Дизайн ЛВС - практика
(II) на примере несложной сети

Network Design

- Постановка задачи
- Разработка топологии
  - Группировка хостов
  - Переподписка
  - Соединения
- Логическая структура
- Проверка сходимости

Organize requirements

When configuring the network, organize the requirements based on the following information.

First, check the requirements of the network service that provides the network.

- **Type and number of endpoints to be accommodated**
- **Segmentation / Filtering** (By grouping on the same terminal, it will lead to simplification of the settings to be input to the device.)
- **Authentication for users and devices** (Authentication flow becomes clear, and it leads to a decrease in switches with necessary functions that tend to be expensive.)
- **Equipment layout** (consider restrictions in the physical environment)
- **Required bandwidth and acceptable oversubscription**
- **Cost calculation**

Next, check the location and scope of the network to understand the scale of construction.

Distance and size are important requirements related to equipment selection and number of units.

Location and number of comms rooms, Building/Floor/Range of area within floor

Reference: Design elements considered in the requirements

- **Spatial range for network construction**
  - Bases, buildings, floors, areas within floors, etc.
- **Network services to be provided**
  - Number of ports
  - Speed/oversubscription
  - Network segmentation
  - Filtering (which packet to pass)
  - Presence / absence of authentication, authentication method
  - PoE/UPoE
- **Type and number of endpoints**
  - Types
    - Desktop computer
    - IP phone
    - Video terminal
    - Printer
    - Camera
    - etc.

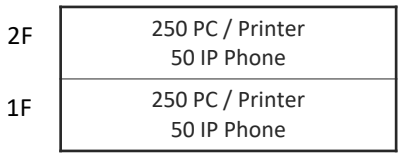
    Number of each
- **Environment / Constraints: Check switch installation location**
  - Wiring closet
  - Server room
  - Rack configuration
- **Environment / Constraints: In-floor cabling**
  - Existing / new
  - Splice box
  - UTP
    - category
    - cable length
  - Patch panel
- **Environment / Constraints: Floor-to-floor cabling**
  - Existing / new
  - Cable type (SMF / MMF / UTP)
  - Optic type DSF, NZ-DSF
  - Cable length
  - Splice box

Access layer configuration example

Organize your requirements using two specific campus network examples.

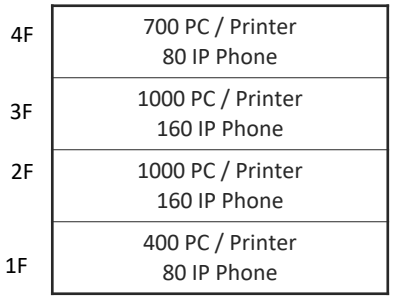
A) small-scale configuration scenario

- **Requirements for network services**
  - *** Types and number of endpoints to accommodate (see figure below)**
  - Required bandwidth
  - PC: 1Gbps, Printer: 500Kbps, IP Phone: 100Kbps
- **Requirement 2: Confirmation of location and scope of network provision**
  - 1 building 2 floors



B) large-scale configuration scenario

- **Requirements for network services**
  - *** Types and number of endpoints to accommodate (see figure below)**
  - Required bandwidth
  - PC: 1Gbps, Printer: 500Kbps, IP Phone: 100Kbps
- **Requirement 2: Confirmation of location and scope of network provision**
  - 1 building
  - 4 floors



Endpoint grouping

Group endpoints according to requirements. Grouping is essential to determine the optimal access switch model, number, and accommodation method.

Need for grouping:

- Optimal distribution of endpoints to access switches to accommodate them and distribute the extent of failure appropriately
- It is possible to clarify the required number of functions required for access switches (eg, with or without PoE), which leads to cost reduction by consolidating switch model numbers.
- Bringing together the same endpoints simplifies the configuration pattern for each switch, clarifies the communication flow, and realizes a network that is less prone to failure and easier to manage.

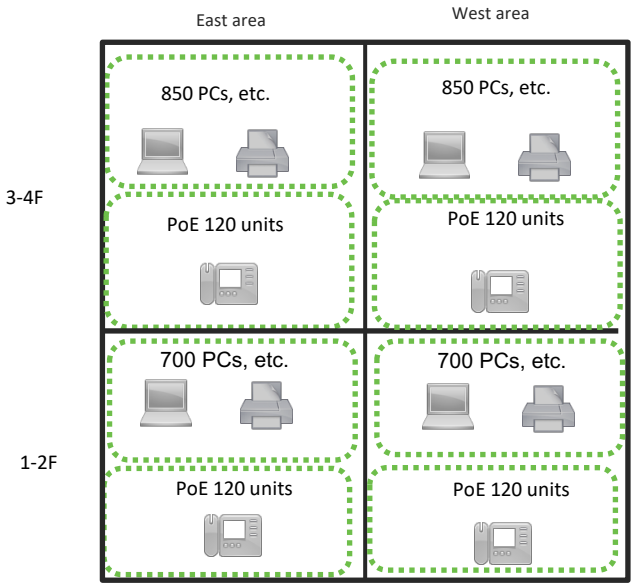
The endpoint grouping policy is roughly divided into the following three.

1. **Classification of endpoint types**
2. **Place to mount**
3. **Redundant distribution**

Classification of endpoint types

In order to simplify the setting / select the accommodation switch with the appropriate function, the following policy is summarized.

- Unify with the same endpoint type. If you mix too much, the setting will be complicated, so we recommend up to two types.
- Consolidate endpoints that require PoE as much as possible to minimize the number of PoE model number switches and reduce costs.
- Spread the same endpoint type across two or more switches. This is to prevent endpoints in the same floor area from being completely cut off due to a single switch failure.



Case B configuration
Endpoint type (with or without PoE)
Place to mount (1-2F / 3-4F)
Redundant distribution (east / west)

Allocate grouped endpoints

1. Endpoints also have various extra attributes

- General users / High-end users (broadband) / Users who handle confidential information
- IP Phones （PoE）
- Video conferencing (wideband, using QoS ）
- Printer (with burst traffic)

2. Place to mount

Grouping optimizes the distance between the endpoint and the access switch. Secure location.

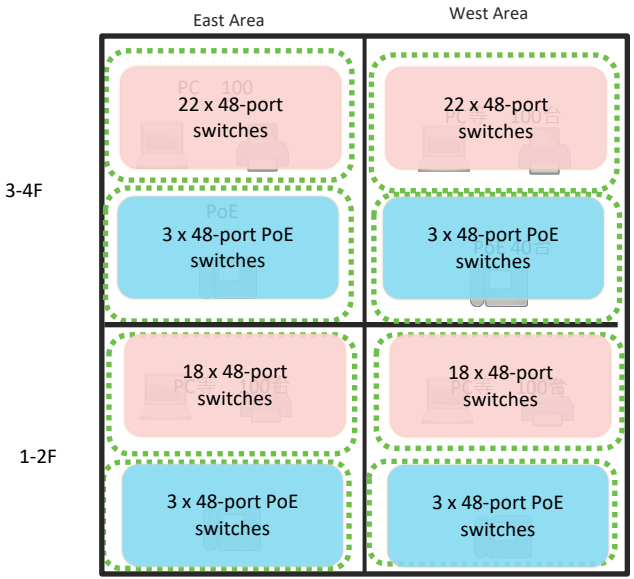
3. Redundant distribution

Divide groups to prevent endpoints within the same floor area from being completely disrupted due to a single switch failure. (Refer to the figure on the previous page for an example of the results of grouping.)

We recommend that you estimate the number of access switch ports that accommodate endpoints as follows.

- **For 24-port model: 20 ports accommodated, 4 ports spare**
- **For 48-port model: 40 ports accommodated, 8 ports spare**

Assign access switches to the segregated end groups with the above expected number of accommodated ports. The results are shown in the figure on the right.



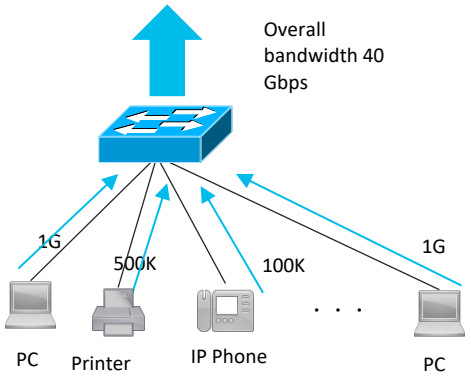
Select an access switch based on grouping

Calculate the total bandwidth for each switch

By allocating endpoint groups to access switches, each access switch uplink determines the total amount of bandwidth required.

Determine the total bandwidth according to the following points.

- Determine the required bandwidth for each endpoint
  - PC : 1Gbps
  - IP Phone : 100Kbps
  - Desktop video conferencing terminal : 5Mbps
  - Printer : 500Kbps
- Consider changes in the nature of traffic over time
  - Burst type: A large amount of traffic flows temporarily Example: Web traffic
  - Real-time type: Traffic that cannot tolerate delay. Example: Video conferencing
- Consider the amount of bandwidth that can handle future changes in network usage （Assuming a situation where the quality of network services cannot be maintained even if QoS is used）
  - Introducing video conferencing
  - Use of VDI, etc.



Determine uplink bandwidth based on oversubscription ratio

Once you know the overall bandwidth, consider the oversubscription ratio and decide which bandwidth to provide on the uplink.
(Oversubscription ratio may vary by endpoint group depending on requirements)

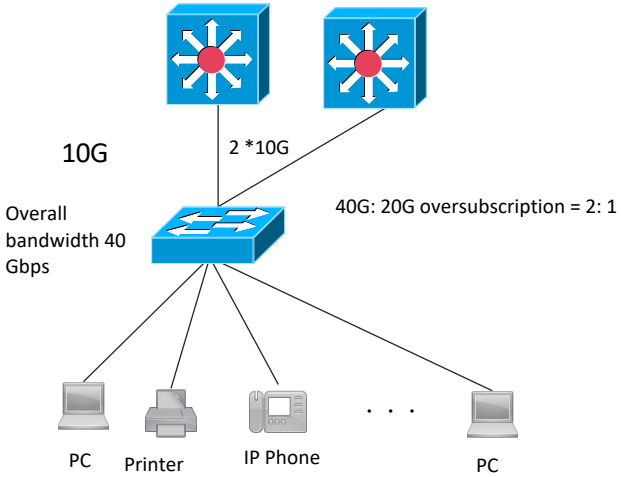
- For PC: bandwidth-focused 1:1 non-blocking to cost-focused 20:1 can be considered according to your requirements.
  Older design guides said it was 20:1, but it's not a good idea to scrutinize the oversubscription ratio for each endpoint group to reduce costs. This is because the cost per bandwidth is now dropping significantly. (Example: 10G)
- For latency-sensitive IP phones, video conferencing terminals, etc., 1: 1 with no oversubscription is recommended.

Once the oversubscription is determined, the uplink bandwidth can be considered to determine the number of uplinks required and the specific oversubscription value can be calculated.

Examples of uplink types are as follows.

- 2/4 links x 1 / 10 G
- （In some cases, 2x40G etc.）

With the above, the number of ports required for the access switch, the type of port, and the amount of bandwidth required for the uplink have been determined. When selecting an access switch, considering the config of the uplink requires distribution information, which will be explained in the next chapter. **Therefore, in this chapter, the access switch is tentatively decided**.



Case study (access layer)

A) small-scale configuration scenario

2F	250 PC / Printer 50 IP Phone
1F	250 PC / Printer 50 IP Phone

Group endpoints according to requirements.
Classification of endpoint types:
- Presence / absence of PoE
- Place to place: 1/2 Floor
- Redundant distribution: Yes

500 PC / Printer
without PoE
36 devices / 1 switch

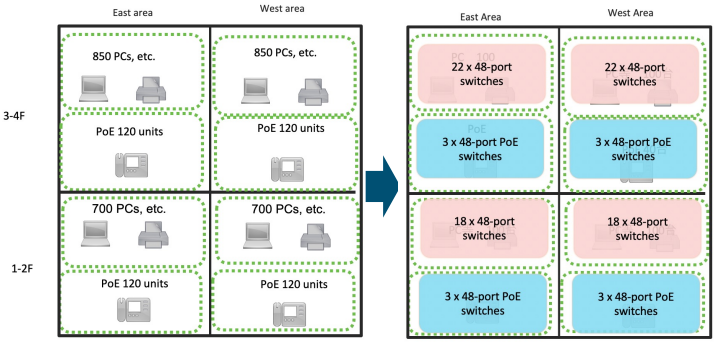
14 * 48 port switch

With PoE
100 IP Phone
25 devices / 1 Switch

4 * 48 port POE switch

B) large-scale configuration scenario

Group endpoints according to requirements
Classification of endpoint types:
- Presence / absence of PoE
- Place to place: 1-2/3-4 Floor; East/West
- Redundant distribution: Yes



18 * 48 port switch

3 * 48 port switch with POE

1-2F East

18 * 48 port switch

3 * 48 port switch with POE

1-2F West

22 * 48 port switch

3 * 48 port switch with POE

3-4F East

22 * 48 port switch

3 * 48 port switch with POE

3-4F West

Distribution Layer Configuration

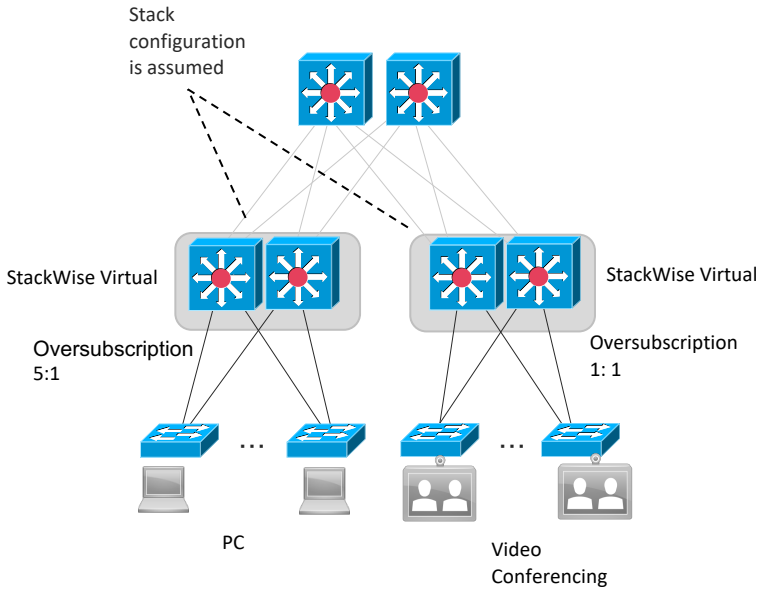
The distribution aggregates the various uplink types from the access layer and passes them to the core. When using existing wiring, it is necessary to consider the location of the distribution switch and its conditions.

- **Oversubscription varies by endpoint**
  Even within the same LAN network design, the bandwidth requirements (oversubscription ratio) required for each group of endpoints may differ. Endpoints that require a wider bandwidth than typical endpoints require a lower oversubscription ratio (1: 1-2: 1)

- **About future expansion**
  You need to consider expanding the access switch and increasing the bandwidth of the access switch uplink. Increasing bandwidth from 1G to 10G to 40G by replacing transceivers is recommended because it is easy to manage and to work with.

- **Utilization of stack technology**
  The distribution switch is premised on the utilization of StackWise and StackWise Virtual. The benefits of operating the distribution as a single logical switch are described earlier.

  - StackWise Virtual - reminder
    It is a function that realizes StackWise by using the conventional port without using the Stack cable. Therefore, it is necessary to secure a separate interfaces for StackWise Virtual.



Determine connections Access<->Distribution

Determine the connection method between access and distribution. This determines the access uplink method and the access switch model.

After checking the required bandwidth, decide the distance, media (cable), and connection method. (Required bandwidth is determined in the access chapter).

* The distance used depends on the required distance, such as inter-floor wiring, intra-floor wiring, and indoor wiring.

- Check whether the media (cable) is the existing wiring or the new wiring.
  If it is new, select from the following:
  - Multimode fiber OM1, OM2, OM3, OM4
  - Single mode fiber G.625
  - UTP category 5E, 6, 6A, 7
- Select the connection method.
  - MMF 10GBASE-SR, 10GBASE-LRM, 1000BASE-SX
  - SMF 10GBASE-LR, 1000BASE-LX
  - UTP 1000BASE-T

Based on the above information, determine the access switch equipment and the transceiver to be used for the access switch uplink.

Considering uplinks from distribution

When considering the uplink bandwidth between the distribution and the core, various factors are taken into consideration, such as the amount of bandwidth used for cloud services and the use of QoS to make it appear that there is no oversubscription from the endpoint side. Will be done.

- Oversubscription ratio

Try to keep it in the range of 1:1 to 4:1. If you introduce a wideband link, the uplink may be excessive, but this is not a problem.

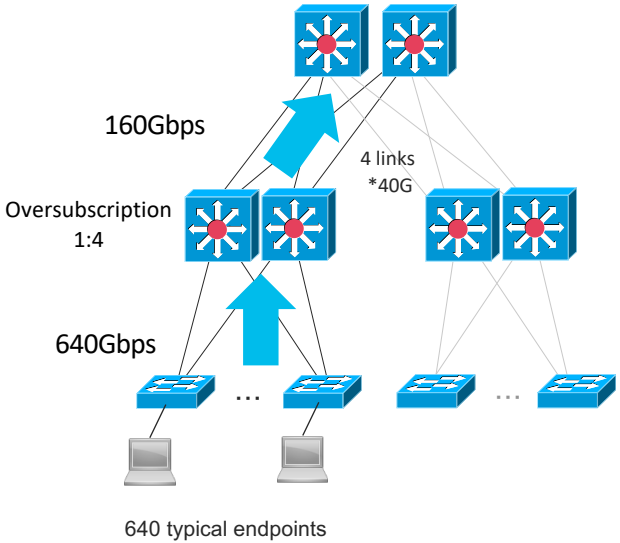
- Uplink review

  Determine the oversubscription based on the required bandwidth and select the uplink type. You have the option of forming a channel or choosing more bandwidth.

  - 10G / 40G / 100G
  - Etherchannels (Example: In the case of 40G, 4 * 10G or 1 * 40G)

- If you have an existing cabling system

  You should carefully consider oversubscription and decide which distribution switch use to aggregate.



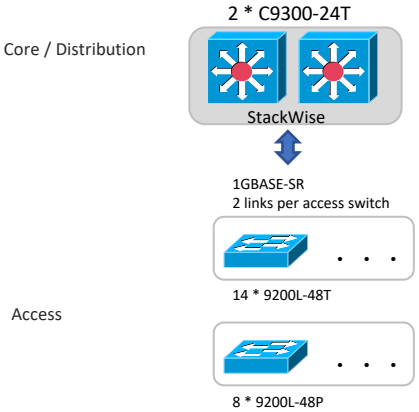
Taking the above into consideration, the final decision on the model of the distribution switch is made.

Case study (distribution layer)

A) small-scale configuration scenario

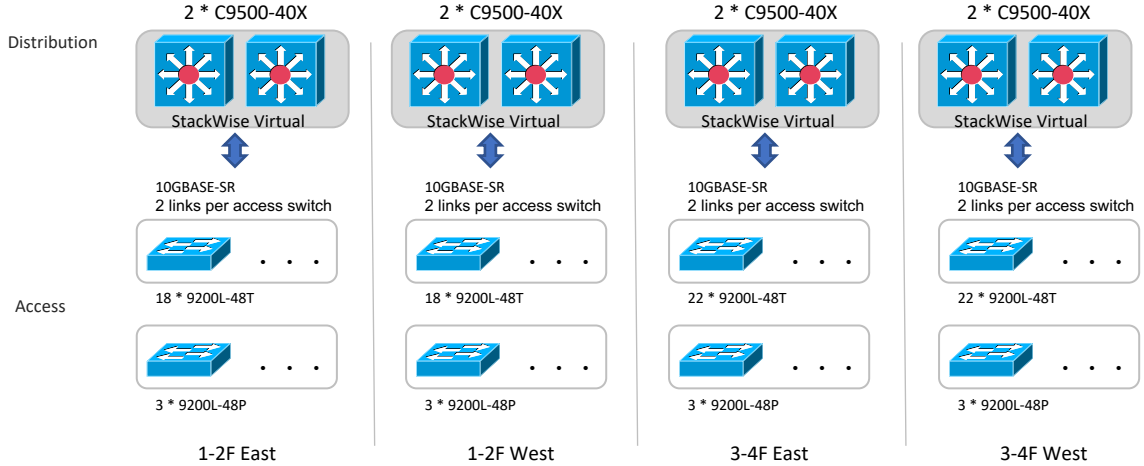
Since the A configuration has a small number of ports, it is completed with a two-layer configuration in which one switch has both core and distribution roles.

Each distribution switch accommodates 22 uplinks from the access switch.



B) large-scale configuration scenario

Between access and distribution, if uplink 10G * 2 is adopted for each access switch that accommodates 40 terminals, the oversubscription 40G:20G is approximately 2:1.
C9500-40X was selected to accommodate 21 or 25 10G uplinks from the access switches per distribution switch.



Core – Distribution: Determine the connection Select the model of the core switch

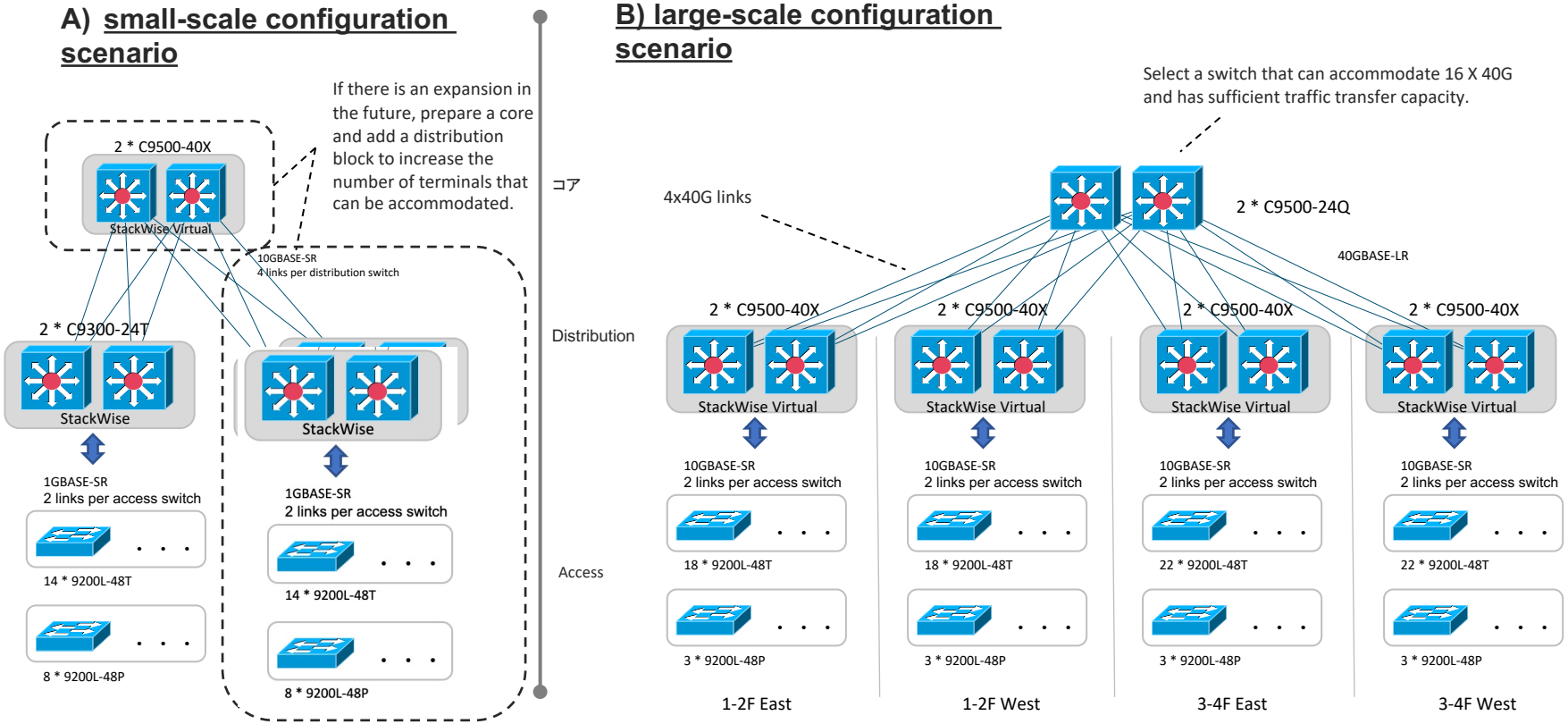
Next, the core device is determined by determining the connection method between the cores from the distribution.

- After confirming the required bandwidth, decide the distance, the cable to be used, and the connection method.
- The media and connection method used for the distance differ depending on the required distance, such as inter-floor wiring, intra-floor wiring, and indoor wiring.
- Check whether the media (cable) is the existing wiring or the new wiring. If it is new, select from the following.
    - Multimode fiber OM1, OM2, OM3, OM4
    - Single mode fiber G.625
    - DAC (Direct Attach Cable)/AOC (Active Optical Cable)
- Then select the connection method.
    - MMF
    - SMF
    - DAC/AOC

Based on the above information, determine the core device.

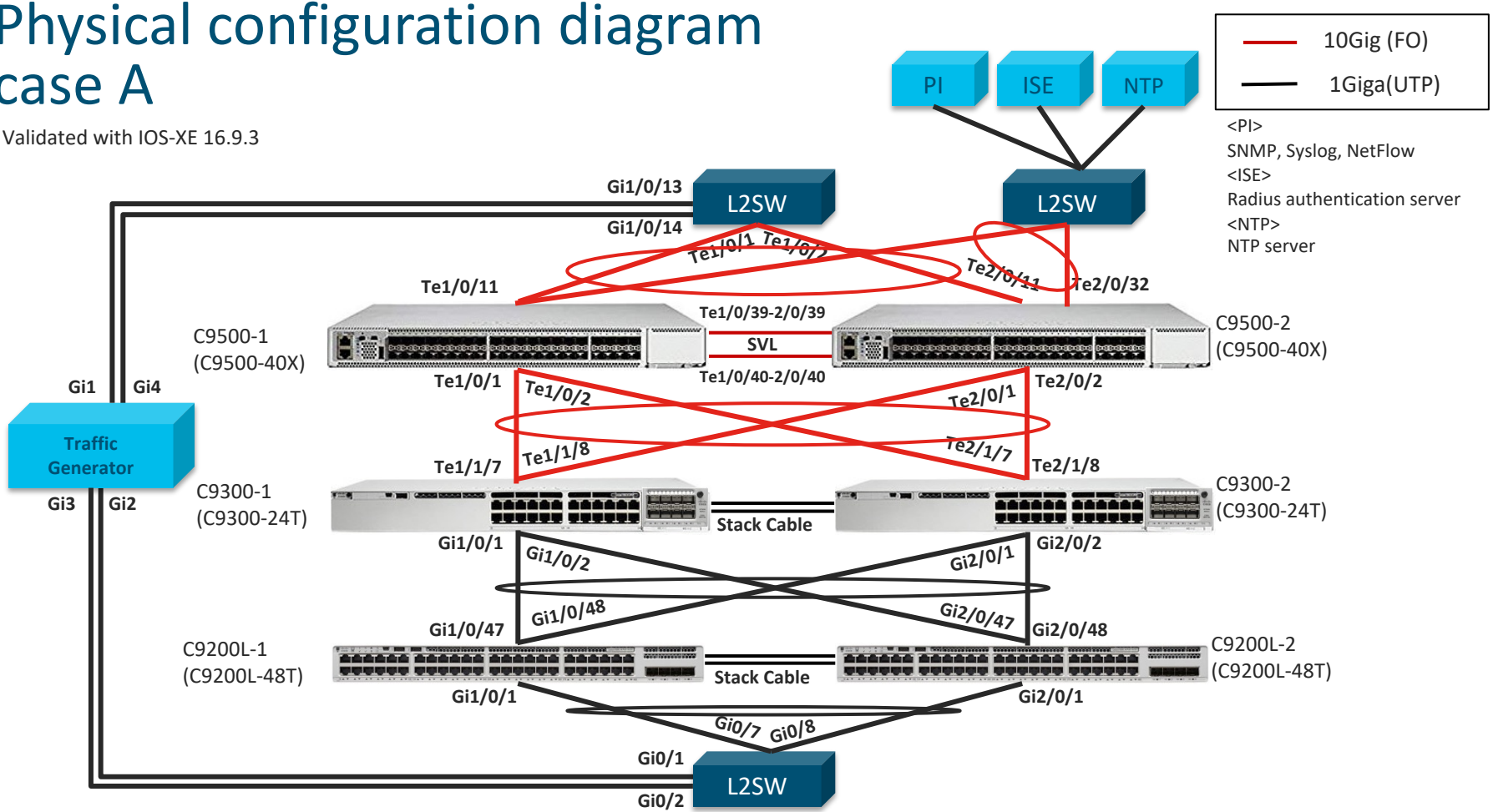
* The necessity of physical connection between core switches depends on the consideration of applying StackWise Virtual to the core

Case study (core layer)

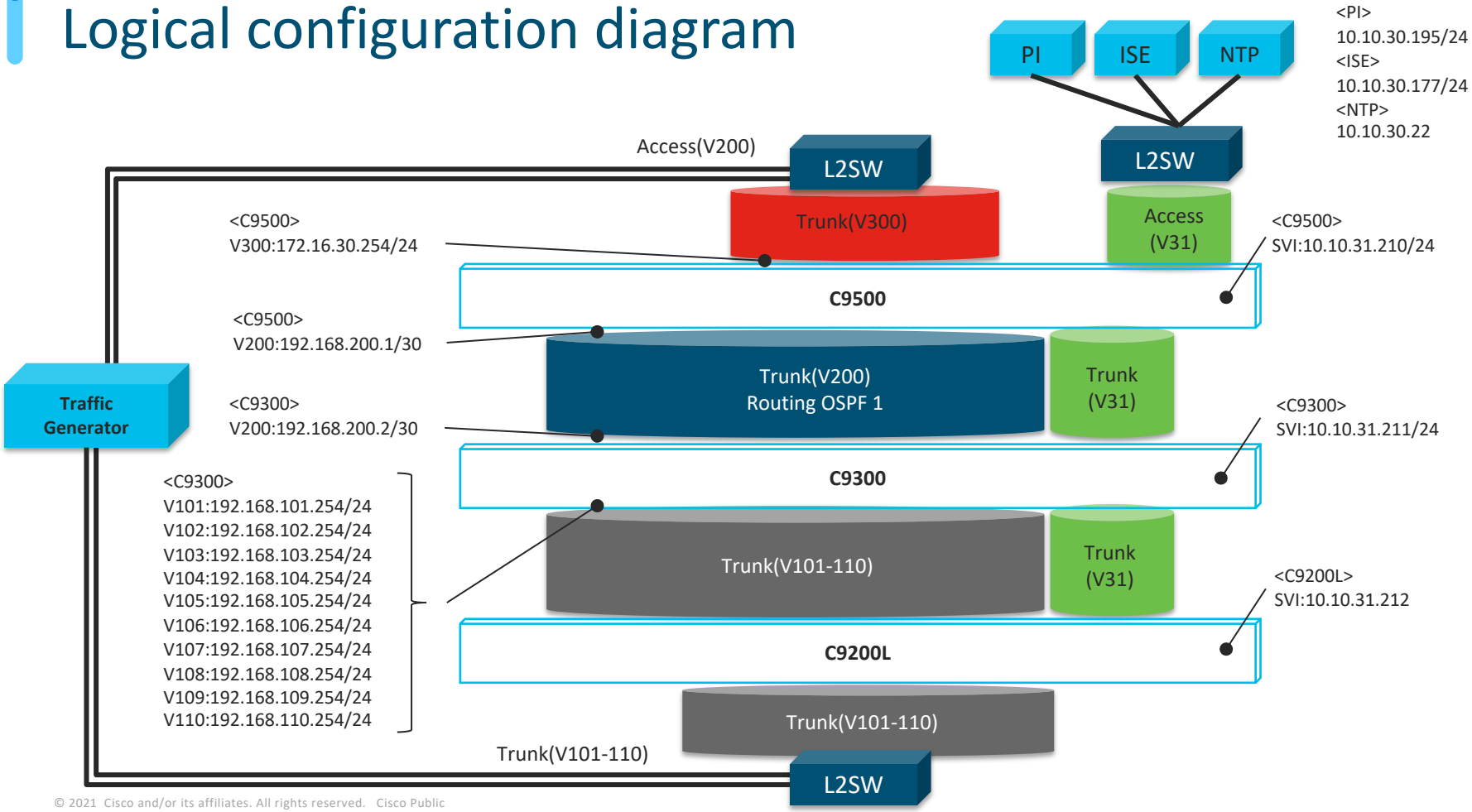


Physical configuration diagram case A

* Validated with IOS-XE 16.9.3



Logical configuration diagram



Segment structure

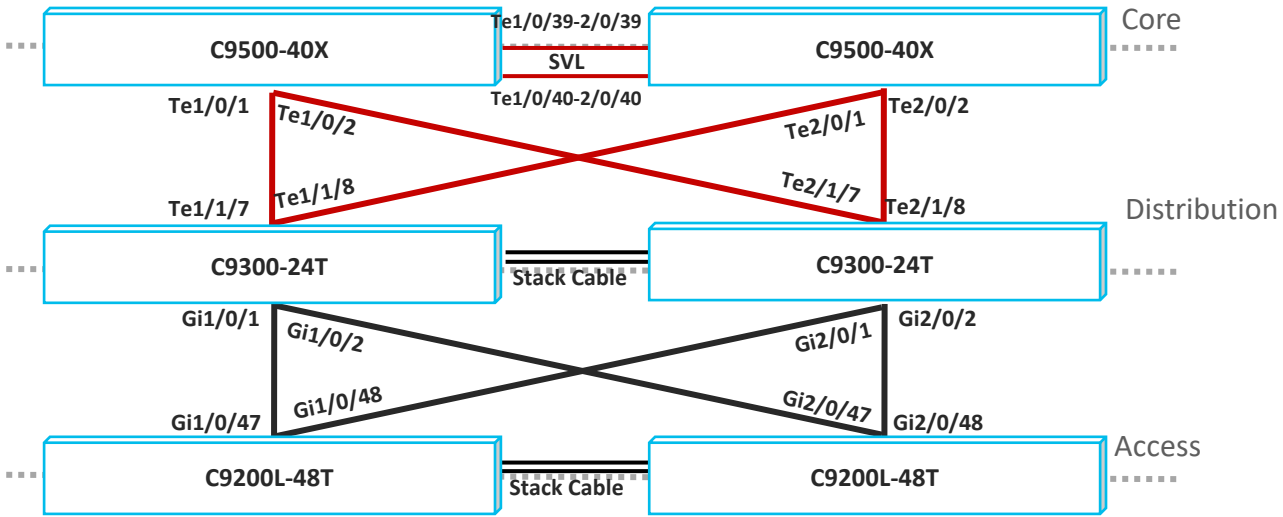
VLAN ID	Network	Purpose of use	Use color	Remarks
31	10.10.31.0/24	Management segment		Separated from user segment
101	192.168.101.0/24	User segment 1		Default gateway on C9300
102	192.168.102.0/24	User segment 2		〃
103	192.168.103.0/24	User segment 3		〃
104	192.168.104.0/24	User segment 4		〃
105	192.168.105.0/24	User segment 5		〃
106	192.168.106.0/24	User segment 6		〃
107	192.168.107.0/24	User segment 7		〃
108	192.168.108.0/24	User segment 8		〃
109	192.168.109.0/24	User segment 9		〃
110	192.168.110.0/24	User segment 10		〃
200	192.168.200.0/30	Core-Dist switch inter-segment		Routing by OSPF
300	172.16.30.0/24	Server segment		Default gateway on C9500

Kit list

Role	Device name	Device model	OS version	License
Core	C9500-1	C9500-40X	16.9.3	Network Advantage Cisco DNA Advantage
	C9500-2	C9500-40X	16.9.3	Network Advantage Cisco DNA Advantage
Distribution	C9300-1	C9300-24T	16.9.3	Network Advantage Cisco DNA Advantage
	C9300-2	C9300-24T	16.9.3	Network Advantage Cisco DNA Advantage
Access	C9200L-1	C9200L-48P	16.9.3	Network Essentials Cisco DNA Essentials
	C9200L-2	C9200L-48P	16.9.3	Network Essentials Cisco DNA Essentials

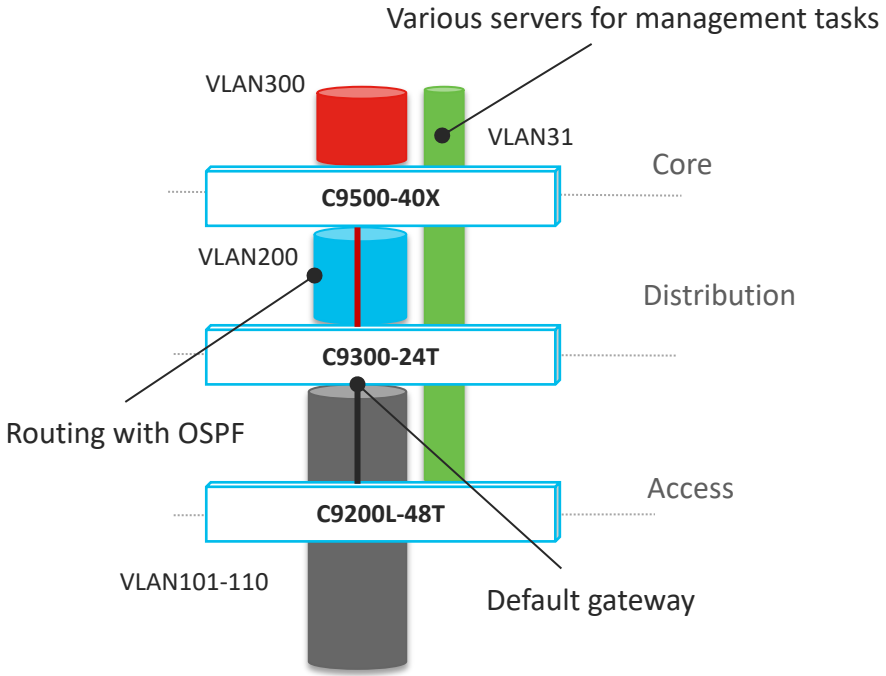
Connections

- 10G Ethernet (fiber optic) between cores and distributions
- 1G Ethernet (UTP) between access and distribution



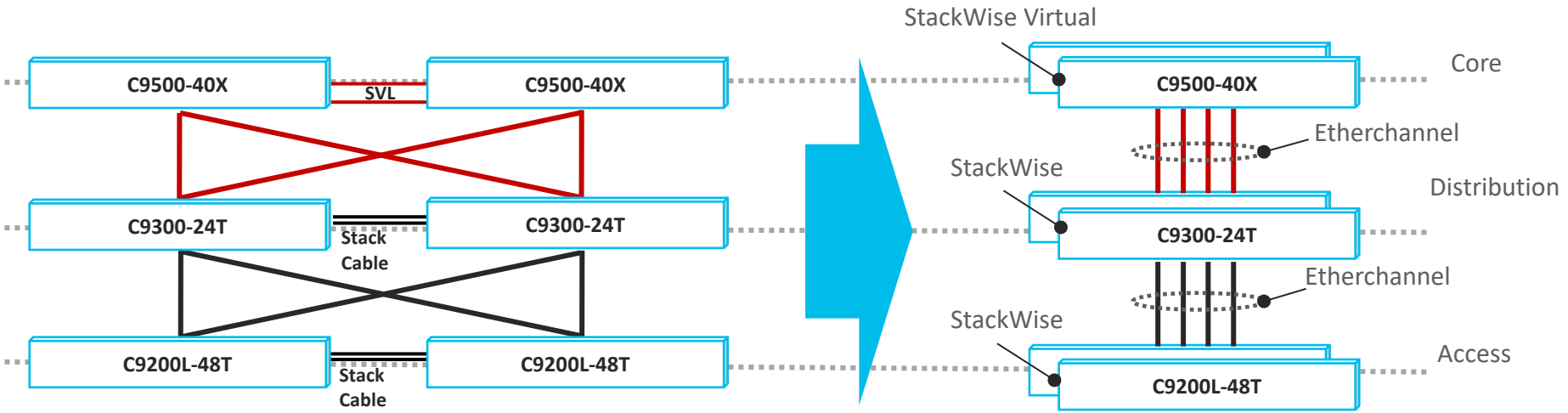
Logical configuration

- Core, distribution switch is L3
- Access switch is L2
- Configure on a VLAN basis and use SVI for L3
- The default gateway of the user terminal is on the distribution switch
- OSPF between core and distribution switches
- For management, various server segments are logically divided by VRF * However, the access switch does not support VRF.



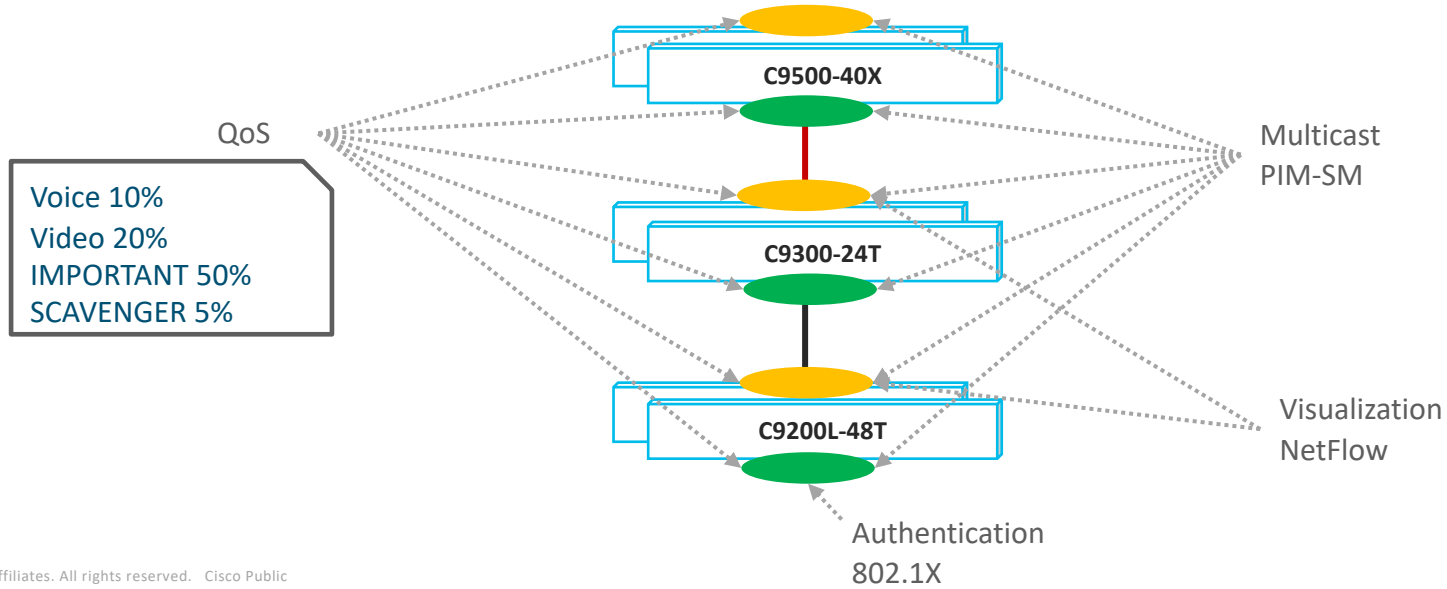
Redundant configuration

The core, distribution, and access switch are all redundant is stacks, and the links are redundant using EtherChannel.



Main functions

- **QoS** : Controls bandwidth for phone, video, critical traffic, and other traffic
- **Multicast** : Configure multicast PIM-SM for video distribution
- **Authentication** : Authenticate the users with 802.1X
- **Visualization** : Setup NetFlow to visualize flow information



Related configuration snippets

QoS

```
!
policy-map Queueing
 class VoIP
  priority level 1 percent 10
 class VIDEO
  priority level 2 percent 20
 class IMPORTANT
  bandwidth remaining percent 50
 class SCAVENGER
  bandwidth remaining percent 5
policy-map system-cpp-policy
!
. . . .
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 31,101-110
 switchport mode trunk
 load-interval 30
 channel-group 2 mode active
 service-policy output Queueing
!
```

Multicast (PIM-SM)

```
!
ip multicast-routing
ip domain name cisco.com
!
. . . .
!
interface Vlan200
 ip address 192.168.200.1 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf 1 area 0
!
. . . .
!
ip forward-protocol nd
ip pim bsr-candidate Vlan200 0
ip pim rp-candidate Vlan200
!
```

Related configuration snippets

Authentication (802.1X)

```
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 10.10.30.177 server-key cisco
 auth-type all
!
radius server ISE
 address ipv4 10.10.30.177 auth-port 1812 acct-port 1813
 key cisco
!
interface GigabitEthernet1/0/1
 switchport mode access
 device-tracking
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication port-control auto
 authentication periodic
 mab
 dot1x pae authenticator
 spanning-tree portfast
```

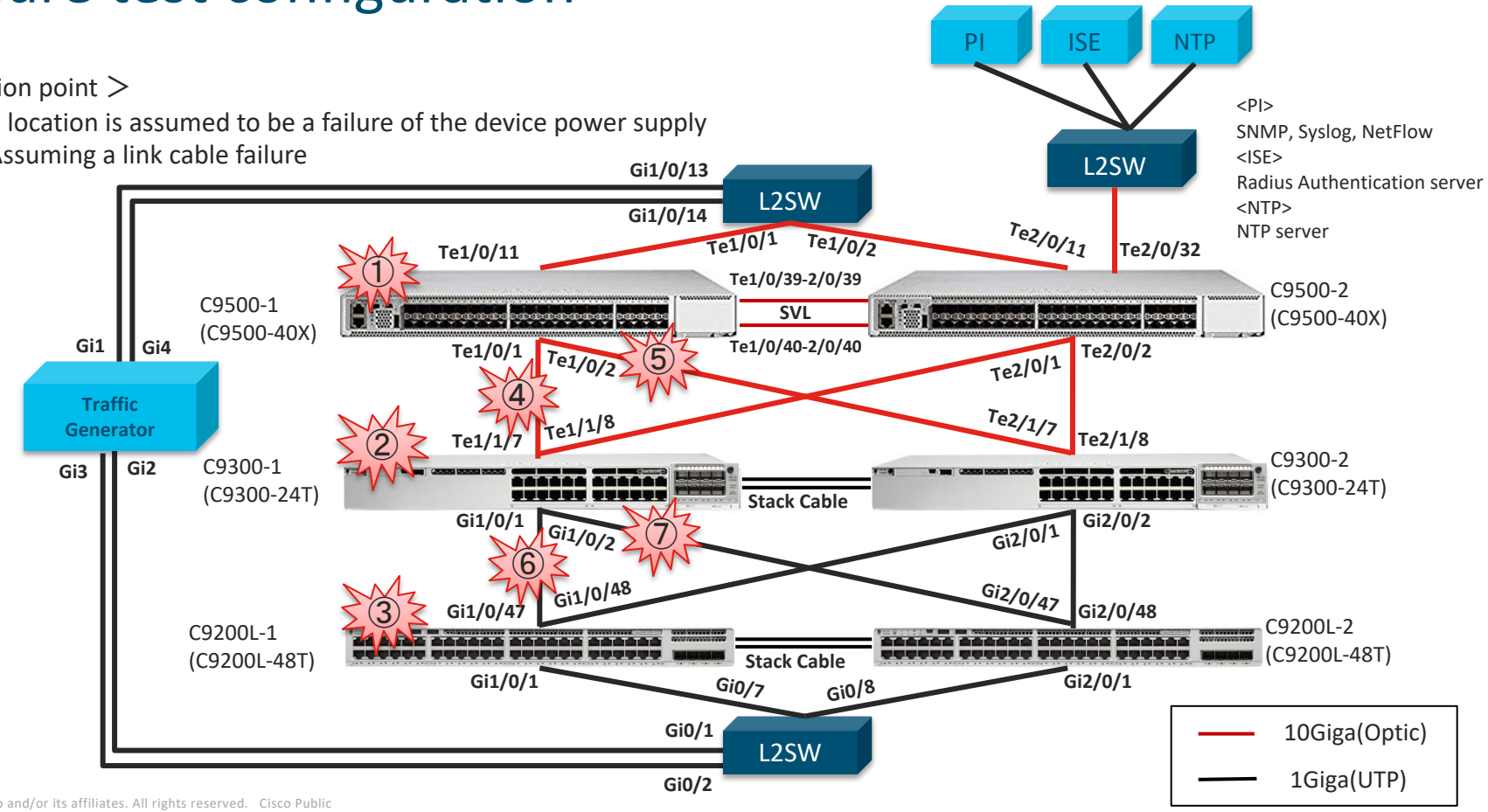
Visualisation (NetFlow)

```
!
flow record FLOW_RECORD
 match ipv4 version
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
!
!
flow exporter NETFLOW_TO_PI
 description Export Netlfow to PI
 destination 10.10.30.195
 source Loopback0
 transport udp 9991
!
!
flow monitor IPv4_NETFLOW
 exporter NETFLOW_TO_PI
 cache timeout active 60
 record FLOW_RECORD
```

```
!
interface GigabitEthernet2/0/47
 switchport trunk allowed vlan 31,101-110
 switchport mode trunk
 ip flow monitor IPv4_NETFLOW input
 ip flow monitor IPv4_NETFLOW output
 load-interval 30
 macsec network-link
 mka policy macsectest
 mka pre-shared-key key-chain macsectest
 channel-group 1 mode active
 service-policy output Queueing
!
```

Failure test configuration

＜ Verification point ＞
①②③ The location is assumed to be a failure of the device power supply
④⑤⑥⑦ Assuming a link cable failure



Failure test results – experimental, not a reference

Failure pattern	Downlink		Uplink		Remarks
	Disconnect (millisecond)	Switch back (millisecond)	Disconnect (millisecond)	Switch back (millisecond)	
① C9500-1 Power failure	26	9	29	7	
② C9300-1 Power failure	67	18	69	20	
③ C9200-1 Power failure	1680	20	1557	9	
④ C9500-1 Link failure Te1/0/1	4	4	93	4	
⑤ C9500-1 Link failure Te1/0/2	4	3	127	20	
⑥ C9300-1 Link failure Gi1/0/1	0	3	76	24	
⑦ C9300-1 Link failure Gi1/0/2	0	1	44	26	

Configuration samples – for lab usage only

It is the samples of configs for each device used in the verification.
Click the icon to display the settings.

Switch model	Sample configuration file
Catalyst 9500	Microsoft Word Document
Catalyst 9300	Microsoft Word Document
Catalyst 9200	Microsoft Word Document

Thank you!

www.cisco.com/go/cvd