IEC 62439-1

Edition 1.0 2012-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

AMENDMENT 1
AMENDEMENT 1

Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods

Réseaux de communication industriels – Réseaux de haute disponibilité pour l'automatisation – Partie 1: Concepts généraux et méthodes de calcul

IEC 62439-1:2010/A1:2012

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l’édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d’études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62439-1

Edition 1.0 2012-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour
inside

AMENDMENT 1
AMENDEMENT 1

Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods

Réseaux de communication industriels – Réseaux de haute disponibilité pour l'automatisation – Partie 1: Concepts généraux et méthodes de calcul

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX
L

ICS 25.040.40; 35.100.01
ISBN 978-2-83220-098-8

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

FOREWORD

This amendment has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation, working group 15.

The text of this amendment is based on the following documents:

FDIS	Report on voting
65C/684/FDIS	65C/691/RVD

Full information on the voting for the approval of this amendment can be found in the report on voting indicated in the above table.

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

3.1 Terms and definitions

Add the following new terms and definitions 3.1.67 and 3.1.68:

3.1.67
bridge
device connecting LAN segments at layer 2 according to IEEE 802.1D

NOTE The words “switch” and “bridge” are considered synonyms, the word “bridge” is used in the context of standards such as RSTP (IEEE 802.1D), PTP (IEC 61588) or IEC 62439-3 (PRP & HSR).

3.1.68
network recovery time
time span from the moment of the first failure of a component or media inside the network to the moment the network reconfiguration is finished and from which all devices that are still able to participate in network communication are able to reach all other such devices in the network again

NOTE When a network redundancy control protocol (like RSTP) reconfigures the network due to a fault, parts of the network may still be available and communication outages may vary in time and location over the whole network. In the calculations, only the worst case scenario is considered.

3.2 Abbreviations and acronyms

Add, in alphabetical order, in the list of abbreviations the following new abbreviation:

RRP Ring-based Redundancy Protocol, see IEC 62439-7

3.4 Reserved network addresses

Add at the end of the list given in the second paragraph, the following new item:

- RRP (see IEC 62439-7) uses 00-E0-91-02-05-99.

Add at the end of the list given in the third paragraph, the following new item:

- RRP (see IEC 62439-7) uses 0x88FE.

4.1 Conformance to redundancy protocols

Add at the end of the existing list, the following new item:

- compliance to IEC 62439-7 (RRP).

5.1.1 Resilience in case of failure

Add, at the end of the fourth paragraph ("… are met"*), the following new sentence:*

A network provides a deterministic recovery if it is possible to calculate a finite worst case recovery time of a given topology when a single failure occurs.

5.1.4 Comparison and indicators

Add, in the existing Table 2, the following new line between the existing lines "BRP" *and* "PRP"*:*

RRP	IEC 62439-7	Yes	In the end nodes	Double (switching end nodes)	Single ring	8 ms in 100BASEX, 4 ms in 1000BASEX

8 RSTP for High Availability Networks: configuration rules, calculation and measurement method for deterministic recovery time in a ring topology

Replace, in the existing title of this clause, the words "for deterministic recovery time in a ring topology" *by* "for predictible recovery time".

Add, between the existing title of this clause and the existing title of 8.1, the following new note:

NOTE In the context of this Clause, the word “bridge” is used in place of “switch”, respectively “bridging” instead of “switching”.

Add, at the end of this clause, the following new Subclause 8.5:

8.5 RSTP topology limits and maximum recovery time

NOTE In the next edition of IEC 62439-1, this new Subclause 8.5 will be renumbered as 8.2.

8.5.1 RSTP protocol parameters

This subclause explains the RSTP protocol parameters that impact network recovery times and shows how a specific topology and protocol configuration influence them. First, RSTP-specific terms are defined. Then, basic guidelines on network design are given and finally a method to determine an approximation of an upper bond worst case network reconfiguration time for meshed RSTP networks is given.

This subclause particularly deals with RSTP networks that are composed of more than a single ring. For a single Ethernet ring running RSTP, the network reconfiguration time can be determined as 8.2 shows. However, the subsequent statements concerning RSTP parameters are also applicable in a ring network.

8.5.2 RSTP-specific terms and definitions

NOTE These terms are inherited from IEEE 802.1D.

8.5.2.1 Transmission Hold Count (TxHoldCount)

Each port of an RSTP bridge includes a counter TxHoldCount. This counter starts at zero and is incremented for each BPDU the port sends. A timer decrements every second the counter. If TxHoldCount reaches the maximum value, no further BPDU are transmitted over that port until the counter has been decremented again, regardless of the importance of the BPDU to network reconfiguration. The default maximum value of TxHoldCount is 6 and the maximum configurable number is 10.

8.5.2.2 Bridge Max Age

Each RSTP bridge includes a parameter Bridge Max Age that should be configured to the same value in each bridge. Bridge Max Age defines the maximum total number of “physical hops” or links between the root bridge and any bridge participating in the same RSTP network. Its default value is 20 and it can be configured to from 6 to a maximum of 40. In special cases, Bridge Max Age is configured differently in some bridges.

Because Bridge Max Age defines the maximum extension of an RSTP network, it is sometimes referred to as “network diameter”. But “Bridge Max Age” and the actually usable network diameter are not synonymous, see 8.5.2.4.

8.5.2.3 Message Age

Each BPDU includes a parameter Message Age. Upon reception of a BPDU, a bridge increments Message Age and afterwards compares it to its “Bridge Max Age”. If Message Age is larger than Bridge Max Age, the bridge discards the BPDU and ignores the information it carries.

The root bridge starts by sending BPDUs with Message Age = 0. The first bridge after the root bridge (and subsequent bridges until Message Age reaches Bridge Max Age) receives the BPDU, increment “Message Age” by 1, compares it to the “Bridge Max Age” and transmit BPDUs with the updated information.

8.5.2.4 Network diameter and radius

The “diameter” in an RSTP network is the number of bridges on the longest active path in a network tree between the two bridges that are the farthest away from each other. The diameter does not necessarily correspond to the RSTP parameter Bridge Max Age (see Figure 23).

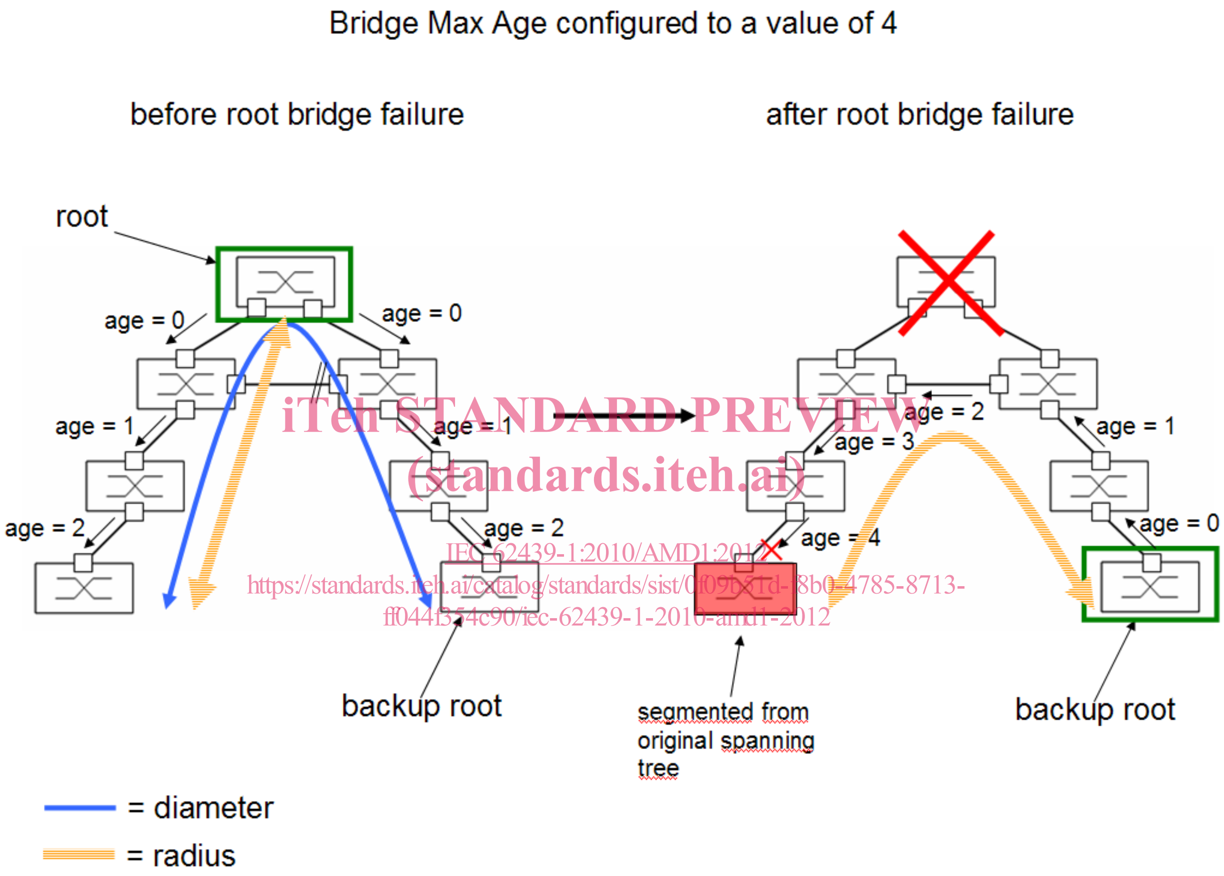
The ”radius” in a RSTP network is the number of bridges from (and including) the active root bridge to the bridge that is the farthest away from this active root in the topology. This is the length (in hops) of the longuest path over which the RSTP protocol information needs to be forwarded (see Figure 23). The maximum supported radius by RSTP can be defined as:

$$\text{max. radius} = \text{Bridge Max Age} + 1.$$

The radius is important to determine worst case topologies. In a worst case fault situation (without an engineered network and consciously placed root bridges), upon failure of a root bridge, the farthest away leaf might be the backup root bridge, which might become the next root. In this case, the diameter of the network can become the radius and it becomes the actual path that the RSTP information to the individual bridges has to travel. (See Figure 23)

NOTE RSTP BPDUs are only transmitted on the link between two directly connected bridges. Each bridge consumes and produces these BPDUs, but the RSTP information which they carry travels distinct paths through the network (in a stable network state without reconfiguration).

8.5.3 Example of a small RSTP tree



IEC 953/12

Figure 23 – Diameter and Bridge Max Age

NOTE 1 The RSTP parameter Bridge Max Age has been assigned the value 4 for the sake of this example although 802.1D does not allow a value lower than 6.

In the example of Figure 23, at first, the network without a failure is in a stable condition with Bridge Max Age = 4 and because the actual radius is 4 (the RSTP configuration could support a maximum radius of 5). The diameter is 7, from one leaf in one branch to the other leaf in the other branch, via the root bridge. Because the root bridge is the root element of a balanced tree, Bridge Max Age = 4 is sufficient for all bridges to receive RSTP BPDUs from the same RSTP root.

A root bridge failure and an unfavorable backup root election changes that. After a root bridge failure, the redundant link that was formerly blocked is activated. The diameter is now 6. At the same time, the radius is also increased to 6. Because one of the leaves of the original branches has now become the root bridge, the Bridge Max Age of 4 is not sufficient for the RSTP root information to reach all bridges of the network, because the RSTP information now has to travel the whole diameter, which is now equivalent to the radius. Thus, the last bridge is segmented, as indicated in Figure 23. This bridge discards the BPDU, because the Message Age has exceeded the configured Bridge Max Age.

To engineer stable and high performance networks, it is necessary to observe and understand the difference between the network diameter and the radius, respectively the Bridge Max Age parameter. The Bridge Max Age parameter is kept as high as necessary not to segment any device in a worst case fault scenario and as low as possible to minimize the network recovery time as shown in the following subclauses. The network radius determines the necessary Bridge Max Age value for each considered topology. The Bridge Max Age can be kept low by positionning both root bridge and backup root bridge at a central position in the network, e.g. on the main ring of a hierarchical multi-ring topology.

NOTE 2 Another method, which is not covered in this document, is to configure different Bridge Max Age values on root and backup root bridge, according to their respective positions in the network.

8.5.4 Assumption on TxHoldCount

Calculation or approximation of an upper bond reconfiguration time is made under the assumption that the Transmit Hold Count (TxHoldCount) is never reached and no BPDU necessary for fast reconfiguration of the network is lost.

This however can occur in practice, especially during network reconfiguration. As soon as the TxHoldCount of one bridge port becomes “saturated”, all bridges connected to the saturated port won’t receive any BPDUs any more until the TxHoldCount has been decremented. If the dropped BPDUs are vital for network reconfiguration, the network reconfiguration time can be extended by several seconds. This assumption is of high practical relevance and is considered as the biggest threat to the network reconfiguration time of RSTP networks.

8.5.5 Worst case topology and radius determination

Because the worst case radius and the lowest possible Bridge Max Age parameter are correlated, determining the worst case radius is important in determining the upper bond worst case reconfiguration time.

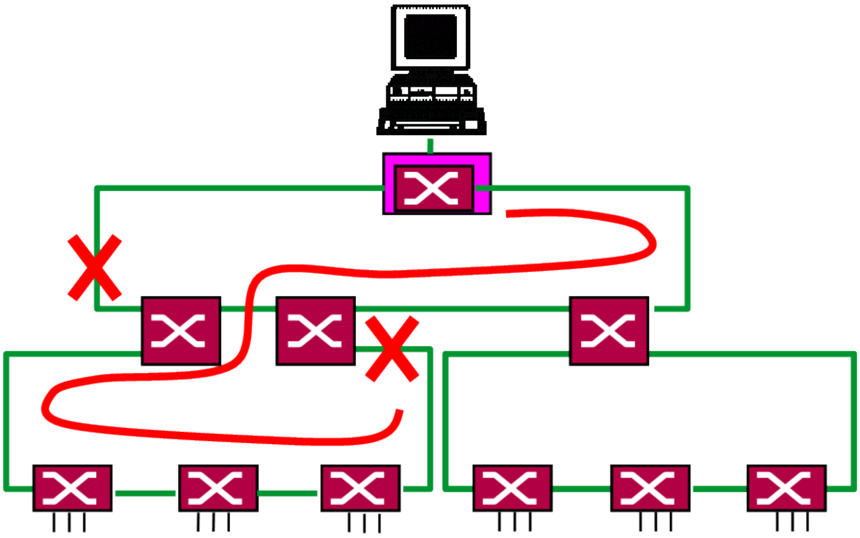
In an arbitrarily meshed network, the reconfigured links of the network in steady state after reconfiguration can be predicted prior to the failure, but as the protocol is based on reception and sending BPDUs in each individual bridge, race conditions can occur during reconfiguration. Therefore the maximum reconfiguration time can only be given as a worst case bound based on the maximum reaction time of each bridge and the maximum number of hops allowed by the protocol.

In addition, some media such as 1000Tx present large link failure detection times. Indeed, auto-negotiation disabled on fiber Gigabit links may jeopardize RSTP failover time in case of link failure.

NOTE Malicious failures such as a bridge unable to forward payload frames but still exchanging BPDUs with its neighbors cannot be considered in the calculations.

When designing a network that operates with RSTP, the network radius from the root-bridge location and from the backup root location to the farthest away leaf bridge has to be calculated.

This radius calculation also considers a worst case failure, because failures in the topology can increase the radius. As an example, Figure 24 shows the root bridge and the backup root bridge located on the main ring. The worst case radius for this specific topology is reached by two simultaneous failures positioned as Figure 24 shows, which is 7 for the indicated root.



IEC 954/12

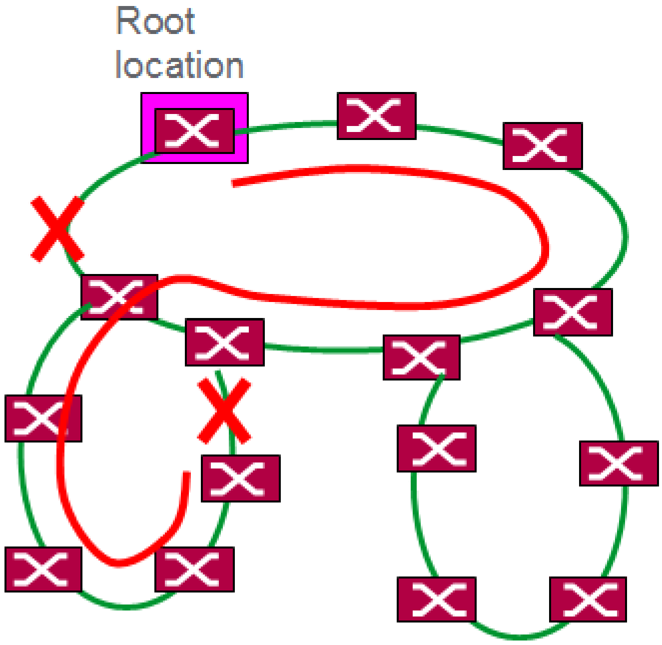
Figure 24 – Worst path determination

Once the worst case radius value for a worst case failure scenario in the network topology has been determined, Bridge Max Age should be configured to exactly this number - 1. This minimizes the upper bond reconfiguration time of the network, since a lower Bridge Max Age limits the time that BPDUs circulate in the network.

8.5.6 Method to determine the worst case radius in case of a ring-ring architecture

In a ring of rings topology, the main ring is made of “N” bridges + 2 × “M” bridges that connect “M” sub-rings redundantly, each made of “R” bridges (excluding the bridge to connect on the main ring).

Figure 25 shows an example of a main ring (N = 3) with two sub-rings (M = 2) connected redundantly via a total of four bridges (two per sub-ring) to the main ring, with R = 4.



IEC 955/12

Figure 25 – Example ring-ring topology

Root bridge and backup root bridge remain on the main ring (this is ensured by configuring the RSTP priority of root and backup root on the main ring with a better priority value than any other bridge in the sub-rings).

Only one failure at the main ring and one failure at the sub-ring are considered. Sustaining one failure in the main ring and simultaneously a second failure in a sub-ring is a corner case.

Then the worst case radius (i.e. the Bridge Max Age that needs to be configured which is equivalent to the worst case radius - 1) is:

$$\text{worst case radius} = N + 2 \times M + R$$

$$\text{Bridge Max Age} = (\text{worst case radius} - 1) = N + 2 \times M + R - 1$$

where

“R” is the number of bridges in the sub-ring with the highest number of devices;

“N” is the number of bridges in the main ring (excluding the bridges that connect the sub-rings);

“M” is the number of bridges in the main ring that connect the main ring to the sub-rings.

In the diagram above, considering that N=3, M=2, R=4, the worst case radius = 11.

Thus, the RSTP protocol parameter “Bridge Max Age” should be configured to a value of 10 to optimize network recovery times.

8.5.7 Worst case radius of an optimized multilayer architecture

With a large number of bridges, the network topology should be optimized in order not to reach the Bridge Max Age limit and to keep worst case reconfiguration times low.

A simple solution is to consider a multilayer topology, consisting of “L” layers, as shown in Figure 26:

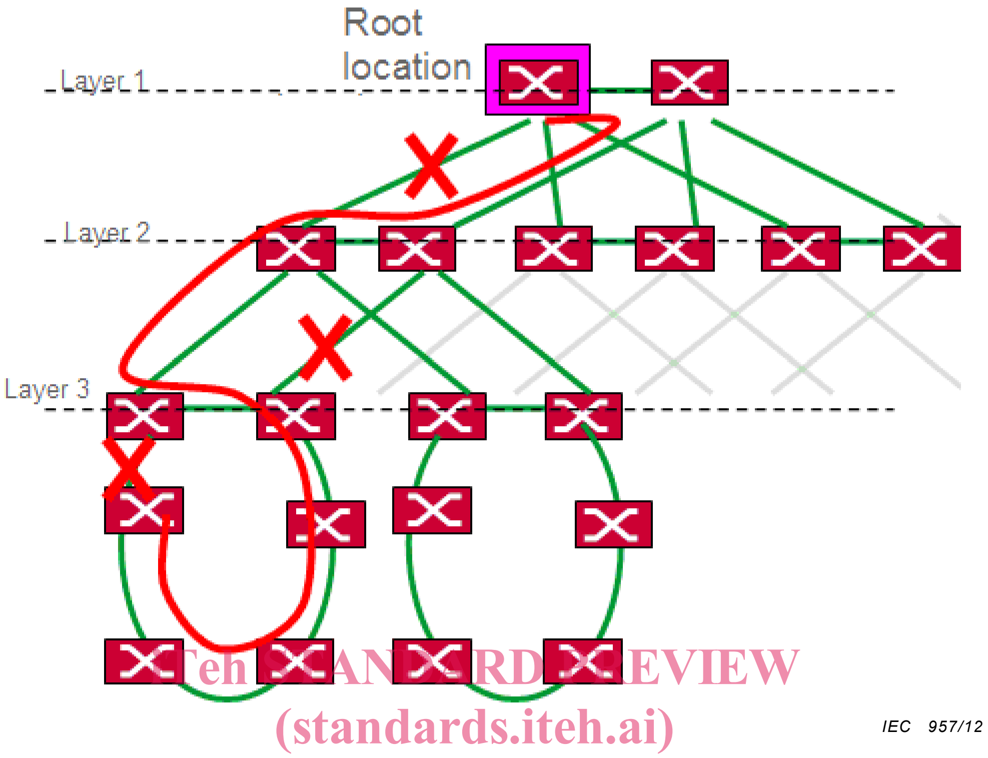


Figure 26 – Example multilayer topology

The upper layer is made of 2 main bridges which are set to be the root/backup root bridges. (Priority value of these bridges is expected to be set consequently to the highest and second to highest priority).

The maximum size of layer 3 is defined by sub-rings made of “R” bridges. The parameter “R” excludes the bridges that connect the individual layer 3 subring to layer 2, which is taken into the calculation through the parameter “L”.

Only one failure per layer is considered.

Then the worst case radius is equal to:

$$\text{worst case radius} = (2 \times L) + R$$

In the above diagram, L=3, R=4, and therefore, worst case radius = 10. This results in a Bridge Max Age parameter of 9.

The interesting point is that this result is not dependant on the number of branch-offs per layers, and this topology is possibly able to support a large number of nodes with a low Bridge Max Age parameter. The limitation is the maximum number of ports of the bridges used at each layer: A large number of physical ports is detrimental to RSTP performance on bridges.

8.5.8 Approximated upper bond reconfiguration time for RSTP networks

The RSTP root bridge failure is the worst case scenario affecting reconfiguration time. The upper bond reconfiguration time is the time needed for recovery after a root bridge failure. The recovery time for link failures or non-root bridge failures will not exceed the root bridge