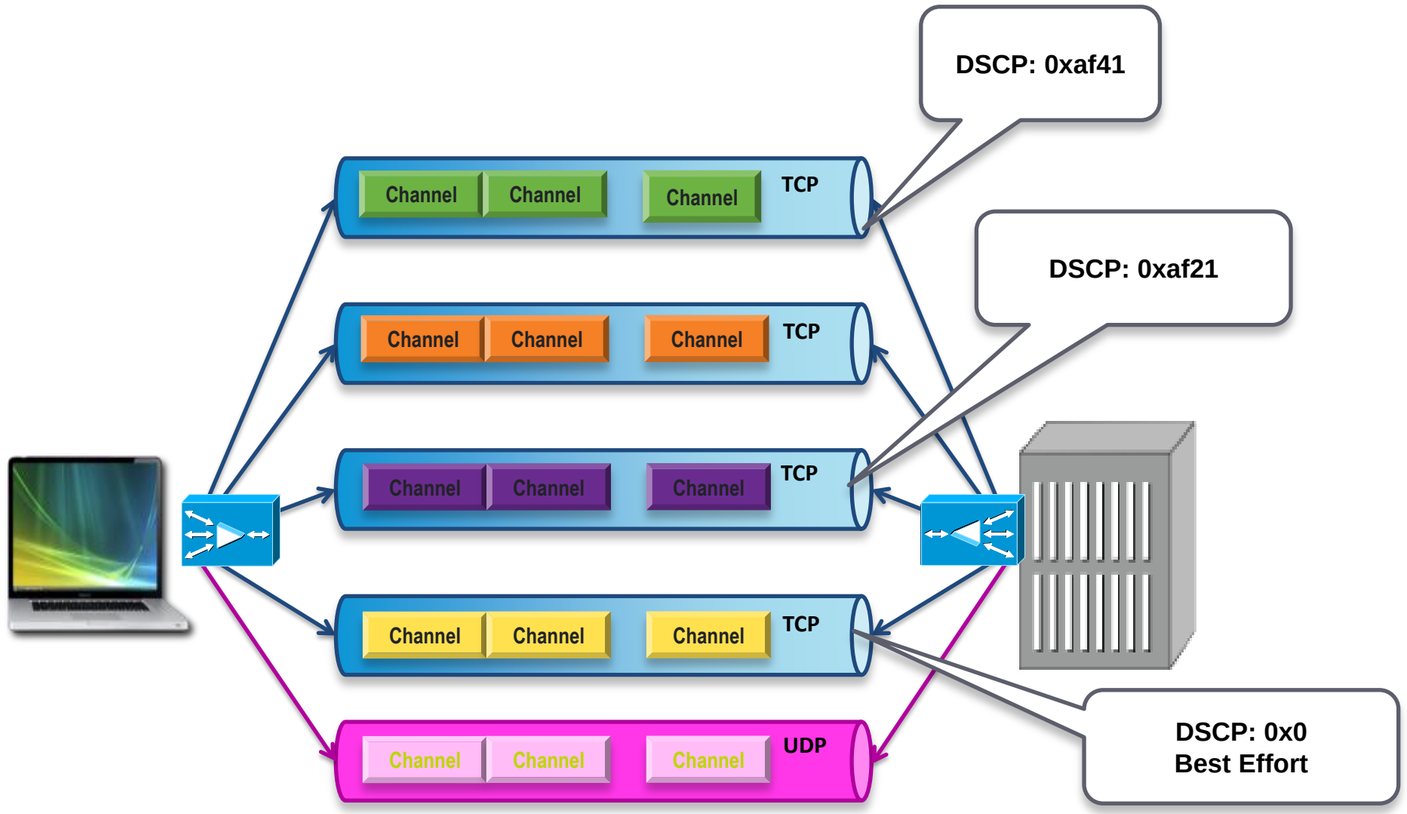
MSI is disabled by default in Citrix today



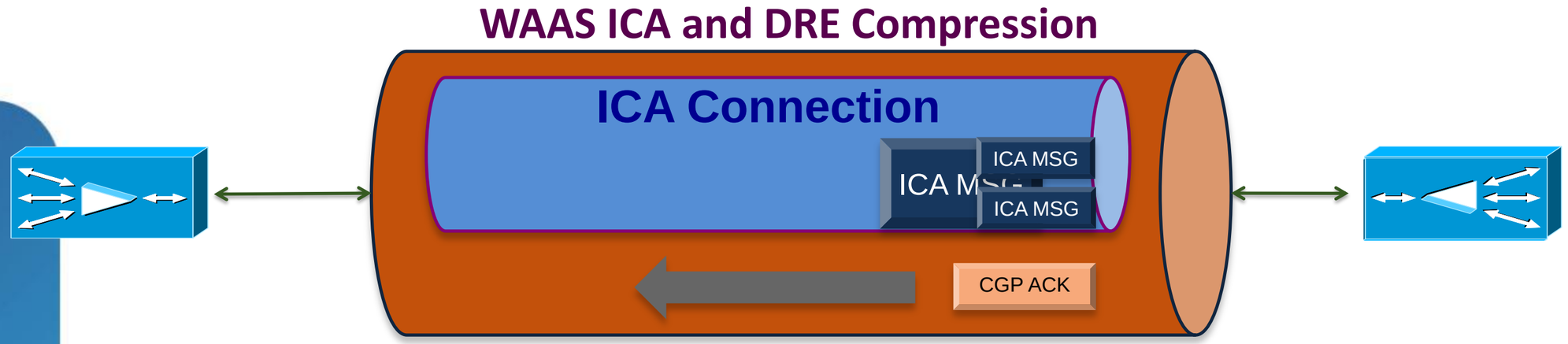
- Enabling Multi-Stream ICA on WAAS automatically enables it through Citrix.
- WAAS automatically optimises channels which use separate TCP connections.
- WAAS can dynamically apply DSCP markings to match Citrix Priorities.

QoS Support for MSI and non-MSI streams

- WAAS can be enabled to implement Differentiated Service Code Point (DSCP) tagging of both MSI and non-MSI ICA and CGP traffic.
- Once enabled, WAAS will interpret the MSI stream type for the TCP connection and enable the appropriate DSCP value.
- The user will be able to enable or disable tagging MSI or non-MSI traffic as well as to define different values for the MSI and non-MSI traffic.



Enhanced Compression and Stream Throughput

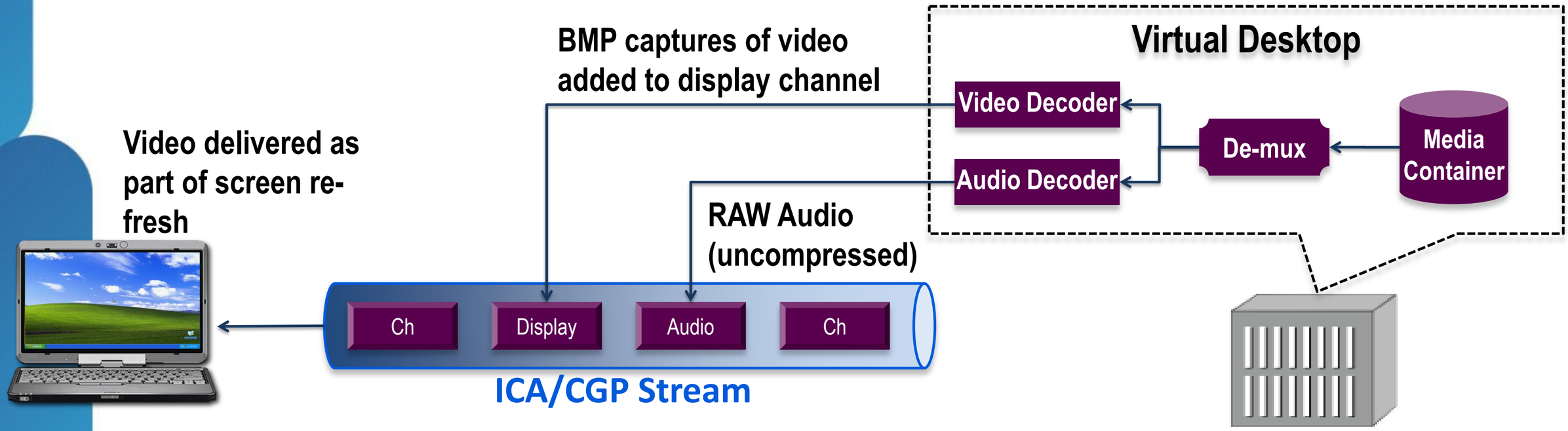


- WAAS 5.1 provides many new enhancements for better compression,
- throughput and capacity
- WAAS further accelerates performance by better processing of CGP ACKs

Agenda

- WAAS Deployments Overview
  - In-Path, WCCP, vPath, AppNav
- Product Update
  - WAAS 5.1
  - Auto Deployments
  - Citrix Optimisation
- Citrix Optimisation Deployments Best Practices
- AppNav Overview
- AppNav Design Considerations

Video for VDI with Server Side Rendering



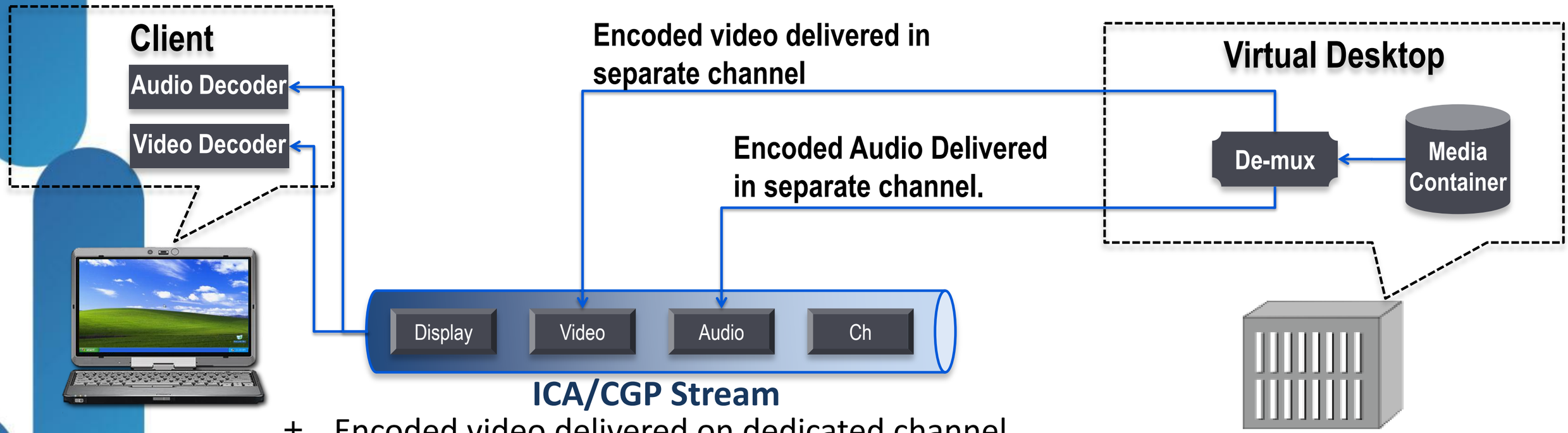
\+ Simplest to configure / no client dependency (Default)

\- Less efficient with BW (~20% or less even with WAN Opt)

\- More susceptible to latency and jitter / poorest user experience

Video for VDI with Client Side Rendering (HDX MS)

Best Practice



+ Encoded video delivered on dedicated channel
+ Improved BW utilisation with WAN Opt
+ Works for all protocols
+ **Default for flash in XD5.5/XApp 6.0**
+ Less sensitive to Latency / Jitter
- Requires client capable of rendering

Summary of Video Options for VDI

WAAS provides benefits for server and client side-rendering

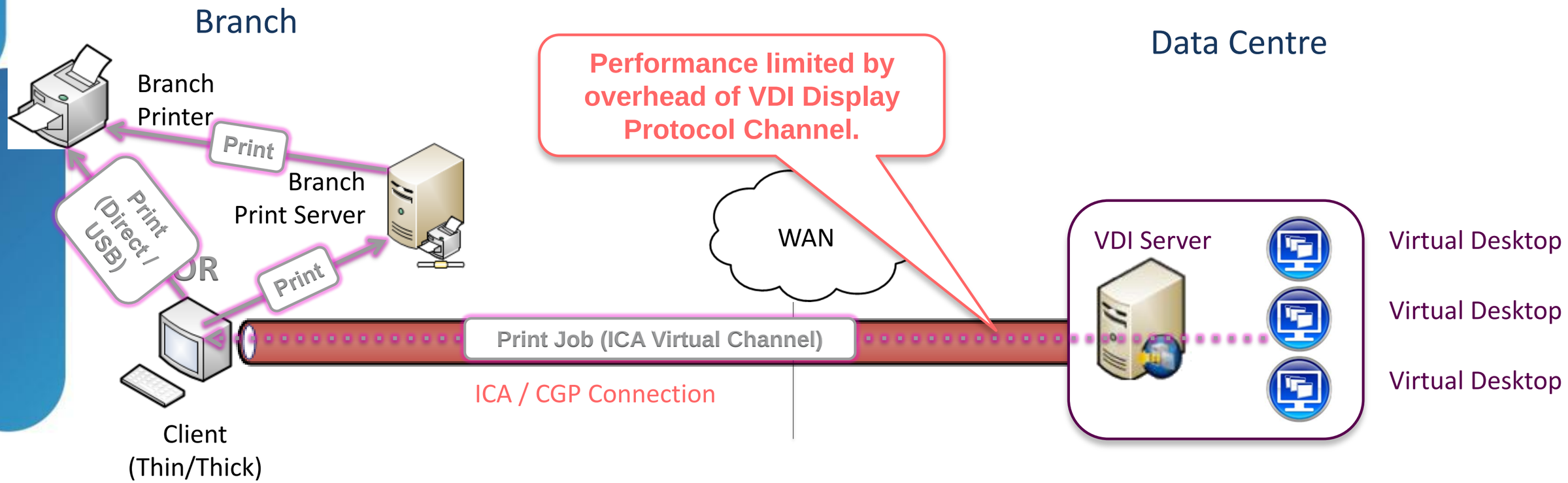
VDI Video over WAN	Without WAAS	With WAAS
Server Side Rendering		
Bandwidth Usage	Bandwidth Hungry	Low reduction (20%-30%)
Client Experience	Very Poor. May not meet user expectations	Moderate improvement
Client Side Rendering		
Bandwidth Usage	Bandwidth Hungry, yet better than server side rendering for the same stream quality	Massive reduction (99%+) for 2nd pass
Client Experience	Better than Server side rendering. May see frames/sec reduction in high latency	Can deliver video to “near HD Quality”

Common Modes for Printing with VDI

Mode	Print Traffic Across the WAN	WAAS Value	Relative Performance
Redirected Print	Channel Within ICA Stream	Optimise as part of ICA	**Lowest**
Direct Print, Centralised Print Server	Separate Print Connection between Print Server and Printer	Optimise Print Connection with TFO/DRE/LZ	**Middle**
Direct Print, Branch Print Server	Separate Print Connection between Virtual Desktop and Printer	Optimise Print Connection with TFO/DRE/LZ and PRINT AO	**Highest**

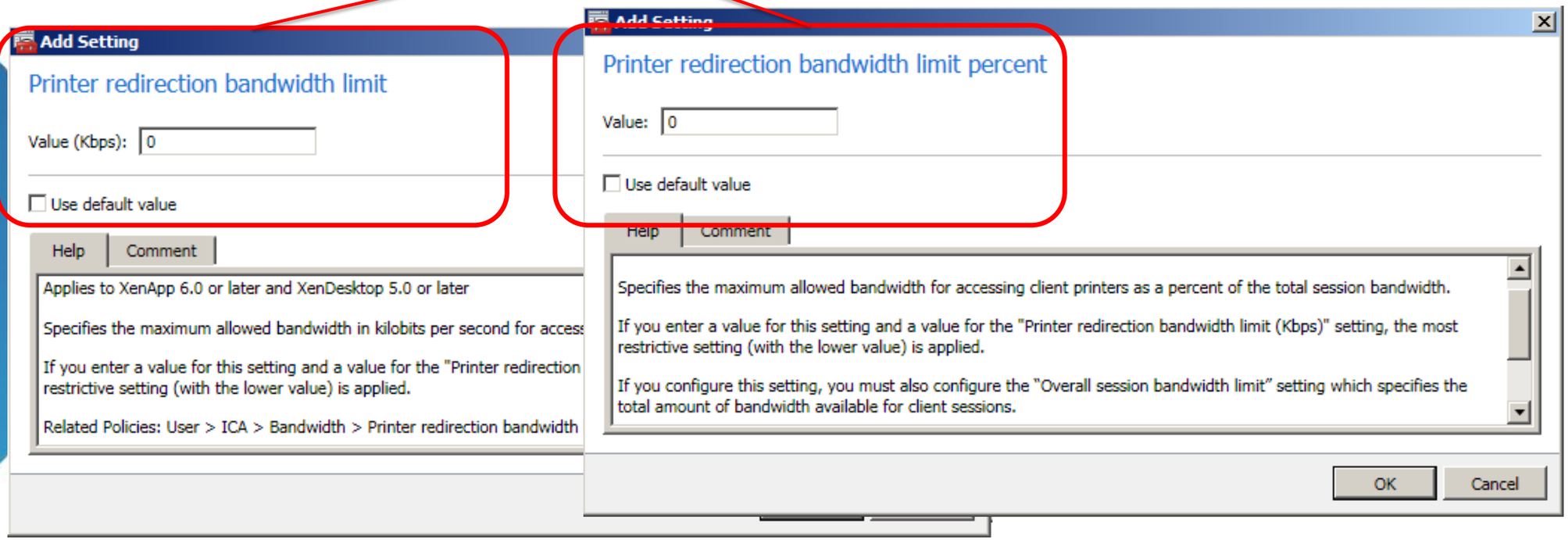
VDI Redirected printing

Default setting. Poorest performance, may impact other apps



Ensure Citrix Printer Bandwidth Limits are Set to Default When Using Redirected Print Mode

Ensure both are set to default of 0

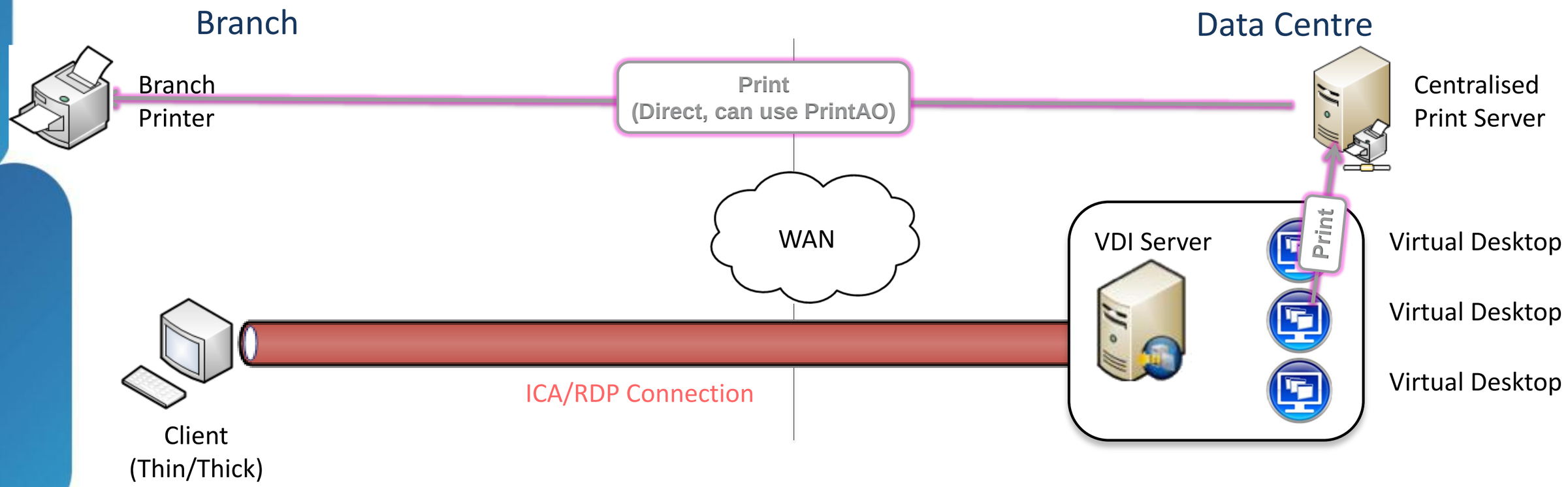


CAUTION

Non-default settings could reduce print performance with WAAS.
Limits will be applied *before* compression

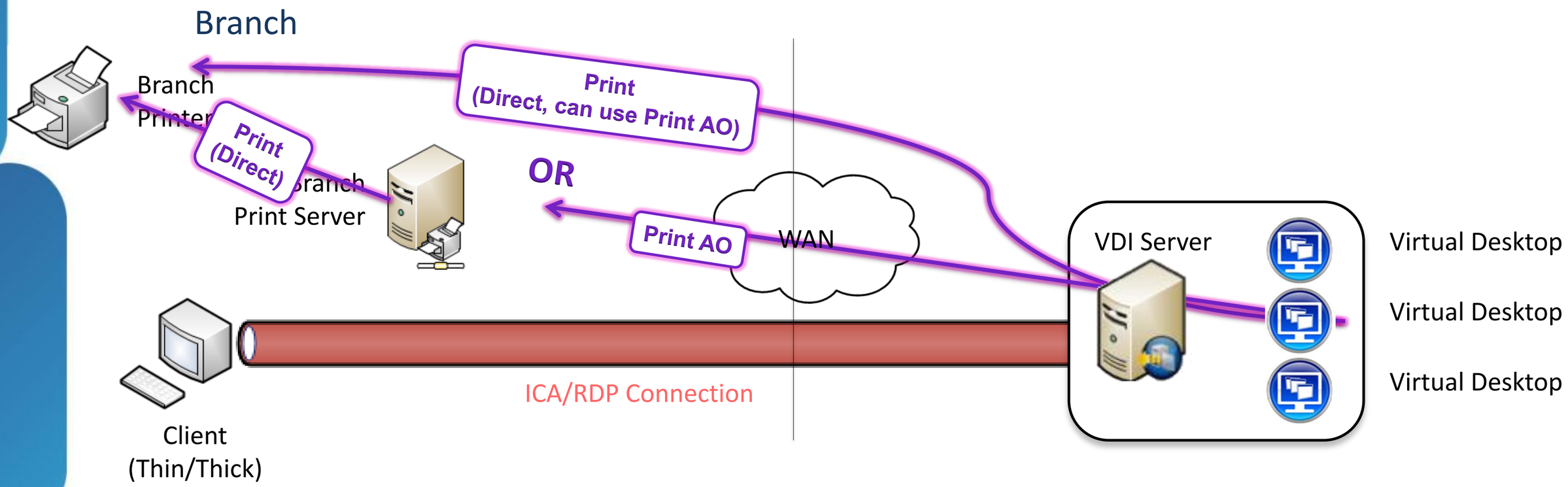
Direct Print, Centralised Print Server

Best Practice



Direct Print, Branch Print Server

Best Practice



Summary of Citrix Deployment Best Practices

- Ensure CGP is enabled for best performance and reliability
- Use Client Side Rendering for HDX Mediastream for flash where possible for optimal end user experience
- Use Direct Print where possible for optimal print performance
- If using Redirected Print Mode, ensure Printer Redirection bandwidth and printer redirection bandwidth percentage settings are set to default (0)
- Test with multiple clients – Performance benefits are more apparent under load
- Find typical user BW consumption to determine sizing requirements
- Dedicated WAAS pool for Citrix in the DC

Agenda

- WAAS Deployments Overview
  - In-Path, WCCP, vPath, AppNav
- Product Update
  - WAAS 5.1
  - Auto Deployments
  - Citrix Optimisation
- Citrix Optimisation Deployments Best Practices
- AppNav Overview
- AppNav Design Considerations

AppNav


WINNER
best of
INTEROP
Awards 2012
Performance Optimization
PRESENTED BY:
InformationWeek
reports

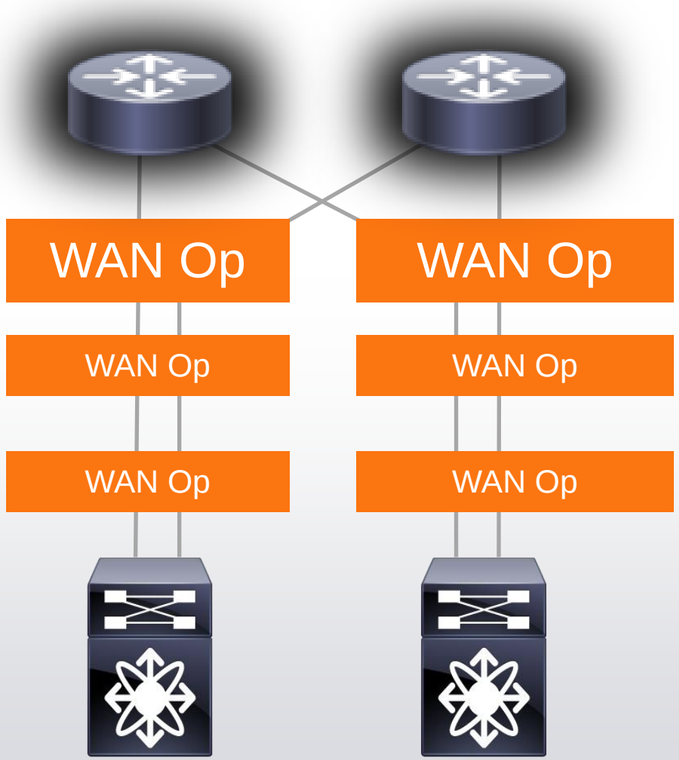
Why AppNav

Public Cloud Performance

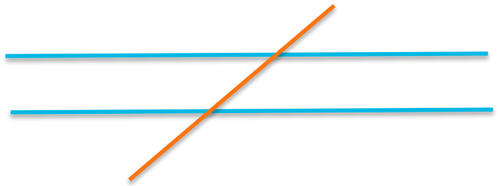
Elastic DC/Private Cloud

Scalability: BYOD, VDI

Current Solutions: Limited and Inconsistent



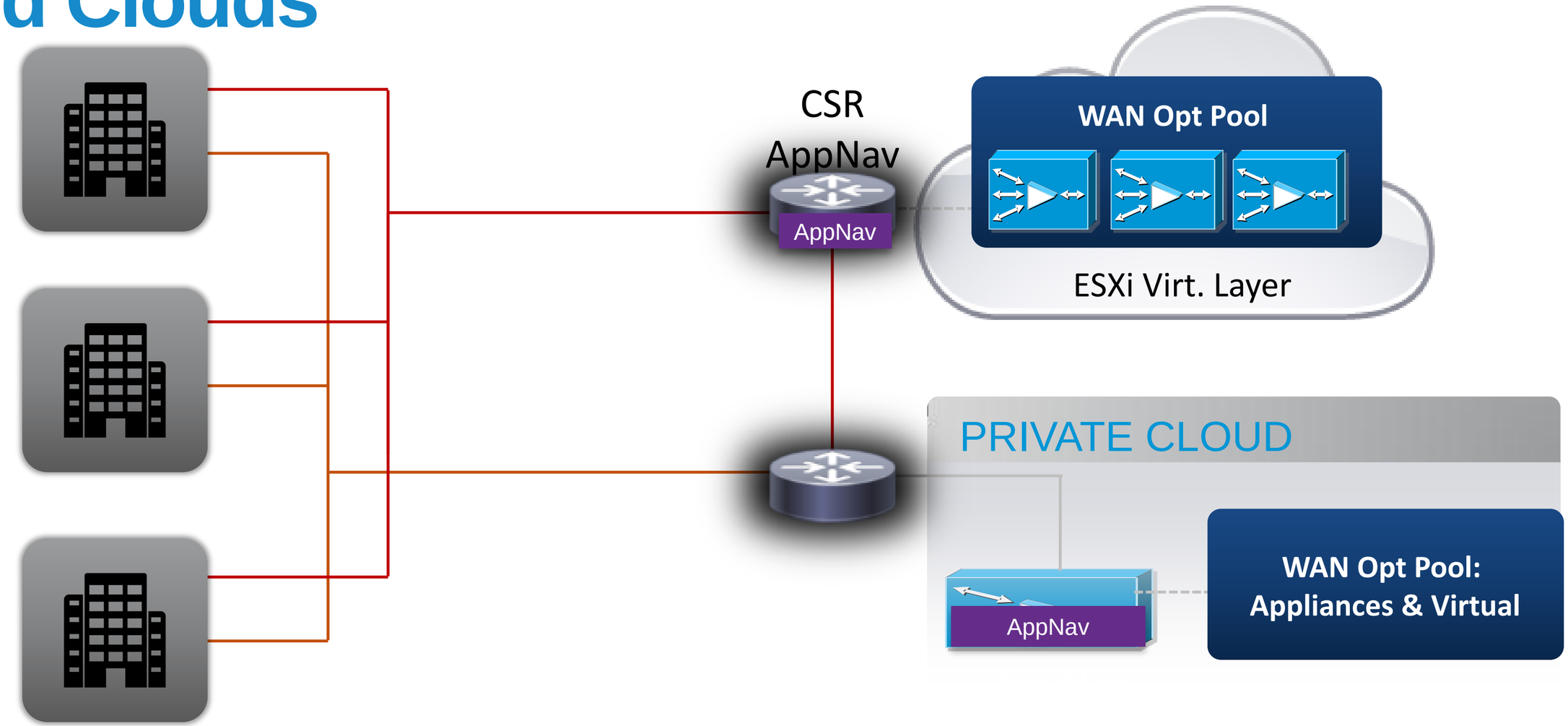
Data Centre: Manual Provisioning



Agent in Every Server

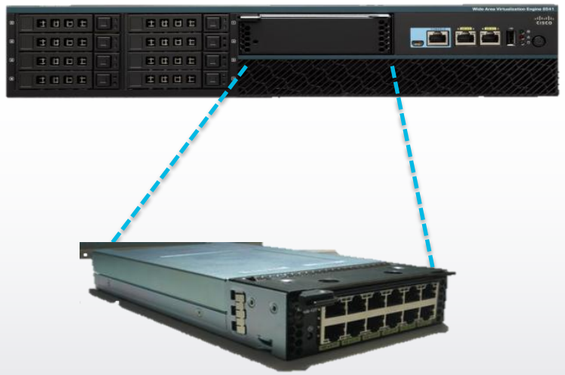
Cloud: Operational Complexity

AppNav: Elastic Deployment For Data Centres and Clouds



Virtualise Your WAN Opt Resources With No Additional Devices Required

WAVE Appliance



AppNav IO Module

- Virtualises up to 32 WAVE instances
- Scales to ~1M connections

Data Centre

Cloud Services Router

AppNav

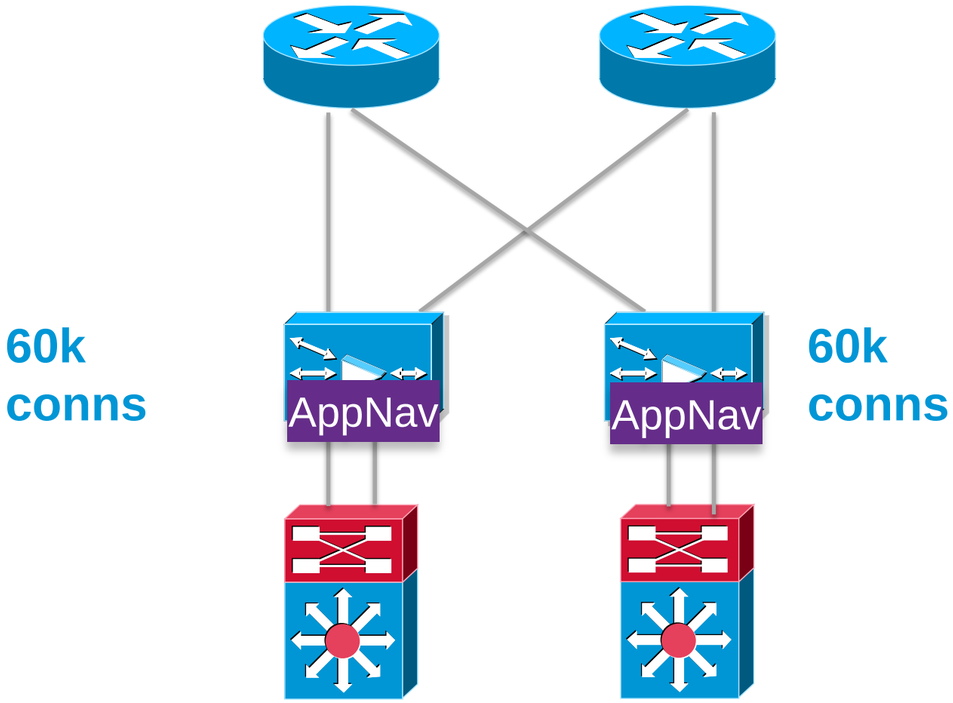
Cloud

ASR 1000

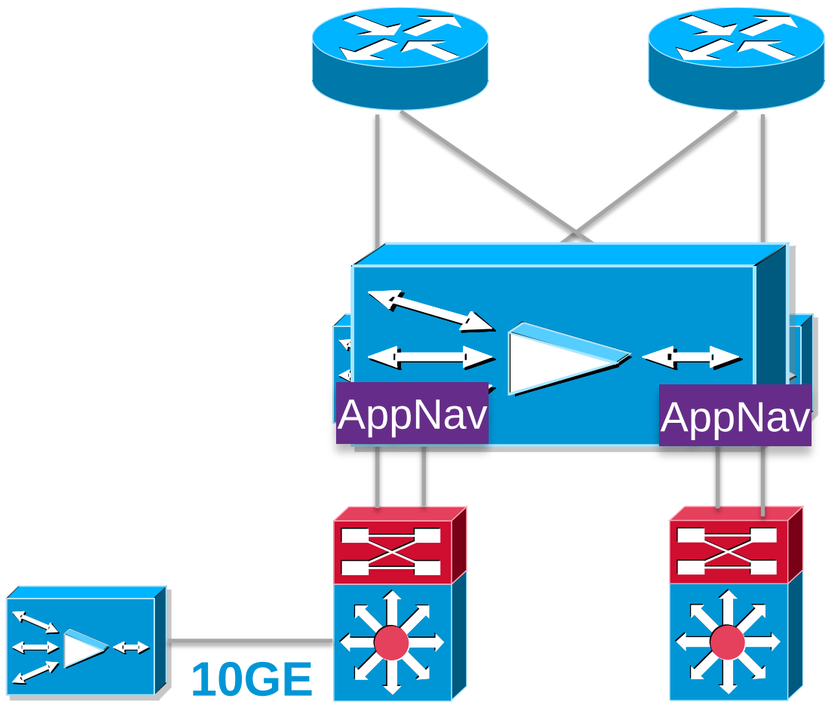
AppNav

WAN Edge

AppNav Creates a Highly Resilient, Elastic Pool of WAN Opt Capacity



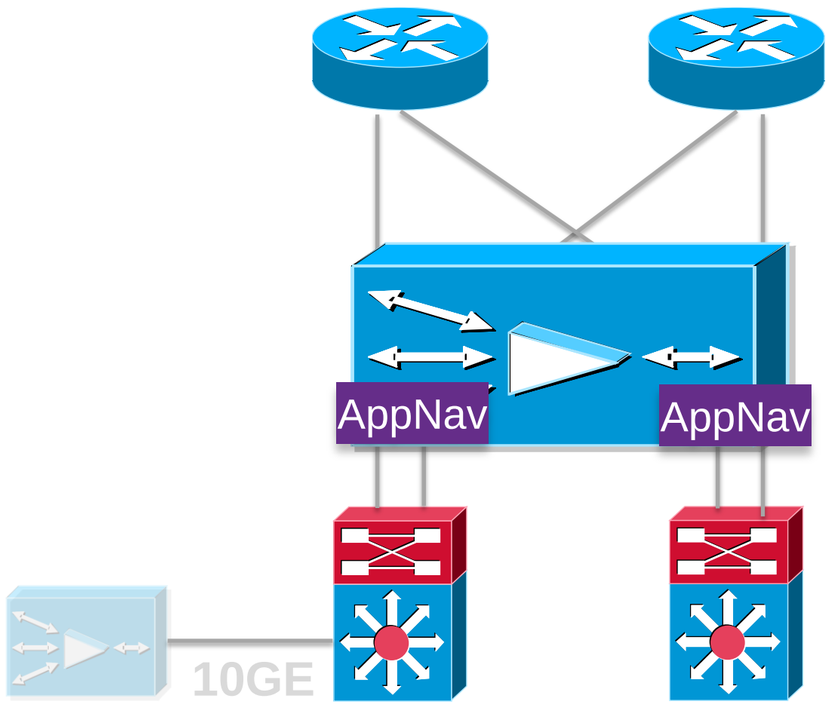
No Changes To Routing/Switching Required



60k conns

150k conns

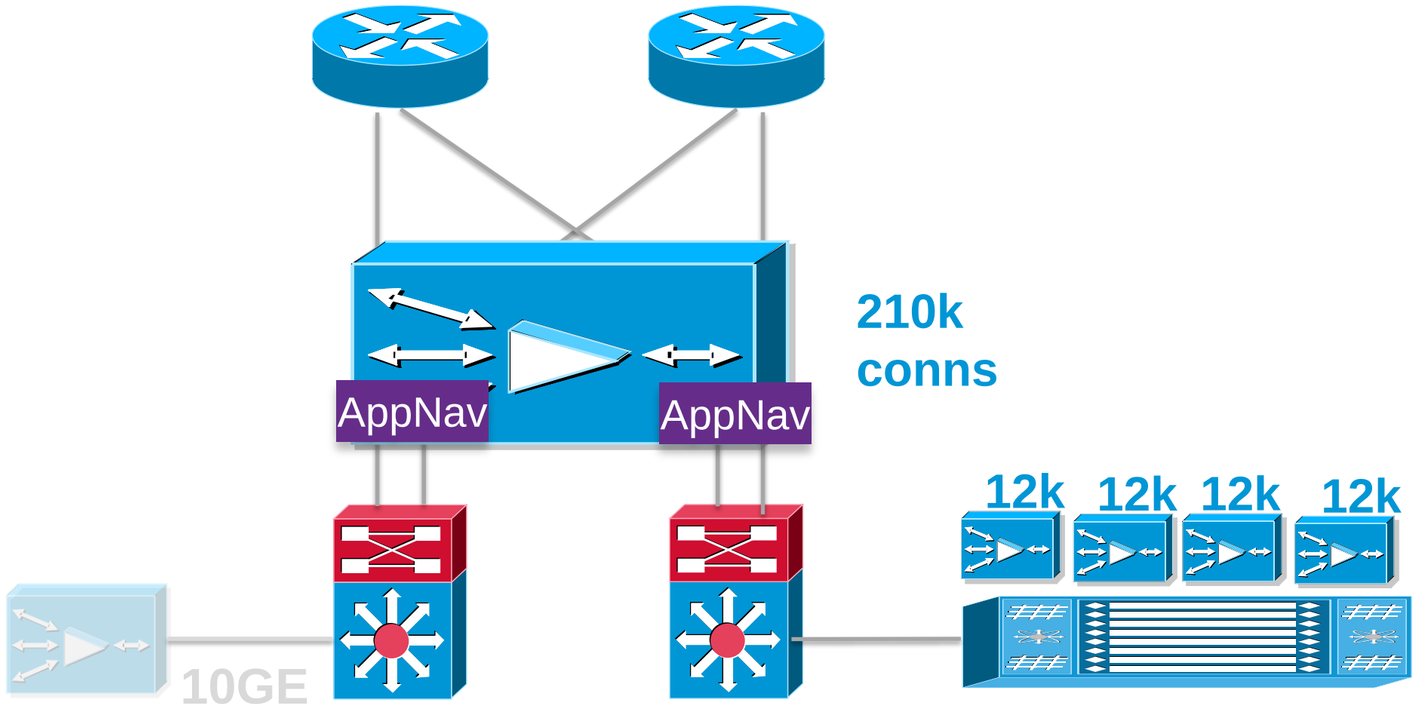
Add Capacity To the “Pool”- Physical



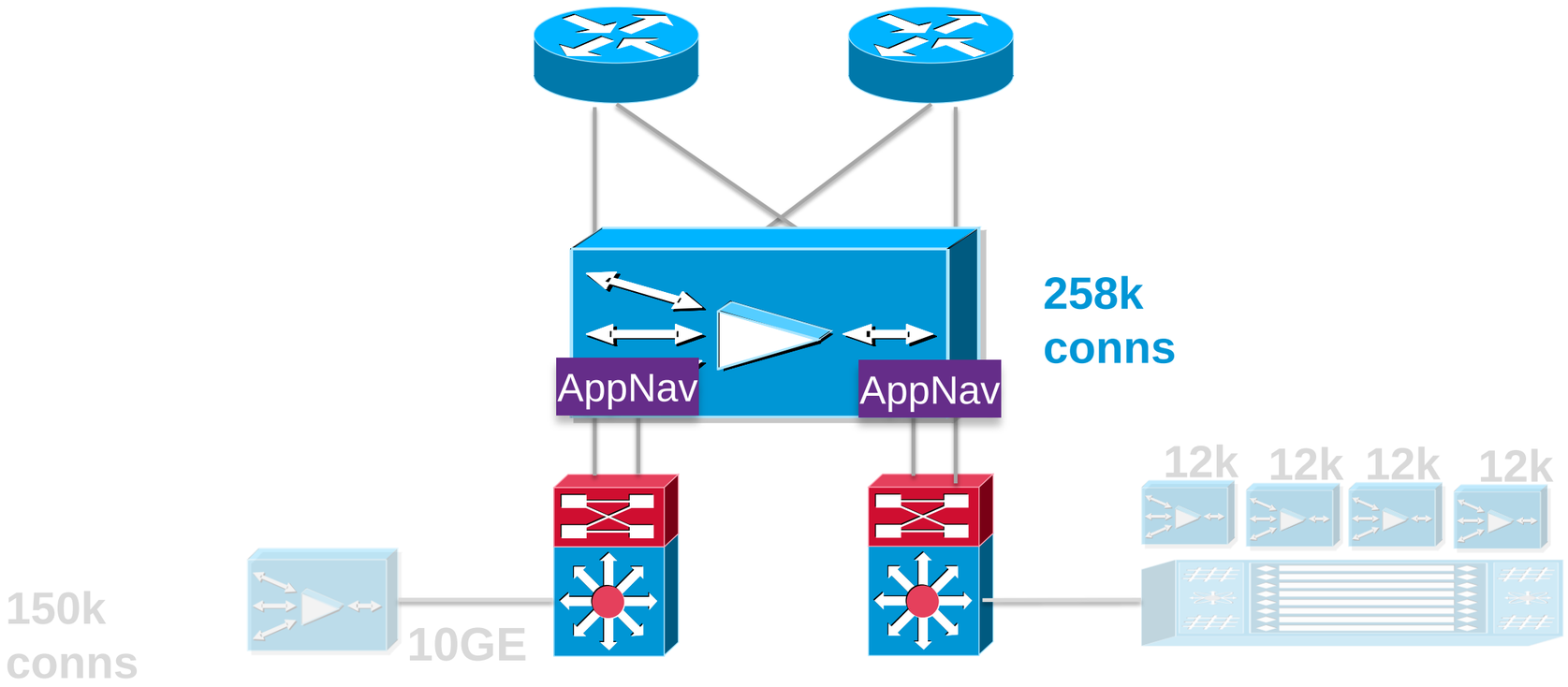
210k conns

150k conns

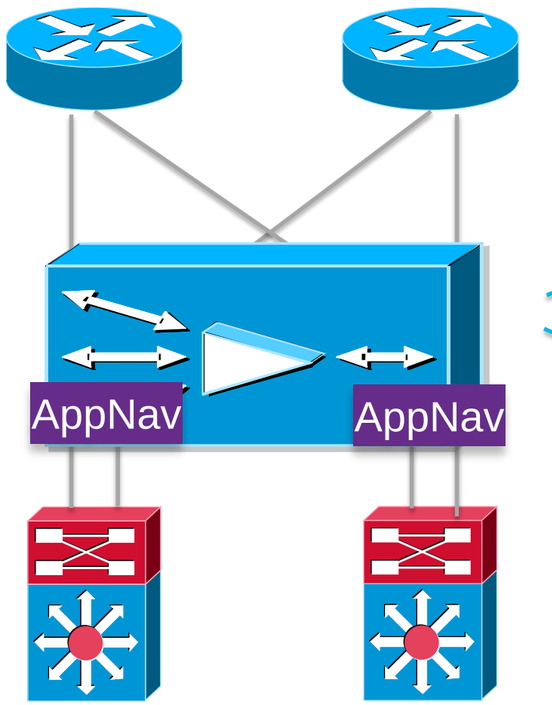
Add Capacity To the “Pool”- Physical And Virtual



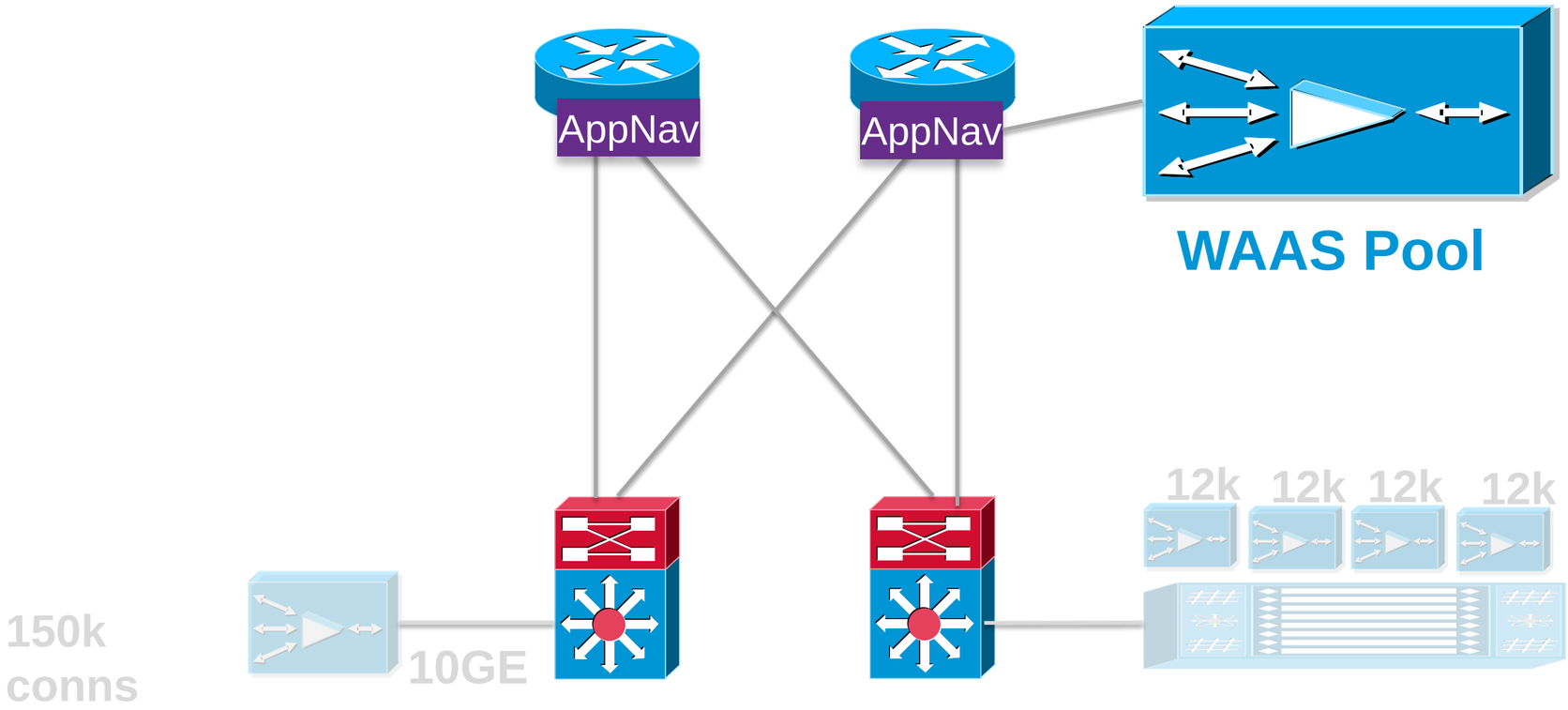
Add Capacity To the “Pool”- Physical And Virtual



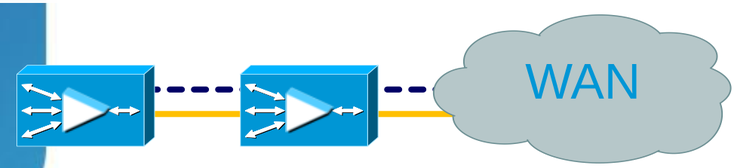
Policy Based Binding To Apps/Locations

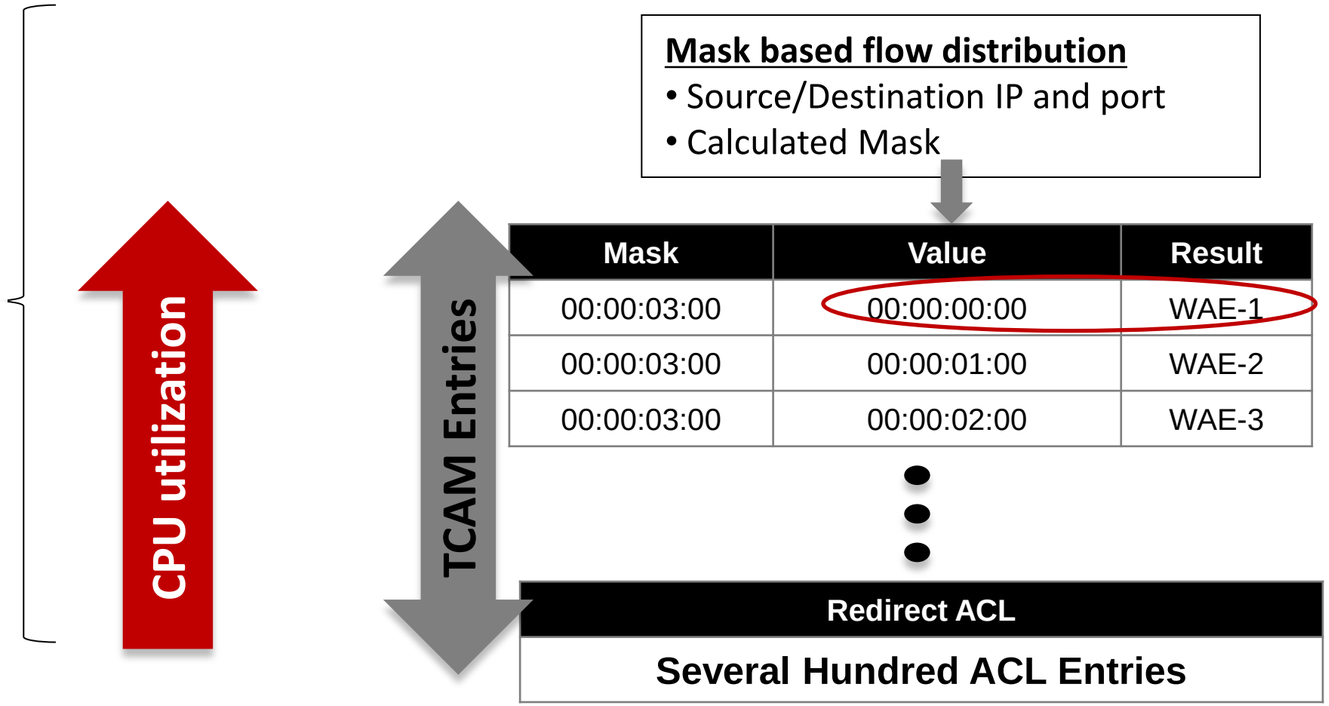


Router Integrated AppNav



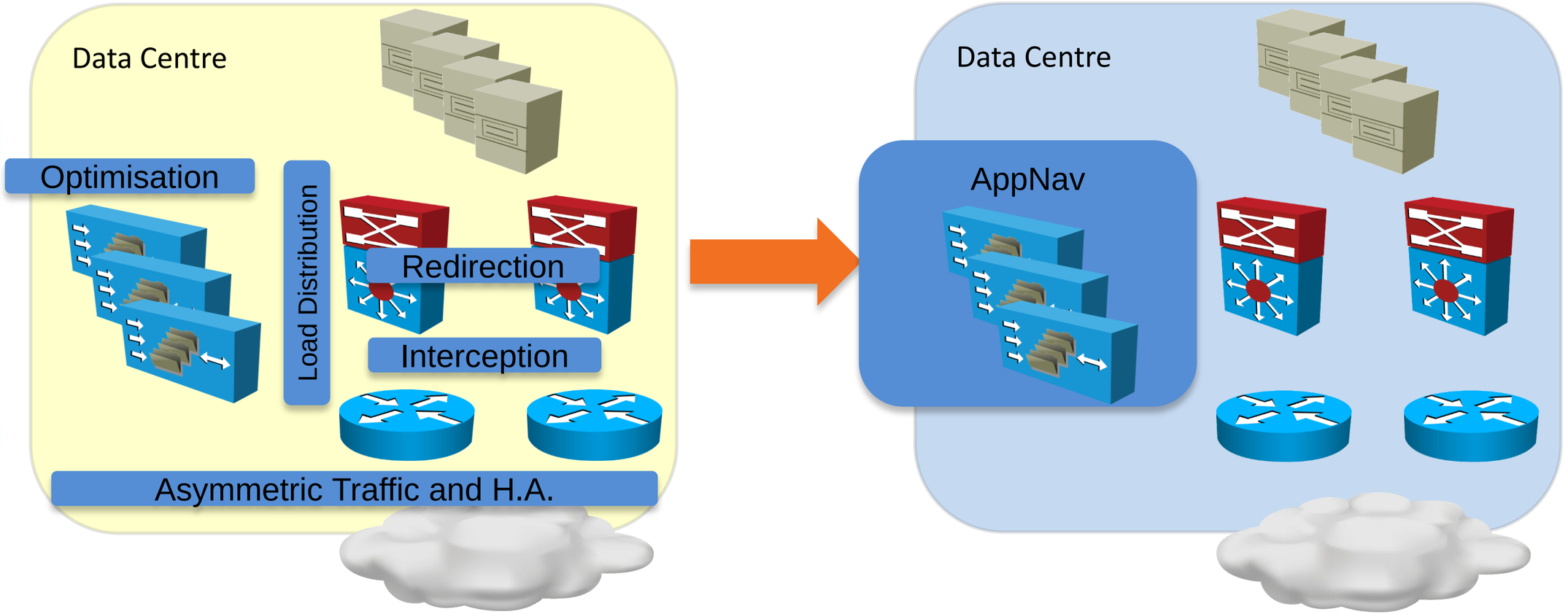
Pre-AppNav Deployment Challenges



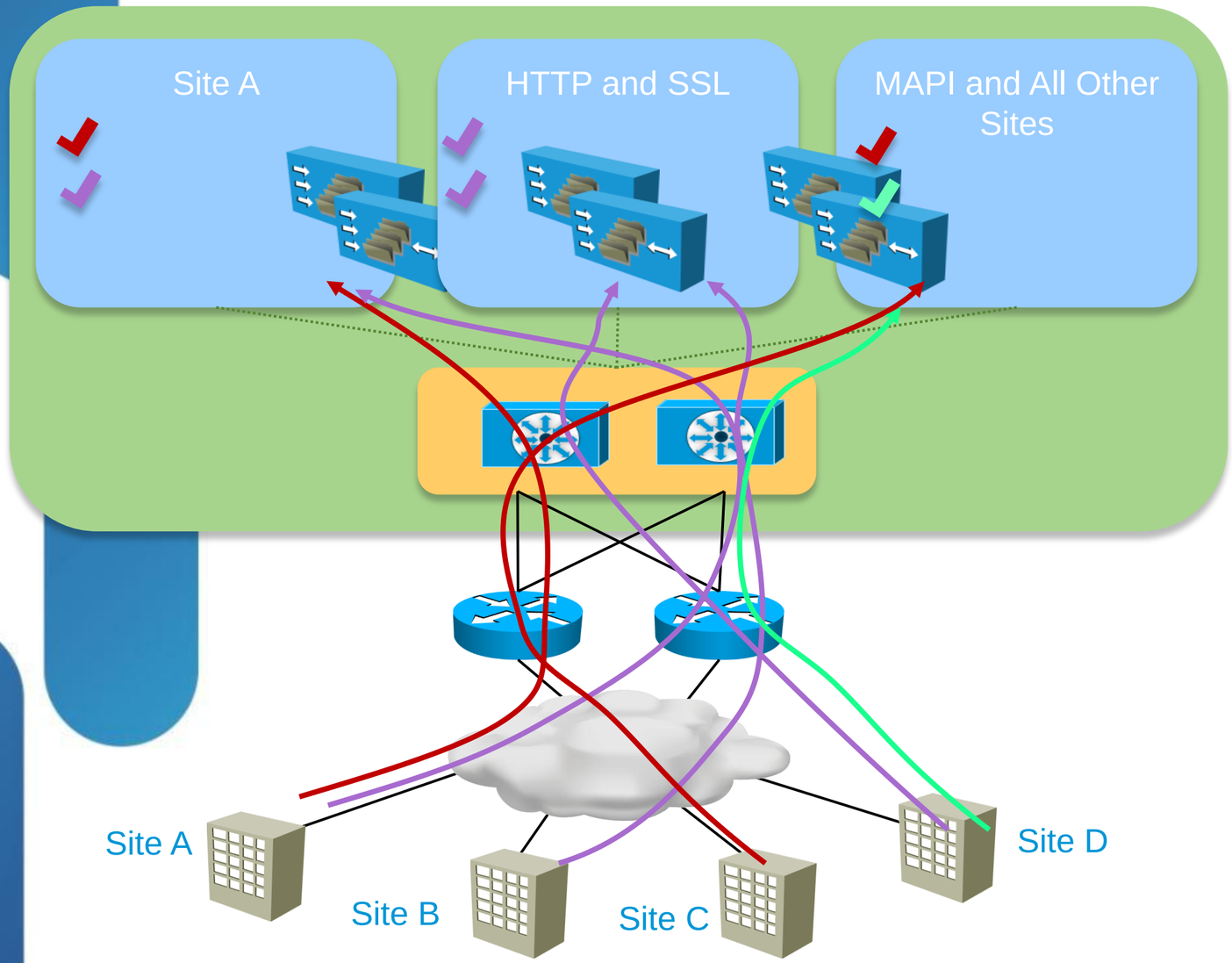


- Traditional In-Line has limited scale
- Un-deterministic branch to DC mapping results in overload
- Heavy administration for redirect ACLs
- TCAM memory and high CPU utilisation

AppNav Solution

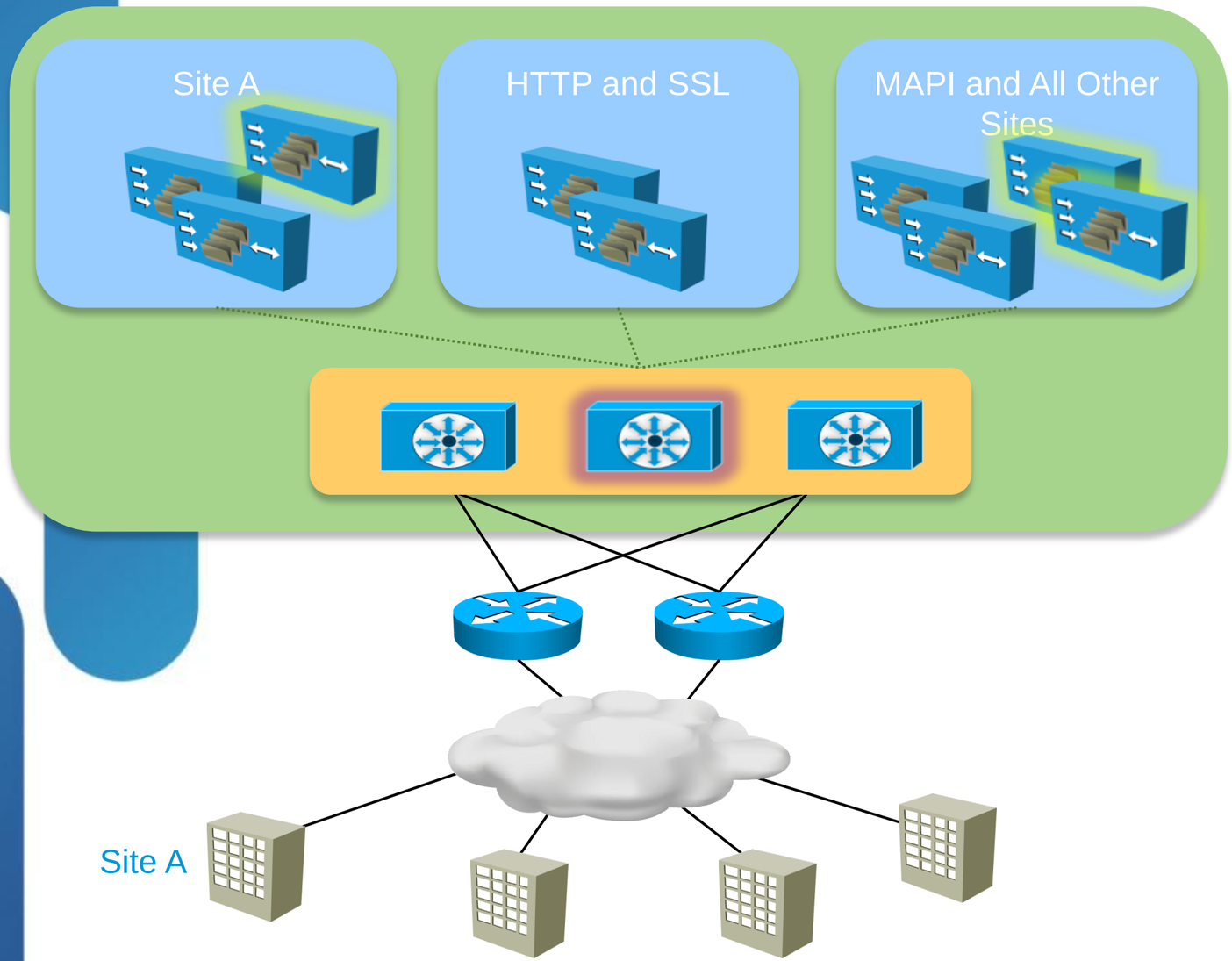


Intelligent Flow Distribution



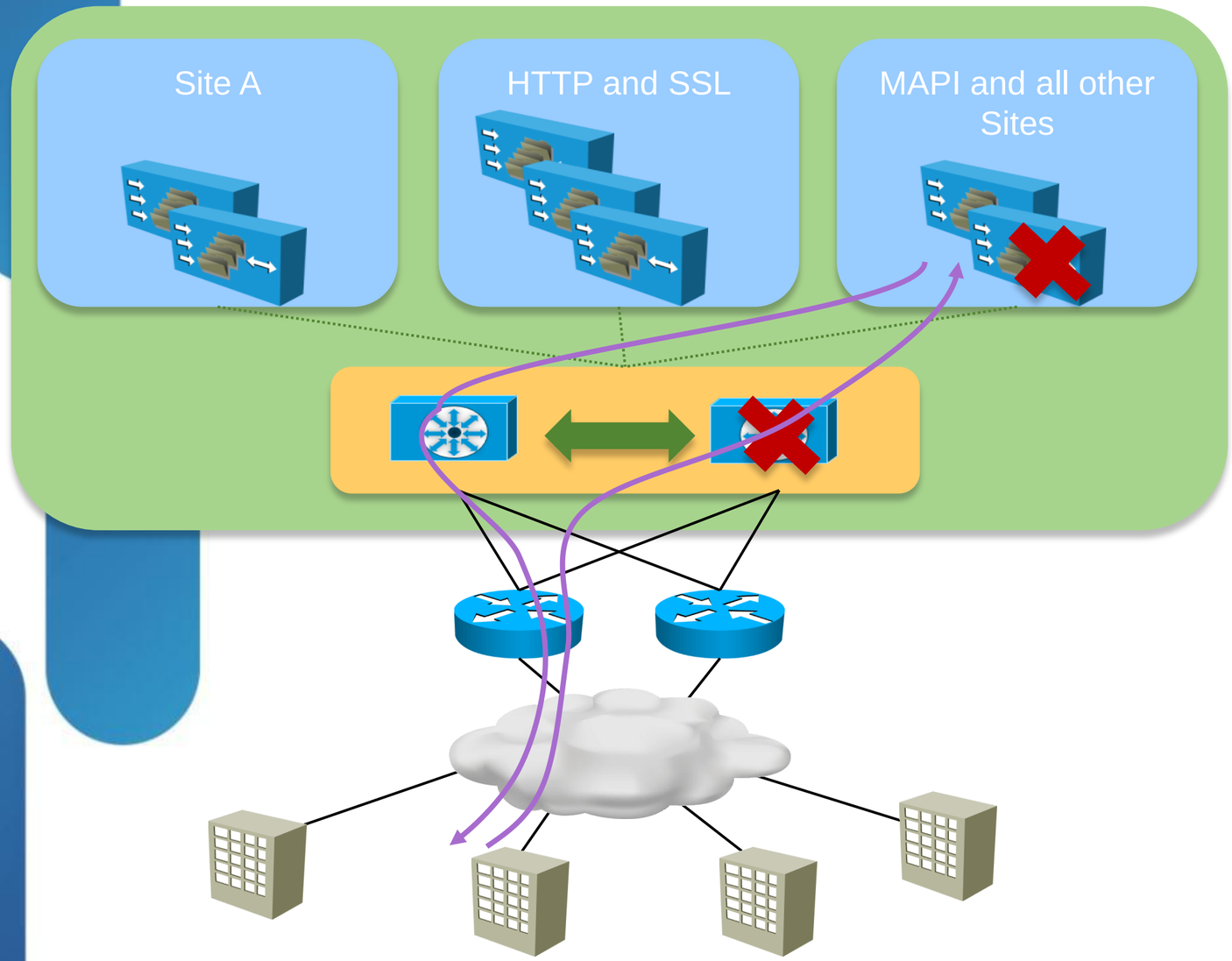
- Site affinity:
  - Identified via branch WAE ID or site IP subnet
  - Reserve optimisation capacity for critical sites
  - Improves compression performance through DRE
- Application affinity:
  - Identified via source/destination IP addresses and ports
  - Reserve optimisation capacity for applications
  - Consolidates application-specific optimisation options

Elastic Provisioning of WAN Optimisation Resources



- Optimisation resources can be added gracefully without disruption, as farms with business driven bindings (branch, application, etc.) scale.
- Interception/redirection/flow distribution resources can be added gracefully without disruption, as data centre scales when adding applications, customers, or raw traffic volume.

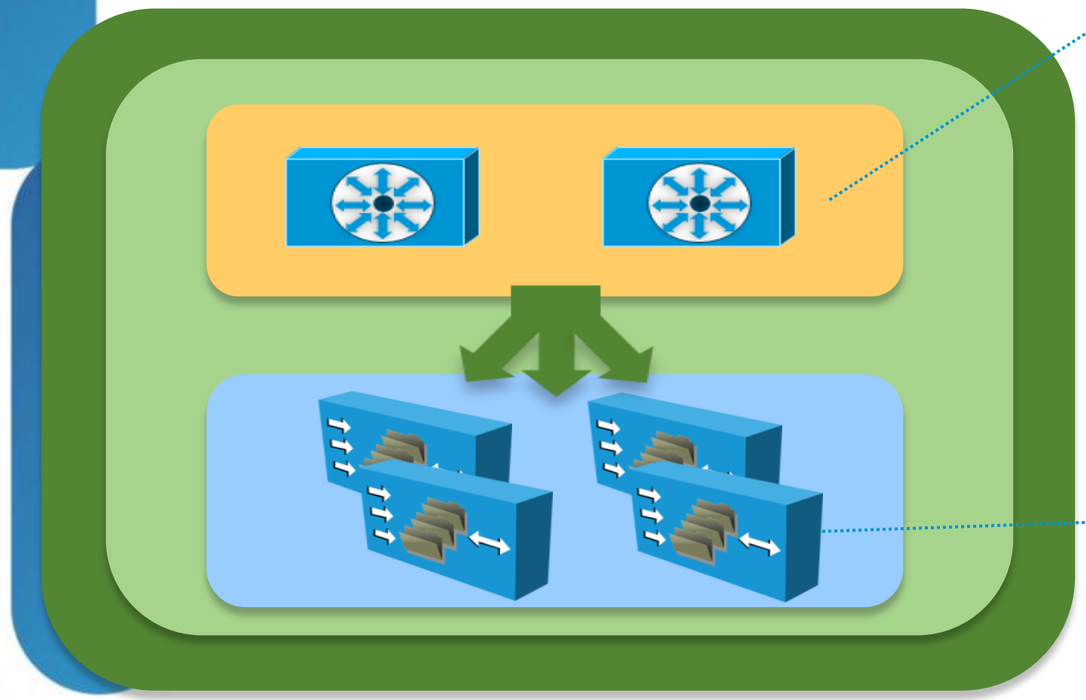
Cluster HA and Asymmetric Traffic Handling



- Health probes between ANCs and WNs:
  - AO Health and load included in reply.
  - WNs enter and exit the cluster gracefully.
- Heartbeats between ANCs synchronise cluster information:
  - Flow distribution tables, WN reachability, and WN load are shared.
  - ANCs enter and exit the cluster gracefully without impacting traffic flows.
  - Asymmetric traffic is distributed consistently.

AppNav Building Blocks

Building Blocks



Both roles can coexist on the same device: An ANC can also optimise.

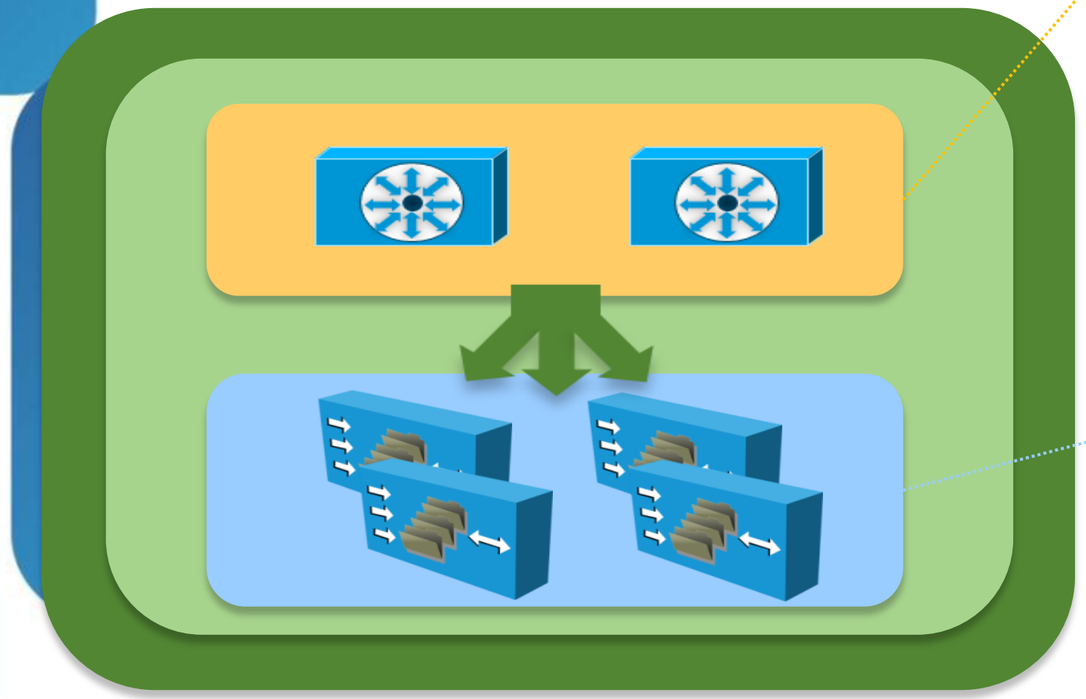
AppNav Controllers (ANCs)

- Requires AppNav IOM, compatible across chassis and cold-pluggable.
- Hardware-based network integration and interception component.
- Provides service aware flow distribution capabilities.

WAAS Nodes (WNs)

- Current WAAS components responsible for traffic optimisation and acceleration.
- Any current WAE version 5.0(1) and above can be a WN, including WAAS appliances and vWAAS.

AppNav Groups



AppNav Controller Groups (ANCGs)

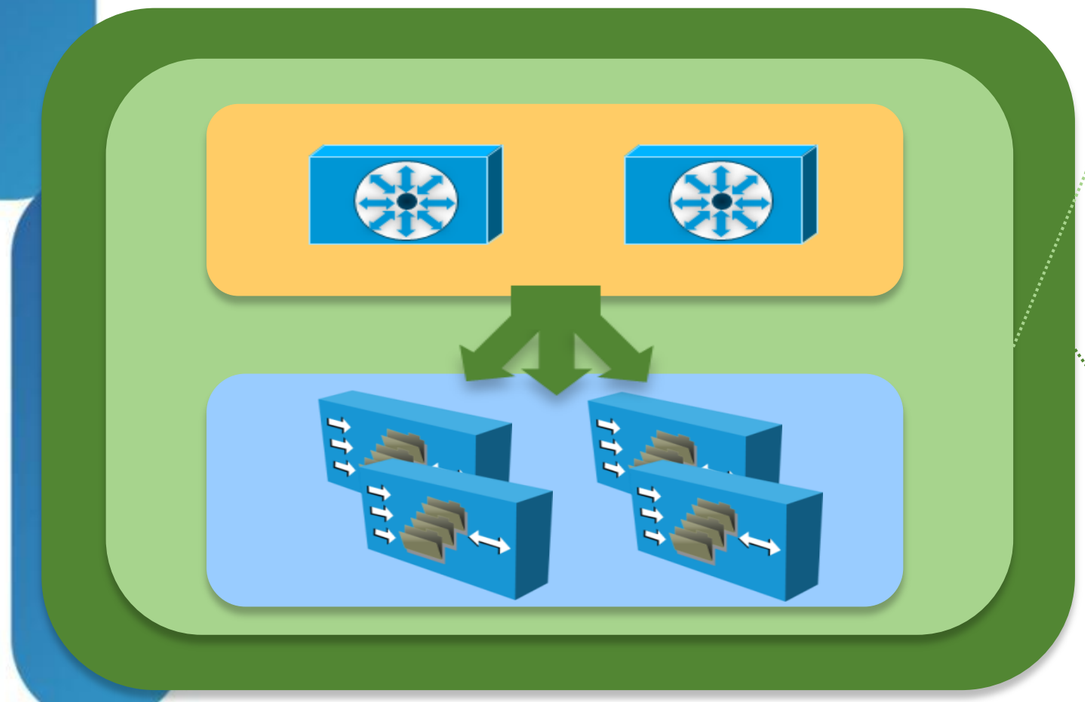
- Each ANCG can have up to 8 ANCs.
- All ANCs in an ANCG share flow distribution information, facilitating handling of asymmetric traffic.
- Multiple ANCGs can be implemented in the same site, with inter-site membership.

WAAS Node Groups (WNGs)

- Facilitate the implementation of branch and application affinity.
- Up to 32 WNGs can be configured per cluster.

Clusters and Service Contexts

Only one ANCG and flow distribution policy per cluster.



Cluster

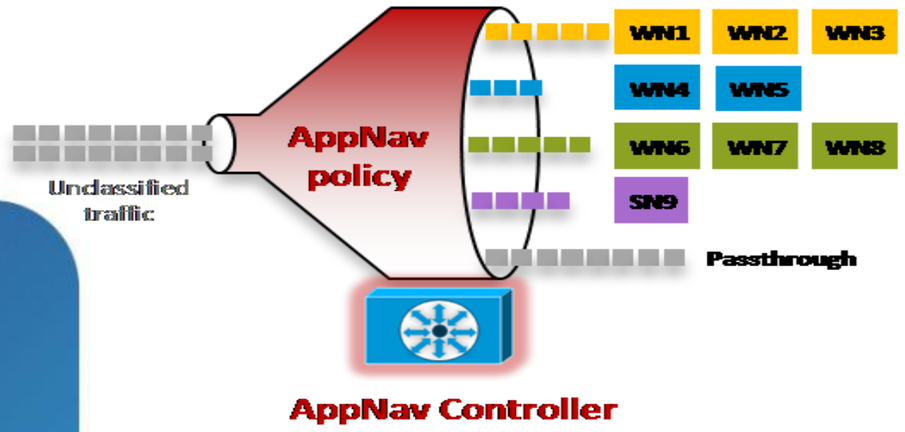
- The group of all ANC and WN devices within a service context.
- Member ANCs discover each other via heartbeats.
- Member WNs are discovered by ANCs using probes.

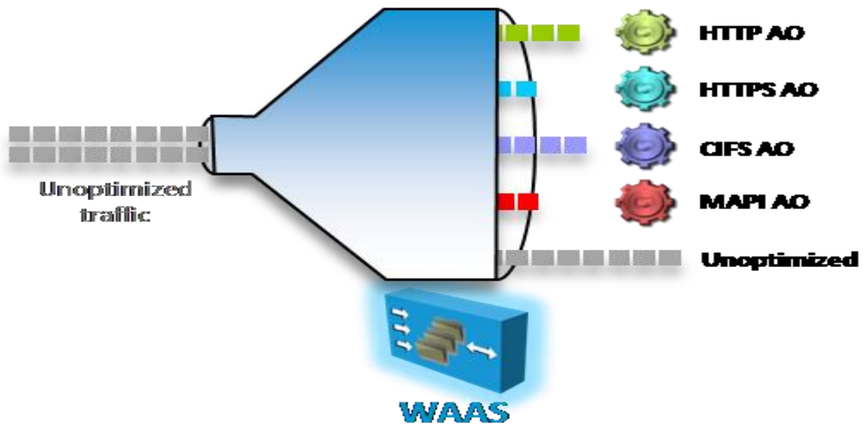
Service Context

- A cluster with an associated flow distribution policy.
- Each context can handle up to 2 million flows for distribution. WN optimisation capacity depends on WAE model.
- Flow policies can classify up to 64 traffic classes.

1 million passthrough, 1 million redirect by default (configurable).

AppNav and Optimisation Policies





AppNav Policy

Flow distribution policy:

- AppNav class-map traffic classification:
  - Per peer OR 3 tuple SRC/DST IP and DST port
  - Mix one peer + SRC/DST IP and DST port
- AppNav policy:
  - Primary and backup WNGs
  - Monitoring of AOs
  - Nested policy

Optimisation Policy

Optimisation/acceleration associated with given traffic:

- Optimisation class-map identifying traffic
- Optimisation/acceleration tied to the traffic:
  - TFO
  - LZ
  - DRE (Uni, Bi, Adaptive)
  - AO

Cisco AppNav

WAAS 5.0

Cisco AppNav 10Gbps

AppNav Off path deployment only appliance

4 x 10G SFP+

WAAS 5.0

Cisco WAVE:

WAVE-8541
WAVE-7571
WAVE-7541
WAVE-694

Cisco AppNav IOM:

12 x 1G copper
12 x 1G SFP

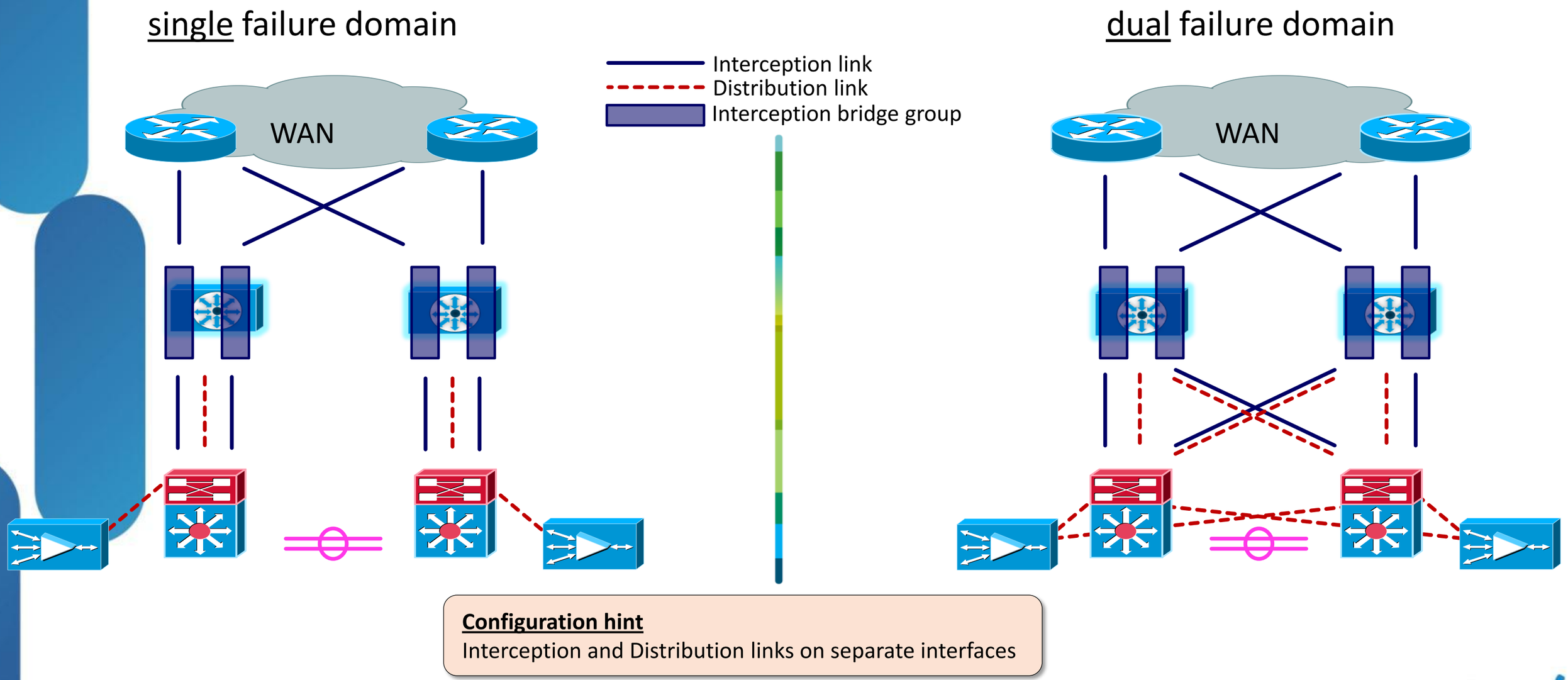
Cisco AppNav

WAAS + Cisco AppNav

Cisco AppNav 1Gbps

Off path or in path deployment

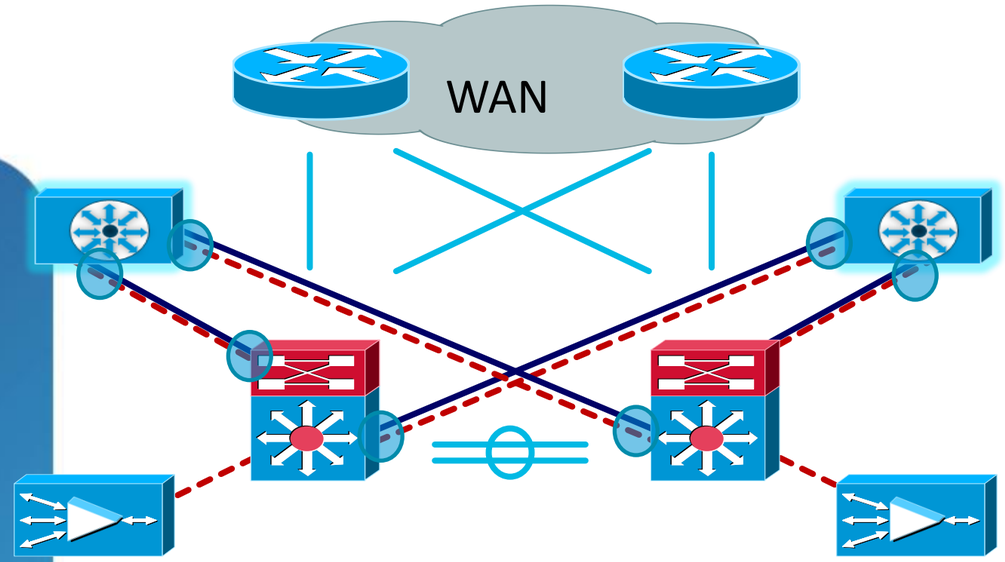
AppNav Controller: In-path deployment



Configuration hint
Interception and Distribution links on separate interfaces

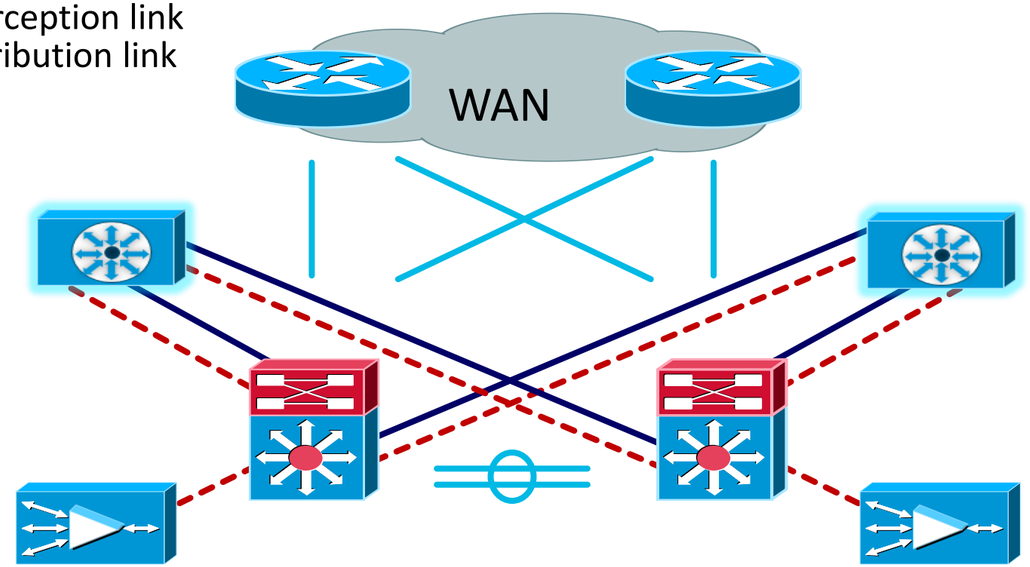
AppNav Controller: Off-path deployment

Interception & Distribution:
Same interface



Interception link
Distribution link

Interception & Distribution:
Separate interface



Configuration hint

Interception and Distribution links may be on same interface

wccp interception (& redirection)

- single service group
- simple (host) mask (only mask and no hash assignment)

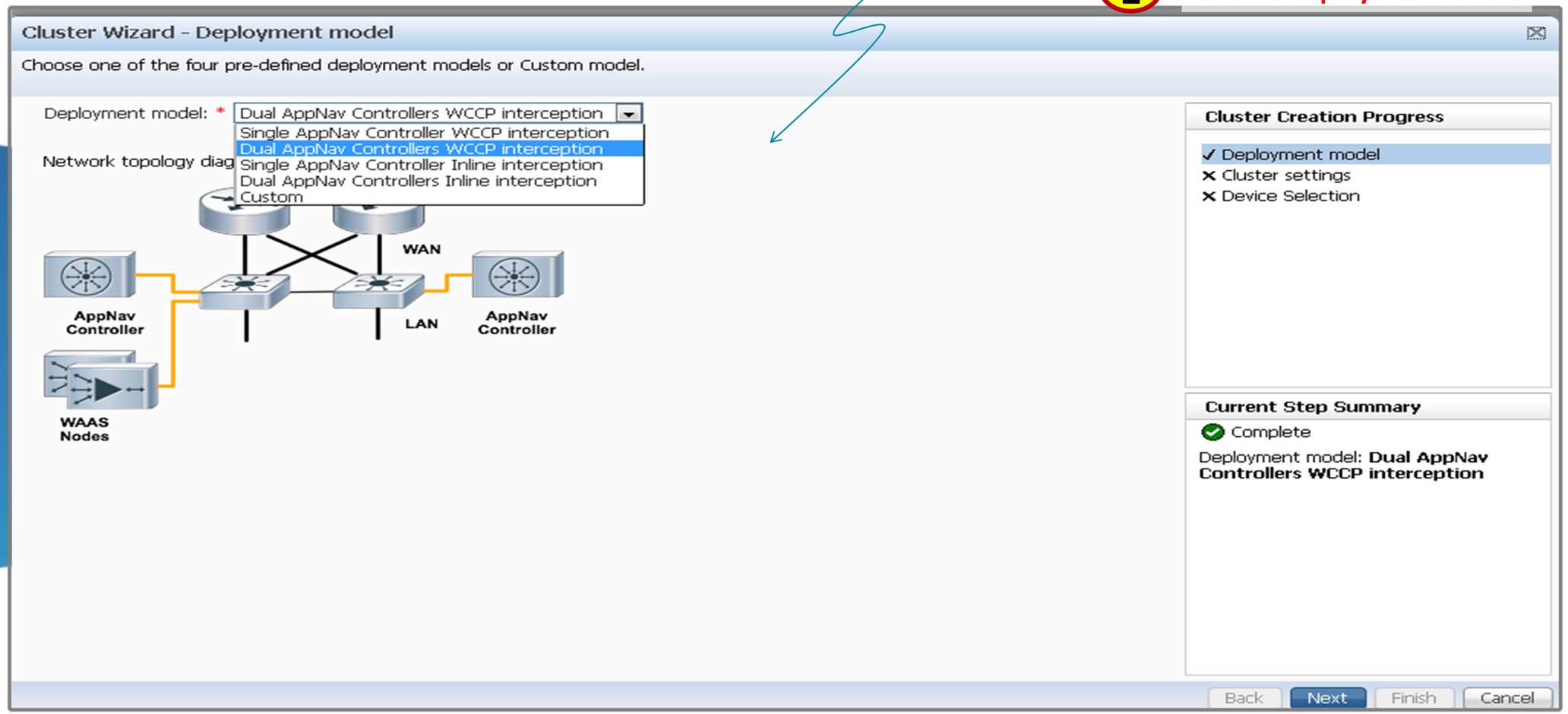
WCCP Methods

Forwarding	Egress (automatic)
GRE	Generic GRE
L2	WCCP L2 return

Central Manager Integrated and Simple

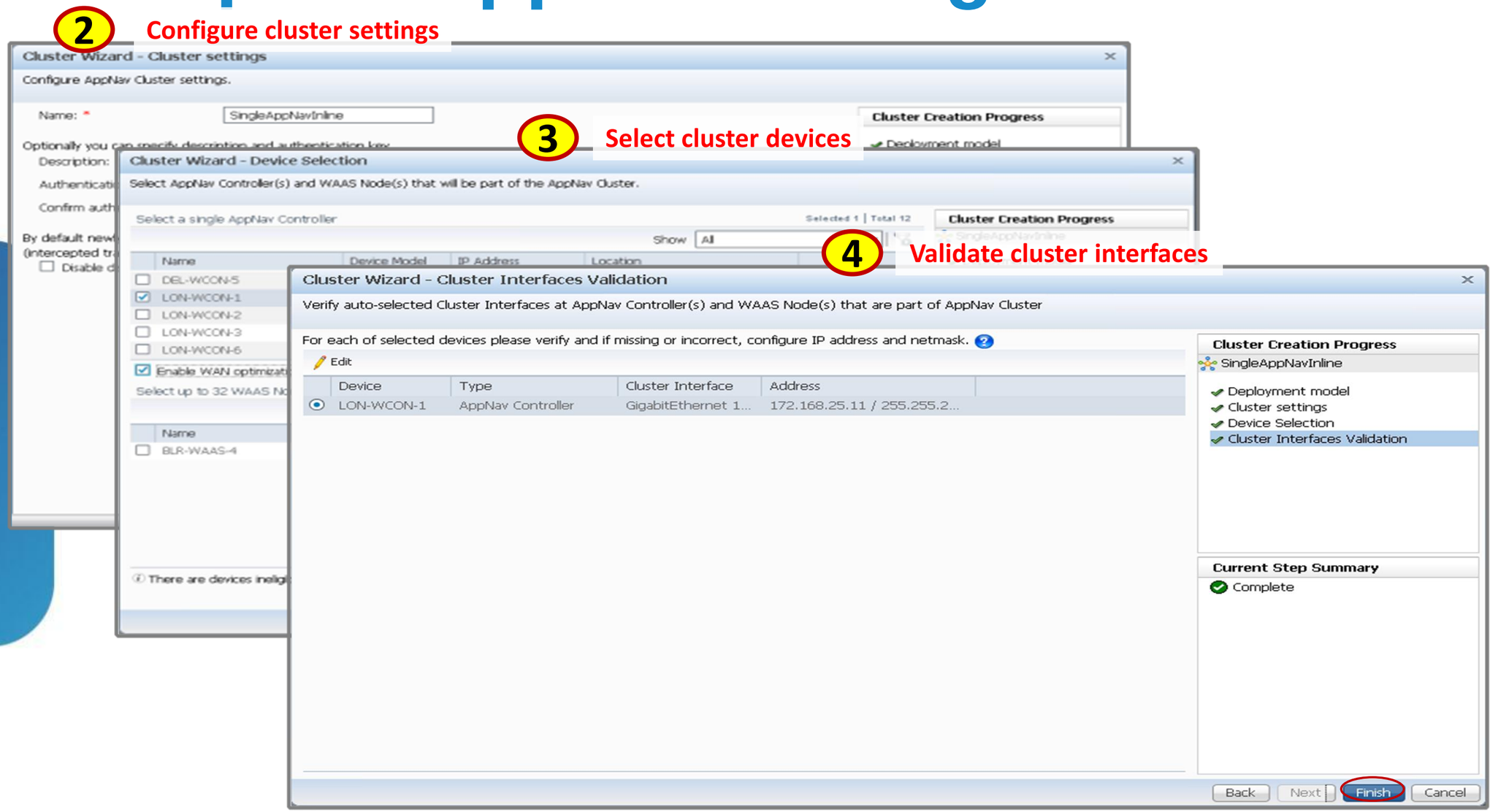
Step by step configuration of AppNav cluster through cluster wizard

1 Choose deployment model



Validation and step by step feedback to prevent errors and misconfiguration

Complete AppNav Configuration

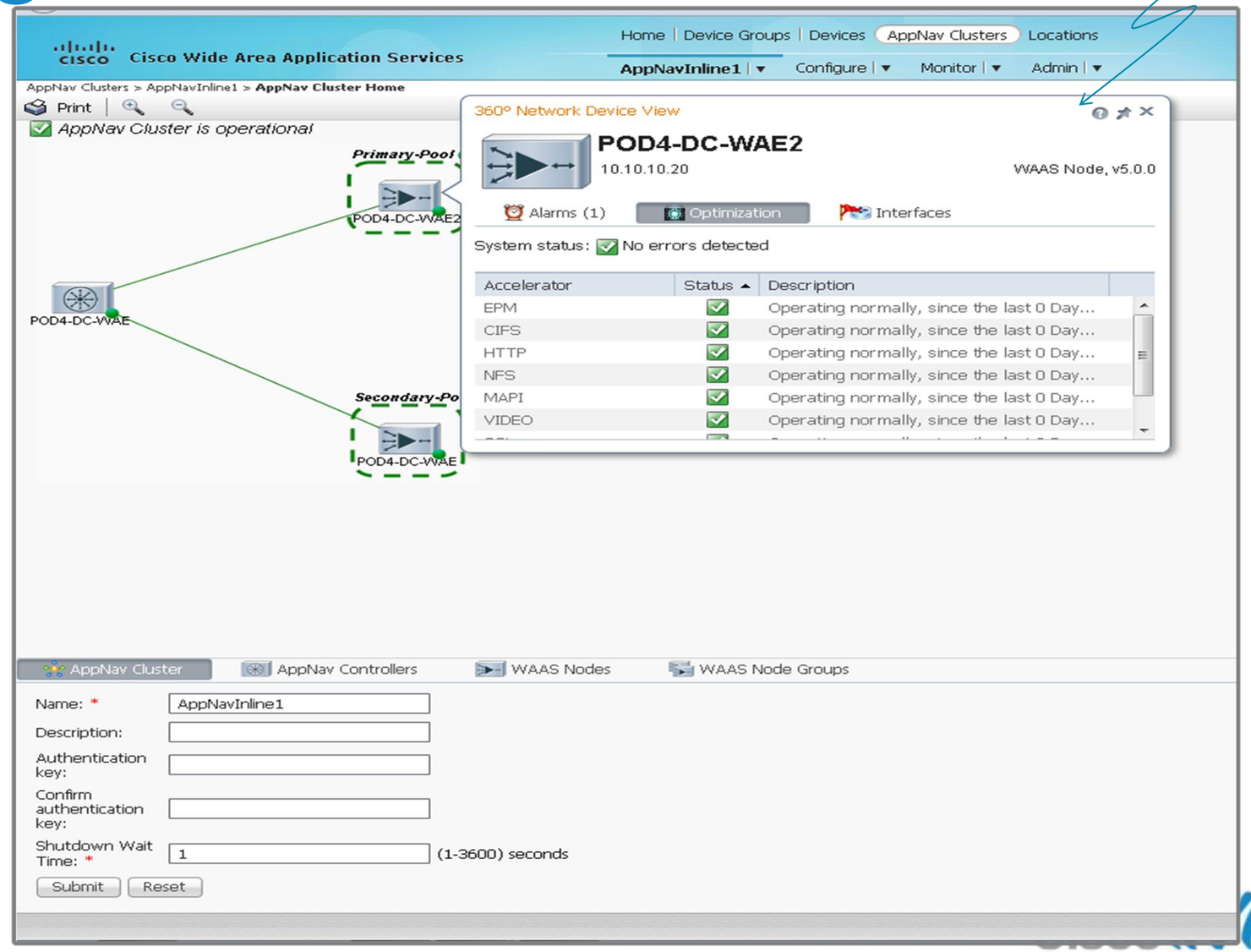


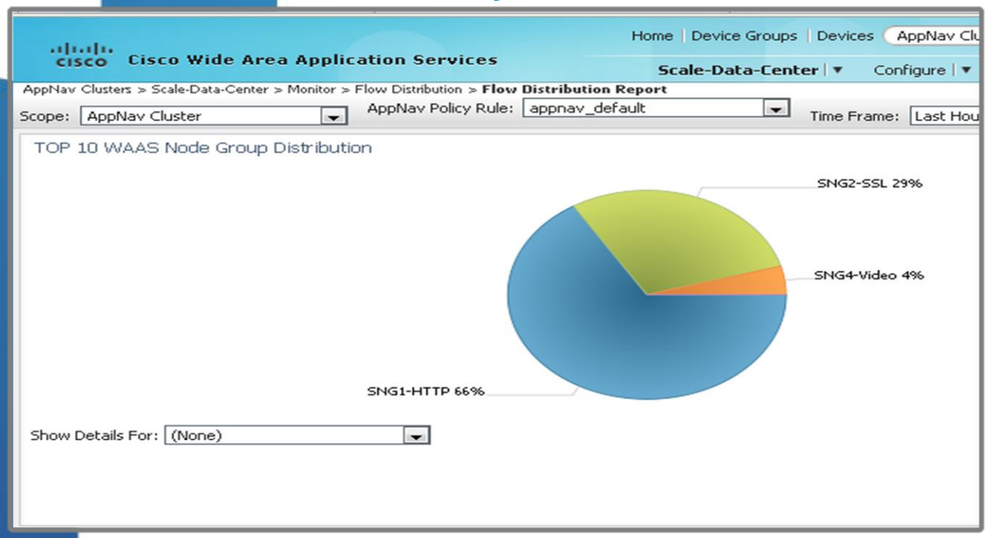
Comprehensive Monitoring & troubleshooting

At a glance device & health statistics through 360º network view

Overview of AppNav cluster state

Detail reports of flow distribution

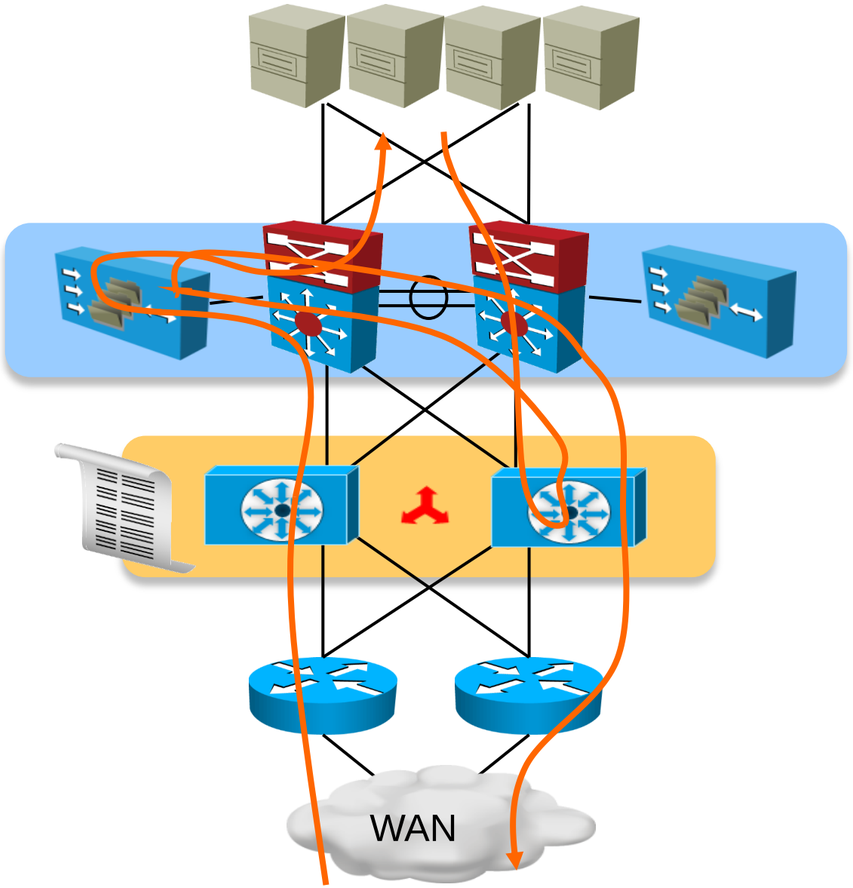




Agenda

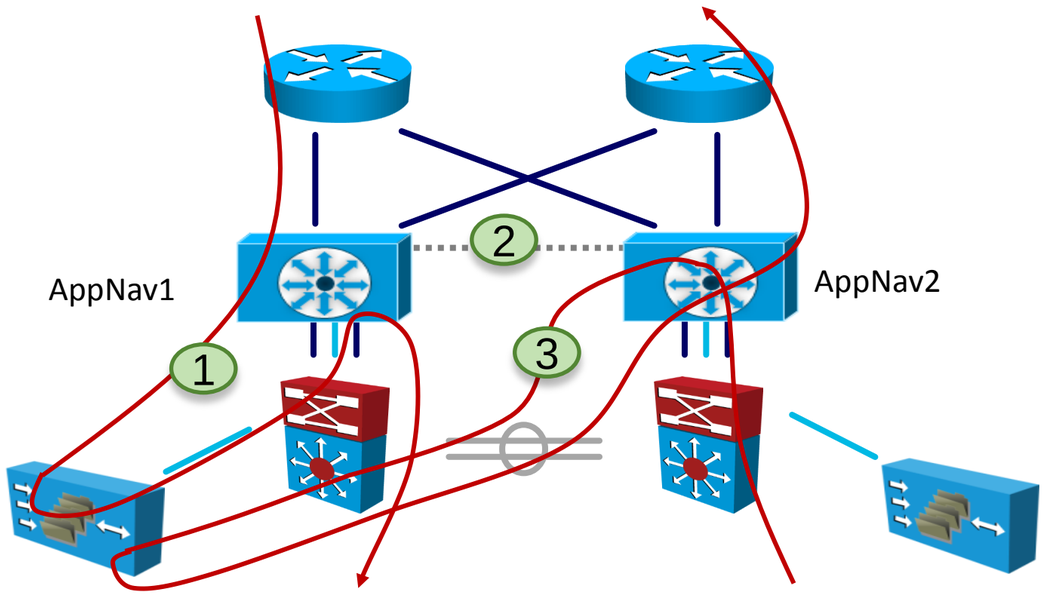
- WAAS Deployments Overview
  - In-Path, WCCP, vPath, AppNav
- Product Update
  - WAAS 5.1
  - Auto Deployments
  - Citrix Optimisation
- Citrix Optimisation Deployments Best Practices
- AppNav Overview
- AppNav Design Considerations

A Day in the Life of a Flow



- ANC2 receives a TCP SYN packet from one of the branches containing a WAAS device.
- The ANC classifies the flow, redirecting it to WN1.
  A pending entry is made into the flow database.
- The frame is GRE-encapsulated and transmitted to WN1. WN1 processes the frame and continues the autodiscovery process.
- The other ANCs are updated with the flow information and the frame is transmitted to its destination.
- A TCP SYN-ACK frame is returned from the destination device and in this example goes to ANC1. ANC1 checks the flow database, finds a matching entry, and sends the response frame to WN1.
- WN1 processes the frame and returns it to ANC1 which in turn forwards the frame to the original source.

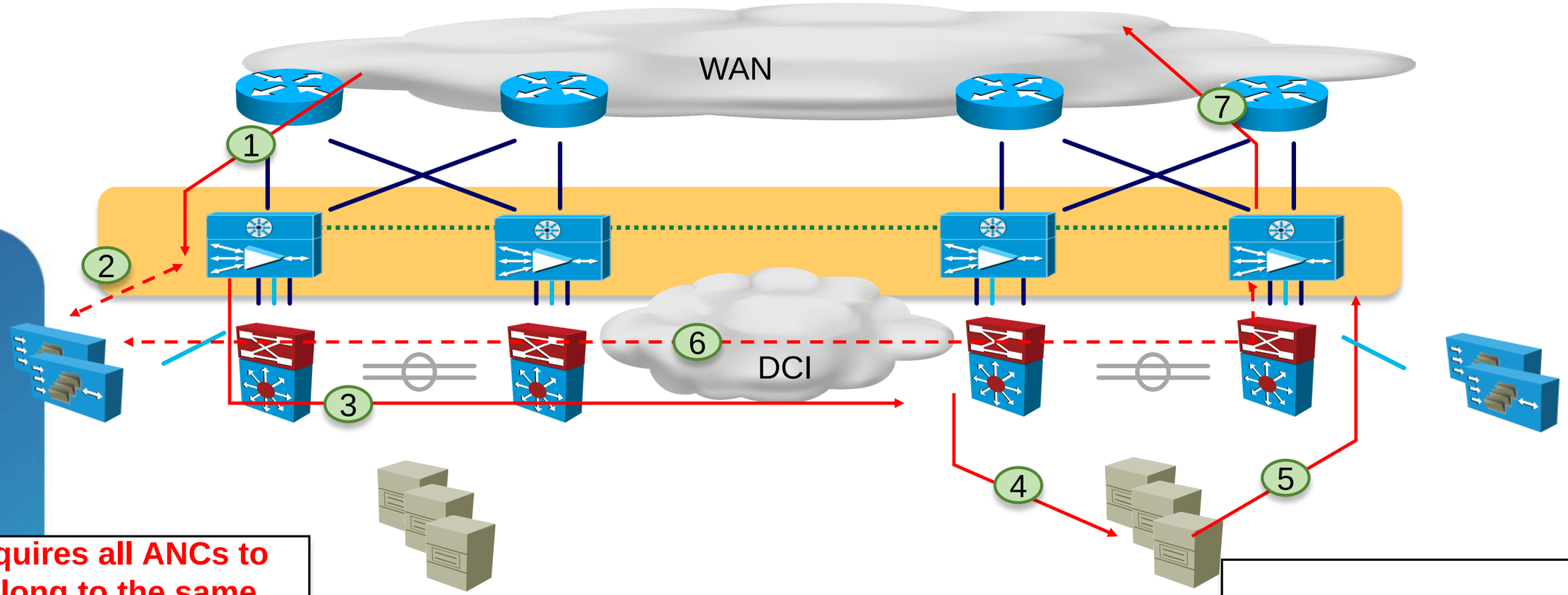
Automatic Intra-DC Asymmetry Handling



- AppNav Cluster is flow aware.
- Automatic asymmetry handling.
- Maintains natural traffic path.

Step	Description
1	Forward path to WAAS through AppNav1.
2	Flow updates between AppNav units.
3	Reverse path to the WAAS through AppNav2.

Automatic Inter-DC Asymmetry Handling

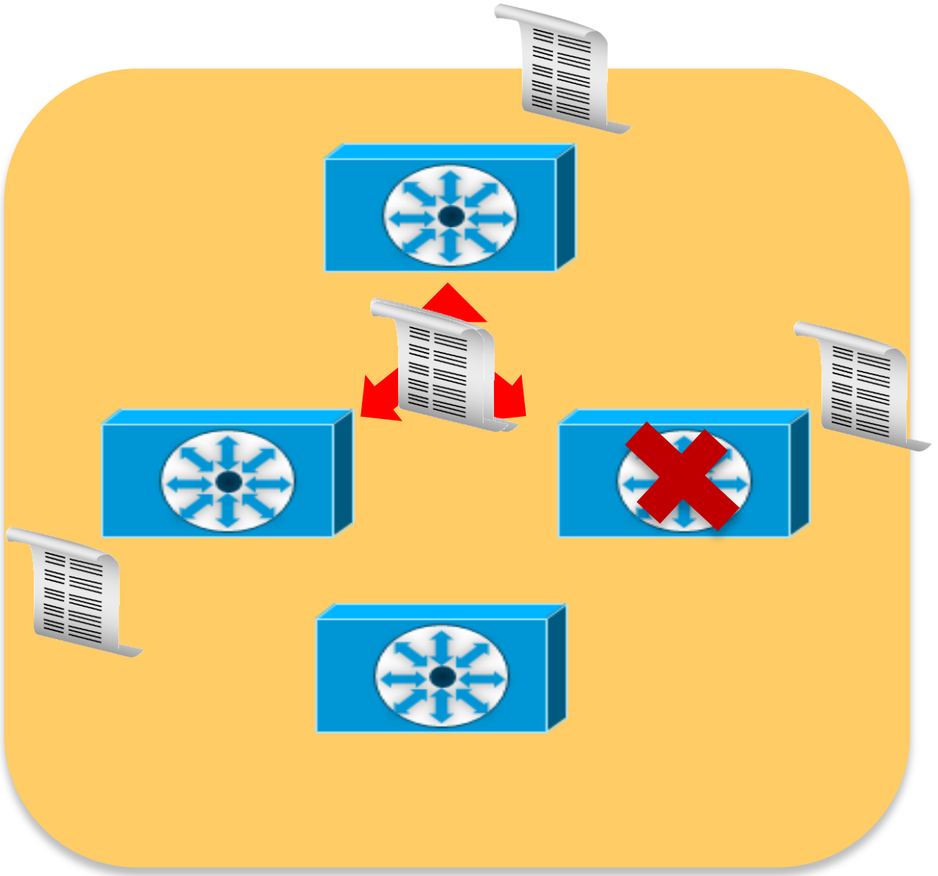


Requires all ANCs to belong to the same cluster for flow information to be exchanged.

- AppNav Cluster–flow aware
- Automatic asymmetry handling
- Maintains natural traffic path

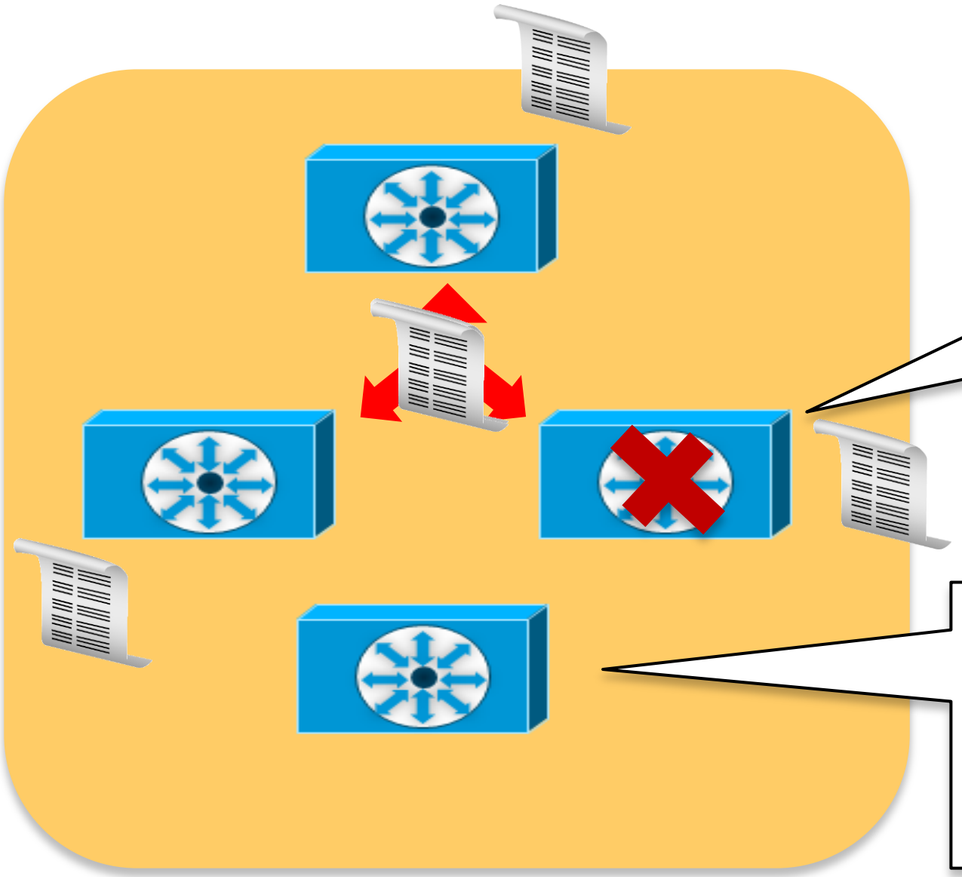
ANCs in each DC can have **different flow distribution policy**.

AppNav High Availability



- Each ANC gathers its own local view of the cluster.
- ICIMP shares local views and a global view becomes known to all ANCs.
- An operational cluster consists of ANCs that have consistent views and can all see each other. This is called a “stable state.”
- New ANCs enter the cluster gracefully by holding the ANC down until all flow states are synchronised.
- HA is built in as all the ANCs share the flow states. ANCs can exit the cluster at any time without impacting flows distribution.

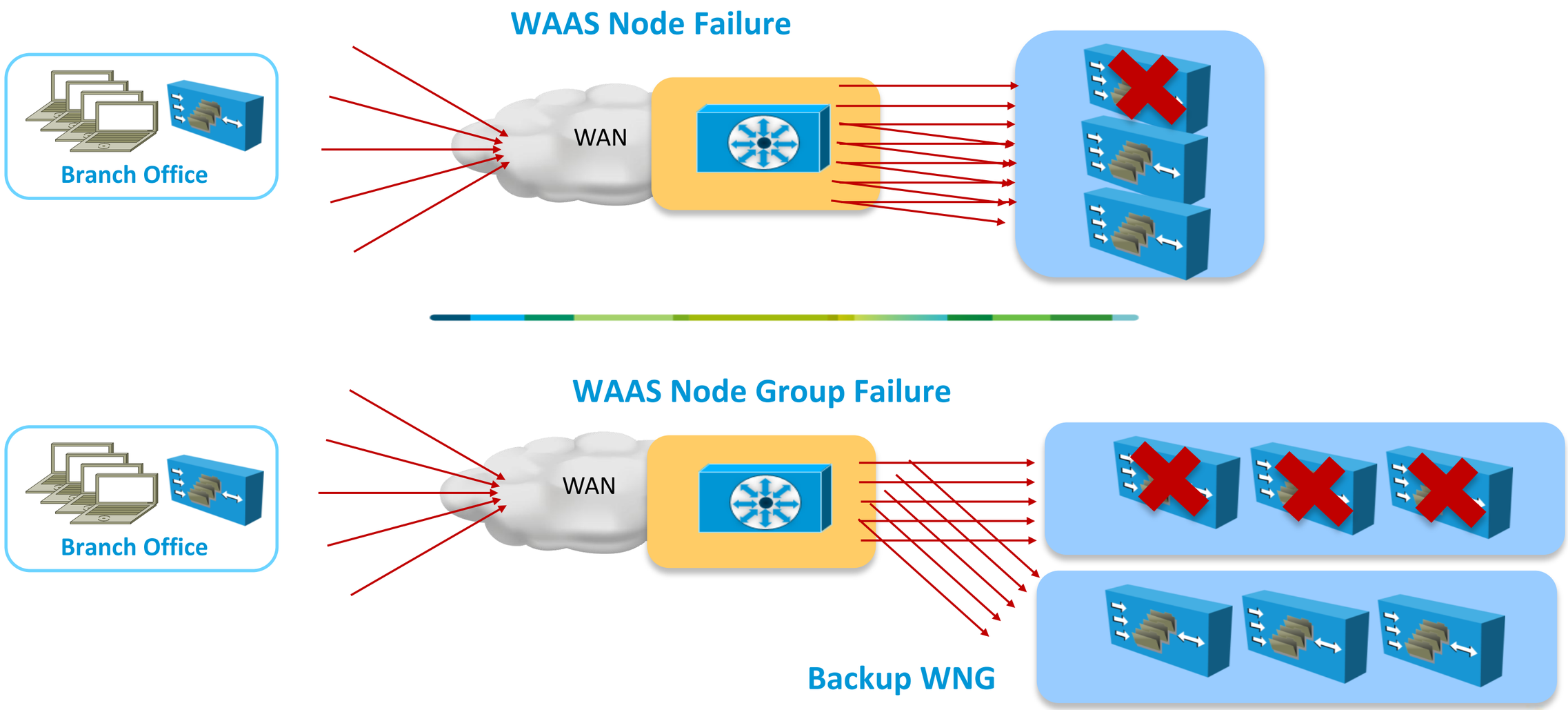
The Nature of Clusters



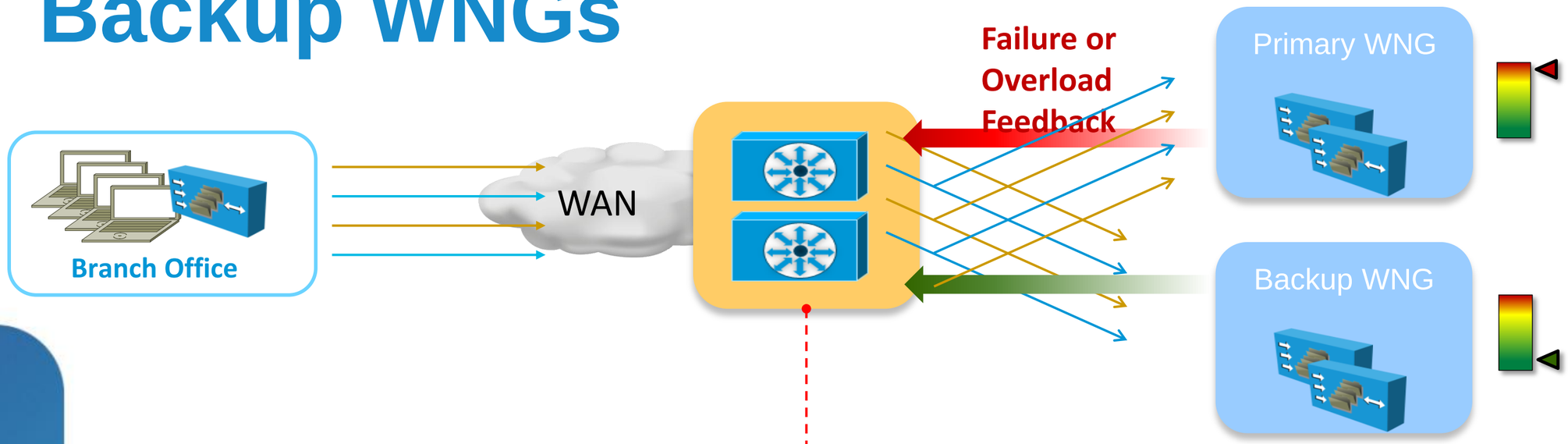
Clusters are aggressive: Bad news travels fast (5-second timer for ANCs or WNs to be removed from stable state).

Clusters are cautious: Good news travels slow (2-minute timer for ANCs to wait until convergence is complete; interception path is shut down until then).

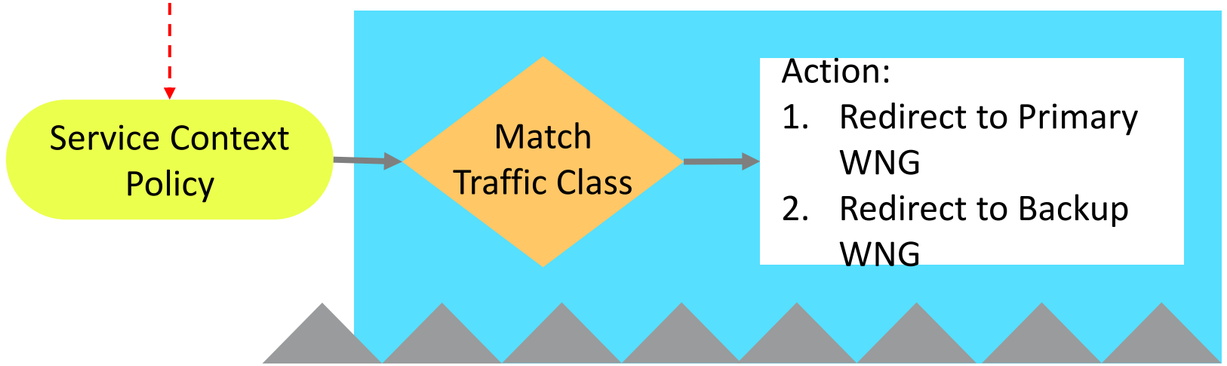
WAAS High Availability



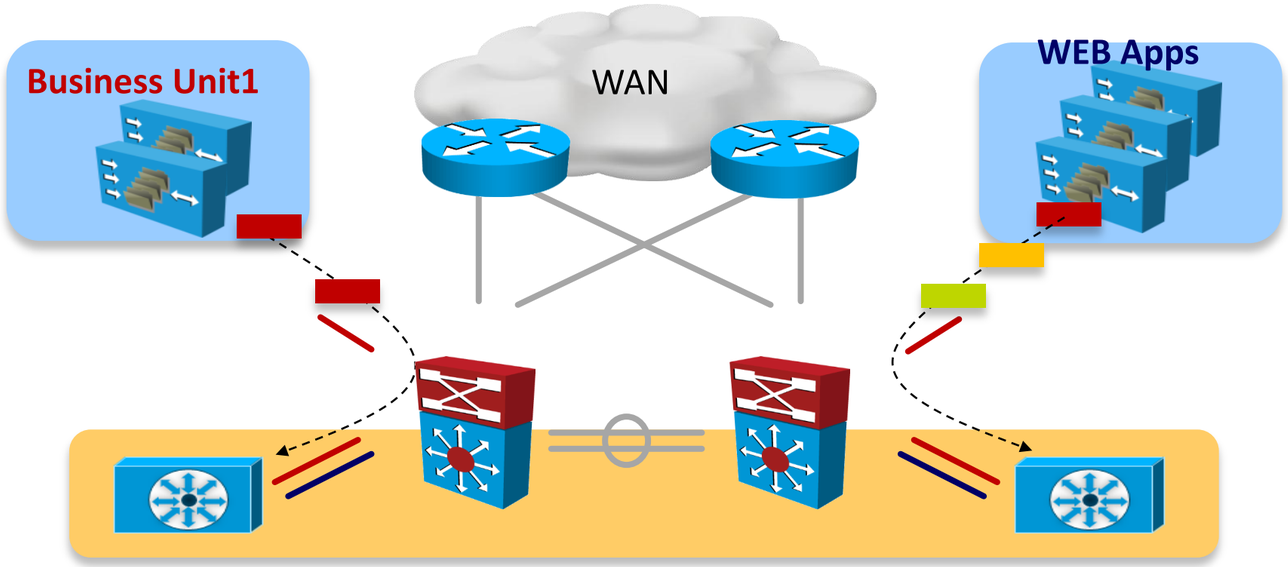
Backup WNGs



- Up to 1 backup WNG per primary WNG.
- Both failure and overload conditions cause new flows to be redirected to backup.
- Backup WNG can also be primary WNG for another traffic class.



Flow Distribution Manager



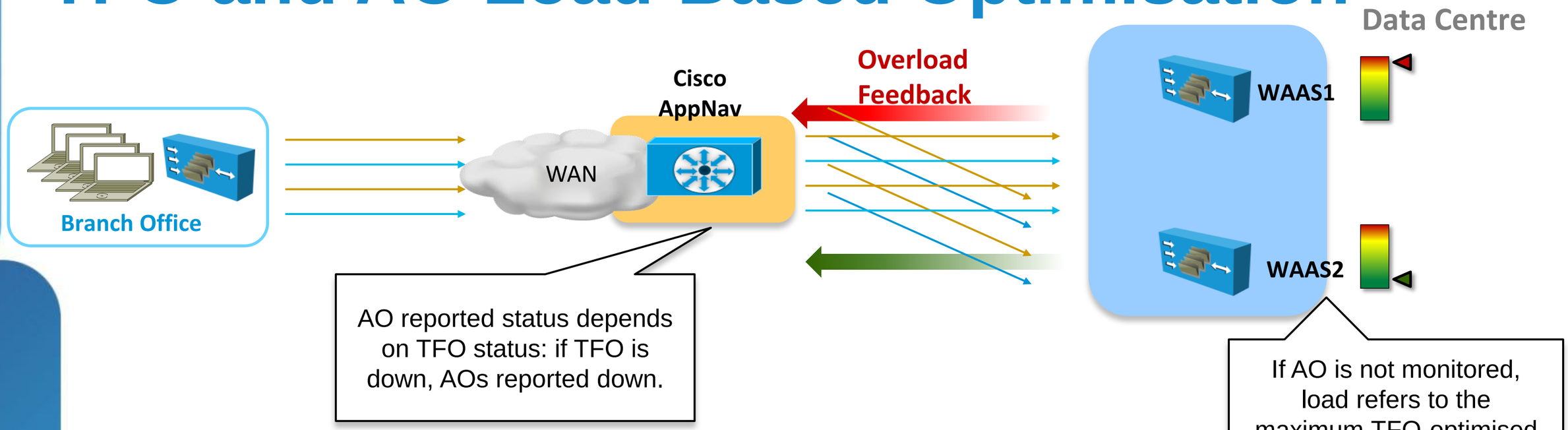
- Business driven bindings
- Dynamic service aware policy

Logical/Business Bindings for WAAS Pools

Dynamic service aware flow distribution:

- **Green:** WAAS accepts new and existing connections
- **Yellow:** WAAS only accepts existing connections
- **Red:** WAAS can not accept any connections

TFO and AO Load-Based Optimisation

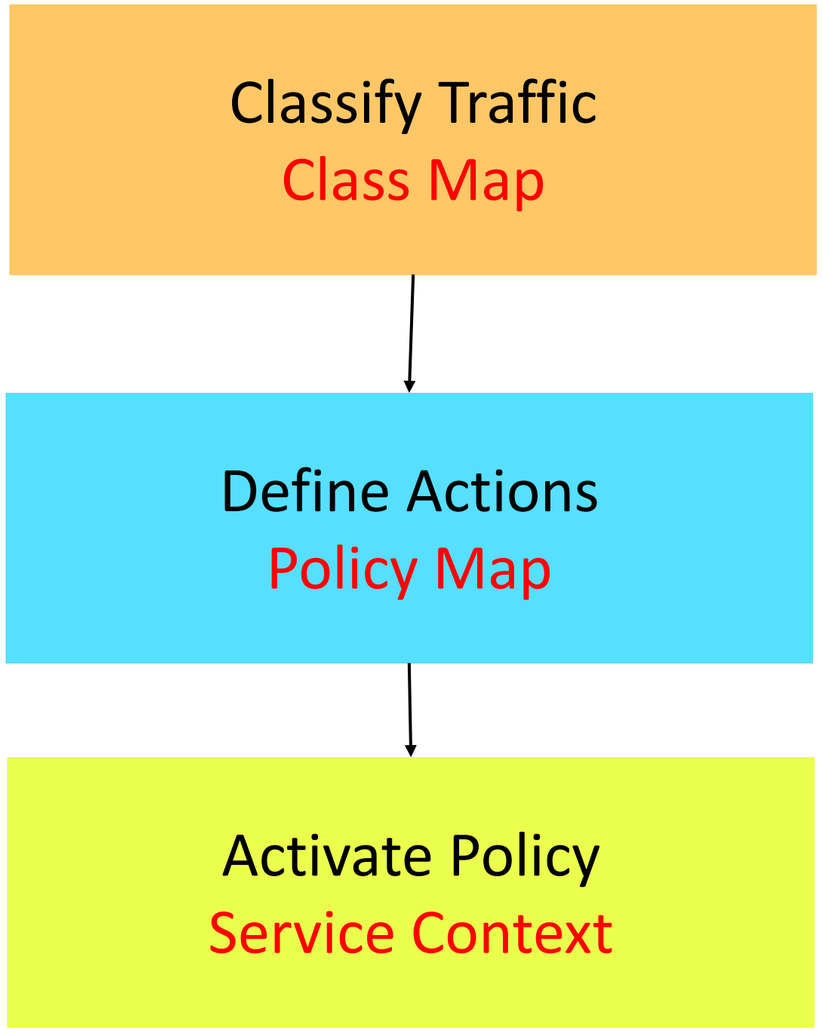


AO not running (not configured, not licensed or disabled)

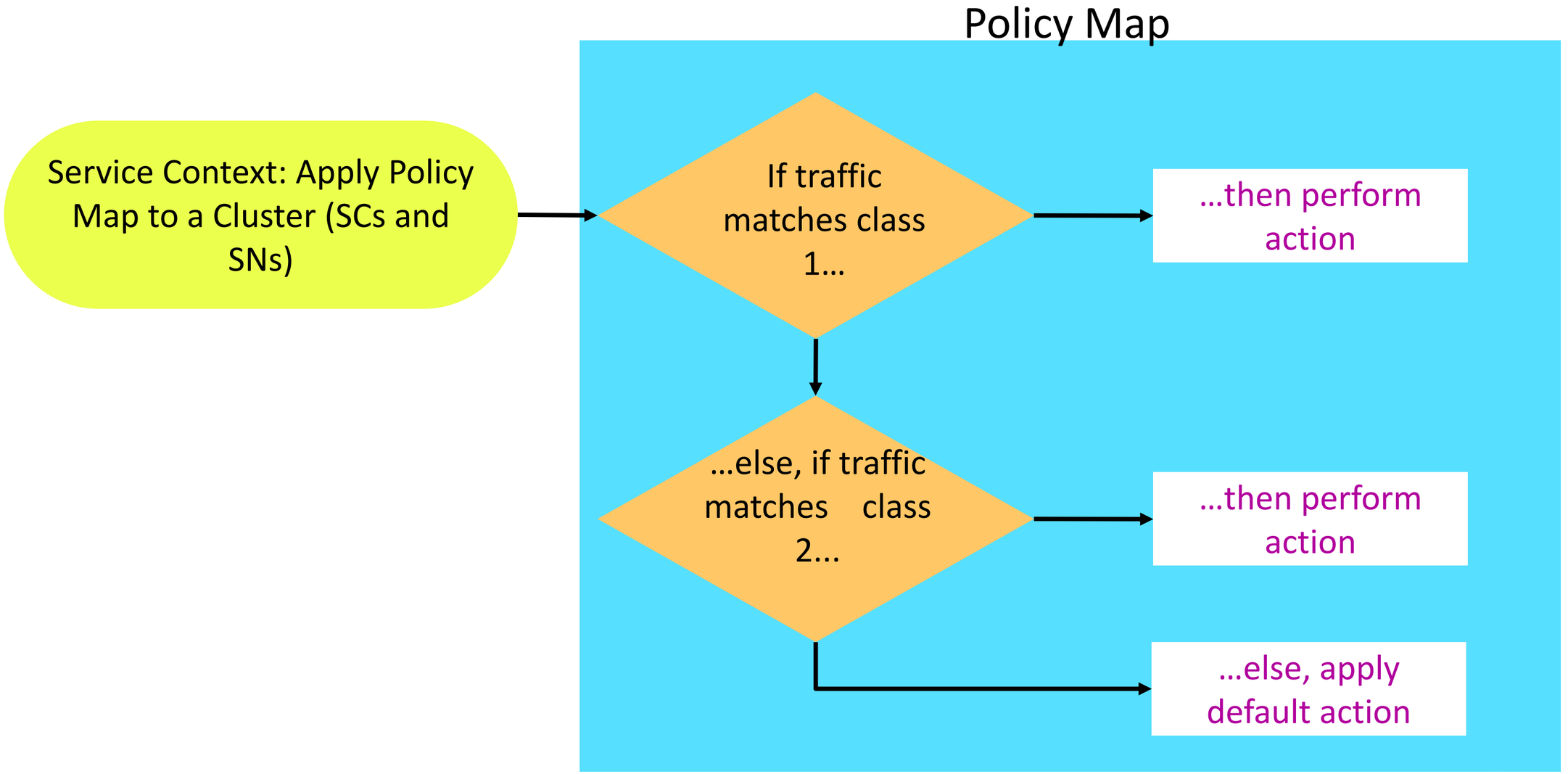
- AO running but no new connections accepted due to:
  - Its connection/resource thresholds exceeded (default 95%)
  - Its license has been revoked
  - It is losing keepalives with policy engine (may be overloaded)
  - Overall device connection/resource thresholds exceeded
  - DRE processing latency is above threshold

Flow Distribution Policies

– Class maps: Identify traffic according to one or more match conditions based on:
  - 3-tuple of source IP, destination IP, and destination port
  - Peer device ID
– Policy maps: Define actions for classified flows:
  - Specify a primary WNG
  - Specify a backup WNG
  - Monitor the load of associated WN
  - Specify a nested policy map
– Service context: Activates policy maps for a given ANCG and WNGs.



Modular, Object Oriented Configuration

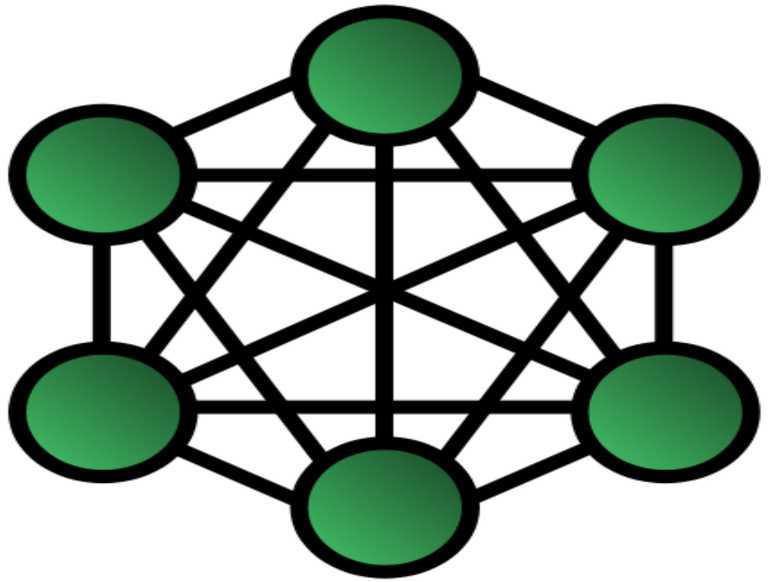


High Availability Considerations

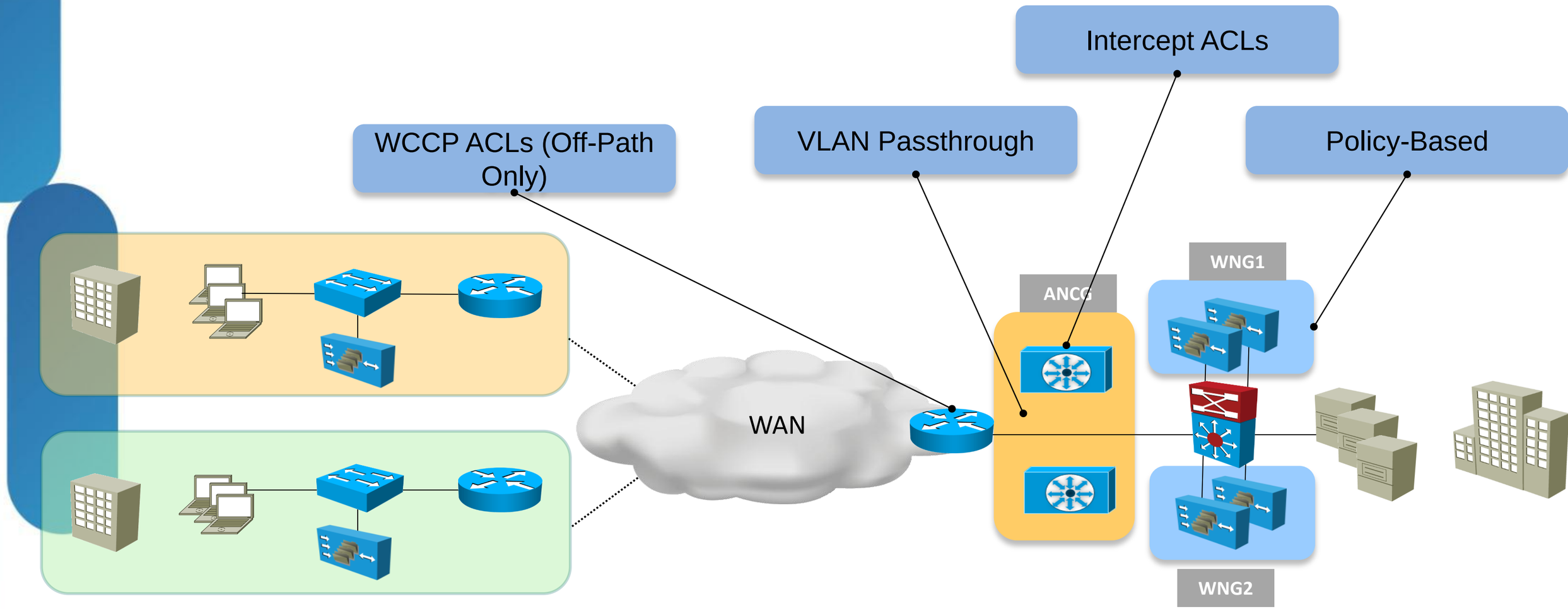
Best Practice

- You must monitor AOs if you want to consider AO load for HA or flow distribution. AOs are NOT monitored by default.
- Consider ANC and WN high availability in separate analysis.
- Consider the implications of oversubscription when defining number of ANCs and WNs.
- Consider using one backup WNG per mission-critical optimisation farm.
- Consider using one or more WNGs as backups for all farms for N+1 high availability.
- Consider also using backup WNGs as a scalability/spillover tool.

Only one AO can be monitored per class in a policy.



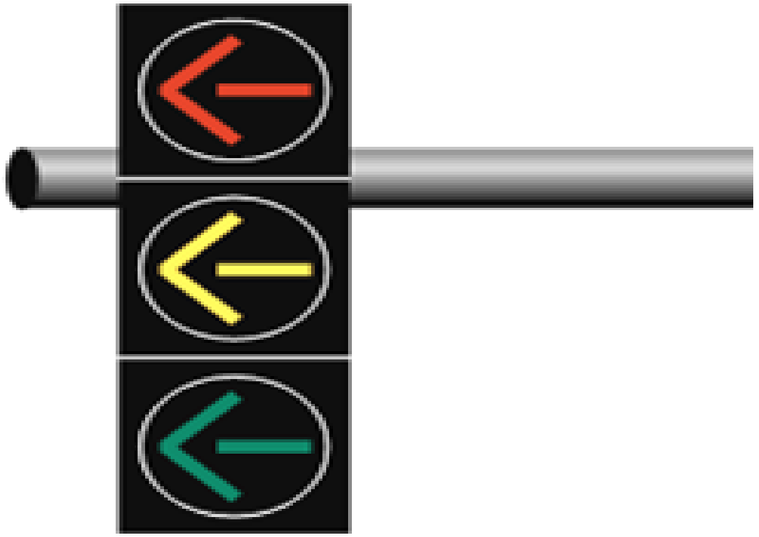
Traffic Bypass Options



Flow Distribution Considerations

Best Practice

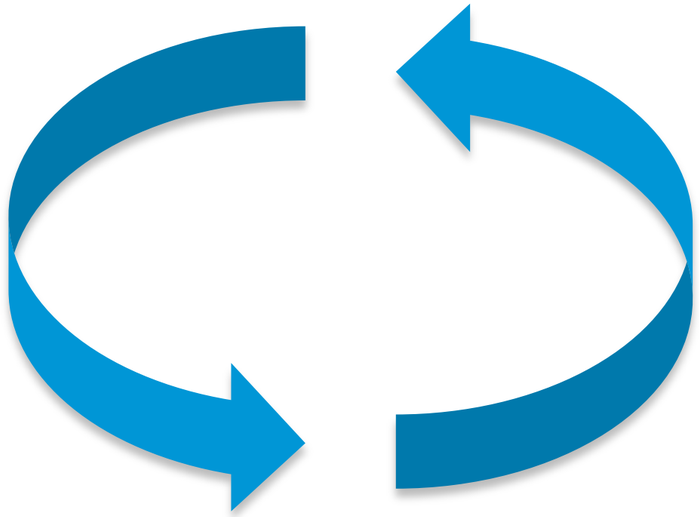
- Use interception ACLs when possible as a bypass tool. It is the most granular and efficient way to create passthrough exceptions.
- Use peer ID in site affinity scenarios for simplified processing.
- Use 3-tuple of source IP/port and destination IP in affinity scenarios for accuracy.
- Used nested policies for modularity to combine sit application affinity.
- Traffic classification is not classful: consider per-destin matching for applications that negotiate ports dynamically.
- Consider using different VLANs per WNG in Private Cloud environments to further segregate customer traffic at layer 2.
- Monitor AOs for load-based flow distribution. Only TFO (connection load) is monitored by default.



Asymmetry Handling Considerations

Best Practice

- In all cases, including inter-DC scenarios, all ANCs must belong to the same ANCG (same cluster).
- Consider tuning heartbeat timers (from default 5 seconds) in inter-DC scenarios to consider inter-DC delay for heartbeats.
- Plan for alarm detection in degraded cluster scenarios, where partial visibility or splits will affect asymmetry handling.
- In inter-DC scenarios, configure local ANCs to distribute flows to the local WNGs for flow distribution proximity.



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!