The bridge to possible

Роль SD-WAN в сервисах совместной работы

Юрий Довгань

Системный инженер

ydovgan@cisco.com

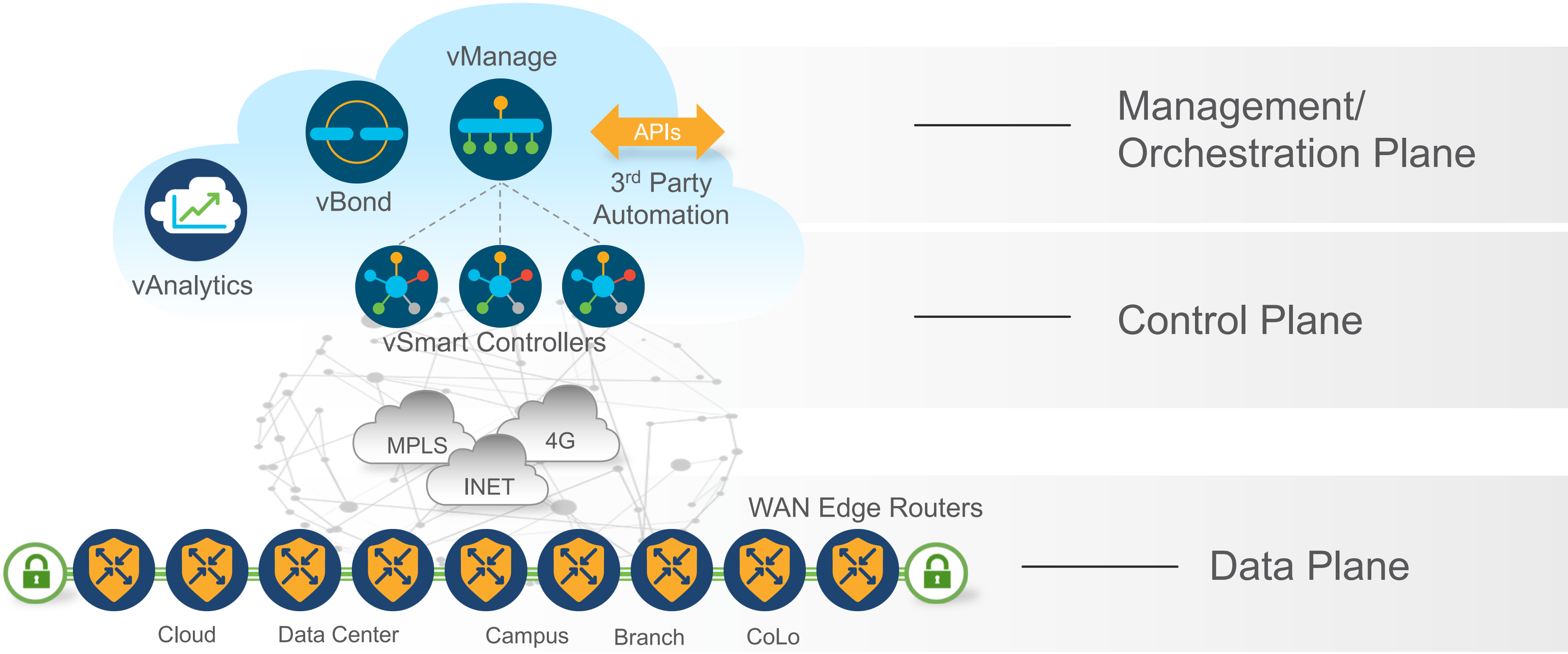
Содержание

- Обзор Cisco SD-WAN
- Внедрение UC на ISR и Catalyst 8000 в режиме SD-WAN
- Оптимизация унифицированных коммуникаций с помощью SD-WAN
- Ключевые выводы

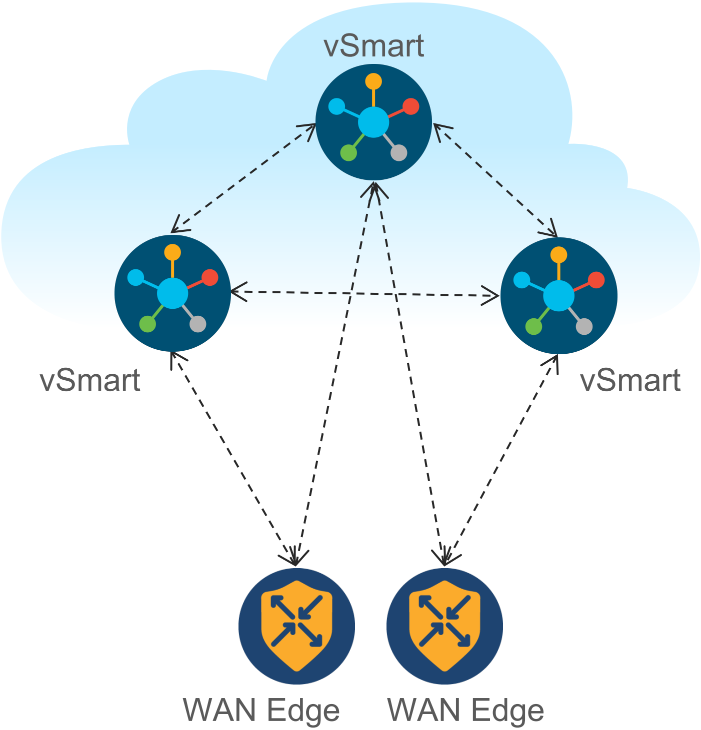
Обзор Cisco SD-WAN

Обзор решения Cisco SD-WAN

Применение SDN подходов к WAN-сетям



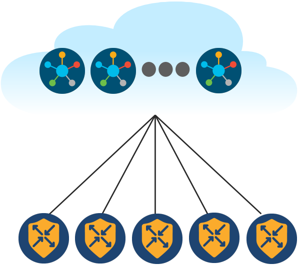
Overlay Management Protocol



Note: WAN Edge routers need not connect to all vSmart Controllers

- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane complexity and raises overall solution scale

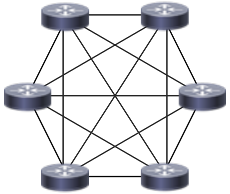
SD-WAN



O(n) Control Complexity

VS

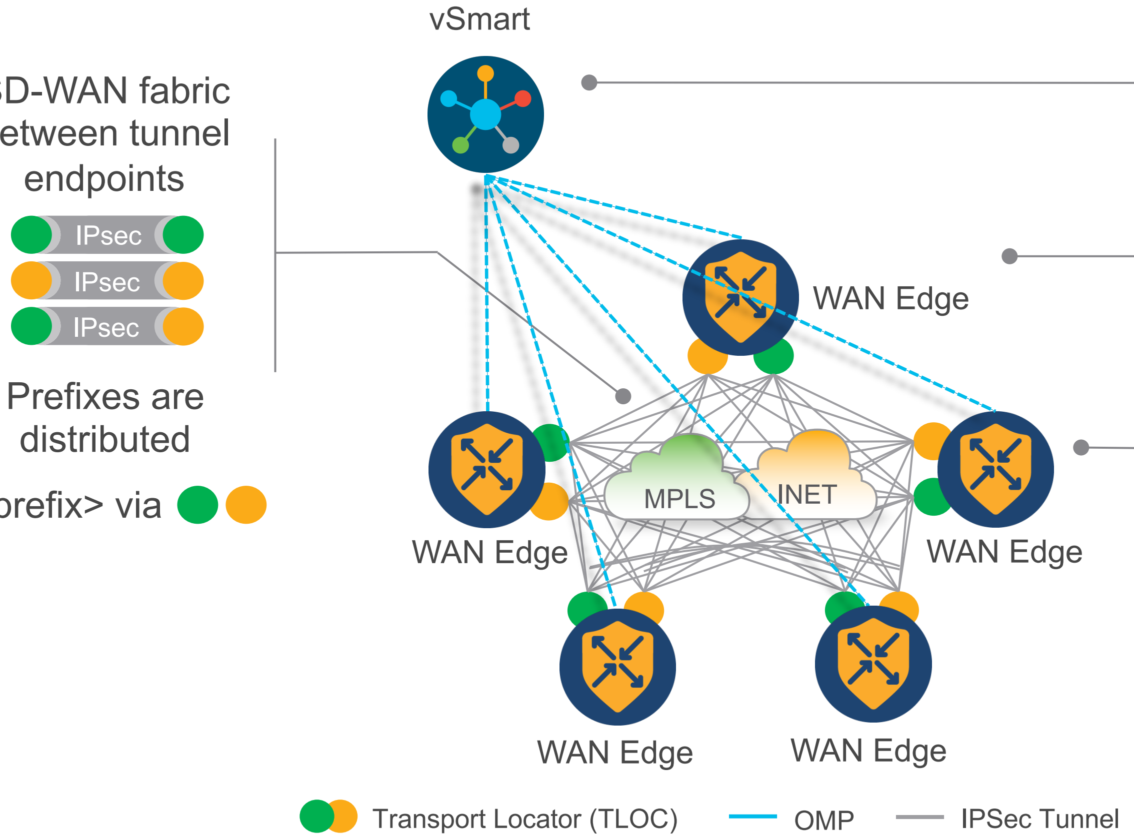
Traditional



O(n^2) Control Complexity

Data Plane – установка туннелей

SD-WAN fabric between tunnel endpoints



Prefixes are distributed

<prefix> via

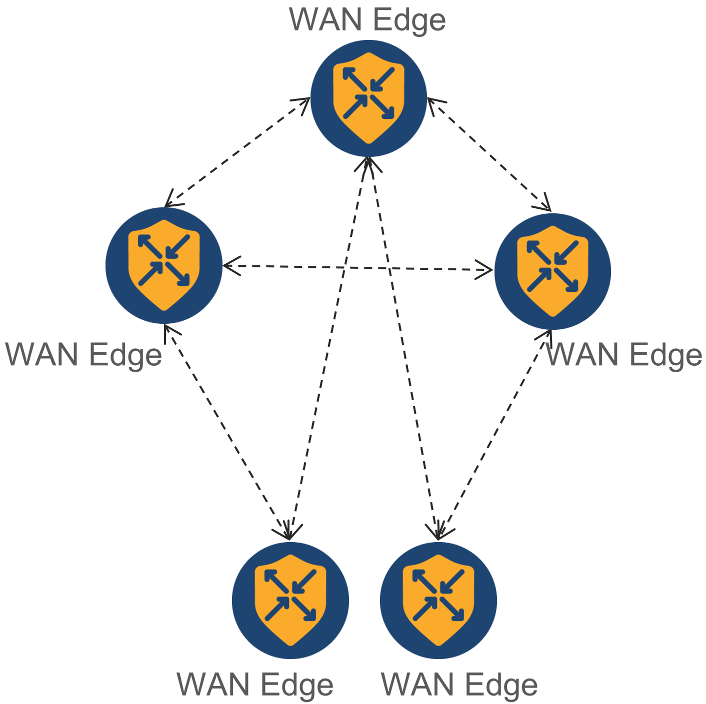
vSmarts advertise routes to WAN Edges in OMP updates

Routes advertised to vSmarts in OMP updates

Local Routes

- Local prefixes (OSPF/BGP)
- SD-WAN tunnel endpoints (TLOCs)

Bidirectional Forwarding Detection (BFD)



Path liveliness and quality measurement detection protocol

- Up/Down, loss/latency/jitter, IPSec tunnel MTU

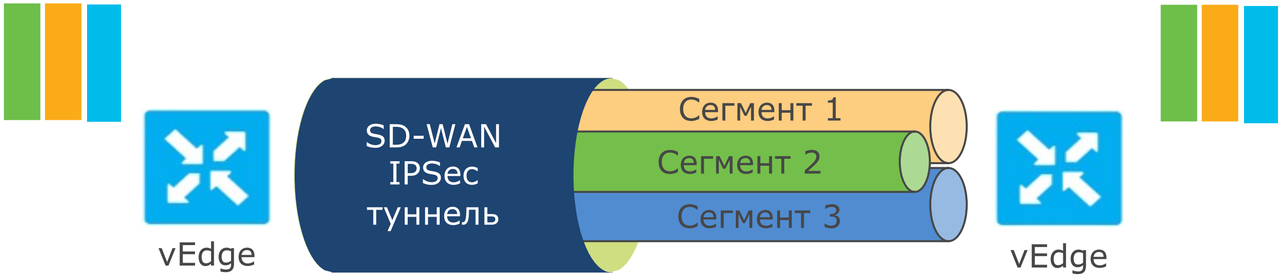
Runs between all WAN Edge and WAN Edge Cloud routers in the topology

- Inside IPSec tunnels
- Operates in echo mode
- Automatically invoked at IPSec tunnel establishment
- Cannot be disabled

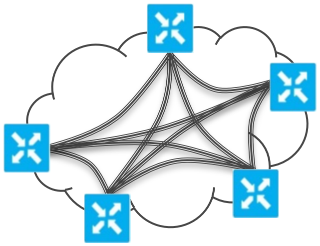
Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection

- Fully customizable per-WAN Edge, per-color

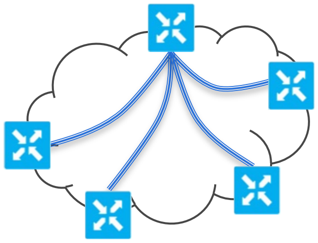
Безопасная сегментация



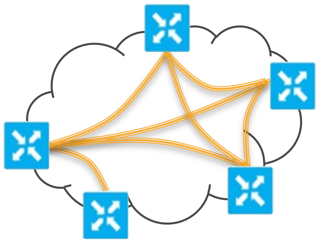
Уникальная топология для каждого VRF



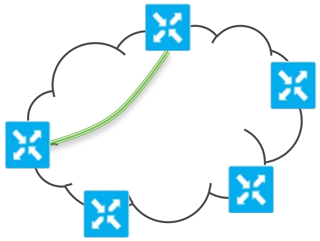
Full Mesh топология



Централизованная
Hub-and-Spoke

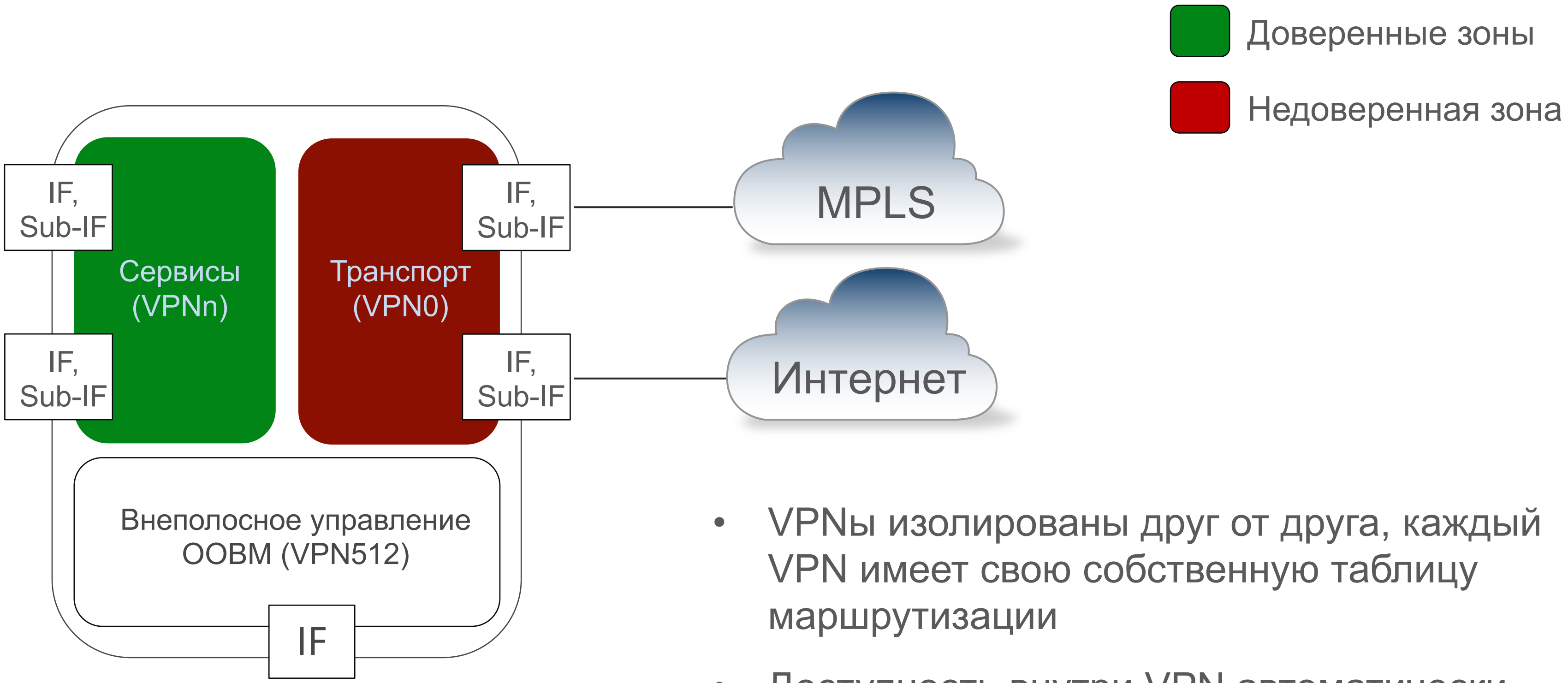


Частично связанная
Partial Mesh



Точка-точка
Point-to-Point

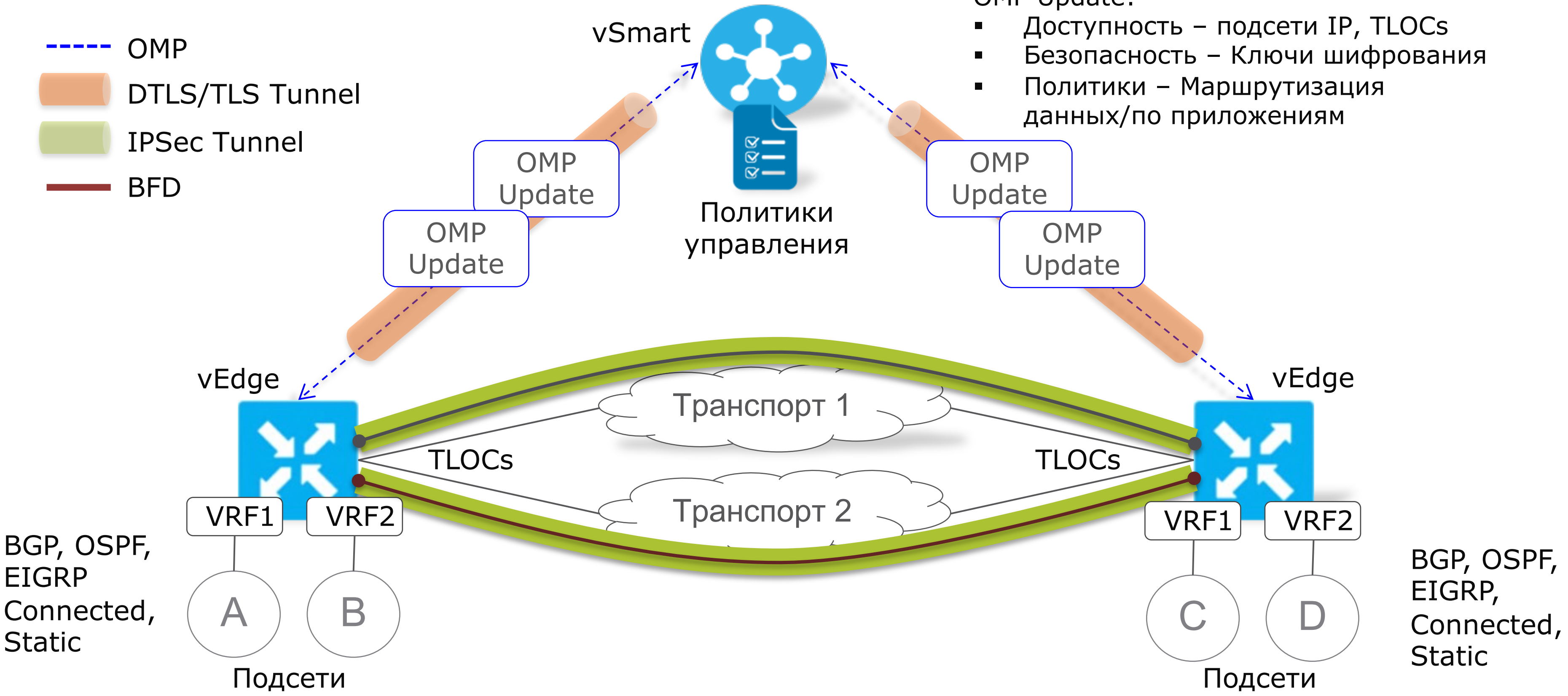
Понятие VPN (VRF) и зон безопасности в vEdge



- VPNы изолированы друг от друга, каждый VPN имеет свою собственную таблицу маршрутизации
- Доступность внутри VPN автоматически анонсируется через OMP

Как работает SD-WAN фабрика

OMP Update:
- Доступность – подсети IP, TLOCs
- Безопасность – Ключи шифрования
- Политики – Маршрутизация данных/по приложениям



Платформы для Cisco SD-WAN

Только SD-WAN

vEdge 100

50-100M

vEdge 1000

175-300M

vEdge 2000

vEdge 5000

1-2G

ISR 1100-4G

125-220M

ISR 1100-6G

300-550M

SD-WAN с сервисами (поддержка UC)

ISR 1000

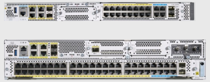
Next-gen Performance Flexibility

50-200M

ISR 4000

Modular Integrated services

Catalyst 8000



ASR 1000

High-performance with redundancy

1.6-19G (Basic)
0.7-9G (Medium)

Виртуализация

ENCS 5100

ENCS 5400

Публичные и частные облака

amazon web services

KVM

Microsoft Azure

vmware ESXi

Внедрение UC на ISR и Catalyst 8000 в режиме SD-WAN

Поддержка унифицированных коммуникаций (для vManage 20.3-20.4)

Problem

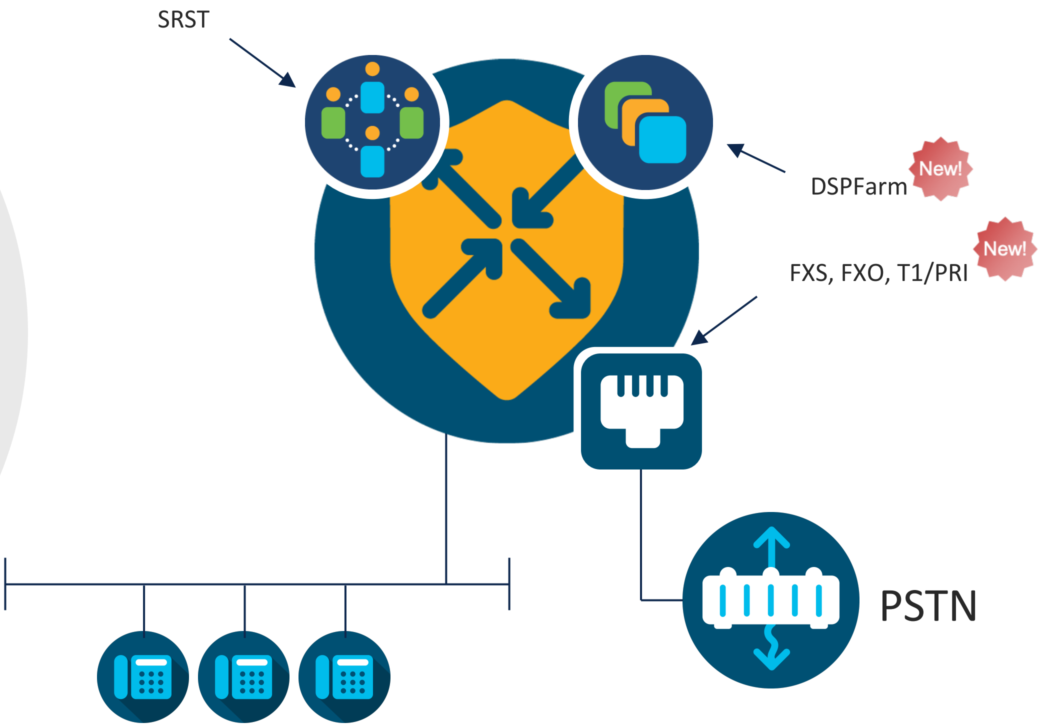
Customers seeking UC and SD-WAN integration were previously forced into a two-box solution at the branch. One box to terminate the SD-WAN fabric and another to handle UC termination. This increased cost, complexity and operational overhead.

Solution

As of v20.1 and 17.2.1 (Phase 1), Cisco SD-WAN now supports UC and SD-WAN within a single box (analog, basic SIP and SRST). Version 20.3 / 17.3 (Phase 2) adds additional capability for T1/PRI termination, DSPfarming and Fax Passthrough.

Caveats / Prerequisites

IOS-XE (cEdge) ISR only, 4GB DRAM is supported, CUBE is not supported, H323/MGCP/SCCP are not supported, T1/PRI requires separate PVDM



FXO/FXS поддержка в SD-WAN

Connect to PBX or key systems, or provide off-premises connections to the public switched telephone network (PSTN)

Built-in DSP with high analog port-density support

NIM-2FXO
NIM-4FXO
NIM-2FXSP
NIM-4FXSP

NIM-2FXS/4FXOP
SM-X-8FXS/12FXO
SM-X-16FXS/2FXO
SM-X-24FXS/4FXO

SM-X-72FXS

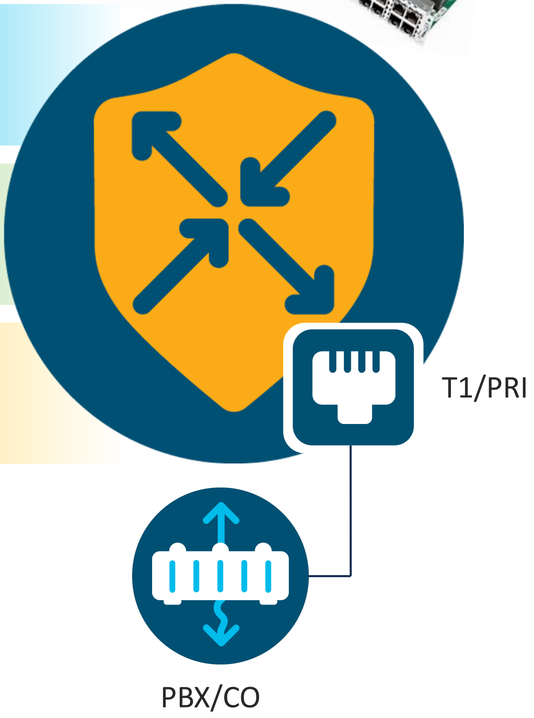
T1/E1 голосовая PRI поддержка в SD-WAN

Packet Voice Solutions support (PBX & Central-Office Connectivity)

PSTN termination with multi calls per port: T1 PRI (23) and E1 (30)

NIM-1MFT-T1E1
NIM-2MFT-T1E1
NIM-4MFT-T1E1
NIM-8MFT-T1E1

NIM-1CE1T1-PRI
NIM-2CE1T1-PRI
NIM-8CE1T1-PRI



TIP

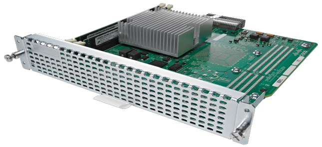
- T1/E1 Voice module contains onboard PVDM4 Slot
- PVDM4 Module required for T1/E1 packetization (purchased separately)
- Supported ISDN Switchtypes: QSIG, NET5, NTT, 4ESS, 5ESS, DMS100, and NI

DSPFarm сервисы в SD-WAN

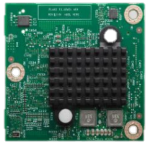
Multi party audio conferencing with (8,16, 32) participants

Save bandwidth with audio codec transcoding

Media Termination Point for IP Calls
(DTMF Conversion, SIP call bridging, Trusted Relay Point, etc.)



Form Factor:
SM-X-PVDM-500
SM-X-PVDM-1000
SM-X-PVDM-2000
SM-X-PVDM-3000

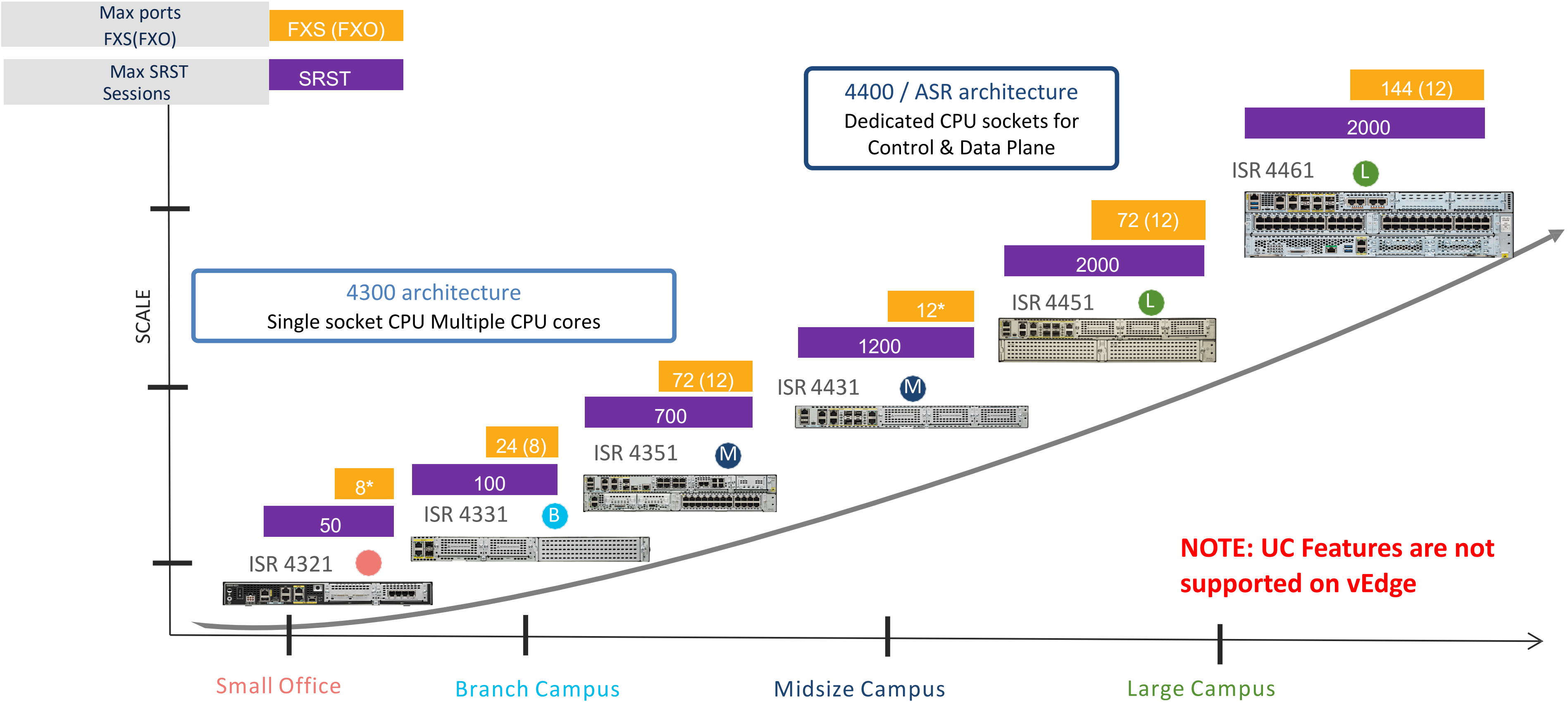


Form Factor:
PVDM4 – 32
PVDM4 – 64
PVDM4 – 128
PVDM4 – 256

Form Factor:
NIM-PVDM-32
NIM-PVDM-64
NIM-PVDM-128
NIM-PVDM-256

NIM-PVDM Modules for IP Voice Services
SM modules for high density DSP usage

ISR 4000 IOS XE / SDWAN UC Scale



[DSP Calculator]

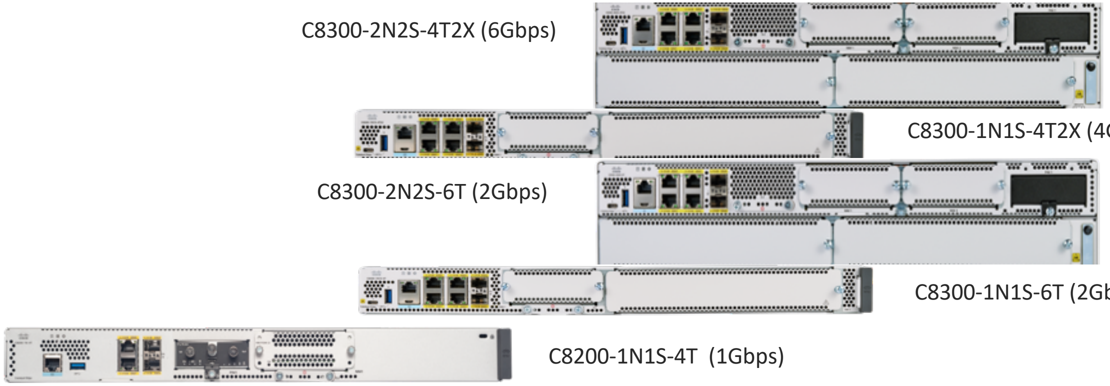
[ISR UCM Datasheet]

Cisco Catalyst 8000 Edge Platforms Family

The Leading SD-WAN Edge Platforms with Rich Services

Performance and Rich Services

2500 Phones on each platform



Scalable Architecture with x86 and QFP

Number in () is SD-WAN IPsec throughput with IMIX

UC настройка и политики

vManage

Does not participate in Call Routing

Provisions ISR for UC

- Distributed Dial Plan (SIP Dial Peer)
- Call Manipulation (Translation)
- Media/Codec Selection
- SRST

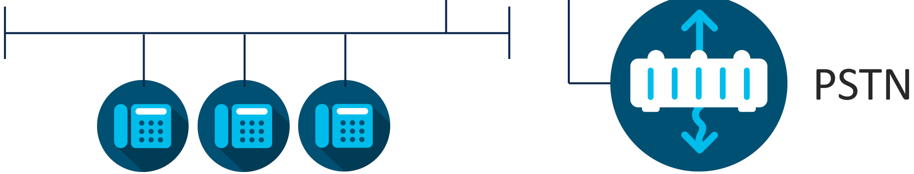
Participates in Data Plane

Provides extended Dial Plan support

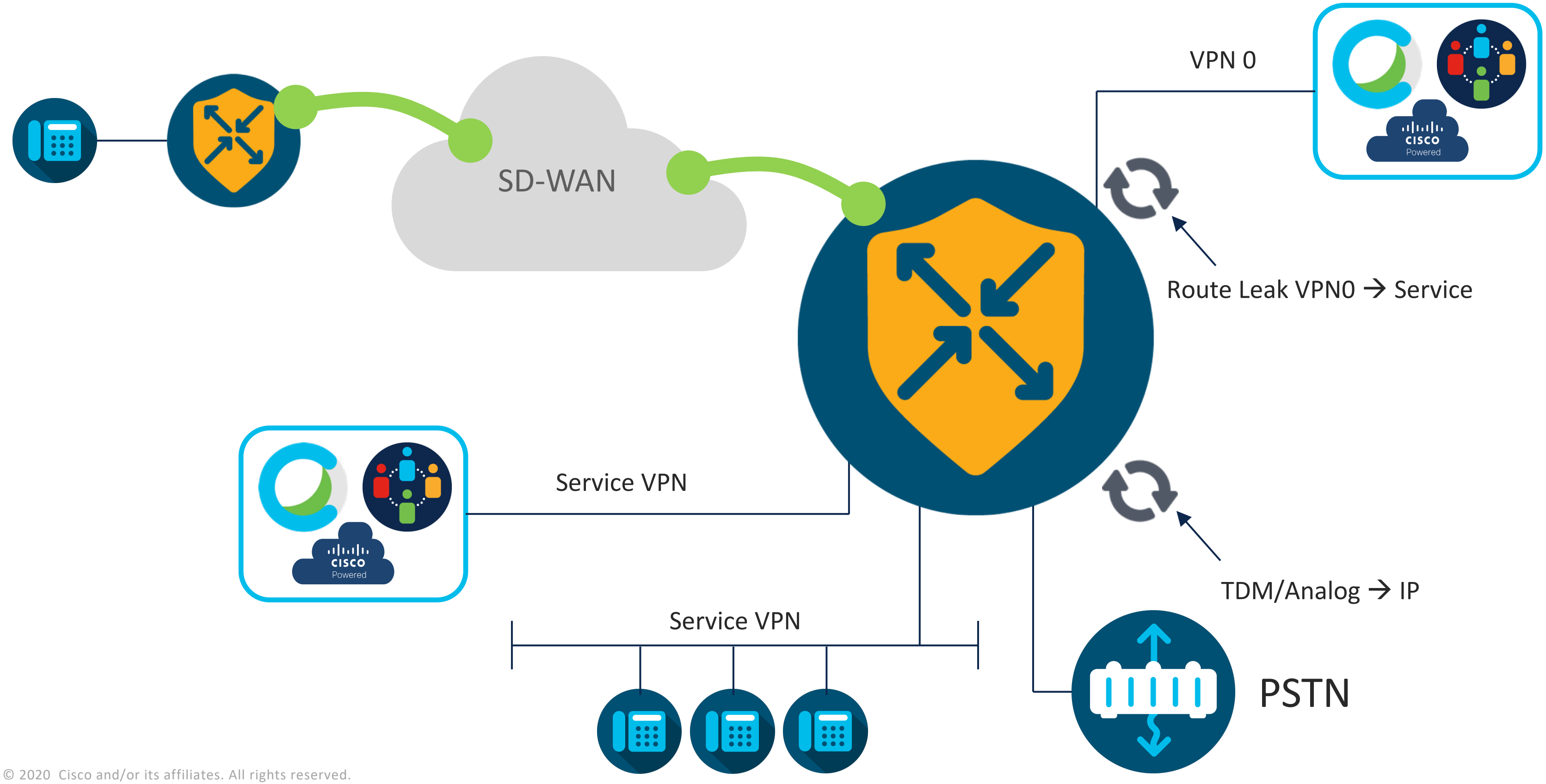
- Enterprise call routing
- Media Termination
- SIP

Does not invoke configuration change

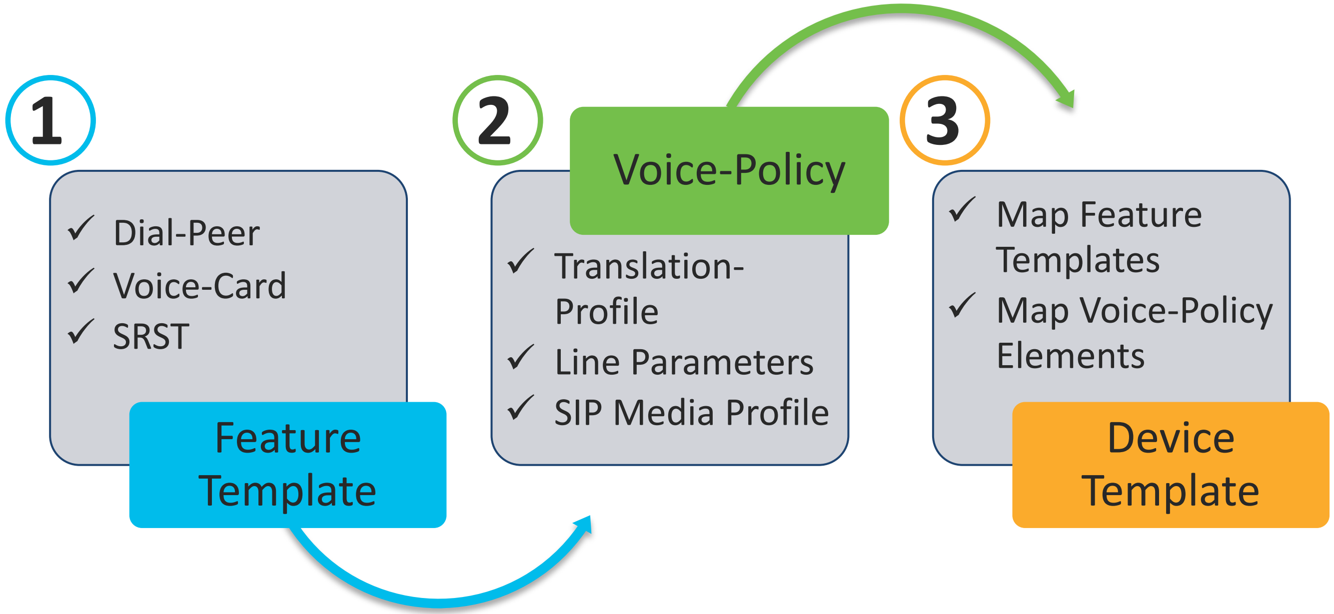
Call Control (CUCM)



Поддерживаемые сценарии управления вызовами



Процесс внедрения UC в SD-WAN

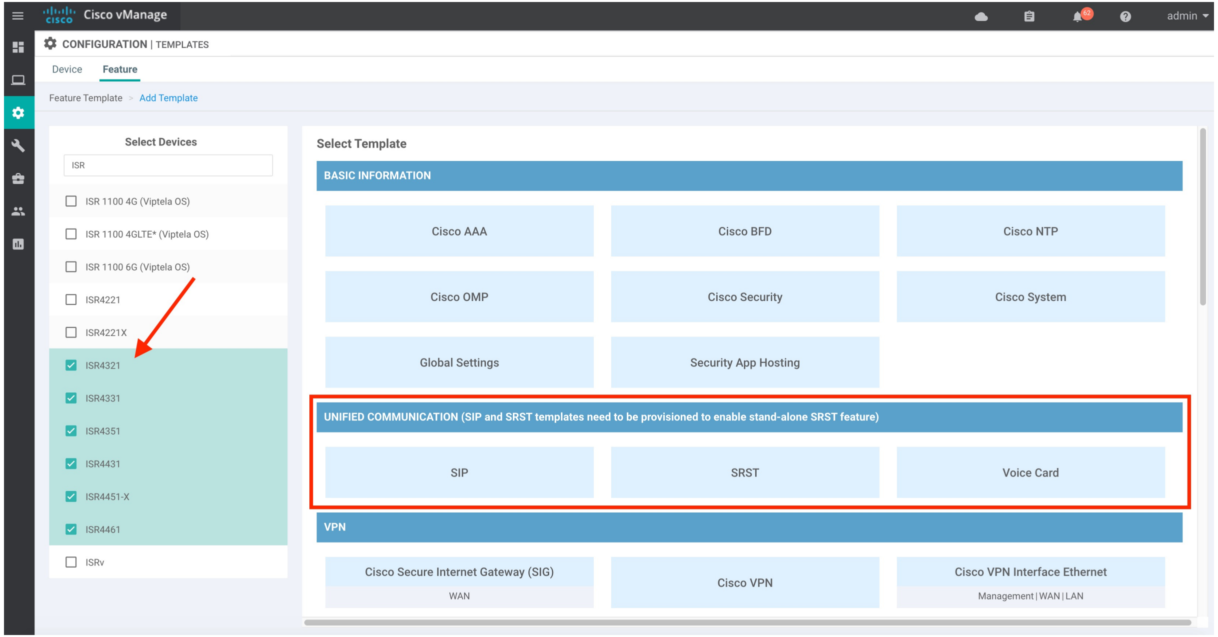


DEMO

Voice Template Configuration

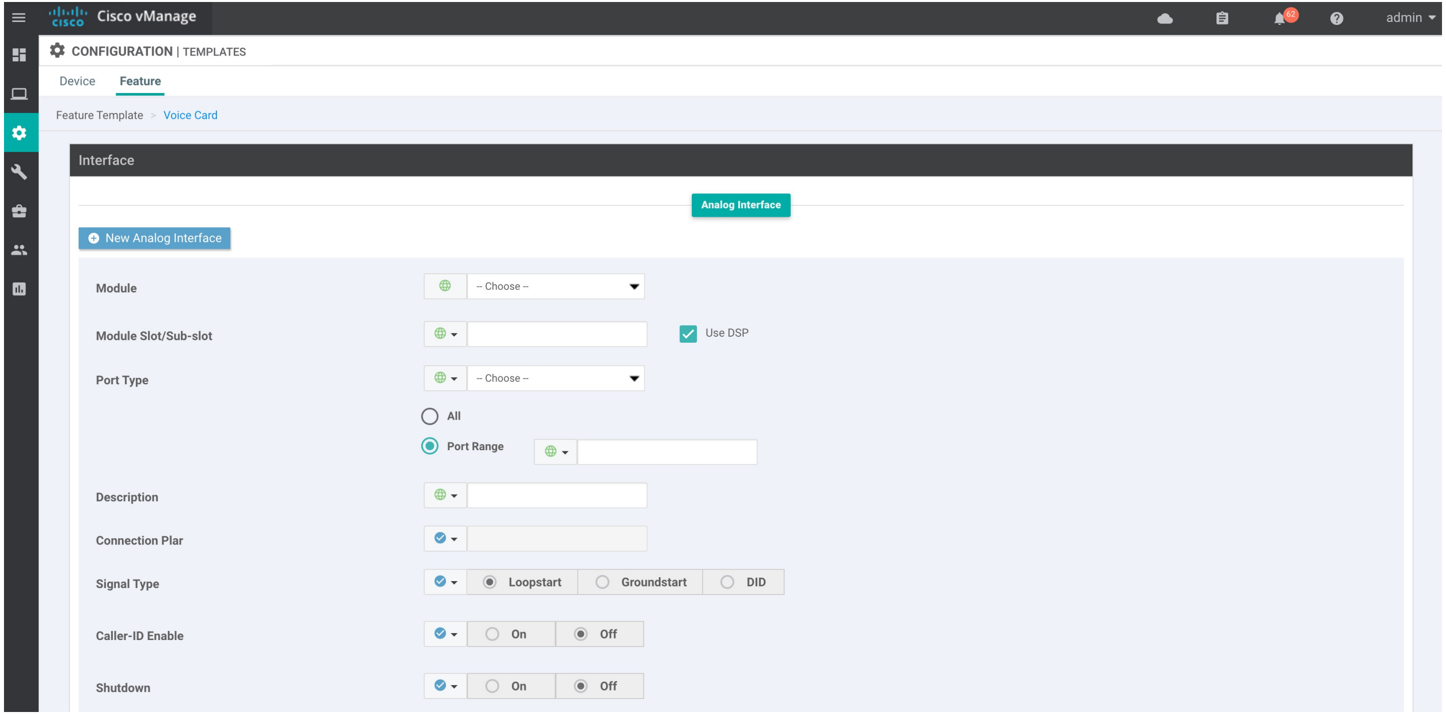
Configuration → Templates → Feature (Tab) → Add New

Configuration of voice-ports and their associated Dial Plan is handled through vManage Templates. Feature Templates are created first to define physical port parameters (slot, subslot, etc.), POTS/SIP Dial Plan and SRST parameters. These parameters are then attached to a Device Template along with a Voice Policy.



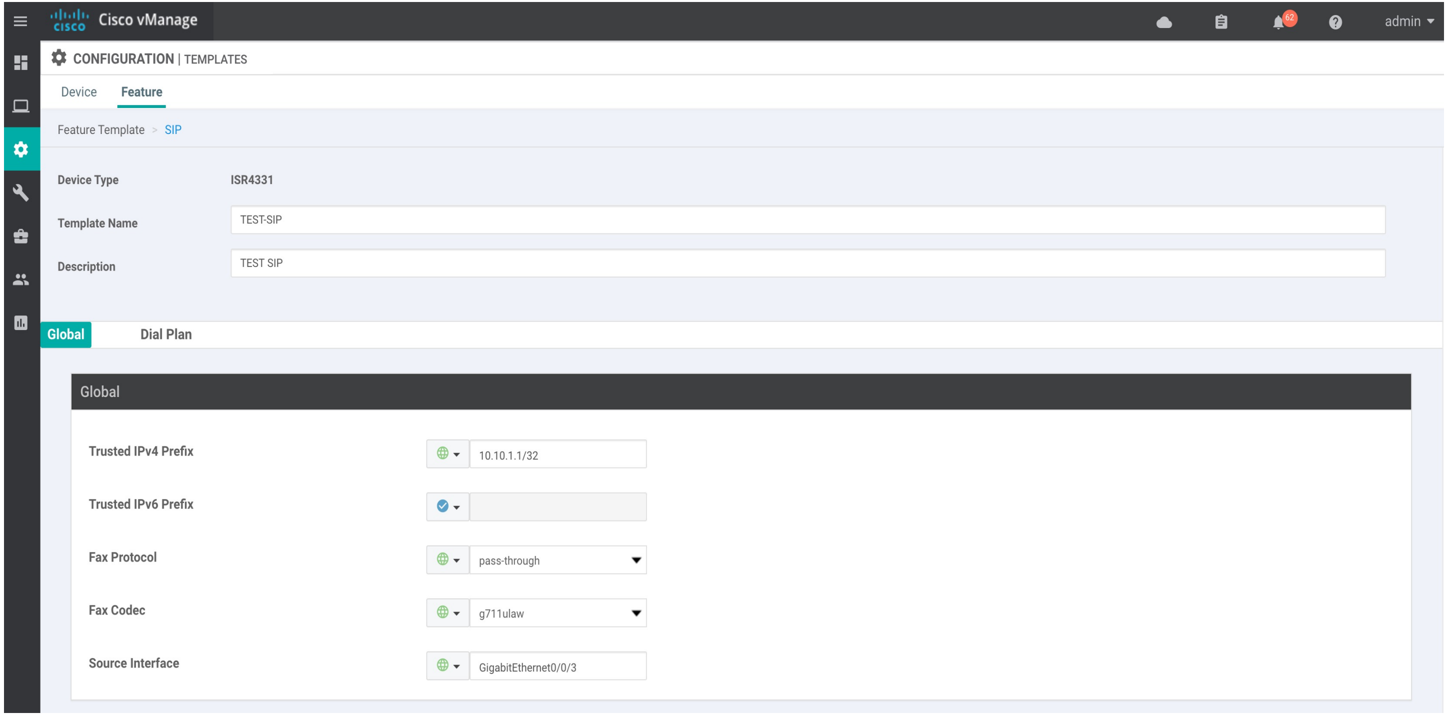
Voice Template Configuration

Configuration → Templates → Feature (Tab) → Add New → (Select ISR) → Voice-Card



Voice Template Configuration

Configuration → Templates → Feature (Tab) → Add New → (Select ISR) → SIP



Voice Template Configuration

Configuration → Templates → Feature (Tab) → Add New → (Select ISR) → SIP

Dial Plan

Upload Dial Peer List | New Dial Peer

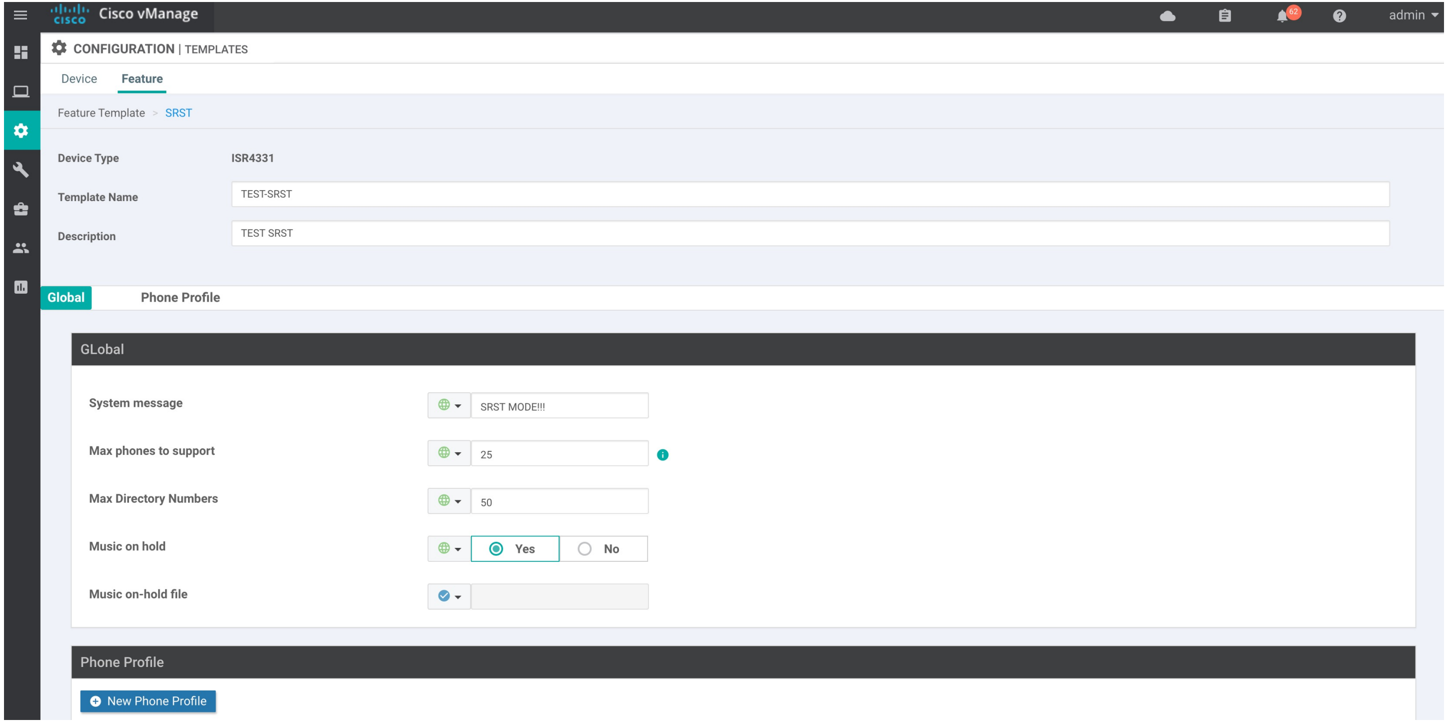
Search Options

Total Rows: 3

Tag	Dial Peer Type	Direction	Description	Number Pattern	Forward Digits Type	Transport Protocol	Action
100	POTS	Incoming		.	None		
200	SIP	Outgoing		9T	None	UDP	
101	POTS	Incoming		,	None		

Voice Template Configuration

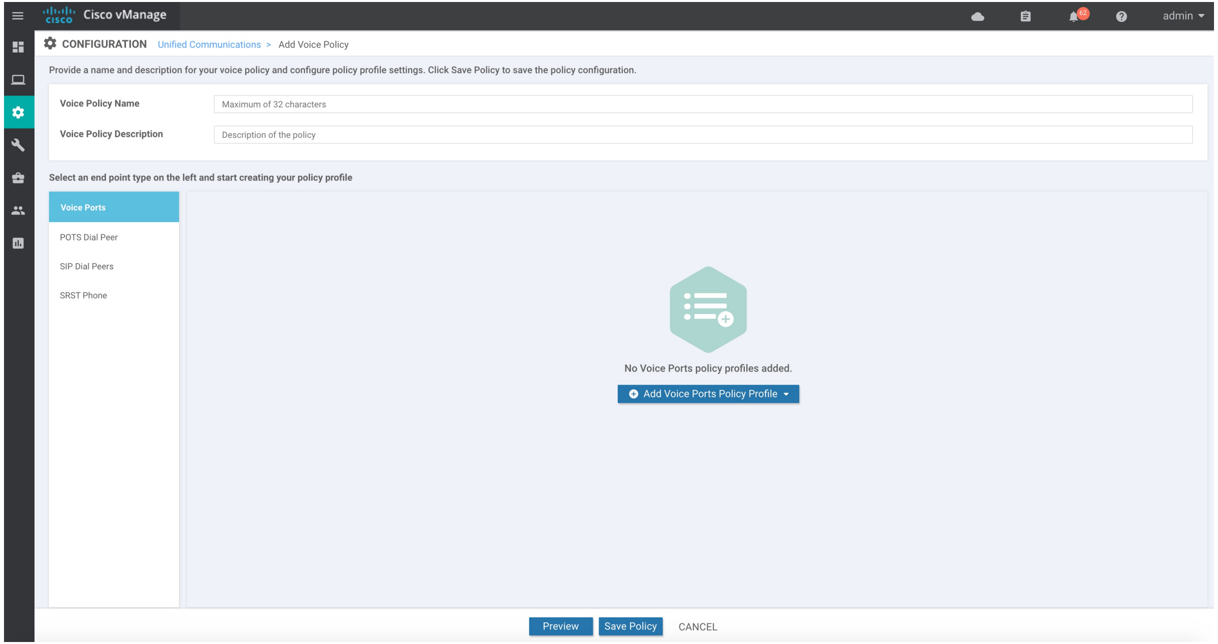
Configuration → Templates → Feature (Tab) → Add New → (Select ISR) → SRST



Voice Policy Configuration

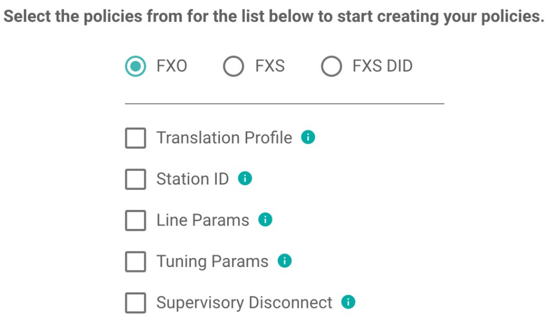
Configuration → Unified Communications → Add Voice Policy

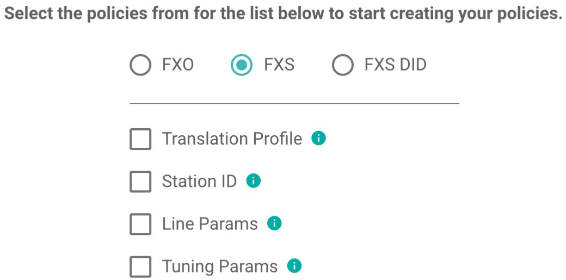
Configuration of Voice Policy is handled through the Policy workflows of vManage (similar to Localized Data Policy). Voice Policy defines many of the parameters that augment voice-ports and Dial Plan (such as Translation Profiles, Supervisory Disconnect, Station ID, DTMF relay, etc.).

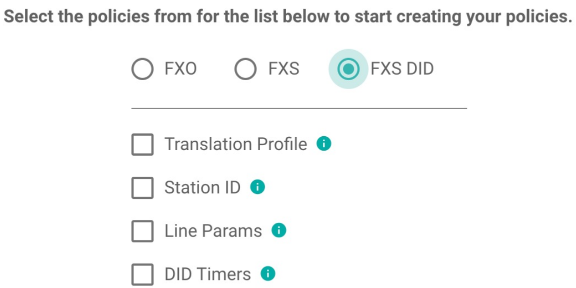


Voice Policy Configuration

Configuration → Unified Communications → Add Voice Policy → Add Voice Ports Policy Profile

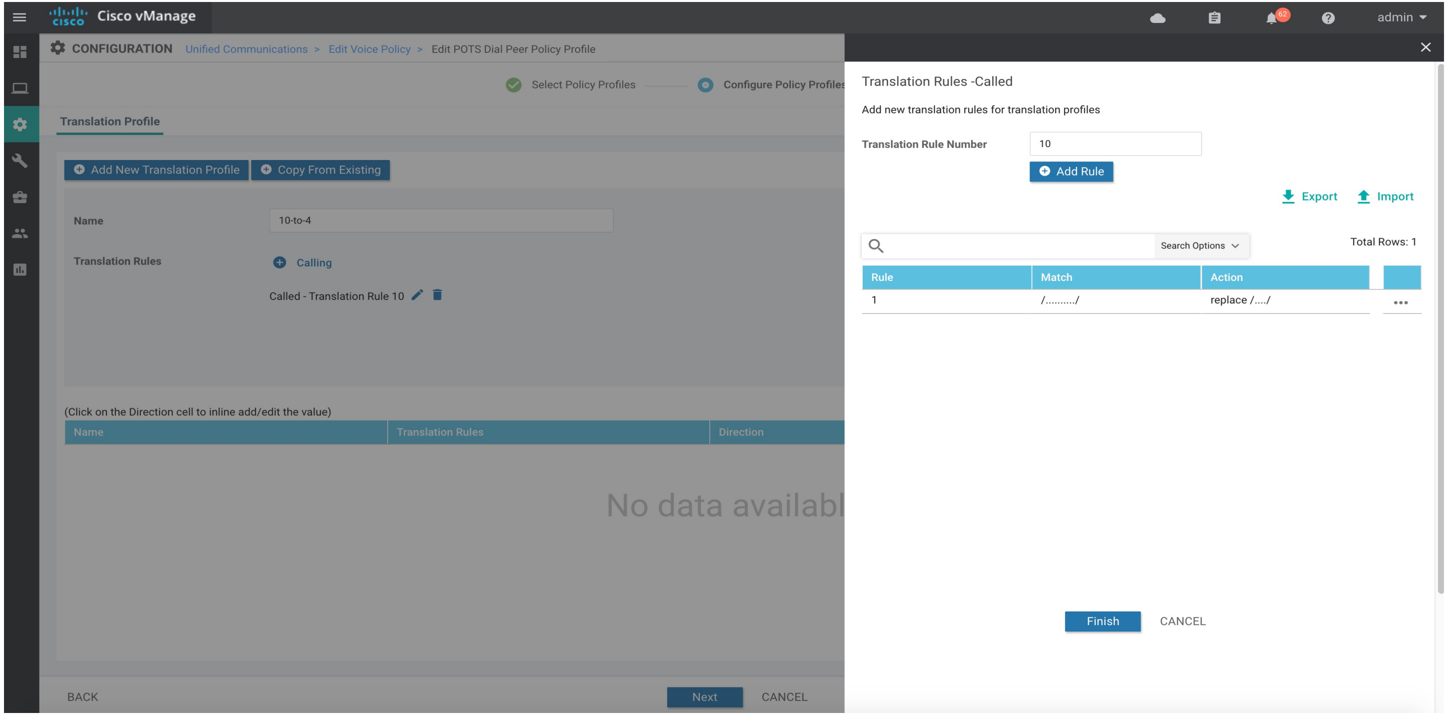






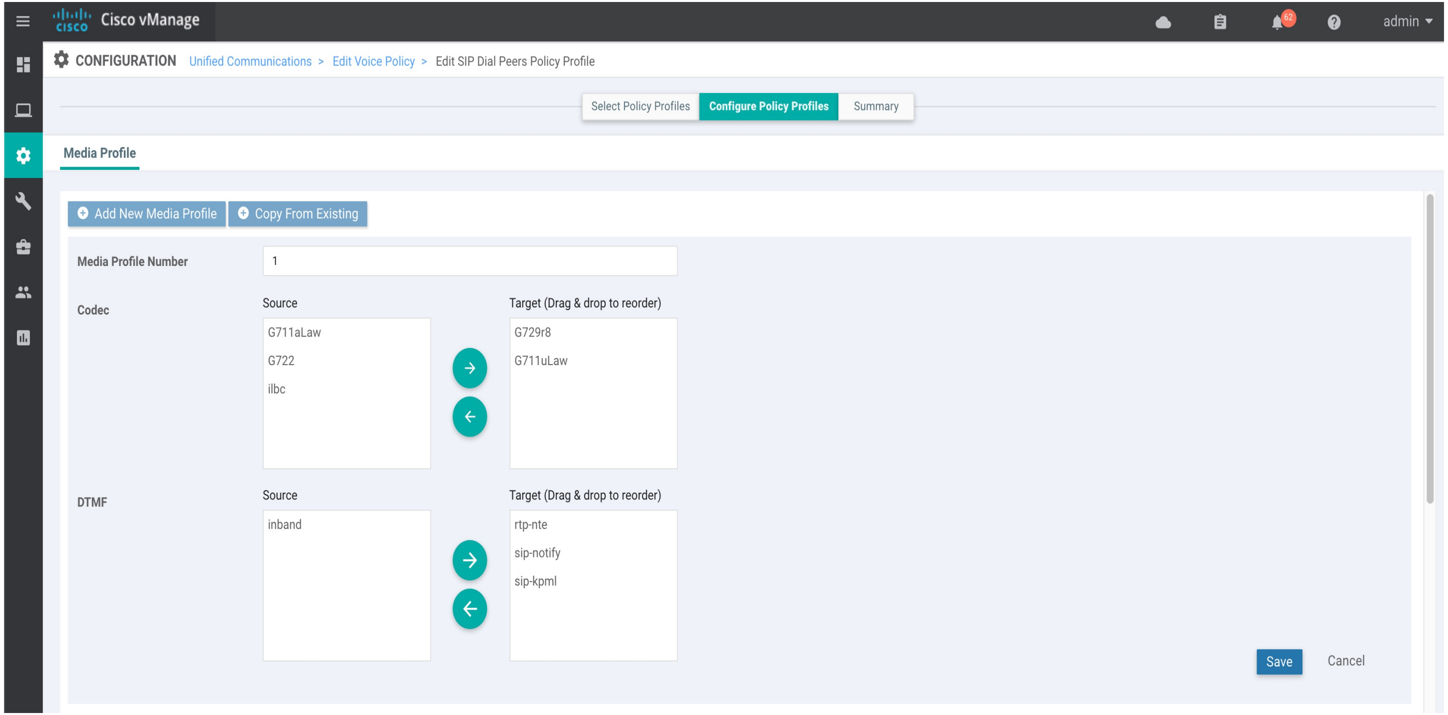
Voice Policy Configuration

Configuration → Unified Communications → Add Voice Policy → Add POTS Dial Peer Policy Profile



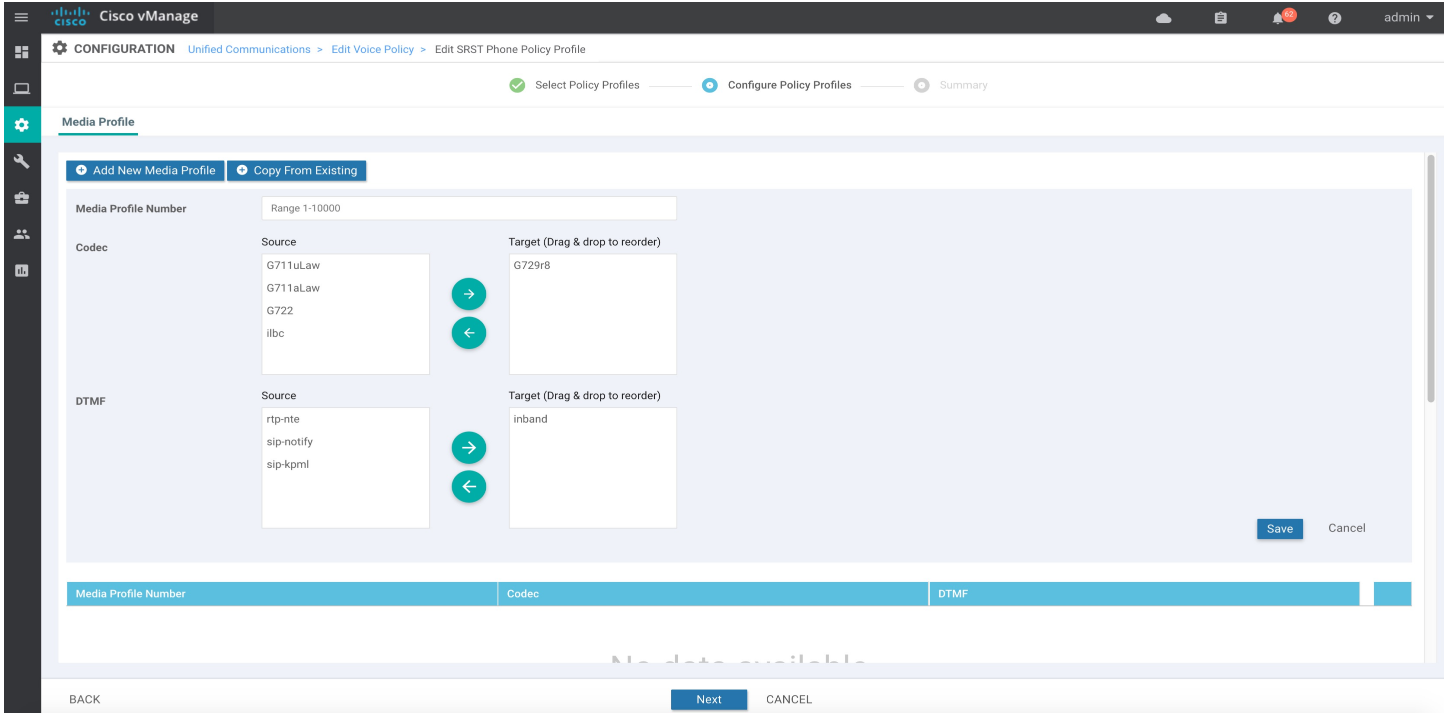
Voice Policy Configuration

Configuration → Unified Communications → Add Voice Policy → Add SIP Dial Peer Policy Profile



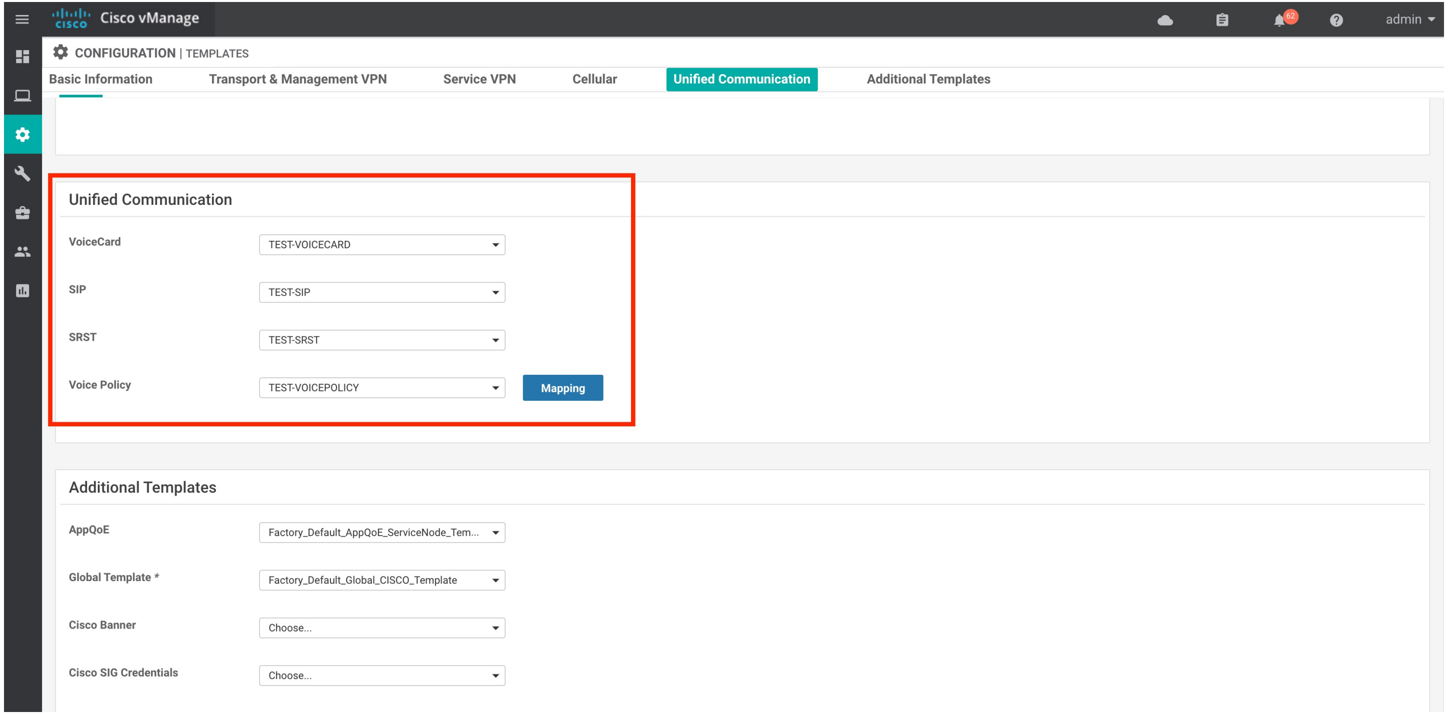
Voice Policy Configuration

Configuration → Unified Communications → Add Voice Policy → Add SRST Policy Profile



Voice Template Configuration

Configuration → Templates → Device (Tab) → (Select ISR) → Unified Communications (Section)



Configuration Snippet

```
sip-ua
voice class codec 1
 codec preference 1 g722-64 bytes 160
 codec preference 2 g729r8
 codec preference 3 g711ulaw bytes 160
!
voice class codec 2
 codec preference 1 g722-64 bytes 160
 codec preference 2 g729r8
 codec preference 3 g711ulaw bytes 160
!
voice service voip
 allow-connections sip to sip
 no supplementary-service sip handle-replaces
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 sip
  registrar server expires max 300 min 200
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
 !
 ip address trusted list
  ipv4 10.0.0.0 255.0.0.0
 !
 fax protocol t38
!
voice register global
 max-dn   48
 max-pool 24
 system message "SRST Mode"
!
```

Voice Policy

SIP Template

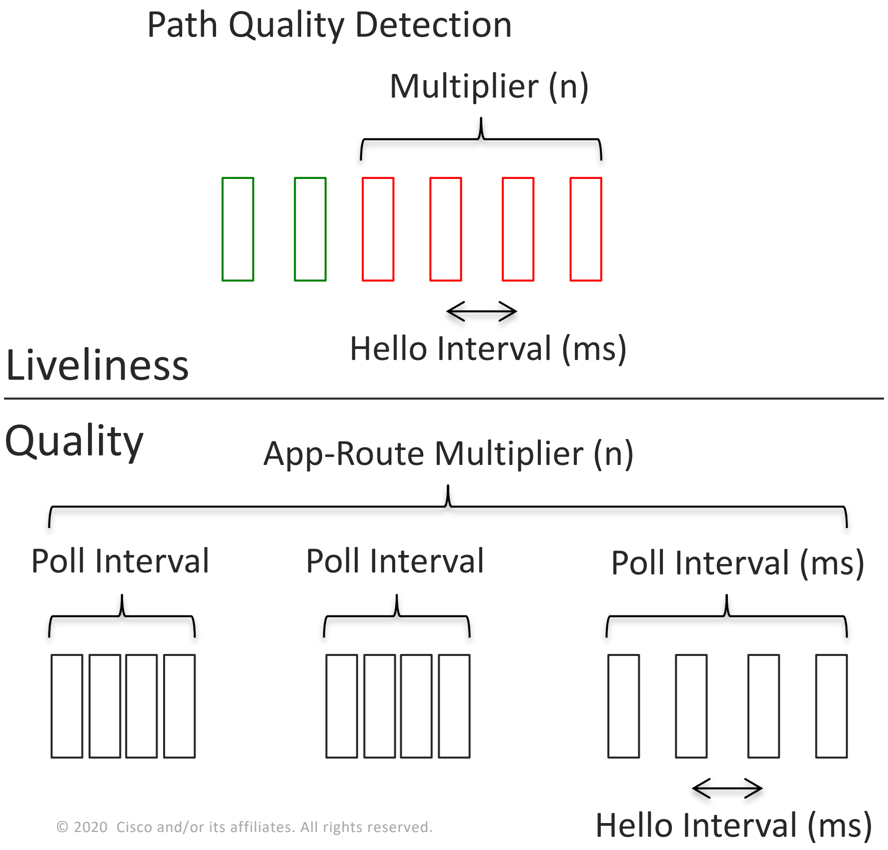
SRST Template

```
voice register pool 1
 voice-class codec 1
 dtmf-relay rtp-nte sip-notify
!
voice-card 0/2
 no local-bypass
!
dial-peer voice 2 voip
 voice-class codec 2
 session protocol sipv2
 dtmf-relay rtp-nte digit-drop sip-notify
!
dial-peer voice 100 voip
 destination-pattern .T
 no shutdown
 session protocol sipv2
 session target ipv4:10.21.24.35
!
dial-peer voice 101 pots
 incoming called-number .
 port    0/2/0
 no shutdown
!
dial-peer voice 911 pots
 destination-pattern 911
 forward-digits all
 port          0/2/0
 no shutdown
!
voice-port 0/2/0
 caller-id enable
 secondary dialtone
!
```

Voice-Card Template

Оптимизация унифицированных коммуникаций с помощью SD-WAN

Bidirectional Forwarding Detection

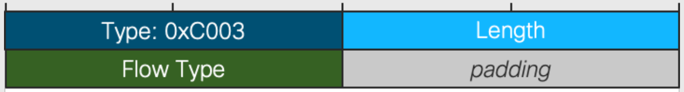


- Each WAN Edge router initiates BFD packet every hello interval
  - Echo mode, no neighbors
  - Tunable to sub-second level
- Poll interval determines the window for calculating path quality
  - Averaged
  - Tunable to sub-second level
- App-route multiplier determines number of poll intervals for establishing overall average path quality
  - Compared against application aware routing thresholds

Cisco SDWAN Key Features & Cross Architecture Development for Webex

- **Webex Per Flow Type Signatures: Webex Desktop App 39.3+**
  - Video, Audio and High Frame Rate Sharing
  - Additional development needed for Webex Endpoints and MPP Phones
- **SD-Application Visibility and Control**
- **Application Aware Routing**
- **BFD Probes Monitor Transport Health Across SDWAN Fabric**
- **Quality of Service Prioritization**
- **Trackers**

Webex Desktop App
Per Flow Signatures



- Flow Type (2 bytes):
  - probe (connectivity check)
  - webex-video
  - webex-audio
  - webex-app-sharing

NBAR2 Protocol Pack 47

WEBEX-VIDEO

Name/CLI Keyword	webex-video
Full Name	Webex Video
Description	Webex provides online meeting, web conferencing, and video conferencing services. It supports face-to-face meetings with real-time sharing of data, audio, video, and apps. Webex uses SSL as its underlying protocol.
Reference	https://www.webex.com/
Global ID	L7:1250
ID	1250

WEBEX-AUDIO

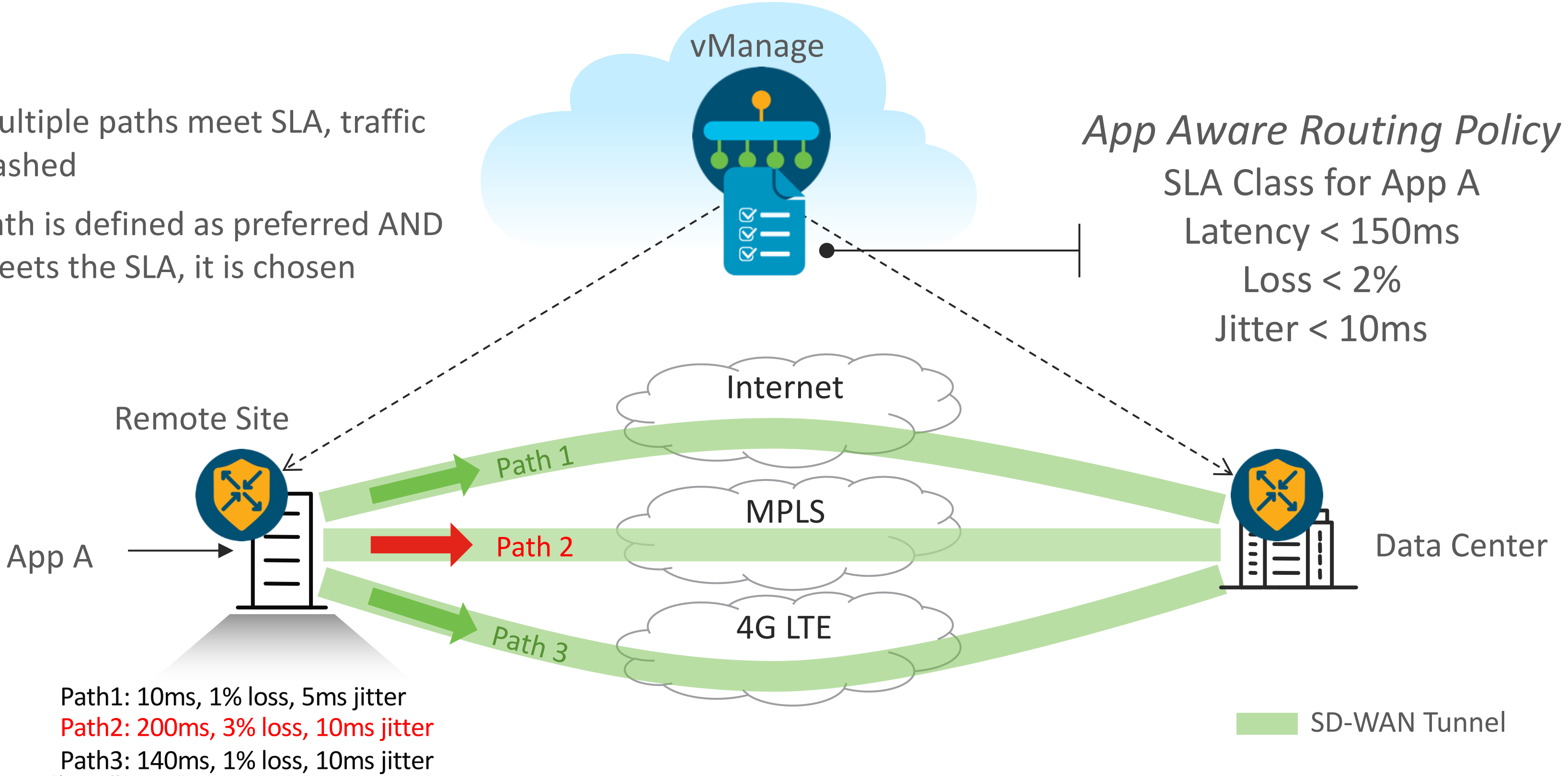
Name/CLI Keyword	webex-audio
Full Name	Webex Audio
Description	Webex provides online meeting, web conferencing, and video conferencing services. It supports face-to-face meetings with real-time sharing of data, audio, video, and apps. Webex uses SSL as its underlying protocol.
Reference	https://www.webex.com/
Global ID	L7:1251
ID	1251

WEBEX-APP-SHARING

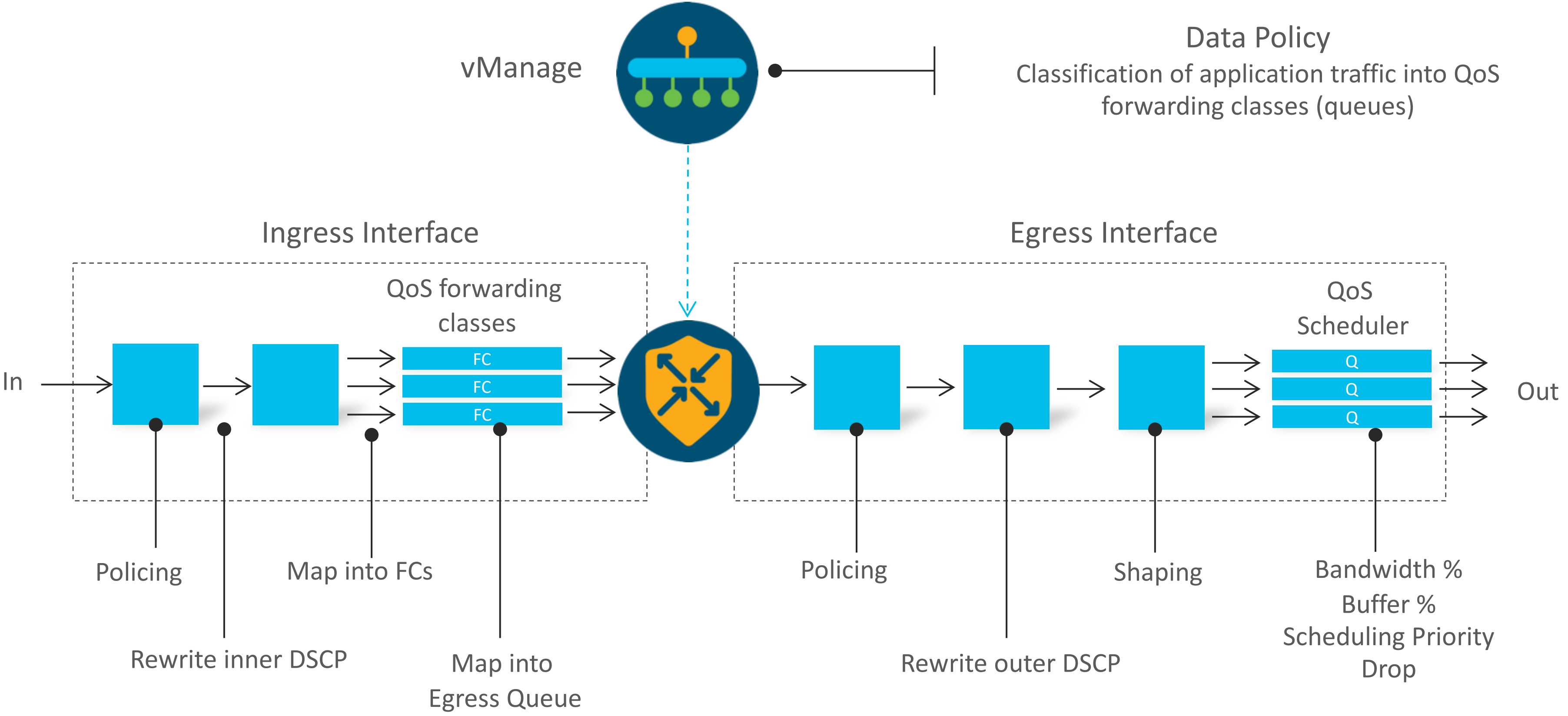
Name/CLI Keyword	webex-app-sharing
Full Name	Webex Application Sharing
Description	WebEx-App-Sharing is granular classification of WebEx protocol application sharing traffic, configured with HTTP-proxy.
Reference	http://www.webex.com/
Global ID	L7:546
ID	1480

Application Aware Routing

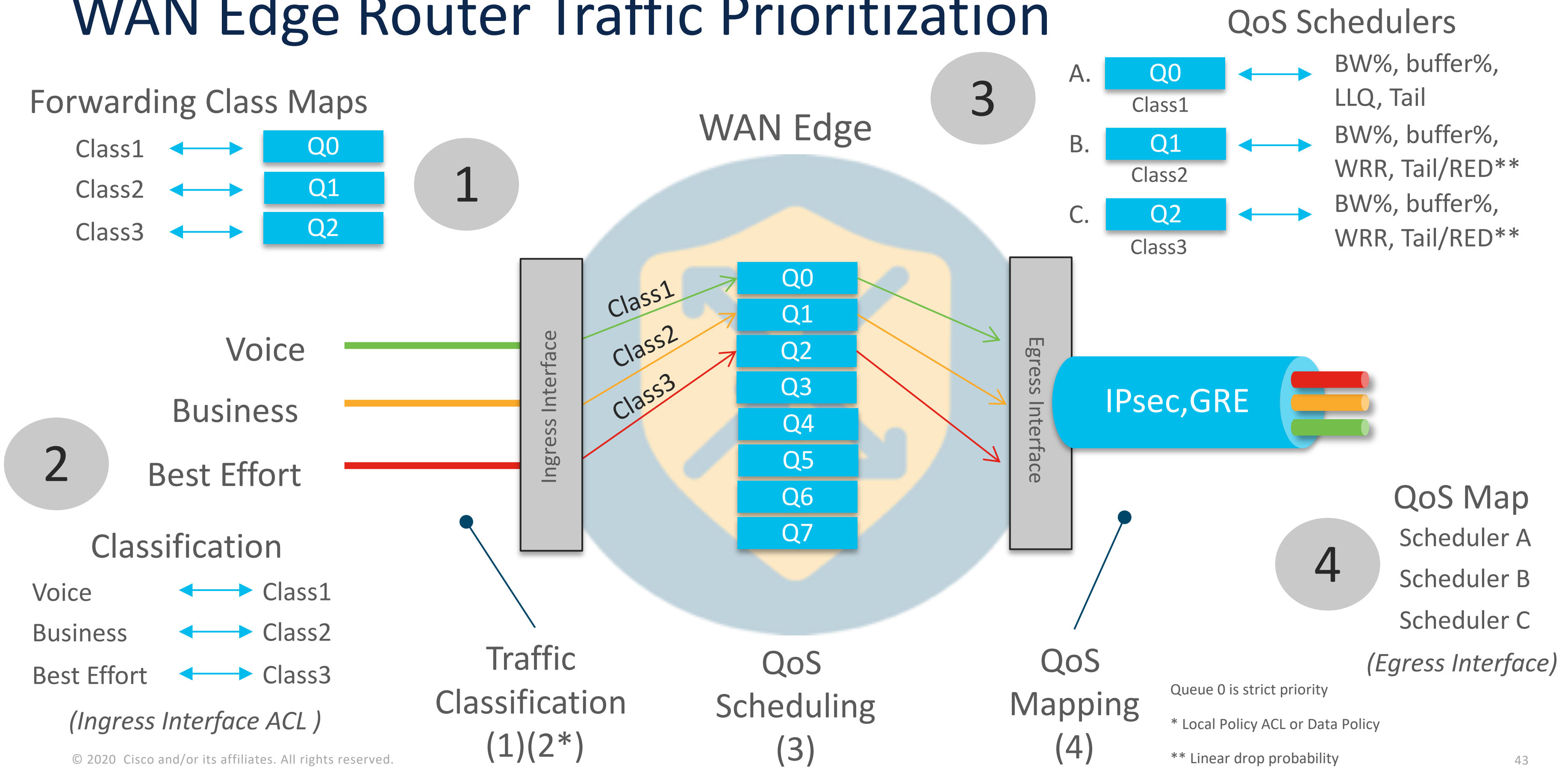
- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



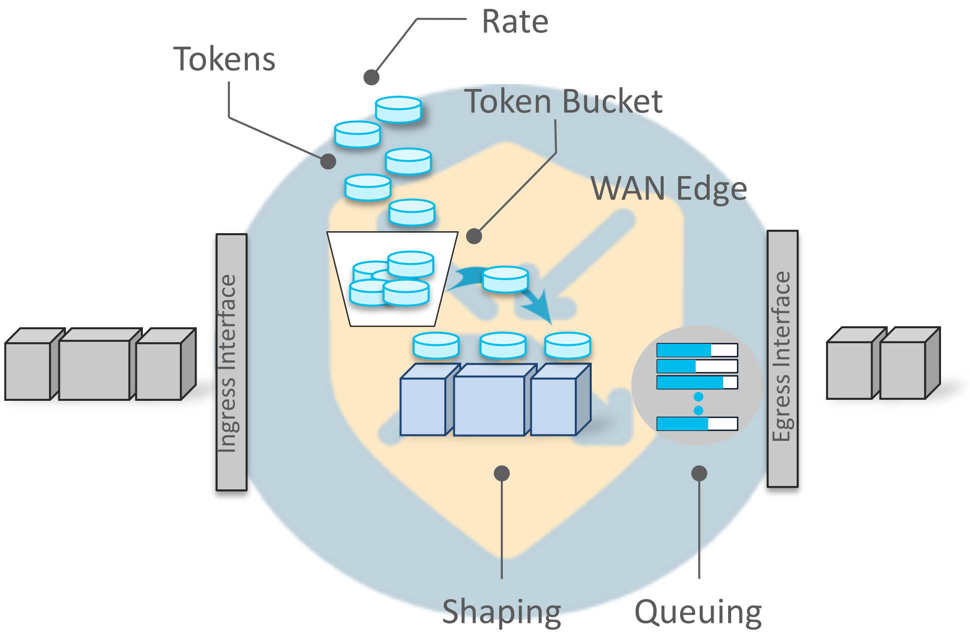
WAN Edge Router QoS Overview



WAN Edge Router Traffic Prioritization



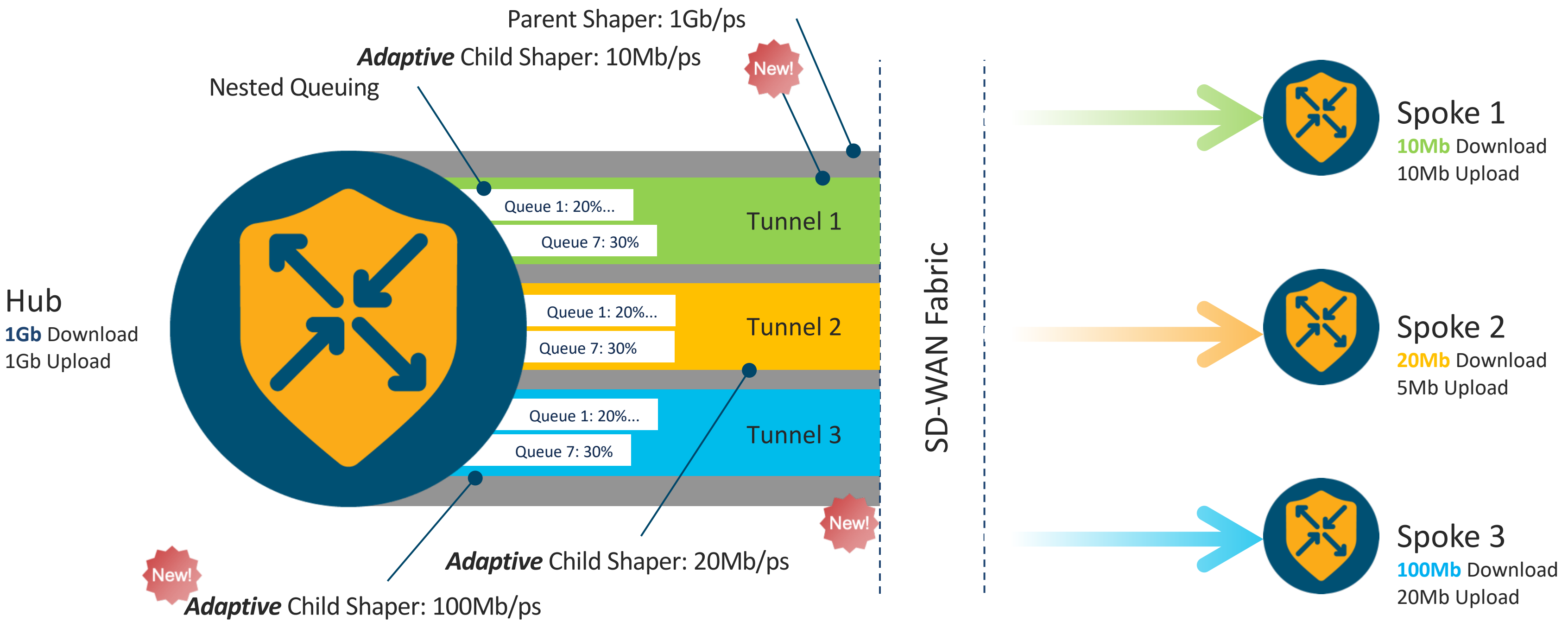
Shaping



Note: Shaping determines link bandwidth considered for queuing

- Shaping effective on egress physical interfaces
  - Not supported on sub-interfaces
- Forward traffic that conforms to configured shape rate
  - Tokens available in the bucket
- Queue traffic that exceeds configured shape rate
  - Tokens not available in the bucket
- Weighted Round-Robin for queued packets

Per-Tunnel QoS with Adaptive Shaping



Per-Tunnel QoS allows the Hub site to dynamically adjust the sending rate of its traffic to accommodate lower bandwidth circuits at remote locations. Adaptive shapers measure the ***true*** circuit capacity at any given moment – rather than relying on static configuration.

Работа на плохих каналах

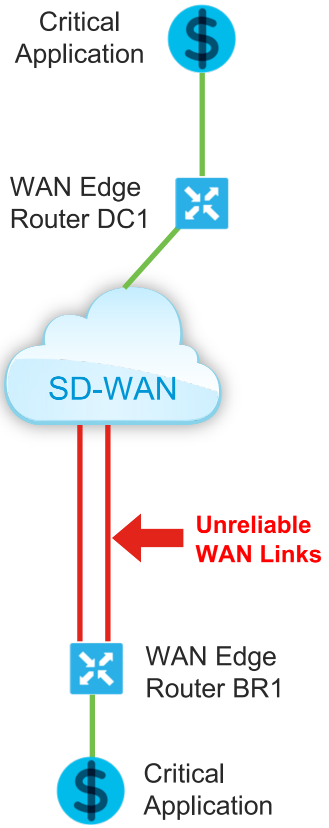
Problem: transactional data over WAN links, which has few percent packet loss (up to 10-20%).

Main Goal: 0 packet loss on the application level.

Solution 1: Forward Error Correction (FEC) send additional parity packet for every 4 data packets, which will be used by the receiving router to reconstruct one lost packet.

Solution 2: Packet Duplication will duplicate packets for critical apps over both WAN links.

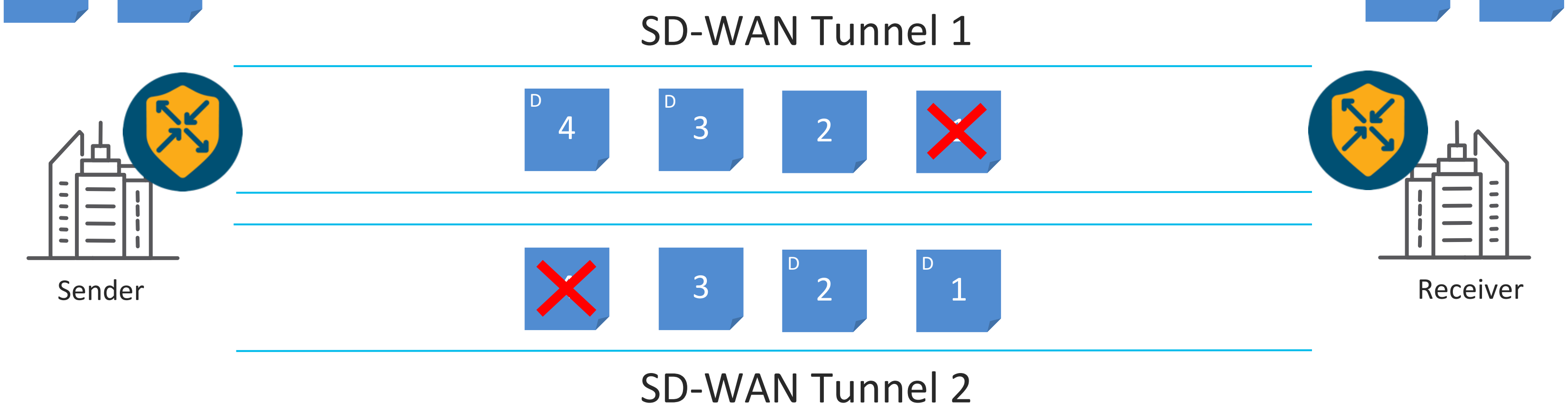
New in RLS 16.12



Packet Duplication

Highlights:

- Protects against packet loss for critical applications (i.e. Voice)
- Protocol agnostic (TCP/UDP)
- Works only over multiple tunnels
- Duplicates are discarded on receiver



Dynamic On-Demand Tunnels

Problem

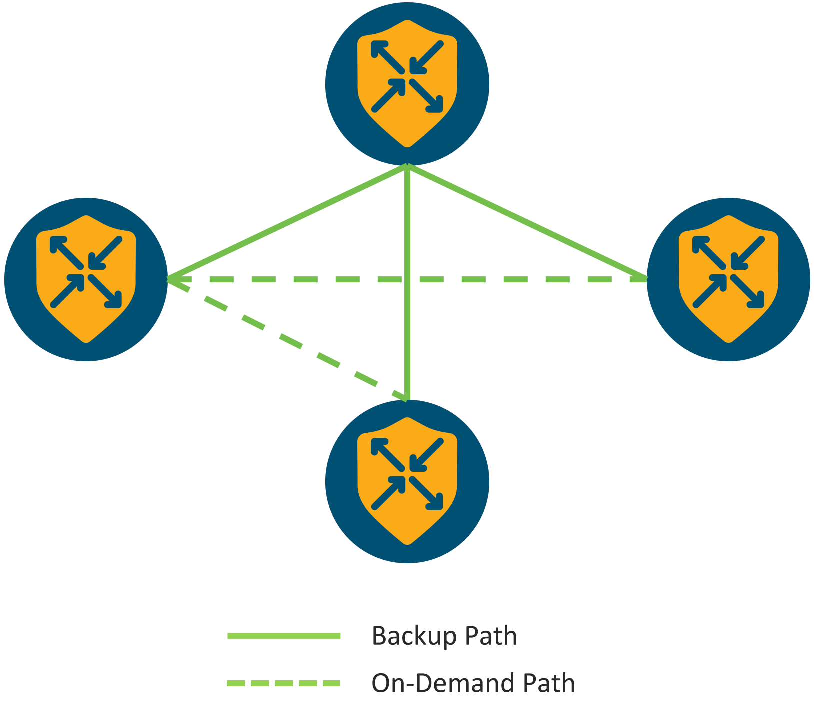
By default, Cisco SD-WAN operates in full-mesh. While topology modification is possible, full-mesh carries a huge computational burden on branch resources and, therefore, becomes difficult to scale. Enterprise customers need full-mesh connectivity, but also need a way to offset the resource burden that full-mesh generally entails.

Solution

SD-WAN v20.3 / 17.3 now support Dynamic On-Demand Tunneling. Branch routers will maintain an "always-on" tunnel to a hub location, then dynamically build site-to-site tunnels, where necessary.

Caveats / Prerequisites

Spoke locations must receive TLOC and vRoute of remote, must have backup path and Service TE set (see supporting slides)



Route Leaking

Problem

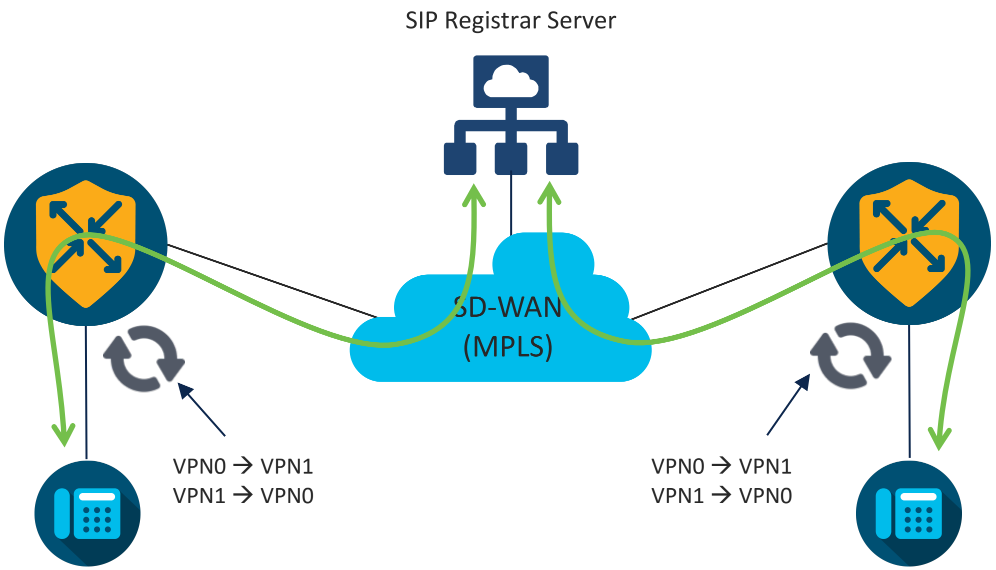
Many customers have expressed a need to expose underlay services within the SD-WAN overlay (such as hosted PBX/VoIP being made available to phones that exist in a Service VPN/VRF). At present (v17.2 / 20.1), SD-WAN only supports this type of route leaking between Service VPNs.

Solution

Cisco SD-WAN v20.3 / 17.3 now support route leaking between Service VPNs and the Transport VPN.

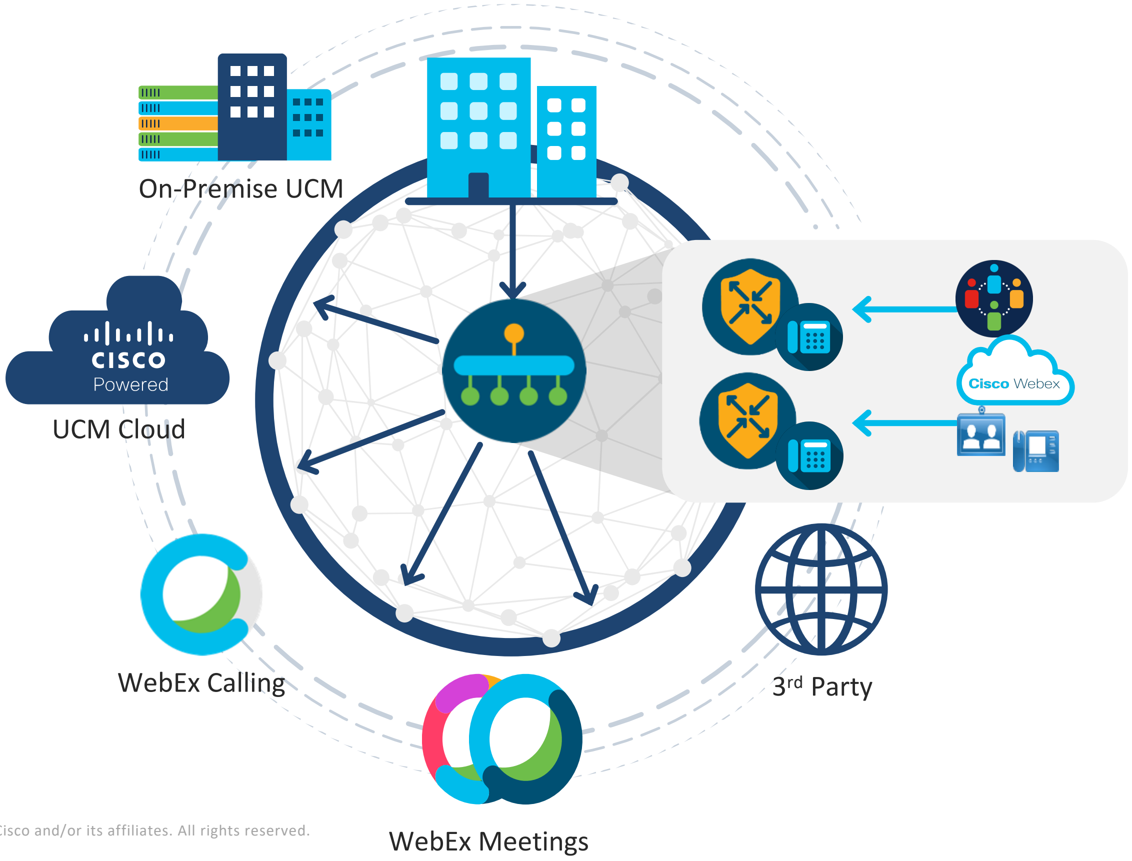
Caveats / Prerequisites

IPv4 only, no EIGRP support, SSNAT + Route Leak is not supported, VPN0 cannot be transit VPN, cEdge has additional restrictions (see supporting TDM)



DEMO

Ключевые выводы



Flexible Connectivity

Directly connect Cloud or On-Premise call control and Webex Meetings services with WAN optimization improving the user experience

Large Scale VoIP Provisioning

Leverage the power of vManage Templating and Policy orchestration to provision scalable, consistent UC across the enterprise

Hardware Consolidation

Reduce CapEx and OpEx by consolidating UC and SD-WAN into a single CPE

Спасибо!

The bridge to possible