

## Alcatel-Lucent's New Enterprise Class of High Availability

Enterprise networks must be highly available to support the latest business-critical applications and IP communications. They must be reliable and secure such that hardware failures cause no interruptions and intruders are prevented from accessing and harming the network.

In a converged environment that supports voice traffic and real-time data, this is especially important, since the network infrastructure must deliver the same or better availability as the public 911 safety network.

Alcatel-Lucent's approach to high availability is based on the premise that availability needs to be extended throughout the enterprise to ensure an easily managed and future proof infrastructure that provides uninterrupted flow of information to users and resources.

# Table of Contents

---

<b>1</b>	<b>Reasons and requirements for high availability</b>
1	Availability requirements
<b>2</b>	<b>Techniques for high availability</b>
2	Device techniques for high availability
3	Network topology techniques for high availability
3	Virtual Router Redundancy
4	Reliability
4	Measuring Availability
5	Hardware Requirements for High Availability
5	Chassis Management Modules
5	Network Interface Modules
5	Server Techniques for High Availability
5	Server Load Balancing and Redundancy
6	Smart Continuous Switching
6	Spanning Tree / Rapid Reconfiguration
6	OSPF Equal Cost Multi-Path
6	Network with link aggregation and SLB
6	Link Aggregation
7	Good network management improves availability
7	Security and Availability
7	Network Security
8	Firewall Clustering
<b>9</b>	<b>Relative cost of redundant configurations</b>
9	Improving availability with Alcatel-Lucent is a good value
9	Improving availability is insurance for applications
<b>10</b>	<b>Alcatel-Lucent Switching Platforms Deliver a New Enterprise Class of Availability</b>
10	Alcatel-Lucent OmniVista Network Management System
10	Alcatel-Lucent Access Guardian
11	Alcatel-Lucent OmniSwitch 9800 and OmniSwitch 9700 chassis
11	Resiliency – maximized network uptime
11	Alcatel-Lucent’s cost-effective server load balancing
12	Alcatel-Lucent OmniSwitch 6850 and 6850L chassis
12	Alcatel-Lucent OmniAccess Wireless LAN switching platforms
<b>12</b>	<b>Conclusion</b>
<b>13</b>	<b>Abbreviations</b>

## Reasons and requirements for high availability

---

The trend towards convergence of voice and data on a single network infrastructure while supporting business critical networking that could be life-saving applications, is gaining momentum, making it necessary for enterprise networks to deliver a new class of high availability.

In today's enterprise networks, downtime can be very expensive, with significant costs that need to be evaluated when designing a high-availability network. It can also be more than money that is lost; it can be customers, business transactions, even lives if the network supports a healthcare environment. The enterprise network infrastructure must deliver the same level of availability as the public safety network.

Every business has as its core objective or goal to provide the best possible products, customer service and support to the marketplace.

To accomplish this, businesses have invested in mission and business critical applications such as SAP, or Oracle, or some vertical specific application, which allows the company to provide paychecks to sales forecasts. In essence, the information needed to meet the business objectives.

To access this information, a network has been built that fosters collaboration and other productivity gains that happen when information is easily accessible and freely exchanged. This productivity gains have allowed the company to size itself to accomplish its business goals and objectives, but what happens if the fundamental building block of productivity – the network – is not reliable?

The inability to access information in a timely manner manifests in poor customer interactions and less than optimal support, which could be the deciding factor in continuing to conduct business with you. This means that the expense incurred for downtime is more than the cost or replacement equipment or the service call, it is also the potential in lost revenue and injured prestige and market persona.

***If users can't access mission-critical applications, the business is losing money.***

### **Availability requirements**

To achieve the highest possible availability, suitable operational processes must be in place for all facets of the network: hardware, software, applications, security, networking, server farms and backup systems. Network management and security must be designed to maintain availability, taking advantage of automated features to reduce human error, prevent problems and minimize the associated downtime.

Network availability must go beyond the devices and hardware redundancy. Availability must be built into the infrastructure and extend throughout the network links and paths to ensure that all computing resources, applications and services are readily available to users at all times. It requires good network management practices and implementation of security policies and practices to protect the network and the critical resources. To maximize interoperability across the enterprise, the network must also comply with industry standards to enable businesses to make full use of their investment in existing equipment and applications.

### **Device techniques for high availability**

For years, enterprise network equipment providers strived to deliver 99.999% availability which is the standard major telecommunications companies deliver. This type of reliability is desirable and it is expected when it comes to phone service. If enterprise networks are to support IP phones, they too must deliver similar availability.

For enterprise high availability, the design of the network is critical and many areas need to be addressed. At the device level, all system components, including the management processor and fabric, must be redundant, hot swappable and capable of failovers that are fast and transparent to users. There needs to be redundant:

- Secure, power sources (UPS)
- Hot-swappable hardware for each node
- Management module
- Network interface modules
- And switch fabric

Proper implementation of redundancy means that not only is there backup hardware and software, the fail-over when it happens must be “smooth” and imperceptible to the network user. Smooth failover, which is sometimes referred to as smart continuous switching, is a feature that must be built into every layer of the network.

The implementation must also make smart use of redundancy at each layer as well. Failure to do so makes smart continuous switching impossible.

The biggest challenge of all may be whether a vendor has built in affordable redundancy or whether it is an expensive add-on to the base system. Network equipment that has redundancy built into its design and is not an expensive add-on afterthought, will typically satisfy the requirements of smooth failovers and redundancy at every layer of the network.

## Network topology techniques for high availability

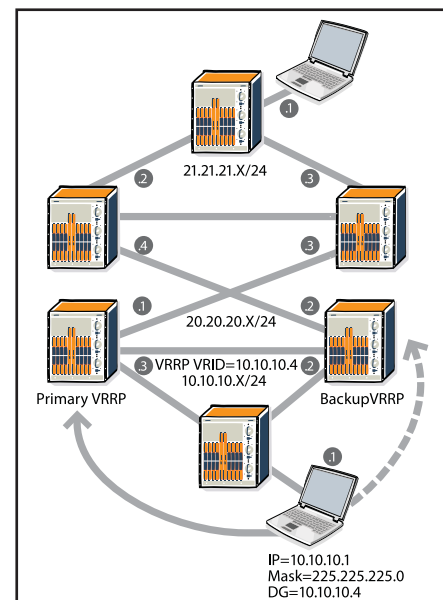
At the network level, there must be topological redundancy and resilience in the network links to ensure that no single point of failure exists. Multiple physical paths through the network need to exist that consist of interconnecting closets and core/aggregation networking devices. IEEE standards are used to promote efficient use of those links via dynamic link aggregation control protocol and per VLAN spanning tree protocol. Then, technologies such as rapid spanning tree and equal cost multi-path routing are used to quickly detect and divert traffic when failures occur. Lastly, virtual router redundancy protocol (VRRP) is used to provide automatic backup for critical routers and gateways.

### VIRTUAL ROUTER REDUNDANCY

The Virtual Router Redundancy Protocol (VRRP) is a standard protocol that provides topological redundancy and resilience by eliminating the single point of failure inherent in static route environments. VRRP dynamically assigns the responsibility for a virtual router to a physical router, allowing several routers within a network to use the same virtual IP address, which is referred to as the Virtual Router IDentification (VRID).

If the physical router becomes unavailable, the highest priority backup router switches over to the master state. As shown in Figure 1, a VRRP router is a physical router, such as an OmniSwitch 9000. Both gateway switches are configured for VRRP functionality. The client sets gateways to the Virtual Router IDentification (VRID) and forwards all packets to that IP address. In the case of an active failure, the backup VRRP switch will immediately begin forwarding packets as the active VRRP switch.

Figure 1: Virtual Router Redundancy



The implementation of VRRP provides node redundancy for packets exiting a broadcast domain without the need to configure dynamic routing or router discovery protocols. Alcatel-Lucent's implementation can also load share traffic when both routers are running.

A hot swapping capability is required for adding, removing or replacing a component while the switch is operating. Load sharing allows multiple components to run at the same time, with the intelligence to determine which components are available and algorithms that determine how the load is to be shared. So, how is 99.999% availability measured and what does it really reflect?

## RELIABILITY

Reliability can also be enhanced by adding components in parallel. As an example, if one component has an availability of 99% and the aim is to achieve 99.999%, two redundant components need to be added so that there are three operating in parallel. Serial or sequential components, such as cabling or network links where only one is operating at a time, are different as adding further serial components actually decreases reliability. For example, if three components each with a 99% reliability are connected in series, the reliability is reduced as the failure of one component will impact the other two. To increase the reliability of serial components, redundancy or parallel paths need to be deployed.

## MEASURING AVAILABILITY

While the terms availability and reliability are often used interchangeably, it is important to note that availability is usually defined as network uptime and the ability of a network to deliver continuous operation without interruption to users. Reliability is a part of availability; it is a measurement based on the life expectancy or failure rate of the components. There are two parts to the measurement of availability: the Mean Time Between Failures (MTBF) and the Mean Time To Repair (MTTR). The equation to measure availability is as follows:

$$MTBF = (.9xxx) MTBF + MTTR$$

MTBF refers to reliability and the average time between failures. As the reliability of a component usually decreases over time, replacing components before it is anticipated that they will fail can improve this metric and the overall availability. MTTR is the average time needed to repair (or restore) the system and bring it back into service or operation. In the case of redundant configurations, this includes how quickly failovers, hot swapping and other fault tolerance mechanisms operate in order to minimize any disruption to operation.

### **99.999% Availability**

*The goal of networks that support voice is 99.999% availability, which equals about five minutes of downtime per year, or just under one second per day. Typically, this measurement does not include any "planned downtime" for scheduled maintenance and system upgrades. Surprisingly, in the voice world, 99.999% only applies to a few components in the Private Branch Exchange (PBX); it does not extend to the phones or user devices.*

*For example, availability in a PBX typically applies only to the central processor, power supplies and switch matrix; it does not usually include the line cards, electrical power supply, software, operating system or planned downtime (maintenance, upgrades, fixes). The most common way to increase reliability is to introduce redundancy, which involves a cost trade-off. This generally means having redundant components running in parallel, for example, "hot standby" components.*

## Hardware requirements for high availability

### CHASSIS MANAGEMENT MODULES

Chassis Management Modules (CMM) are the management / supervisory modules that are critical to the entire operation of the switch. They are typically designed to run in redundant configurations with one CMM having the primary role and the other a secondary role. The primary manages the current switch operations, while the secondary runs in parallel, serving as a "hot standby". In the event of a failure, the secondary CMM takes over. What is critical to availability is how fast this failover occurs. With an intelligent design, the CMMs are synchronized at all times, and smart continuous switching is used to ensure that there is no interruption to users or to the flow of data.

### NETWORK INTERFACE MODULES

Network interface (NI) modules are the interface cards that provide the connectivity for ports and switching intelligence through local forwarding tables, local spanning tree, and local intelligence.

The NI modules are incorporated with additional technologies, including IEEE 802.3ad dynamic link aggregation, server load balancing and IEEE 802.1w rapid reconfiguration, to provide a fail-safe, scalable and flexible environment. These technologies may be combined to maximize throughput and availability for mission-critical applications and server farms. Not only is this a performance advantage, distributed forwarding means continuous forwarding during a CMM failover.

For some vendors, this is an option that requires additional money. To contain costs, look for a vendor that offers distributed forwarding as part of the design and is built-in to the equipment.

## Server techniques for high availability

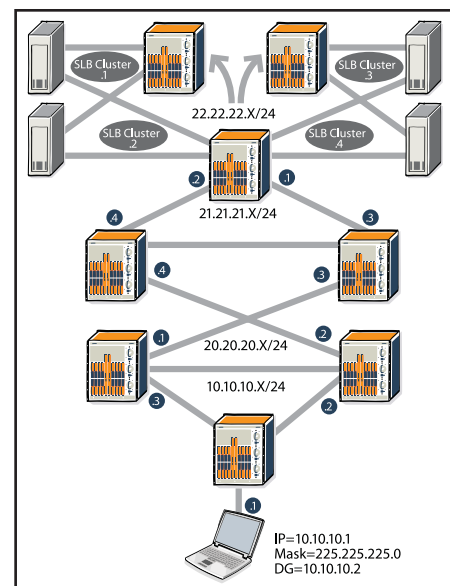
### SERVER LOAD BALANCING AND REDUNDANCY

The IT infrastructure combines servers running Windows, UNIX, Linux, grid computing applications, as well as data center appliances. The infrastructure also includes application front ends, SSLs, VPNs, and firewalls. To successfully provide server load balancing, a standards-based approach is required so that users can combine the various servers and operating systems with the various devices and appliances.

Server load balancing is a technique that achieves the goals of high availability and increased performance by promoting multiple paths to business critical servers, and supporting one virtual IP address for multiple servers.

Server load balancing with fully redundant servers, dual homing (use of two redundant connections), clustering and backup servers are all recommended so that applications and information are always accessible. Redundant servers must have identical content so that there is no loss of mission critical data or information. Figure 2 shows an example of a typical server load balancing configuration. Critical servers are dual homed and clustered for node and link redundancy to provide maximum performance and throughput as well as high availability.

Figure 2: Server Load Balancing (SLB)



## SMART CONTINUOUS SWITCHING

In the case of smart continuous switching, all source learning, spanning tree functions and established routes are distributed throughout the network interface modules instead of using a central engine. In the event of a management module failure, the system automatically switches over to the hot standby with no loss of connections or switch fabric capacity. Established layer-2/ layer-3 traffic, including voice conversations, continues without interruption. Furthermore, smart continuous switching enables new connections to be made, ensuring that all users have access to network resources – an industry first for the enterprise.

## SPANNING TREE/RAPID RECONFIGURATION

The Spanning Tree algorithm and Protocol (STP) is a self-configuring algorithm that provides data path redundancy, while ensuring there is only one data path between any two switches. The STP allows IEEE 802.1Q tagged ports and link aggregate logical ports to participate in the calculation of the STP topology. Multiple paths can be provided between two or more switches, but only one path can be active at any one time. The remaining paths are placed in a “blocking” mode. If a primary path fails, an alternative data path is brought out of the blocking mode into a forwarding state, thereby re-establishing the connection between switches. The transition takes between 30 and 50 seconds for the IEEE 802.1d STP.

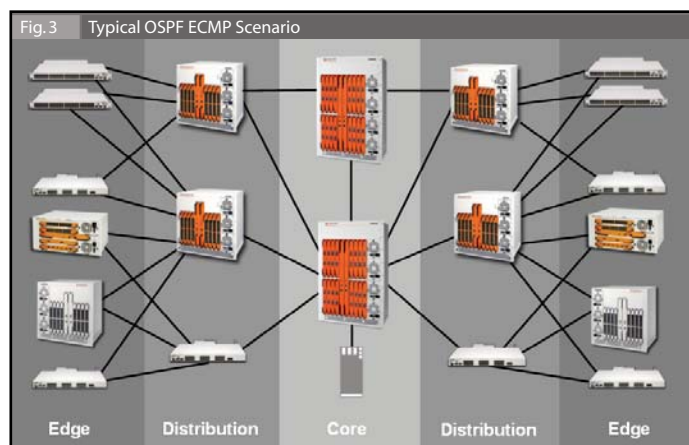
## OSPF EQUAL COST MULTI-PATH

The Open Shortest Path First Equal Cost Multi-Path (OSPF ECMP) routing technique is implemented for routing packets along multiple paths in a load sharing configuration. The cost is a value or metric assigned to a path; it is typically based on the number of routing hops, distance or link speed to a specific destination. In Alcatel-Lucent switches, the forwarding engine identifies the available paths and the next hop by using OSPF ECMP and the equal cost metrics that have been established for a specific destination.

## NETWORK WITH LINK AGGREGATION AND SLB

Figure 3 shows a typical OSPF ECMP scenario. Nodes with equal cost paths have the ability to load share their traffic across multiple paths using round robin, which can enhance performance in addition to providing redundancy in the event of a network path or device failure.

Figure 3: Typical OSPF ECMP Scenario



## LINK AGGREGATION

Dynamic link aggregation provides redundancy with a resilient uplink capability, allowing multiple virtual links to be established between two switches. If one link in an aggregate fails, all traffic is routed through the remaining links in that aggregate. Dynamic aggregate groups can be created using the standard IEEE 802.3ad Link Aggregation Control Protocol (LACP) for standardized dynamic link aggregation in multi-vendor environments. Alcatel-Lucent also supports static link aggregation using OmniChannel, a technology designed specifically for linking Alcatel-Lucent legacy enterprise products. Dynamic aggregate groups can be created between an OmniSwitch 9000 and another vendor’s switch if that vendor supports the LACP standard. Link aggregation can be made more resilient by utilizing multiple GNI or ENI modules to guarantee maximum availability in the event of a link or interface failure.

## **Good network management improves availability**

Up to this point the discussion has focused on the role hardware plays in ensuring network availability. However, a smart network management system is also required to ensure the network stays available. Supporting this is a recent study by a leading analyst group that revealed that up to 80% of network outages are caused by human or process error such as mis-configuration of devices. To minimize accidental mis-configuration or process errors in network management, several steps need to be taken.

First, the tasks need to be compartmentalized by allowing access only to commands necessary for their function and limiting “exploring and playing.” Next complex tasks, such as QoS polices, can be automated via tools such as the Alcatel-Lucent OneTouch network management tool, which enabled, automatically identifies high priority traffic – data or voice – and configures the switches from the edge to the core to adopt an enforce high priority polices. Lastly, leveraging the network management system again to identify change time windows and then roll-out software upgrades to the network devices during off hours.

## **Security and availability**

### **NETWORK SECURITY**

Securing the network is absolutely essential if a network is to be highly available. Network security has to be built into the hardware as well as into the network management system. The network management system software must be able to provide security that works with the built-in security features of the hardware. By preventing intrusions or identifying and isolating high-risk intruders before they gain access to the network, the network users are assured of non-stop network availability because of a threat-free environment.

Network devices are protected by using strong management techniques and by demanding encrypted communications to the switch and external authentication servers. Control of who passes traffic through the switch is from using industry standard 802.1x, access control lists (ACLs), dynamic VLAN segmentation which promotes “hands-off” mobility, and by automatically containing network attacks with the OmniVista Quarantine Manger, which is discussed further at the end of this paper.

Lastly, crippling attacks from denial of service can render a switch unmanageable. To address this, a platform is required that automatically identifies the type of attack and immediately reacts and contains it.

By addressing network infrastructure security via communications to, through, and of the switch, greater availability will be possible.

## FIREWALL CLUSTERING

Firewalls are also important tools for securing the network from outside intruders. They must be configured for high availability to ensure that all traffic is properly handled and securely managed. While server load balancing can help balance traffic at layers 3 and 4, firewalls operate at the Medium Access Control (MAC) layer so special clustering mechanisms are needed. On a Firewall cluster, the switch is no longer supposed to 'load-balance' the incoming traffic per say, instead, it is supposed to deliver a copy of every incoming packet to every Firewall part of the cluster. Therefore, Firewall clustering technology provides automatic failover within a firewall cluster, eliminating a possible single point of network failure and ensuring that mission- critical Internet / intranet connections are secure and available.

Figure 4: High availability security network

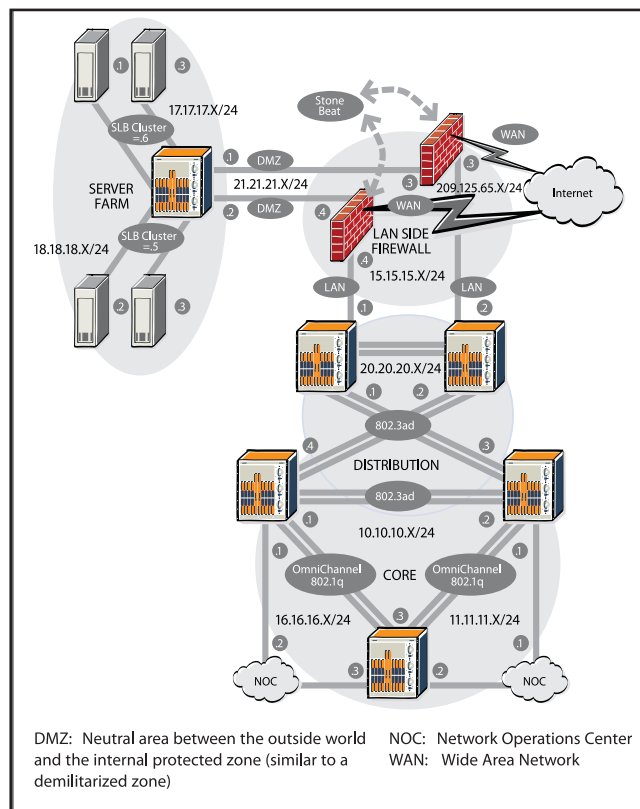


Figure 4 is an example of a high availability security solution. A multilayer hierarchical design ensures the optimal placement of security technologies within a high availability network solution.

## Relative cost of redundant configurations

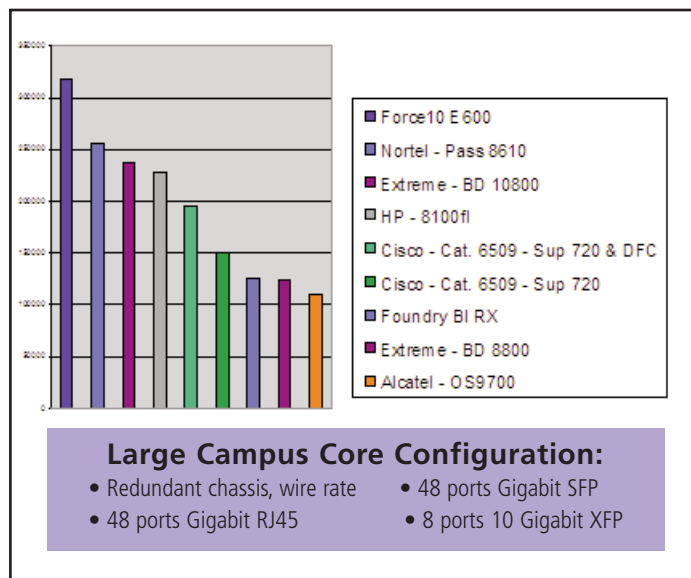
High availability is a requirement in today's converged enterprise environment. With Alcatel-Lucent solutions, it doesn't have to be an expensive proposition.

### Improving availability with Alcatel-Lucent is a good value

Alcatel-Lucent has industry leading technologies that promote and ensure high availability via standards-based techniques, clever engineering and architecture. We've distributed the intelligence to the network interfaces modules, allowing these modules to perform supervisory, routing and switching functions in the network interface (NI) itself, where a failure does not affect the entire switch, just the devices attached to the module. And, Alcatel-Lucent has designed these components to be hot swappable that can be replaced on the fly.

If there is a management module failure, Alcatel-Lucent switches can still learn new routes and forward traffic, which is something Alcatel-Lucent calls Smart Continuous Switching. This is where Alcatel-Lucent switches revert back to the last known good configuration by simply rebooting them, rather than rolling a truck or flying staff to the remote location to restore the switch.

Figure 5: Alcatel-Lucent is the best large campus core value



Alcatel-Lucent has cost optimized its products to provide redundancy bundles which are much less expensive than the competition. See Figure 5 below. The delta for adding high availability to Alcatel-Lucent networking products is a 6% premium versus 28% for Extreme and over 40% for Cisco. As is evident from this chart, no matter what your configuration, Alcatel-Lucent has pricing which STARTS lower than then competition while still maintaining the complex feature sets the enterprise demands to support all IP communications, including voice and video.

### Improving availability is insurance for applications

Alcatel-Lucent is the best value for high availability networks. Alcatel-Lucent provides all of the methods discussed above to improve network reliability and availability: via device, network, server, management and security techniques. It is all combined into a cost effective package ensuring productivity and business growth for your company.

## Alcatel-Lucent switching platforms deliver a new enterprise class of availability

Alcatel-Lucent has taken the lead in delivering the new Enterprise Class of network availability. The Alcatel-Lucent OmniSwitch 9000s, OmniSwitch 6850s, and OmniAccess Wireless LAN switches incorporate a wide range of features, such as smart continuous switching, wire-speed performance, native server load balancing and firewall clustering, all of which are crucial aspects of availability as they help ensure that mission-critical applications and network security are “always on.”

These switches are part of Alcatel-Lucent’s end-to-end enterprise switch family that includes core switches, stackable / modular closet switches, and wireless LAN (WLAN) switches that use the Alcatel-Lucent Operating System (AOS) for security, simplified OneTouch manageability, high availability, and reduced total cost of ownership. Combined with Alcatel-Lucent’s OmniVista Network Management System, high availability of the network is ensured through its security features that offer enhanced intrusion control and remediation.

### **Alcatel-Lucent OmniVista Network Management System**

Alcatel-Lucent OmniVista NMS extends automated intrusion control to the Alcatel-Lucent Omni product family for LAN and wireless LAN infrastructures, as well as basic intrusion control to third party LAN switches. Alcatel-Lucent OmniVista provides fast and simple ways to limit the damage from IP-security breaches and is unique in the industry in that it provides an active, intrusion control response for an all Alcatel-Lucent or multi-vendor enterprise network.

The Alcatel-Lucent OmniVista 2770 Quarantine Manager application protects the network from attacks at the network and application levels by isolating misbehaving users and providing a means for user remediation. Coupled with the strong security features of the Alcatel-Lucent OmniSwitch, these features protect the network from attacks and significantly reduce potential network downtime.

### **Alcatel-Lucent Access Guardian**

Another part of the Alcatel-Lucent security solution that ensures availability is the Alcatel-Lucent Access Guardian, which enables enforcement of device and network security policies. This results in increased privacy and availability of business communications.

Access Guardian authenticates the network users including employees, contractors and guests, confirms their PC’s conformance to security policies, and then provides access rights based on the user’s role. With Alcatel-Lucent’s Access Guardian, the network is able to prevent virus and worm attacks, ensure performance, protect IP telephony devices from any vendor and provide network services to all authorized users. All while protecting the privacy and availability of your business’ communications.

## **Alcatel-Lucent OmniSwitch 9800 and OmniSwitch 9700 chassis**

The OmniSwitch 9800/9700s carry on Alcatel-Lucent's tradition of providing the highest availability possible to support the demands of IP communications and mission-critical applications. Even when a management module (CMM) fails, all existing L2/L3 traffic, including voice conversations, will continue seamlessly without interruption. Plus the OmniSwitch 9700/9800s are capable of creating new connections during this failover.

Alcatel-Lucent's powerhouse OmniSwitch 9000 family delivers future-proof solutions with advanced security and QoS features for use in small-to-large enterprise cores, in the aggregation layer and in wiring closets with flexible power-over-Ethernet support. They deliver wire-rate processing for IPv4/IPv6 and support for unicast and multicast applications such as voice-over-IP and video collaboration.

The switches are capable of supporting future requirements at the network's edge while Gigabit Ethernet to the desktop becomes commonplace and demand for power-over-Ethernet (PoE) capability increases. These switches deliver high availability through a secure network management solution, redundancy, support of smart continuous switching, and server load balancing.

The OmniSwitch 9000s provide multi-layer security with a vast arsenal of security features that can be implemented at the edge, the core, and throughout the network. These include:

- User authentication (802.1x, web-based, telnet-based)
- Virtual local area networks (VLANs)
- Quarantine VLANs
- Access control lists (ACLs)
- Authenticated switch access (Local database, RADIUS, TACACS+, LDAP & ACE)
- Encryption for secure management (SSH / HTTPS / SNMP v3)
- Denial of service protection and notification (for OmniVista Quarantine manager application)

### **RESILIENCY - MAXIMIZED NETWORK UPTIME**

Network resiliency is critical to providing network availability. The OmniSwitch 9800s/9700s offer a superior architecture with no single point of failure in its redundant configuration. All of the OmniSwitch 9000s offer redundant PSU and fans, distributed processing, wide support of open, advanced routing redundancy protocols, load sharing, and mechanisms for fast reconfiguration of links between switches, servers, and other network devices.

### **ALCATEL-LUCENT'S COST-EFFECTIVE SERVER LOAD BALANCING**

Alcatel-Lucent leverages a standards based approach to high availability allowing its customer to combine servers with multiple operating systems with best of breed data center appliances and IP networks to create an end-to-end high availability data center.

With an Alcatel-Lucent solution, layer-3/layer-4 server load balancing is part of the switch operating system - a feature that some vendors charge thousands of dollars. Leveraging OSPF and equal cost multi-path routing ensures robust communications to server clusters. With Alcatel-Lucent's unique implementation of high availability VLANs, traffic destined for the servers can be configured to automatically be sent to multiple switch ports, promoting traffic delivery.

The OmniSwitch 9000 server load balancing implementation provides wire-speed, server load balancing as a native part of the switch architecture. This switch-based server load balancing offers several advantages. It works across all the network interface modules, is wire speed across the switch, does not require the purchase and configuration of an additional device or module, and allows any mix of network interfaces to be used.

## Alcatel-Lucent OmniSwitch 6850 and 6850L chassis

The OmniSwitch 6850 family, which includes the software upgradeable OmniSwitch 6850L series of switches, addresses the needs of modern enterprise and triple-play networking with: high availability; a flexible, stackable configuration; power-over-Ethernet; first-packet wire-speed performance; and fast network response time. All of the models in the family are stackable and perform wire-rate layer-2 switching and layer-3 routing for both IPv4 and IPv6 with optimal quality of service (QoS) for mission critical applications.

Similar to the existing Alcatel-Lucent OmniSwitch, the OmniSwitch 6850 series uses the Alcatel-Lucent Operating System (AOS), ensuring an easy and economical way to upgrade or deploy a new Ethernet network.

As with all Alcatel-Lucent OmniSwitch, the OS6850 family provides the same capabilities as the OmniSwitch 9000s that ensure high availability.

## Alcatel-Lucent OmniAccess Wireless LAN switching platforms

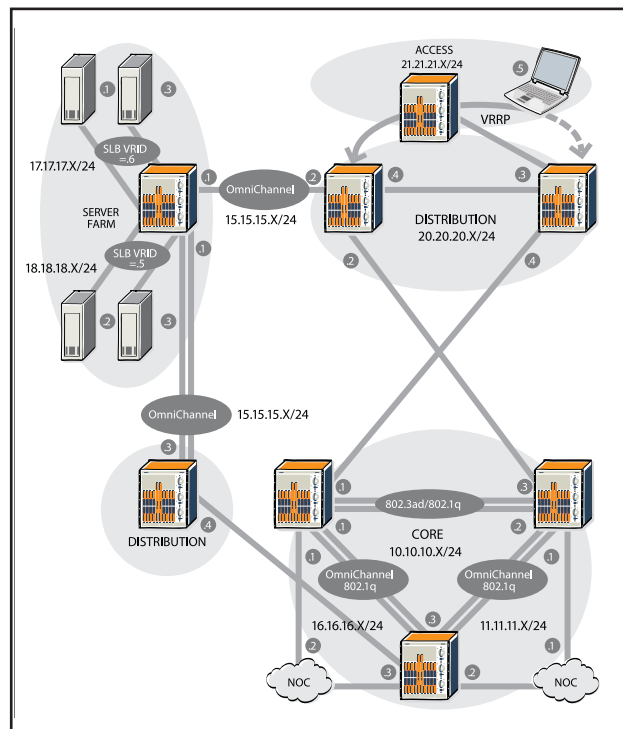
Alcatel-Lucent OmniAccess WLAN switch product family includes the industry's most comprehensive line of modular and non-modular systems - each specifically designed for enterprise campus, building, and branch office environments. All OmniAccess switches were designed to provide the availability businesses and organizations demand and expect of their enterprise network.

## Conclusion

There are many factors and considerations involved in designing a network. Figure 6 shows a typical high availability enterprise network that incorporates many of these features, including server load balancing for mission critical application servers and link aggregation using IEEE 802.3ad and link aggregation to maximize network level availability. With the increasing importance of enterprise networks carrying voice and real-time applications, there is a need to deliver carrier-class availability.

The Alcatel-Lucent approach to achieving high availability in the enterprise is to extend the principles of availability beyond individual devices to the entire network. Alcatel-Lucent's OmniSwitch 9000s, OmniSwitch 6850s, and OmniAccess WLAN switching platforms support IP communications and mission-critical applications, as well as enabling a new enterprise class of availability.

Figure 6: High availability enterprise network



## Abbreviations

---

<b>CMM</b>	chassis management modules
<b>DMZ</b>	Neutral area between the outside world and the internal protected zone (similar to a demilitarized zone)
<b>eMAN</b>	Ethernet metropolitan area network
<b>eMAN</b>	Ethernet-based MANs
<b>ECMP</b>	equal cost multipath
<b>ENI</b>	Ethernet network interface (card)
<b>NI GNI</b>	network interface Gigabit Ethernet interface
<b>NI IP</b>	network interface - Internet Protocol
<b>LACP</b>	Link Aggregation Control Protocol
<b>MAC</b>	Medium Access Control
<b>MTBF</b>	mean time between failures
<b>MTTR</b>	mean time to repair
<b>NEBS</b>	new equipment building system
<b>NI</b>	network interface
<b>NOC</b>	network operations center
<b>OSPF</b>	Open Shortest Path First
<b>PBX</b>	private branch exchange
<b>QoS</b>	quality of service
<b>RRP</b>	Rapid Reconfiguration Protocol
<b>SDH</b>	synchronous digital hierarchy
<b>SLB</b>	server load balancing
<b>SONET</b>	synchronous optical network
<b>SSL</b>	secure sockets layer
<b>STP</b>	Spanning Tree Protocol
<b>VLAN</b>	virtual local area network
<b>VRID</b>	virtual router identification
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>WAN</b>	wide area network

**[www.alcatel-lucent.com](http://www.alcatel-lucent.com)**

Alcatel, Lucent, Alcatel-Lucent and Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.  
© 2007 Alcatel-Lucent. All rights reserved. 031913-00 Rev C 8/07

