



BlueCat Helps Cologne Bonn Airport Redesign its Network Architecture to Improve IPAM, Gain Visibility and Streamline Processes



ORGANIZATION

Cologne Bonn Airport

INDUSTRY

Transportation

PRODUCTS

BlueCat IPAM

BlueCat DNS/DHCP Core Services

BlueCat Threat Protection

RESULTS

Centralized IP address management

End-to-end network visibility

Multiple security layers

Scalability to accommodate growth

THE CUSTOMER

Cologne Bonn Airport is one of the largest commercial airports in Germany. With approximately 9.45 million passengers per year, it is the seventh largest passenger airport, the third largest cargo facility, and one of the only 24-hour airports in the country. It is a hub for the passenger airlines, Eurowings and Germanwings, and also for the cargo airlines, FedEx Express and UPS Airlines. The airport is used by the German Aerospace Center and European Astronaut Center space agencies to train astronauts for space travel. With two terminals, the airport offers 53 shops, bars, and restaurants, as well as three multi-story parking garages. More than 13,000 people are employed at the airport, and an additional 26,000 jobs in the region are dependent on the airport.

THE CHALLENGE

With passengers arriving and departing at a rapid pace as well as flight, maintenance, and ground crews working harder than ever to get planes off the ground on time, airports are bustling with activity. Add in heightened travel-related security concerns, a robust cargo operation and astronaut training, and you've got a very complex environment at Cologne Bonn Airport.

While the airport's home-grown network served it well for many years, growth outpaced the network's capabilities. The boom in Wifi connectivity from personal mobile devices in recent years and greater use of IP-enabled devices, such as security cameras, have dramatically increased network demand. In addition, the airport added many IP-based services to improve the customer experience. With multiple DNS zones, differing technologies, and a segregated network access team, Cologne Bonn Airport didn't have a standardized network configuration or centralized visibility.

“We are in a really good place. Our network is much more stable and secure. We have visibility to see the entire network that we didn’t have before. Overall, the BlueCat solution has been a great value for Cologne Bonn Airport.”

– Frank Tautschnig,
System Engineer Network,
Cologne Bonn Airport

Since the airport had been working with Axians, a German technology company, to purchase devices and other network services, the airport’s network team turned to them for guidance on the project. Axians recommended BlueCat because it offered centralized network management capabilities. With large projects of this nature, the network team also had to evaluate the other major competitors in the networking space—Infoblox and VitalQIP.

Initially, the project scope was limited to creating a centralized IP database, to consolidate the various spreadsheets and tracking methods used by each of the five DNS zone management teams, as well as managing the overall Windows Active Directory authentication environment.

As the airport considered its options, the project grew in scope to a major network redesign effort. Infoblox wasn’t a fit for the large-scale project and QIP’s per-IP address pricing model proved to be too costly. “The pricing didn’t work for us because we had to pay for every single IP address. BlueCat offered a much more cost effective solution,” said Sascha Günther, System Engineer Network at Cologne Bonn Airport.

THE SOLUTION

BlueCat and Axians quickly got to work to tackle the project with a focus on centralized management and bullet-proof security. BlueCat recommended that the network be divided into four areas—one for standard applications and devices, a second area for network services, a third area for all of the IP-based security cameras, and finally a separate zone for the three parking garages and all of the automated IP-based functionality, like exit gates and payment machines. To provide maximum security, BlueCat isolated each area with an internal DMZ using a caching DNS layer to resolve internal IP addresses. The solution architects also recommended a completely separate external DMZ as an added security layer.

Once the infrastructure was in place, the BlueCat project team conducted a data cleaning and migration effort that took just three days. The team had one day to cleanse the data, identify overlapping DNS data, and determine where the data should be located in the new network design. The team also transformed some key spreadsheets into the meta data of the new IP database and redesigned the DNS/DHCP architecture. At the appropriate time, the BlueCat project team successfully migrated all of the data at once. After the data cut over, the airport’s IT team began moving existing machines and services to the new BlueCat architecture and will continue the migration as long as necessary.

The airport is still using Active Directory for system-wide user authentication and, in an effort to streamline its organization, the separate Active Directory team, which granted network access rights, became a part of the larger network team.

Once the new DDI solution was in place, the account team demonstrated BlueCat Threat Protection, a DNS firewall that is installed on the caching layer to help identify malicious activity before it can penetrate the network. According to Günther, “In just 10-15 minutes of the demonstration, we had more than 200 hits on the threat protection report. That was pretty eye-opening.”

VALUE/RESULTS

With the network redesign, the airport created a centralized IP address database across the entire IT department, which eliminated the overlapping DNS data and streamlined IP address management. Previously, if a network administrator needed to change a DNS, he or she had to talk to at least two different administrators to make the change. "Our disjointed, manual process was very time consuming," said Frank Tautschnig, System Engineer Network, Cologne Bonn Airport. "Now, we've streamlined our process, and we have visibility to see changes from all of the area network administrators. The entire team is immediately aware of any changes across the network."

Also, the different administrative teams would sometimes differ in opinion about how to manage network services. Now, a central network team is responsible for all DNS services, and the Linux and Windows teams rely on the network team for DNS changes. This new organizational structure has simplified the process and eliminated any conflicts between the different technology groups.

The network redesign also provided a much more secure infrastructure with the four different areas, the internal DMZs, and the external DMZ. The multiple security layers and BlueCat Threat Protection give Cologne Bonn Airport an extremely high security posture.

Productivity has improved for the entire network team since processes are automated. According to Tautschnig, "It used to take an hour to search for a client name and DHCP address. Now, we can look in one central database to find valid address information to deploy new devices."

Previously, the airport didn't have granular access rights to delegate daily network tasks. Instead, the network team hardly granted any access rights because of the risk that an employee could unintentionally take down the entire network. Now with the BlueCat DDI solution, network administrators can easily assign access rights based on the network zone and delegate daily tasks—without the risk of a catastrophic system failure. In addition, the BlueCat solution keeps a record of access rights and configuration changes to quickly troubleshoot, pinpoint and resolve issues.

The airport is well positioned for growth with BlueCat's highly scalable system architecture. Since the management layer is separate from the services layer, the network team can add new appliances and IP addresses as required to meet its needs. Tautschnig comments, "We have flexibility. We can add boxes without changing our network management. If we need to add a large group of IP addresses, we can easily do that without any issues or redesign."