Tested Solution: VCStack + Link Aggregation

Prior to the advent of the Virtual Chassis Stacking (VCStack) solution, high availability in enterprise networks was achieved by provisioning redundant links (with STP) and redundant routers (with VRRP). In normal operation, bandwidth and routing power would sit idle in the network.

Allied Telesis now provides a truly resilient network. In normal operation, all bandwidth and all routing power in the network are fully available for use all the time. If a link or device fails, some of the bandwidth or forwarding power will be lost, but the network will still be fully operational and all remaining resources will continue to be fully utilized.

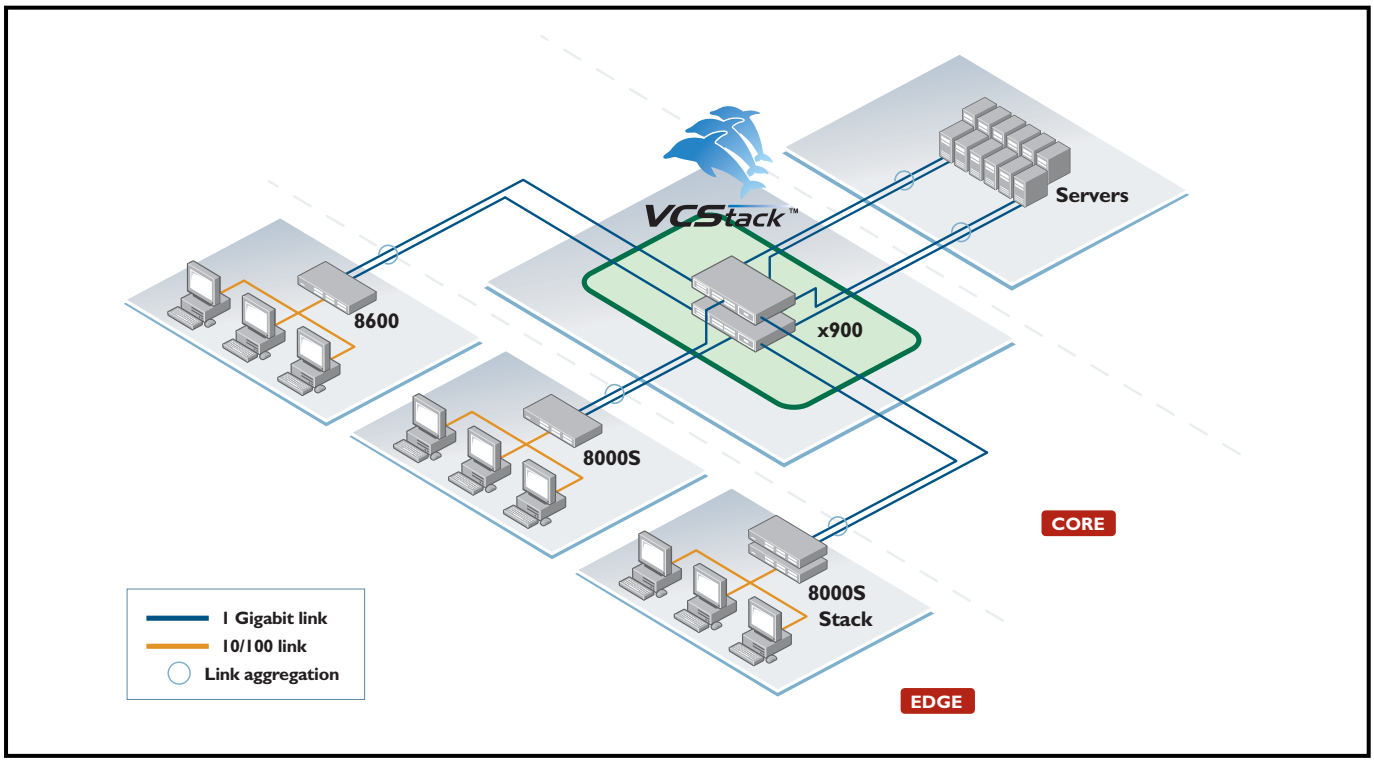


Diagram 1: VCStack + Link Aggregation

Key Benefits of the solution

Full bandwidth utilization and maximum availability

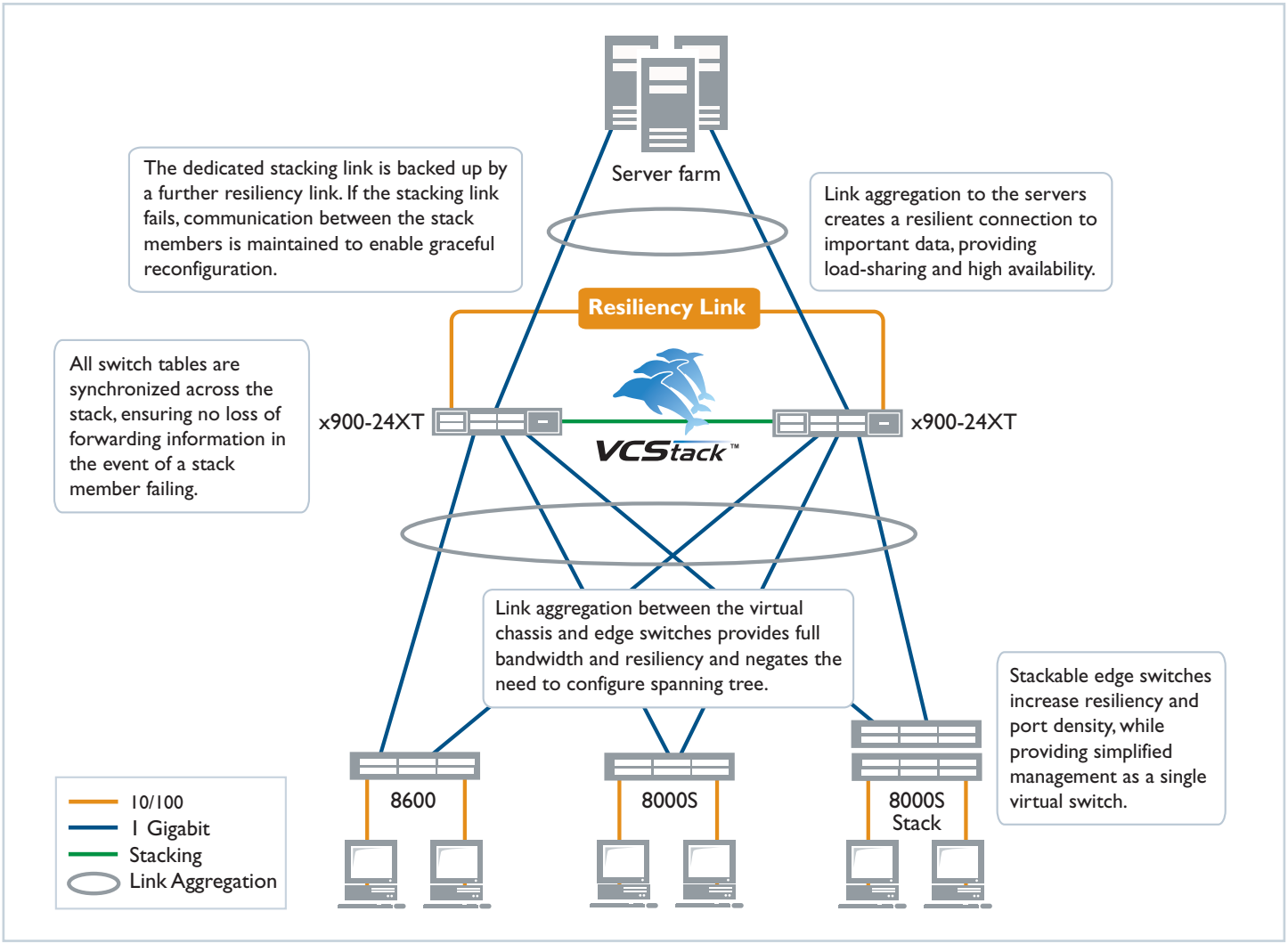
The key advantage comes from configuring the links from the edge to the core using 802.3ad link aggregation. This is possible because VCS supports link aggregation on ports across different virtual chassis members, providing:

- Full network bandwidth, as both ports are active; no links are blocked, as some would be with spanning tree.
- Minimal network disruption if a link fails. The process within a switch when an aggregated link fails is very simple and the virtual chassis almost instantly adapts its data forwarding on the loss of the link.

Customers benefits

Customer requirements met with the VCStack + Link Aggregation resiliency solution:

- A resilient solution without using Spanning Tree
- A simpler replacement for VRRP and/or other legacy redundancy protocols
- Simpler network management - the virtual chassis is managed as a single unit.



Allied Telesis Products

The following products support Virtual Chassis Stacking:

- SwitchBlade x908 advanced Layer 3 modular switch
- x900-12X and 24X series advanced Gigabit L3+ expandable switches

This solution utilizes the following products at the network edge:

- AT-8600 series Layer 3 Fast Ethernet switches
- AT-8000S series stackable Fast Ethernet edge switches

Please see "Resilient Networking with VCStack" for more information on Allied Telesis Virtual Chassis Stacking solution.
www.alliedtelesis.com/solutions

x900 Configuration

All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself

```
log buffered level errors
log host 192.168.10.11
log host 192.168.10.11 level debugging
```

Allow read-only SNMP monitoring from one management station

```
access-list 1 permit 192.168.10.13
snmp-server enable trap auth nsm
snmp-server community public ro 1
snmp-server host 192.168.10.13 version 2c public
```

A resiliency link backs up the dedicated stacking link. If the stacking link fails, communication is maintained to allow graceful reconfiguration

```
stack resiliencylink eth0
```

Use priority to pre-elect the VCStack master switch

```
stack 1 priority 1
```

Create VLANs. VLAN 169 for servers, and VLANs 170-172 for connectivity to edge switches

```
vlan database
 vlan 169-172 state enable
```

Create link aggregation groups across the VCStack members for resiliency. One for servers, and three for edge switches

```
interface port1.0.1
 switchport
 switchport mode access
 switchport access vlan 169
 static-channel-group 1

interface port2.0.1
 switchport
 switchport mode access
 switchport access vlan 169
 static-channel-group 1

interface port1.0.3
 switchport
 switchport mode access
 switchport access vlan 170
 static-channel-group 2

interface port2.0.3
 switchport
 switchport mode access
 switchport access vlan 170
 static-channel-group 2

interface port1.0.5
 switchport
 switchport mode access
 switchport access vlan 171
 static-channel-group 3
```

Create link aggregation groups across the VCStack members for resiliency. One for servers, and three for edge switches

```
interface port2.0.5
 switchport
 switchport mode access
 switchport access vlan 171
 static-channel-group 3

interface port1.0.7
 switchport
 switchport mode access
 switchport access vlan 172
 static-channel-group 4

interface port2.0.7
 switchport
 switchport mode access
 switchport access vlan 172
 static-channel-group 4
```

Assign an IP address to each VLAN. Configure DHCP relay to forward DHCP requests to the server

```
interface vlan169
 ip address 192.168.169.1/24

interface vlan170
 ip address 192.168.170.1/24
 ip dhcp-relay server-address 192.168.169.254

interface vlan171
 ip address 192.168.171.1/24
 ip dhcp-relay server-address 192.168.169.254

interface vlan172
 ip address 192.168.172.1/24
 ip dhcp-relay server-address 192.168.169.254
```

Configure a default route to external networks

```
ip route 0.0.0.0/0 192.168.169.254
```

Configure NTP (Network Time Protocol) with the IP address of the NTP server

```
ntp server 192.168.10.11

end
```

8600 Configuration

To enable secure HTTP management to use certificates, a distinguished name is required and system security must be enabled

```
set system distinguished="cn=switch1, o=alliedtelesis, c=nz"
enable system security
```

Storm control is configured to prevent downstream loops from affecting the inner layers of the network

```
set switch port=1-24 bclimit=3000 mclimit=3000 dlflimit=3000
```

By default, all ports are put into VLAN 171

```
create vlan="edge" vid=171
add vlan="171" port=1-26
```

Spanning tree needs to be disabled on the edge-facing ports, as it cannot co-exist with 802.1x authentication

```
enable stp="default"
set stp="default" mode=rapid
disable stp="default" port=1-24
```

The two gigabit ports are aggregated together to create a resilient link to the network core

```
create switch trunk=aggregation port=25-26 speed=1000m
```

802.1x authentication is enabled on all the client-facing ports. Clients cannot access the network without being authenticated

```
enable portauth=8021x
enable portauth=8021x port=1-24 type=authenticator
```

DHCP snooping guards against rogue server attacks, server exhaustion attacks, arp poisoning attacks and IP spoofing attacks. Any ARP poisoning attempt will be logged

```
enable dhcpsnooping
enable dhcpsnooping arpsecurity
enable dhcpsnooping log=arpsecurity
set dhcpsnooping port=25 trusted=yes
set dhcpsnooping port=26 trusted=yes
```

Attach a management IP address to VLAN171, and provide a default gateway address

```
enable ip
add ip int=vlan171 ip=192.168.171.34
add ip route=0.0.0.0 interface=vlan171 nexthop=192.168.171.1
```

The Radius server is used for authenticating management sessions and also for authenticating 802.1x clients.

```
add radius server=192.168.10.34 secret="testing123-2"
    port=1812 accport=1813
```

Management access is ONLY possible via the core-connected aggregated link. Access via insecure methods Telnet and HTTP are blocked

```
add switch l3filter match=dipaddress dclass=host
add switch l3filter=1 entry dipaddress=192.168.171.34
    action=deny
add switch l3filter match=none import=true
add switch l3filter=2 entry iport=26 action=nodrop
add switch l3filter=2 entry iport=25 action=nodrop

disable telnet server
```

Remote management sessions must use SSH and/or HTTPS

```
enable ssh server serverkey=1 hostkey=0 expirytime=1
    logintimeout=60
add pki certificate="cer_name" location=cer_name.cer trust=true
set http server security=on sslkey=2  port=443
```

All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself

```
create log output=1 destination=syslog server=192.168.10.11
    secure=yes message=20
add log output=1 filter=1 severity=>1
```

Allow read-only SNMP monitoring from one management station. Send traps to that same management station

```
enable snmp
enable snmp authenticate_trap
create snmp community=public
enable snmp community=public trap
add snmp community=public manager=192.168.10.13
add snmp community=public traphost=192.168.10.13
```

System time is provided from an NTP server

```
enable ntp
add ntp peer=192.168.10.3
```

8000S Configuration

Broadcast and multicast limiting prevent downstream loops from affecting the inner layers of the network

```
interface range ethernet 1/e(1-24),2/e(1-24)
port storm-control broadcast enable
port storm-control include-multicast
exit
```

The client-facing ports are configured as portfast so there is no delay in connectivity when client devices attach. Root guard protects against STP spoofing attacks

```
interface range ethernet 1/e(1-24),2/e(1-24)
spanning-tree portfast
spanning-tree guard root
exit
```

Port security guards against MAC spoofing attacks, and limits the ability for intruders to connect to the network

```
interface range ethernet 1/e(1-24),2/e(1-24)
port security mode max-addresses
port security max 3
port security discard trap 60
exit
```

By default, all ports are put into VLAN 170

```
vlan database
default-vlan vlan 170
exit
```

Two gigabit ports, one from each stack member, are aggregated together to create a resilient link to the network core

```
interface range ethernet 1/g1,2/g1
channel-group 1 mode on
exit
```

802.1x authentication is enabled on all the client-facing ports. Clients cannot access the network without being authenticated

```
dot1x system-auth-control
interface range ethernet 1/e(1-24),2/e(1-14)
dot1x single-host-violation discard trap 30
dot1x re-authentication
dot1x port-control auto
exit
```

DHCP snooping guards against rogue server and server exhaustion attacks

```
ip dhcp snooping
ip dhcp snooping vlan 170
interface port-channel 1
ip dhcp snooping trust
exit
```

Attach a management IP address to VLAN170, and provide a default gateway

```
interface vlan 170
ip address 192.168.170.45 255.255.0.0
exit
ip default-gateway 192.168.170.1
```

The Radius server is used for authenticating management sessions and also for authenticating 802.1x clients

```
radius-server host 192.168.10.34 auth-port 1812 acct-port 1813
key testing123-2
aaa authentication login default radius local
aaa authentication dot1x default radius
```

Management access is ONLY possible via the core-connected aggregated link. Access via insecure methods Telnet and HTTP are blocked

```
management access-list mlist
deny service telnet
deny service http
permit port-channel 1
exit
management access-class mlist
```

Remote management sessions must use SSH and/or HTTPS

```
ip ssh server
ip https server
```

All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself

```
logging 192.168.10.11
logging buffered errors
```

Allow read-only SNMP monitoring from one management station. Send traps to that same management station

```
snmp-server community public ro 192.168.10.13 view Default
snmp-server host 192.168.10.13 public traps 2
```

System time is provided from an SNTP server

```
sntp client enable vlan 170
clock source sntp
sntp unicast client enable
sntp server 192.168.10.3
```

The console port can auto-detect the terminal data rate

```
line console
autobaud
exit
```

About Allied Telesis

Allied Telesis is a world class leader in delivering IP/Ethernet network solutions to the global market place. We create innovative, standards-based IP networks that seamlessly connect you with voice, video and data services.

Enterprise customers can build complete end-to-end networking solutions through a single vendor, with core to edge technologies ranging from powerful 10 Gigabit Layer 3 switches right through to media converters.

Allied Telesis also offer a wide range of access, aggregation and backbone solutions for Service Providers. Our products range from industry leading media gateways which allow voice, video and data services to be delivered to the home and business, right through to high-end chassis-based platforms providing significant network infrastructure.

Allied Telesis' flexible service and support programs are tailored to meet a wide range of needs, and are designed to protect your Allied Telesis investment well into the future.

Visit us online at www.alliedtelesis.com.

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

© 2008 Allied Telesis Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners. 617-000170 Rev. L