# Network Redundancy

DESCRIPTION

**NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.



TRADEMARKS

# 1 INTRODUCTION

This document describes the MX-ONE network redundancy. The document is intended for those who want to know more about the functionality as well as technicians that want to learn about certain procedures and specific behavior of the function.

It covers:

- Basic network configurations and techniques used for network redundancy
- MX-ONE network redundancy using Ethernet bonding.

## 1.1 GLOSSARY

**ARP**
Address Resolution Protocol. Used to find out on what hardware address (MAC) a IP address is used.

**Alias address**
An alias IP address tied to a specific network interface. IP aliasing is the process of adding more than one IP address to a network interface

**Base address**
The normal IP address for a network interface.

**Bonding**
Network bonding. See Link aggregation.

**Gratuitous ARP**
An ARP announcement of a MAC and IP address combination.

**LAN**
Local Area Network

**Link aggregation**
One or more links (such as Ethernet) are aggregated together to increase bandwidth or increase redundancy for higher availability.

**Link layer**
The lowest layer in the Internet Protocol suite.

**MSTP**
Multiple Spanning Tree Protocol

**Multi homed protocol**
A protocol where the endpoint could handle two or more IP-addresses at the same time for one session.

**Network element**
Some network equipment for example: server, switch, router and IP-phone

**Network redundancy**
When more than one communication path exists between to specific Network elements.

**Routing**
Forwarding of messages based on IP address (level 3).

In modern routers performed by hardware.

**RSTP**
Rapid Spanning Tree Protocol

**Single homed protocol**
A protocol where the endpoint only handles one IP-address at a time. This is the most common case for IP protocols.

**SMLT**
Split Multi-Link Trunking

**STP**
Spanning Tree Protocol

**Switching**
Forwarding of messages based on Media Access Control (MAC) addresses (level 2).
In modern switches performed by hardware.

**UPS**
Uninterruptible Power Supply

**VLAN**
Virual LAN

**VRRP**
Virtual Router Redundancy Protocol

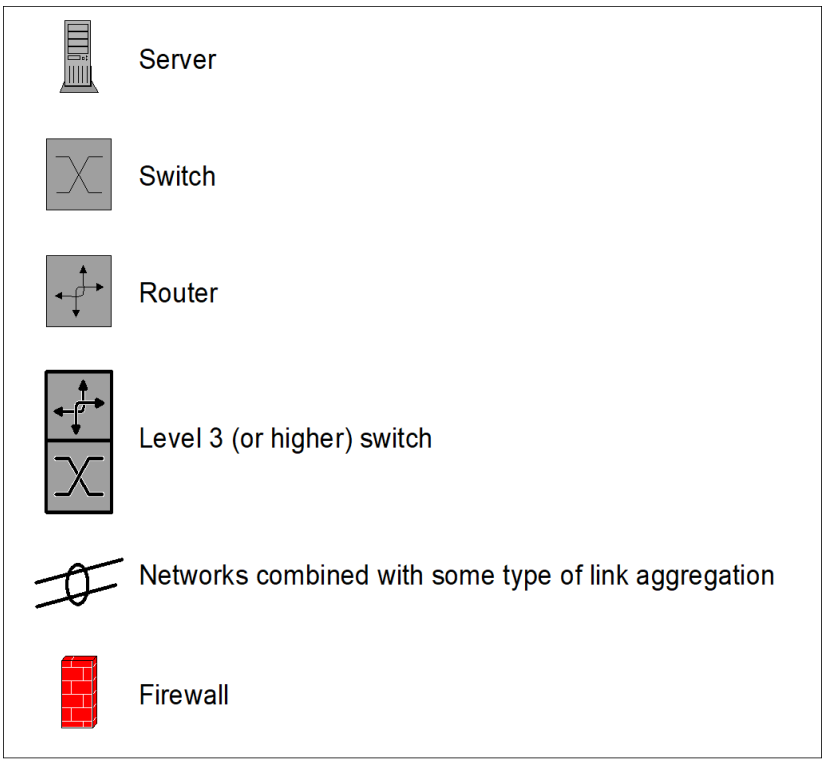


**Figure 1: Symbols used**

# 2 BASIC NETWORK TECHNIQUES FOR REDUNDANT NETWORKS

This chapter describes different types of redundant network configurations and common ways to build redundant networks. Included are different types of switched redundant networks. The Spanning Tree Protocol, Virtual Router Redundancy Protocol and network redundancy with multiple subnets is also covered briefly.

Redundant networks are mainly used for two reasons fault tolerance and load sharing. This document concentrates on fault tolerance.

## 2.1 WHAT MAKES A NETWORK REDUNDANT

There should always exist a redundant equipment part that could be used if another part fails.

Avoid single point of failure for all equipment such as:

- Power supplies
- Links
- Switches
- Routers
- Physical location of equipment

Avoid the common mistake of using different VLANs in the same physical switch for network redundancy. If the switch fails both VLANs will fail.

## 2.2 COMMON TECHNIQUES USED IN NETWORKS

In this chapter some common basic techniques used when building redundant networks are briefly described:

- Spanning Tree Protocol
- Virtual Router Redundancy Protocol
- Link aggregation (bonding)

### 2.2.1 SPANNING TREE PROTOCOL (STP)

The Spanning Tree Protocol (STP) is used in switched networks with redundant links to avoid loops in the network that will, if not blocked, lead to broadcast storms.

The picture below shows a network with three switches interconnected with Ethernet links. With Spanning tree active in the network, redundant links will be blocked, and by that loops and broadcast storms avoided.

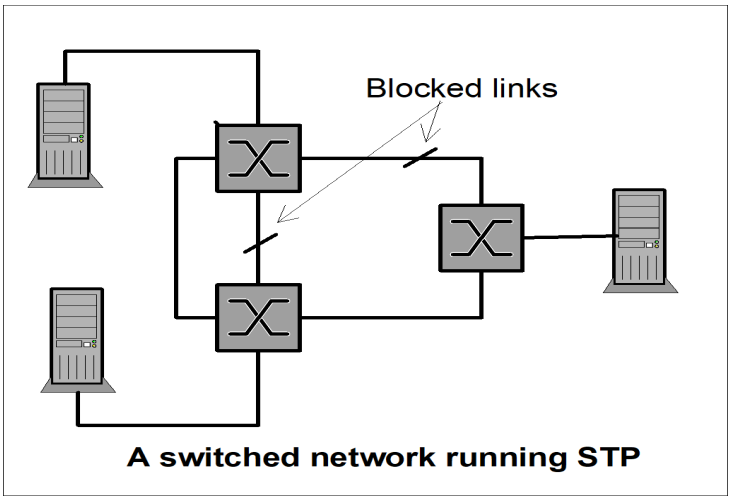


**Figure 2: Spanning Tree**

If any of the links currently in service fails, STP will activate earlier blocked redundant links. Hereby network traffic could continue after a small disturbance. See Figure 3, STP Blocked Link Activated.

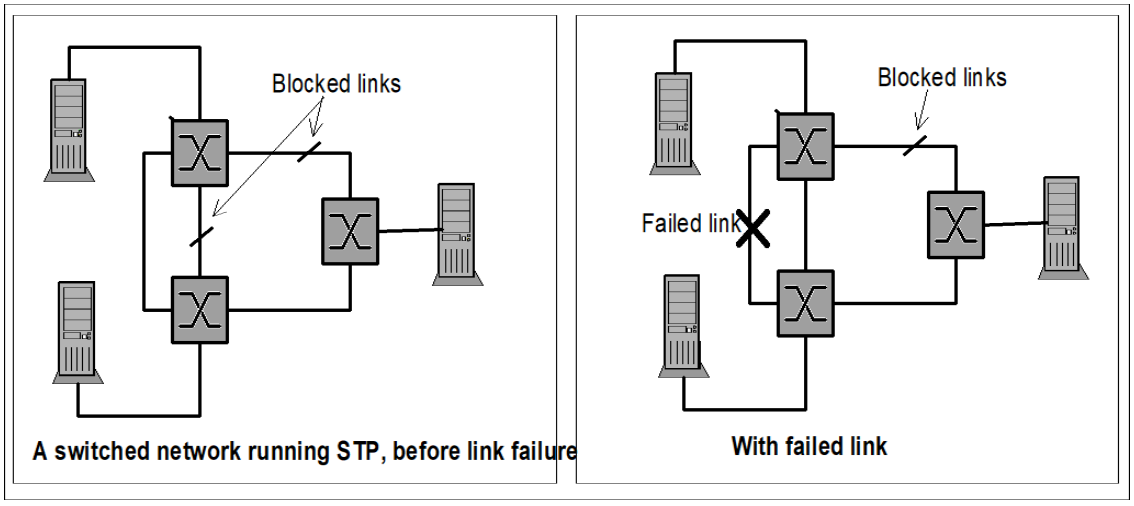


**Figure 3: STP Blocked Link Activated**

The Spanning Tree Protocol exists in different versions:

**Spanning Tree Protocol (STP)** is the oldest version and is much slower than the other versions to de-block redundant links in case of failure. STP is normally too slow, 30-50 seconds, to respond to a change in the network.

**Rapid Spanning Tree Protocol (RSTP)** is a quicker variant of STP and will normally change within 6-30 seconds.

**Note:** RSTP is recommended to be used in all redundancy cases where several switches are involved

**Multiple Spanning Tree Protocol (MSTP)** is a variant of RSTP for Virtual LANs (VLAN). A separate Spanning Tree could be defined for each VLAN. Normally change occurs within 6-30 seconds.

## 2.2.2 VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP)

The Virtual Router Redundancy Protocol (VRRP) makes it possible to have one or more redundant routers as default gateway. With VRRP multiple routers appear as a single virtual router. VRRP is an Internet standard described in RFC 3768.

**VRRP concepts:**

**VRRP Router**
A router running the Virtual Router Redundancy Protocol. It may participate in one or more virtual routers.

**Virtual Router**
An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router ID and a set of associated IP address(es) across a common LAN. A VRRP Router may backup one or more virtual routers.

**Virtual Router ID**
The ID of a Virtual Router (VRID).

**Virtual Router IP**
The IP address of a Virtual Router

**Virtual MAC address**
The MAC address for a Virtual Router. There are a number of reserved MAC addresses for the Virtual Router functionality in format: 00-00-5E-00-01-{VRID} (in hex in Internet standard bitorder).
{VRID} is the VRRP Virtual Router Identifier. This mapping provides for up to 255 VRRP routers on a network. For details see RFC 3768.

**Master**
The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses.

**Backup**
The set of VRRP routers available to assume forwarding responsibility for a virtual router if the current Master should fail.

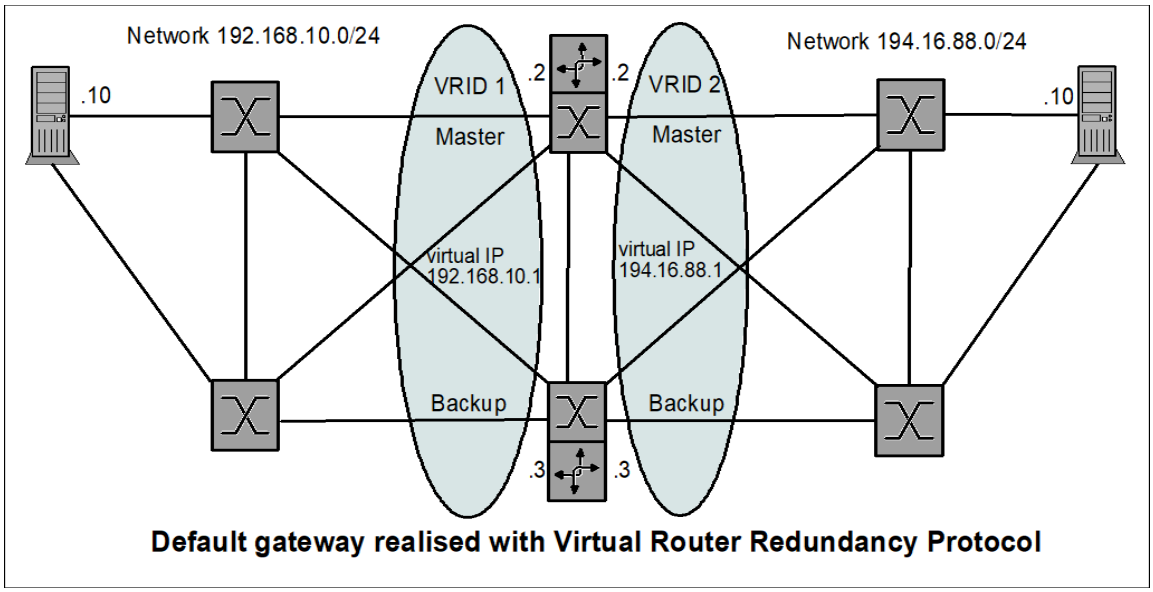


**Figure 4: Virtual Router Redundancy**

Above is a picture with a network that implements one virtual router on the outgoing side (VRID 1) and another virtual router on the incoming side (VRID2). With this setup it is possible to have resilient routing both into and out of the domain without having to run a dynamic routing protocol.

### 2.2.3 LINK AGGREGATION

Link aggregation (network bonding) combines two or more interfaces to look like one interface to the applications. Link aggregation could be used to increase the bandwidth or to increase the redundancy for higher availability.

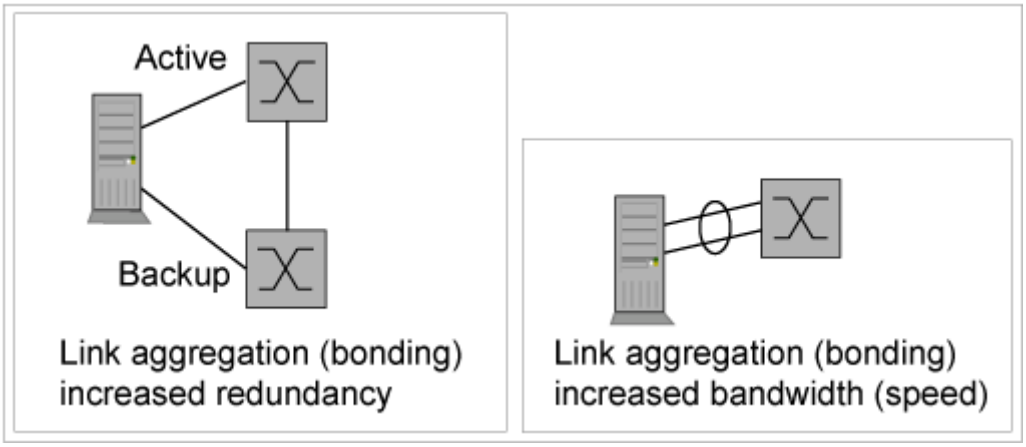


**Figure 5: Link Aggregation**

Link aggregation for increased redundancy could be configured to use either an active/backup mode on the interfaces or an active/active mode where data is sent on both interfaces.

In Link aggregation for increased bandwidth the two endpoints cooperates to use all aggregated interfaces to send data in parallel.

For all modes where aggregated interfaces from the server are active simultaneously the connected switch or switches must support and handle this functionality.

## 2.3 SWITCHED REDUNDANT NETWORK

Many different network solutions exist for switched redundant networks. Redundant networks are usually used in the backbone of a network, but could also be used for user access.

Redundancy for switched networks are handled on link level, for Ethernet that is on Ethernet level.

A switched redundant user access is normally in the form active/backup or active/active. Some kind of link aggregation (bonding) is normally used.

In an active/backup solution one link at a time is used by the user. If the active link fails the backup link will take over. Fail-over is normally handled by the link layer. For Ethernet that is on Ethernet level. The active and backup link normally shares the same IP- and MAC-address. In an active/active solution both links are sending and receiving data at the same time. The most common way when connecting to shared networks is to use the same IP address and MAC address on both interfaces. The outgoing traffic from the server is distributed over the links by some hash algorithm. With an

active/active solution the switches in the network have to support this way of working. For more information on SMLT, see 2.3.3 Split Multi-Link Trunking (SMLT) on page 10.

Below different ways to build switched redundant networks are described:

- Basic switched redundant network
- Switched “Mesh”
- Split Multi Link Trunking

### 2.3.1 BASIC SWITCHED REDUNDANT NETWORK

A basic switched redundant network could be built with almost all types of switches. If redundant links exist in the network this type of network needs the Spanning Three Protocol to avoid broadcast storms. See chapter 2.2.1 Spanning Tree Protocol (STP) on page 5.

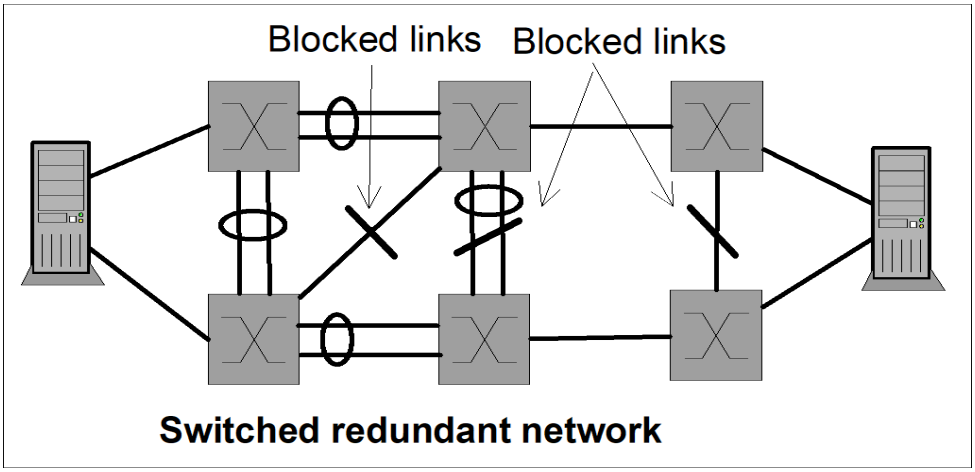


**Figure 6: Switched Redundant Network**

### 2.3.2 SWITCHED “MESH”

Some switches have the functionality to build switch mesh domains.

Switch ports inside a switch mesh domain could have redundant links without creating broadcast storms. There is no need for Spanning Tree inside the switch mesh. Below is a picture of two computers connected to a switched redundant network built with a mesh domain.

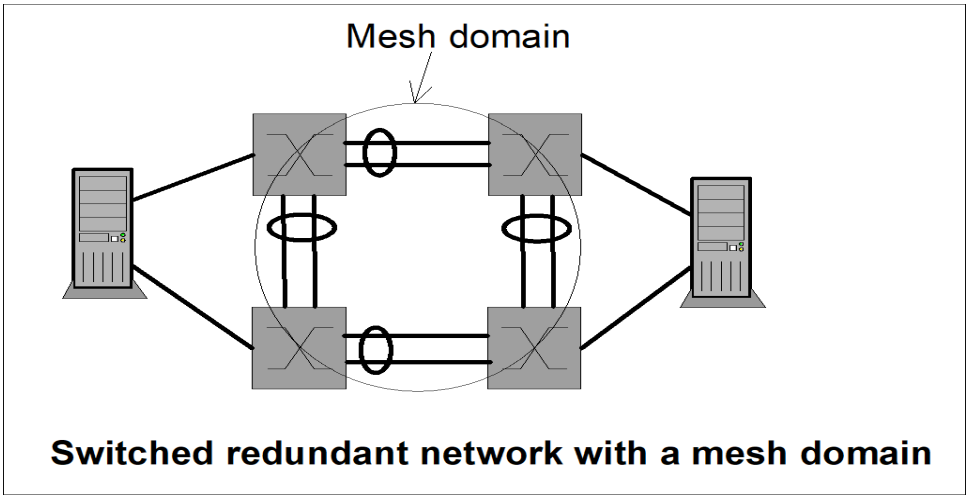


**Figure 7: Mesh Domain**

If ports external to the mesh are connected in a way that results in redundant links the Spanning Tree Protocol must be used to avoid broadcast storms for these ports. See Figure 8, Meshed Domain with Spanning Tree.

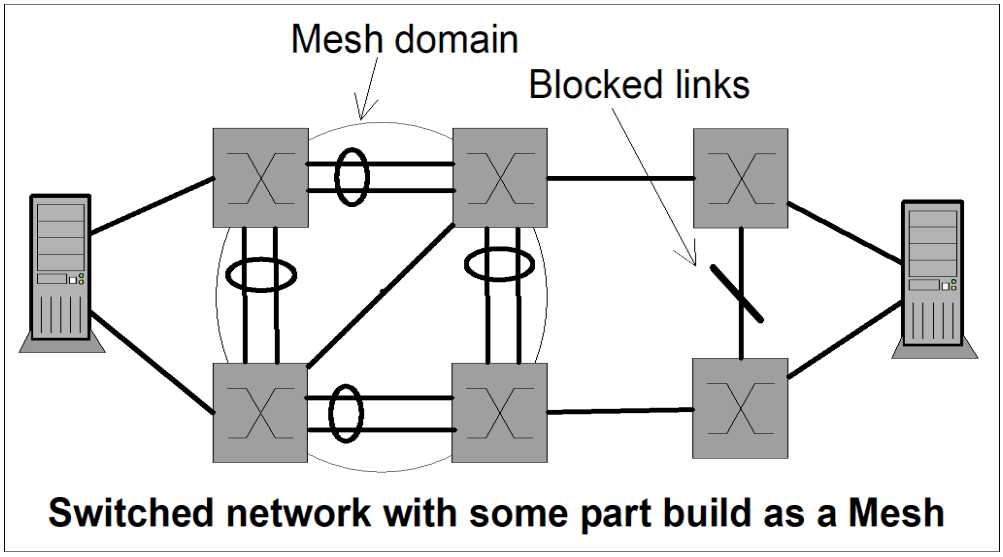


**Figure 8: Meshed Domain with Spanning Tree**

If the network in the picture above is built without the mesh domain more links have to be blocked (by spanning tree). It would be as for the basic switch redundant network, See Figure 6, Switched Redundant Network.

### 2.3.3 SPLIT MULTI-LINK TRUNKING (SMLT)

With Split Multi-Link Trunking two physical switches will look like one switch to the user. SMLT is a link aggregation technology. With SMLT load balancing and link redundancy could be achieved. A requirement is that the user should support IEEE 802.1ax (former 802.3ad).

A network setup would look like the picture below. See Figure 9, Split Multi-Link.

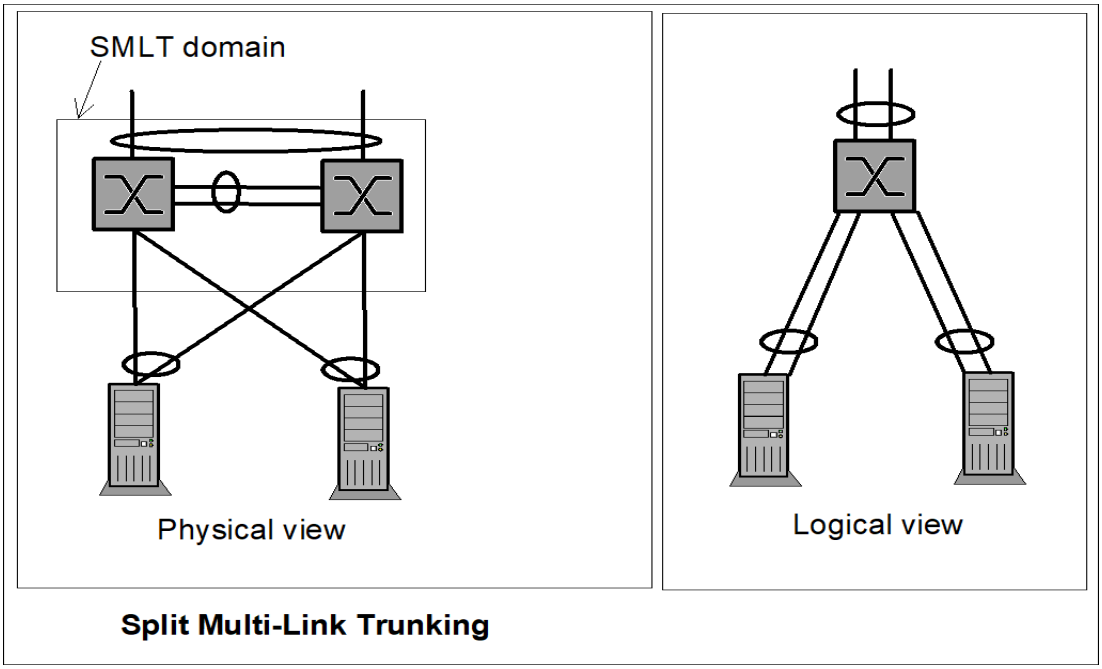


**Figure 9: Split Multi-Link**

In this type of network there is no need for spanning tree protocols as no redundant links in the switch domain have to be blocked. All ports are active and are used for traffic.

When multiple physical switches are used with Split Multi-Link Trunking they will look like one switch to the user.

## 2.4 MULTIPLE SUBNET REDUNDANT NETWORKS

This chapter briefly describes network redundancy using separate subnets. Redundancy based on subnets are redundancy on IP-level. To make failover work on IP-level either IP routing or support on application level is needed. This makes it harder to implement fail-safe applications on multiple subnet redundancy compared to a switched redundant network. Examples of support on application level to make failover work:

- Using a multi homed protocol such as SCTP
- Using single homed IP-protocols such as TCP with more than one session
- Using single homed IP-protocols such as TCP in an active/passive implementation

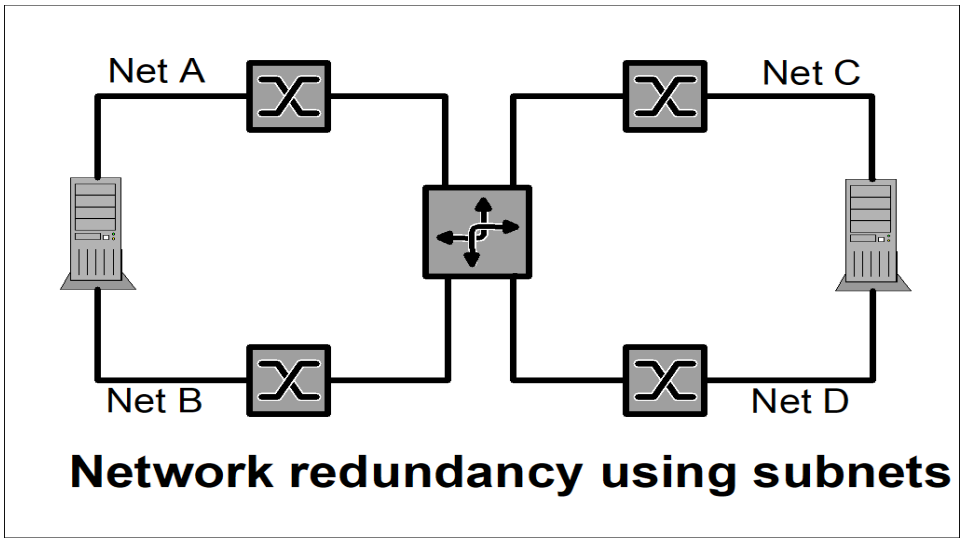


**Figure 10: Network Redundancy using Subnets**

### Default gateway considerations

The servers in the above picture have two subnets connected to the router. A server normally has one default gateway route programmed. To work in a multiple subnet redundant network some mechanism to change default gateway routing in case one network fails has to be used. The server could run some type of ip routing software but that is usually too complicated to be used. Another solution is to run some software locally on the server that will reprogram the default gateway if the current path to the default gateway fails.

### Application failover from net A to net B

If a server is communicating with another server attached to it's own subnet the application have to take measures to change communication path if the link fails. This could be solved in the application with some failover mechanisms or by using a multi-homed protocol such as SCTP.

## 2.5 A MULTI LAYER REDUNDANT NETWORK EXAMPLE

Large networks are normally built in a layered architecture to make them easier to maintain and enlarge.

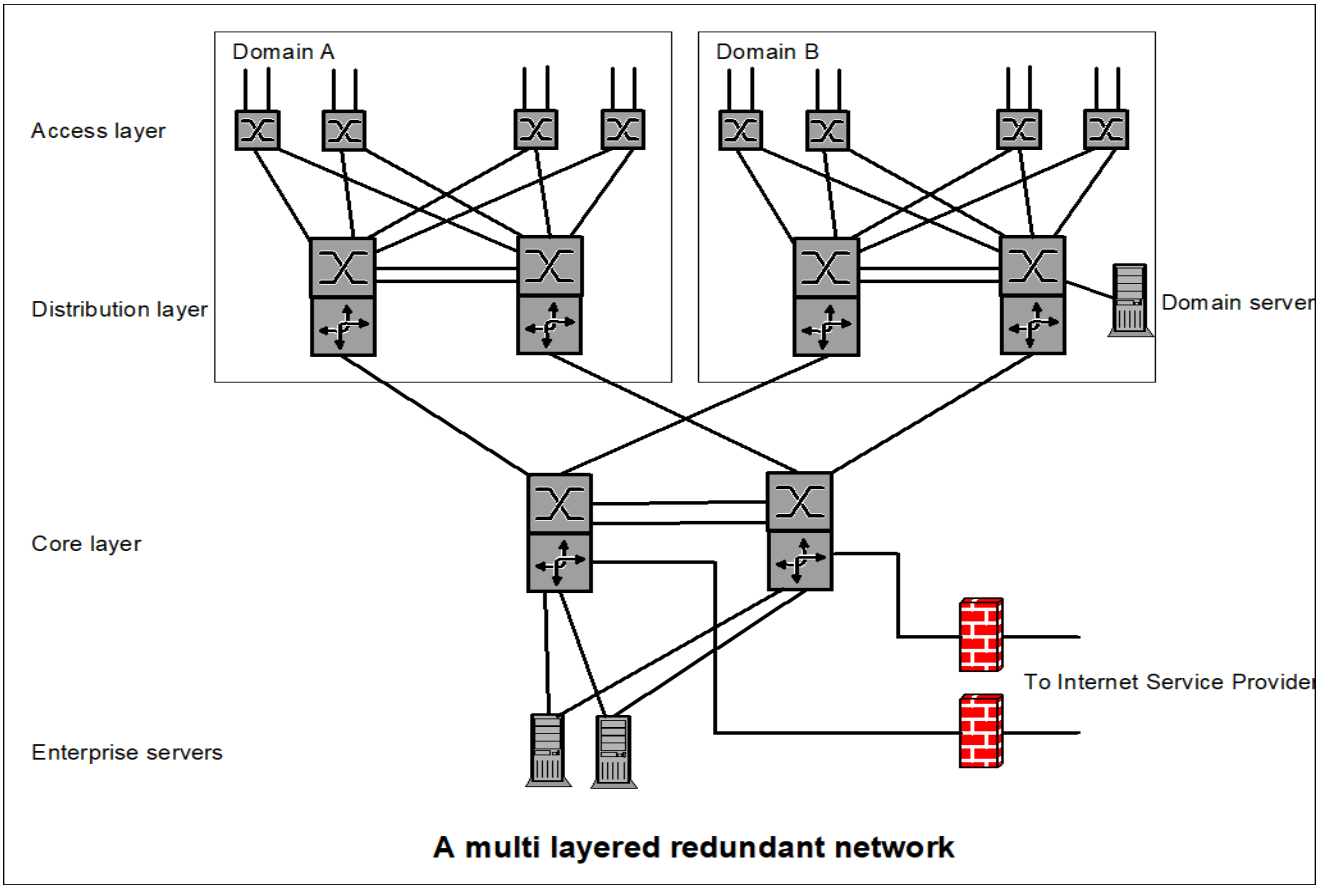


**Figure 11: Multi-Layered Redundant Network**

The picture above contains different layers:

**Access layer**

The users are connected to the access switches that all have redundant connections to the distribution layer. A user that needs redundant connection has to have redundant links to at least two physically separated access switches. The user access could if needed use different VLANs for different users groups.

**Distribution layer**

The distribution layer implements routing between users in different VLANs in the same domain. A domain could be a building or one floor in a building. The distribution layer has switching on level 2 and 3. It also has redundant links to the Core layer. This layer could contain servers that are needed in this domain only.

**Core layer**

This is the backbone of the enterprise network. Supporting switching and routing from level 2 to level 4. Core layer routes between different domains connect enterprise servers and have connection to the Internet Service Providers via firewalls.

Different physical locations such as buildings or a separate floor are implemented as a domain. The number of users is easy to scale by increased number of access switches. A new building would be added to the network as a new domain.

# 3 MIVOICE MX-ONE NETWORK REDUNDANCY

## 3.1 GENERAL

This chapter describes the MX-ONE specific considerations with network redundancy.

The only type of network redundancy supported in MX-ONE is switched network redundancy. This is implemented as Ethernet bonded network redundancy in MX-ONE. The Dual sub-net network redundancy is no longer supported, from MX-ONE 6.0 and later.

## 3.2 ETHERNET BONDED NETWORK REDUNDANCY

### 3.2.1 GENERAL

With Ethernet bonded network redundancy a switched redundant network is used for network redundancy.

Two Ethernet interfaces are aggregated to work together. One interface is active at a time and the other interface is backup. The two interfaces share the same IP and MAC addresses. If one of the interfaces fail, the other one will continue to serve the operations and the MX-ONE Service Nodes (SN) will be available on the functioning interface.

Ethernet bonding is today only supported in the MX-ONE Service Node.

MGU supports active/backup redundancy to be used with Ethernet bonded networks. This is a MGU internal link fail-over mechanism.

The MX-ONE Media Server can use the MX-ONE Service Node's ethernet bonding.

Media gateways could be connected via a local switch. By this local switch, capabilities in the network could recover some network faults. The impact on system behavior depends on the time it takes for the network to recover.

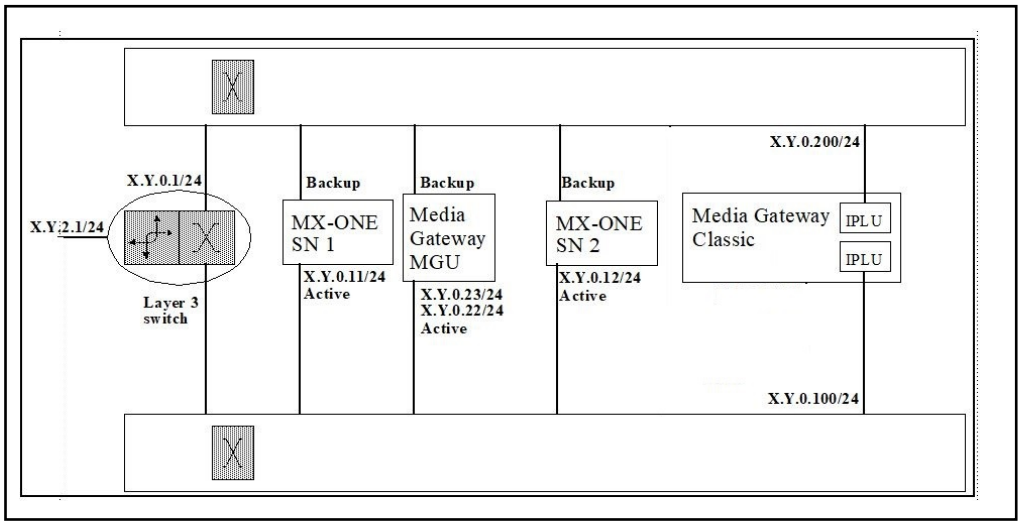


**Figure 12: System with Ethernet Bonding Network Redundancy**

Allowed configurations for Ethernet bonding network redundancy and Media Gateways are shown in chapter 3.2.3 Media gateway considerations and configurations on page 15.

Observe that some kind of Spanning Tree Protocol is needed in the network if it contains redundant network paths. It is needed to avoid Ethernet broadcast storms. The performance on network recovery varies depending on type of Spanning Tree Protocol and network configuration. The Rapid Spanning Tree Protocol (RSTP or MSTP) is recommended.

A better solution is to use switches that support some more modern architecture such as Split Multi-Link Trunking (SMLT). In that case the Spanning tree protocol is not needed.

The following factors need to be addressed when planning for an Ethernet bonding redundant network solution:

- At least two physically separated switches are needed to have a fault tolerant system.
- Certain features, like for example operator queue and ACD backup group, can be duplicated and placed in different MX-ONE Service Nodes. This increases the reliability for specific features.
- It is recommended to locate the phones and application servers on a separate subnet and let them access the Media Gateways and MX-ONE Service Node through a router.

### 3.2.2 LIMITATIONS

This section lists the known limitations with the redundancy solution in MX-ONE that must be considered when deploying Ethernet bonded network redundancy.

- It is recommended to define at least two ARP IP targets per server. If only one ARP IP target is specified and that target is unreachable, communication will change back and forth between the interfaces. If this happens it will most likely lead to lost IP packets and fatal disturbances in the server communication.

### 3.2.3 MEDIA GATEWAY CONSIDERATIONS AND CONFIGURATIONS

The following types of media gateways exist:

- MGU based
  - MX-ONE Lite
  - MX-ONE Classic

In the chapters below considerations and configurations for each specific type of media gateway are described.

“ARP IP Targets for MX-ONE Service Node”, further described below, is recommendations on what to use as ARP IP Targets for the MX-ONE Service Node when installing the system. Maximum three ARP IP Targets are allowed to be configured. **It is recommended to define at least two ARP IP targets per server**.

If only one ARP IP target is specified and that target is unreachable communication will change back and forth between the interfaces. If this happens it will most likely lead to lost IP packets and fatal disturbances in the server communication.

Some of the configurations will introduce network loops. In these configurations some kind of Spanning Tree Protocol is needed to avoid broadcast storms.

### 3.2.3.1 MGU

**MGU configuration with active/backup, redundant solution**

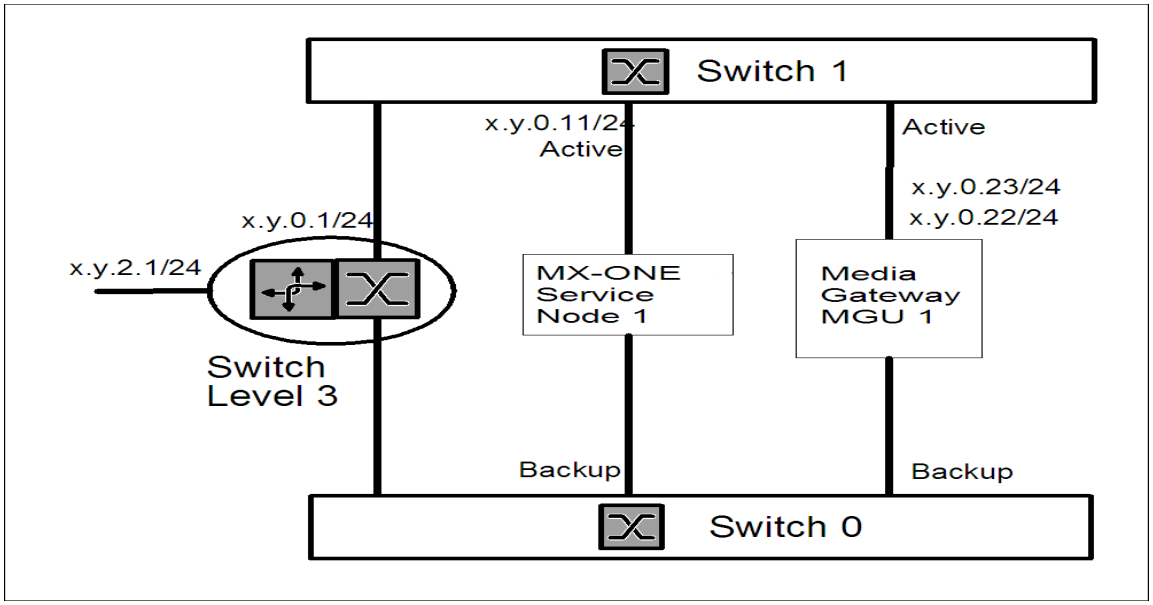


**Figure 13: MGU with Backup Switch**

This solution implements a link failover mechanism in the MGU. If the active link fails the backup link will take over.

ARP IP Targets for MX-ONE Service Node: Default gateway, MGU

Does not introduce any additional network loops.

**MGU configuration, non redundant coupling**

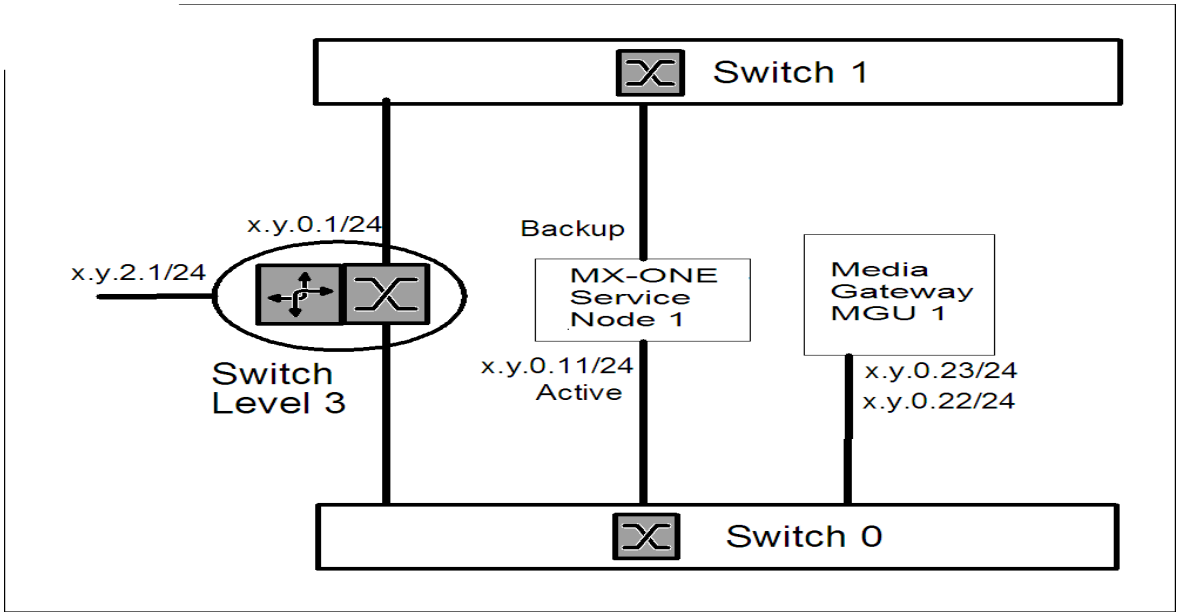


**Figure 14: MGU, Non-Redundant**

The MGU is configured to use one interface only (same as single network configuration). The MGU is coupled in a non redundant way. Media services are lost if a single point of failure occurs in the network to the media gateway.

Several media gateways could be spread between the switches. Hereby half of the media resources will survive a switch failure.

ARP IP Targets for MX-ONE Service Node: Default gateway, MGU

Does not introduce any additional network loops.

### 3.2.4 HOW TO CONFIGURE ETHERNET BONDING

Ethernet bonding can be configured at installation of the MX-ONE system or later in a running system.

See the installation instructions for ISTALLING AND CONFIGURING MIVOICE MX-ONE.

Configuring in a running system is performed via the Maintenance tool (opt/mxone_installl/bin/maintenance).

### 3.2.5 ETHERNET BONDING FAIL-OVER, HOW IT WORKS

Two Ethernet interfaces on the MX-ONE Service Node are aggregated to work together on Ethernet level. It is seen by the applications as one interface.

The type of Ethernet bonding used in MX-ONE is active/backup. Only one interface is active at a time. Nothing will be sent from the backup interface. Both interfaces will use the same MAC and IP address.

The active interface will supervise the defined ARP IP Targets, if connection is lost the communication will fail-over to the other interface. Ethernet frames could be lost in the time passing between the fault happens until the fault is discovered and the fail-over is ready. The missing frames are normally resent by the IP protocols used by the applications (SCTP and TCP).