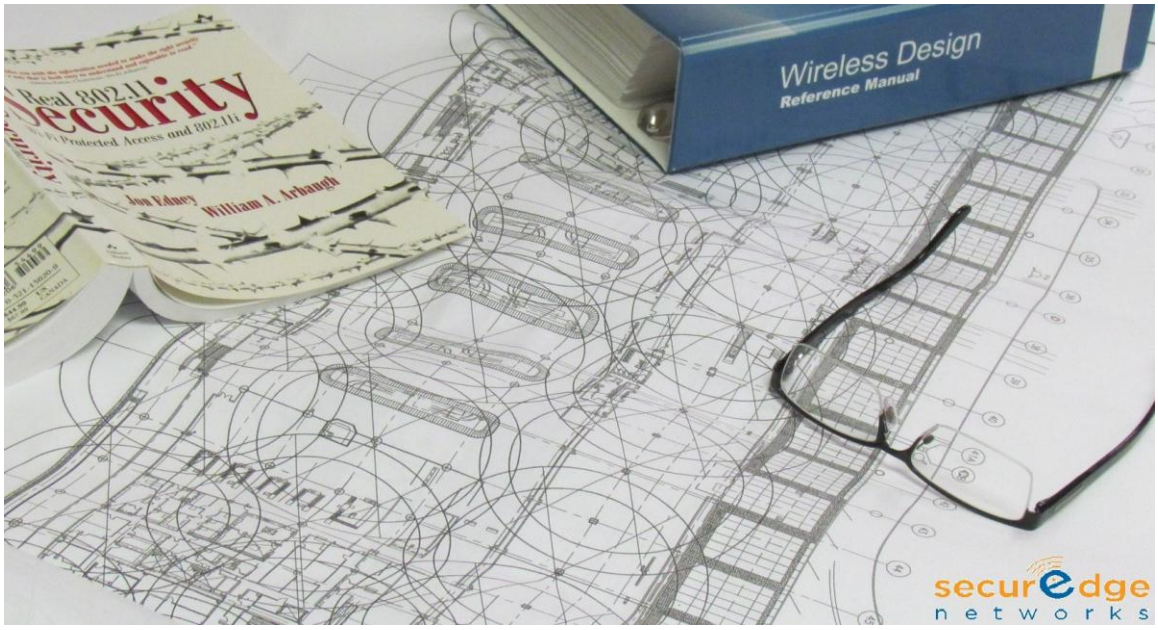
ENTERPRISE WIRELESS NETWORK DESIGN GUIDE



WHAT YOU NEED TO KNOW BEFORE YOU DEPLOY A HIGH CAPACITY, SECURE WIRELESS NETWORK

Table of Contents

1. Overview:

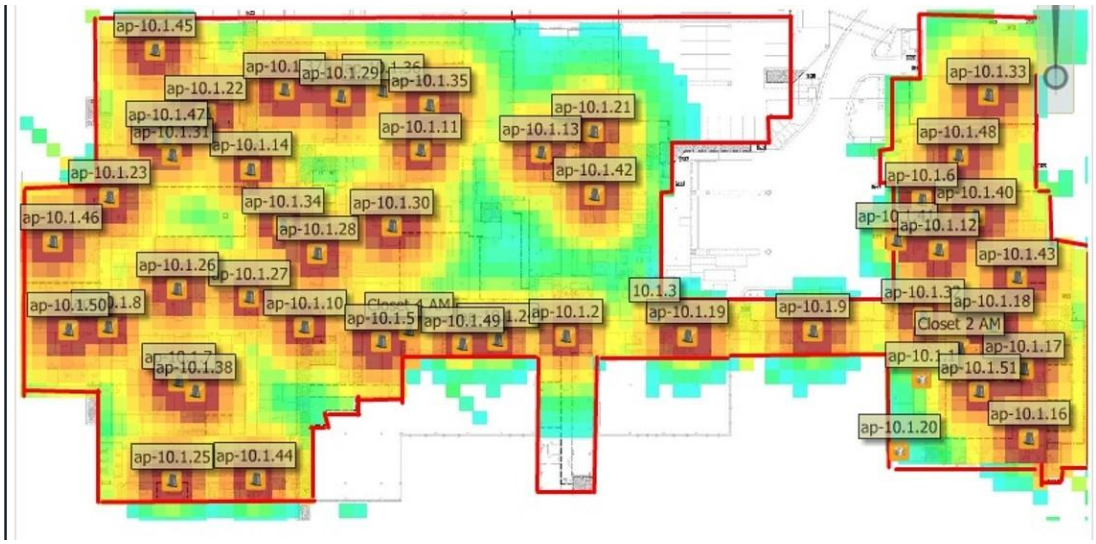
Recently Gartner stated that "**80% of new wireless networks will be obsolete within 18 months due to lack of proper planning**." Your challenge is to build a wireless solution that will support your organization for many years to come. This document will give you some things to consider before you select the technology and put together the wireless deployment plan. We've compiled this information from years of experience planning, deploying and supporting large scale wireless infrastructure (we consider large scale 100+ access points), we hope this will help.

2. Radio Frequency (RF) Planning

The first thing to consider when deploying wireless is regarding Radio Frequency (RF) and where you want to provide wireless access. It's not as easy as just broadcasting a strong signal for devices to associate to. You'll have many different types of devices, users and areas to cover in a large scale environment. You'll need to consider three key things: **Coverage, Capacity**, and **Performance**.

2.1. **Coverage:** These are the areas where you want users and devices to be able to attach to the wireless network. It's important to know:

- **Where do you need RF Coverage? (both indoor and outdoor)** and
- **How much throughput do you want to set as your benchmark**? For example, you want coverage in building A to be at least 180 Mbps. You'll need to define the areas that you want users to be able to attach to your wireless network. Also define the areas that will need to support large numbers of users for capacity planning.



2.2. **Capacity:** Each wireless access point can handle a certain number of wireless clients or devices connecting to the network. This means that you need to consider the areas that may present a high number of users, which means the deployment in that area is more important. Often, an organization will overlook things like classrooms, large meeting rooms, nurse's stations, etc. These are high user density areas that present major issues if not planned properly.

2.3. **Performance**: Knowing a little about your RF environment will go a long way in helping to plan an optimal WLAN. This is where a site survey can come in handy. A site survey will uncover RF occurring already in your environment and advise accordingly. For example, if your site is already saturated with 2.4GHz RF then moving some clients to the 5Ghz spectrum might be advantageous. Also knowing how much bandwidth will be needed to accommodate the applications and clients that will be using the WLAN is also important. With prices of 802.11N equipment at effective cost to performance ratios it is advised to explore going with high speed rather than legacy WiFi for most new deployments.

3. Applications and Devices

Knowing what devices and applications will be running over the wireless network is helpful in planning for the WLAN. Voice and video are two very demanding applications for a wired network much less a wireless one. Knowing the resource requirements of these and other applications intended for the WLAN will provide useful measurements for the planning of the network. If you're reading this, then you are most likely planning what we call a "multi-media grade WLAN", which is to say you need the system to handle anything you want to put on it.

We recommend creating a list of applications and devices you'll need to operate on the network and assigning an order of priority to the applications and devices. The system should be engineered to support the most mission critical applications first. For example, your Nurses' wireless VoIP phones will take priority over the wireless internet access for your guest users. Having these priorities will help design the wireless system effectively.

Devices	Quantity	Applications	Priority
Cisco VoWLAN Phone	650	Wireless VoIP	1
Tablet PC	1000	MRI Imaging/Multimedia Streaming	2
Notebook	1200	Web & Email	3
RFID Tag	1500	Real Time Location Services	4

4. Security

In the past wireless security was considered to be inferior to wired security. This is no longer the case. Most often the wireless implementations can integrate into directory services, allowing you to control access at the user level. Here are some considerations to make when thinking about how to implement the highest level of wireless security possible today.

4.1. **Wireless Intrusion Detection & Prevention** - WIDS is the acronym we use in reference to Wireless Intrusion Detection and Prevention. WIDS is very helpful in being proactive with wireless security. An integrated WIDS system in your WLAN can detect and prevent varying degrees of attacks and hacks that are used to acquire access to your network. It is also useful in something as innocuous as the dreaded “Rogue AP” which is installed by well meaning, but poorly informed employees seeking to gain mobile freedom in the workplace.

4.2. **Roles and Policies**- It helps to think of your user groups in terms of what they need access to. Then consider creating a Security Policy that limits their access to only those systems. An Executive Role would include a Security Policy that allows them access to the financial servers, while an Employee Role would have limited access to sensitive servers.

4.3. **Directory Services Integration-** Integration with your directory services is a critical step to provide wireless security by being able to authenticate each user connecting to the network. The credentials created for each person inside your directory services should also be used to authenticate the user on the wireless infrastructure so that you have one database of users accessing the network.

4.4. **Role Based Access Control-** RBAC is the process of being able to assign a specific security role (for example: Employee) to a user or groups of users that connect to the network. In order to do this your system must have directory services integration and then be able to assign a Role to that user.

4.5. **Wireless Firewalls** – Your system needs to be able to segment traffic by user groups similar to the way a LAN firewall segments VLANS. For example, a guest user should be denied all internal servers and only be able to access the internet gateway to surf the web and check email.

5. Network Infrastructure

The following items are important pieces to the success of any WLAN implementation. Knowing them and making sure you have the right infrastructure in place will ensure an optimal wireless experience for you and your users.

5.1. **Switching** – New 802.11N AP's have potential for 600Mbps speeds. If these AP's are connected to 10/100 Mbps switches the potential will not be reached. We advise and recommend Gigabit switches preferably with POE for connectivity with the AP's.

5.2. **DHCP & DNS** – Static IP networks can present issues with AP and wireless client functionality. It is advised and preferred to have a dynamic IP network. Static IP networks can work but will prove in the end to be an administrative headache. Locally hosted DNS is also preferred as AP's will be dependent on name resolution to find their controllers over layer 3 networks. If your network is a flat layer 2 network then this is not as critical.

5.3. **POE & Power** – Access points can be powered by POE (power over Ethernet) which makes the installation of cabling to the AP's very clean and eliminates the need to have AC power locally at the AP location. Surge protected power will be needed at the location of the POE adapters or switches that are providing power to the AP's.

6. System Management

The biggest challenge with a large scale wireless implementation is trying to manage the users and devices after the system is installed. The RF environment and user patterns are dynamic, if you don't have the ability to manage them from one interface, your operations costs will go up and your user satisfaction will drop. You need to able to build the infrastructure once, then be able to grow it, adjust it, and even provide compliance reporting in some cases.

We suggest varying levels of management based on several criteria and the needs of the organization, but here is a starting point for you to consider:

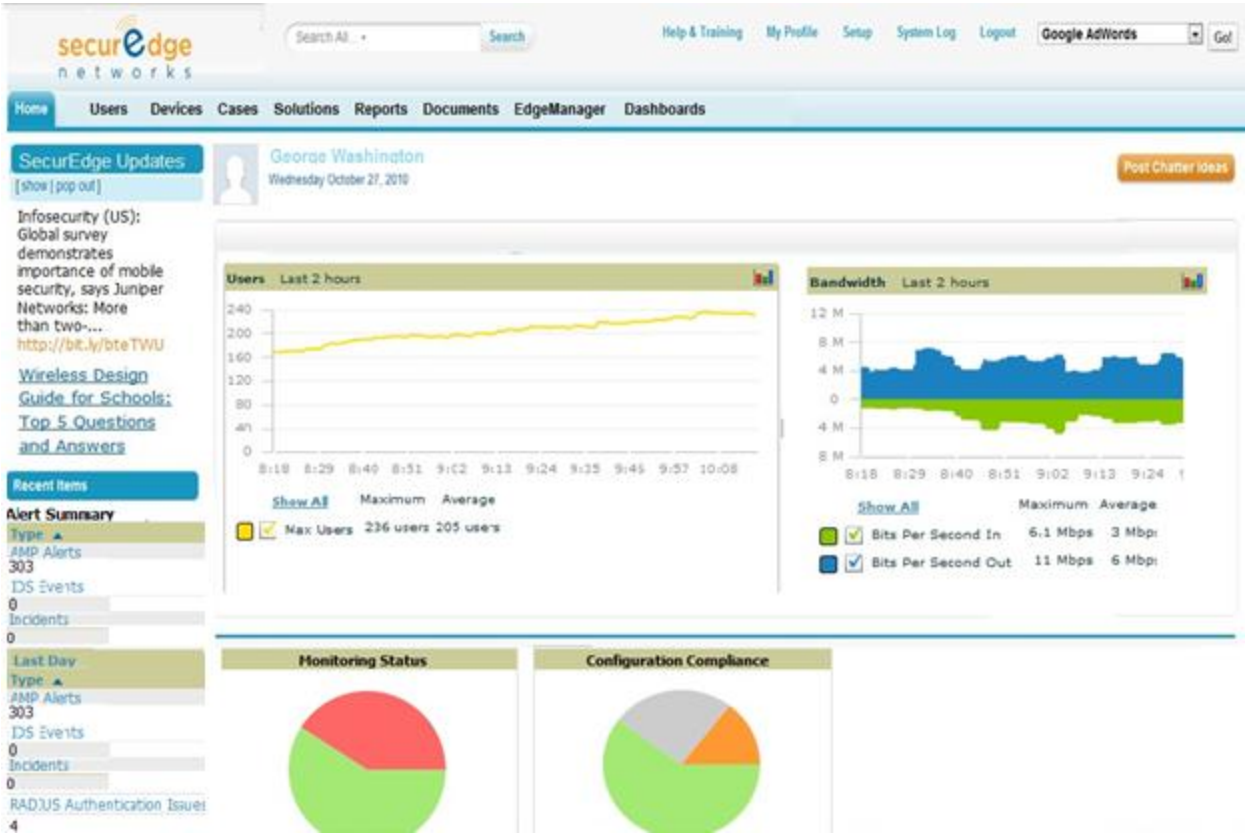
6.1. **User and Device Management**- you need to be able to assign “Bandwidth Contracts” to users or devices. A policy might be: each user is assigned 1 meg of bandwidth from 8 to 5 but 3 meg of bandwidth per user after 5.

6.2. **Adaptive Radio Management**- RF is dynamic; your system should also be dynamic. You’ll want to see RF coverage maps in real time so that you know how to trouble shoot any issues. This is a critical component for those running the user help desk.

6.3. **Change Management**- in the old days, you had to configure each access point on your network separately (can you imagine managing just a 50 ap network?). Today, you can configure one management console and then push the configuration out to every endpoint. Likewise, you should also be able to grow the wireless network simply by applying deploying a new AP an associating it to the network.

6.4. **Help Desk/Administrative Access**- there should be an option to set up levels of access for the management interface. Guest provisioning should be handled by administrative staff or help desk users. But write access for the major system configuration should come with high level privileges.

6.5. **Reporting and Compliance**-process logs, device level reporting, trending, network monitoring



7. Scalability

Don't paint yourself into a corner when choosing a solution for your WLAN implementation. Make sure that whatever solution you choose will be able to easily accommodate your future wireless growth. In our experience as soon as you introduce wireless to your users they will want it everywhere. When planning take into account a full campus or wireless everywhere plan even though you may only have the budget for a few select locations. This will give you an idea of how big you may need to grow and what solutions can achieve this and accommodate the future scaling.

8. Location-Based Services

A location-based service, often known as Real Time Location Services (RTLS), is the ability to physically locate a user or device on a wireless network. Think of it as GPS inside a building. There has been considerable debate about whether a Wi-Fi Network can handle the capacity of RTLS and if it is accurate enough to locate a device within a reasonable distance. The answer to the capacity question is that the right platform can easily handle the load as the data traffic from a Wifi-enabled RFID tag is very minimal. As for accuracy, the system uses wireless access points to "triangulate" on a user or device, so the more access points are deployed, the more accurate the system will be. If considering RTLS, we recommend defining how accurate you need the system to be, for example: within 20 ft., then having a wireless consultant (like us) help define how dense an access point deployment you may need.

9. Redundancy and Reliability

Wireless when implemented correctly will quickly become your user's main means of connectivity and they will become reliant on it heavily. Because of this it will be important to you and your users that you have ensured High Availability for your WLAN. In order to achieve High Availability you will need to build in redundancy and other means of reliability for the system. For many of our customers who are hospital systems or college campuses, if the system goes down, critical functions are interrupted (quite literally in the hospital wireless network). Consider the cost of downtime and how it will impact the organization during the design process. Then work with an expert to deign as much high availability into the system as necessary.

See our sample design for an example of redundancy on the next page.

Redundancy Design:

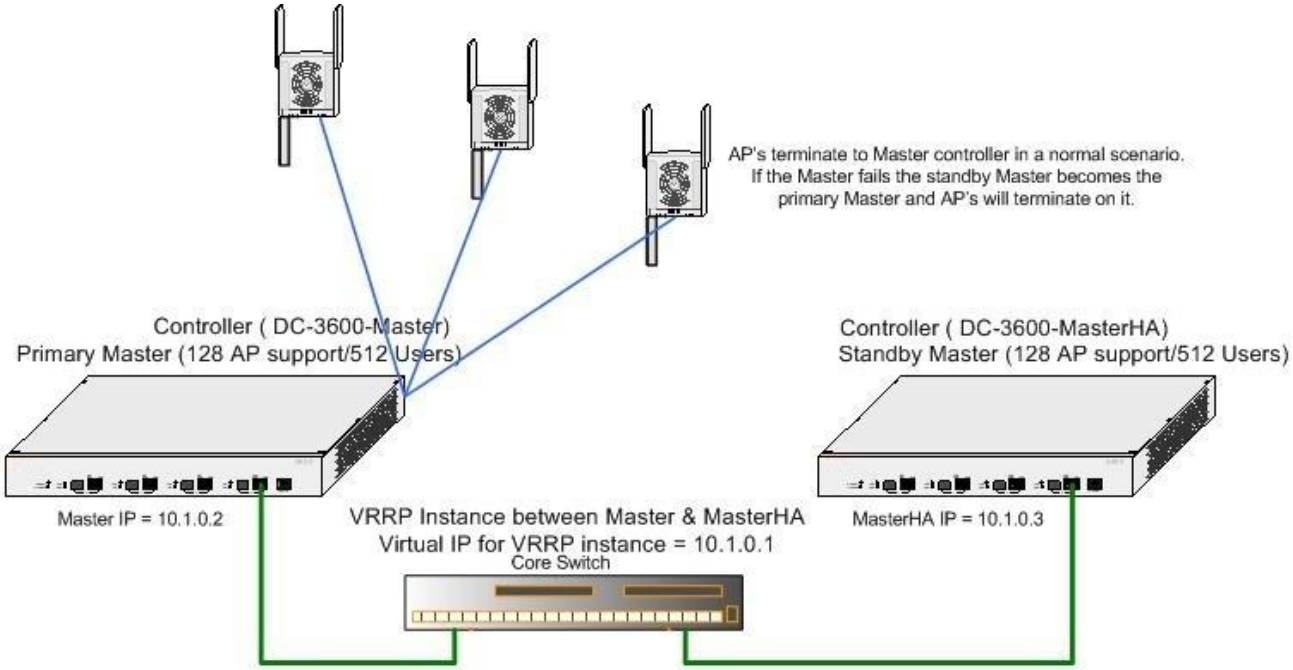


Fig. A

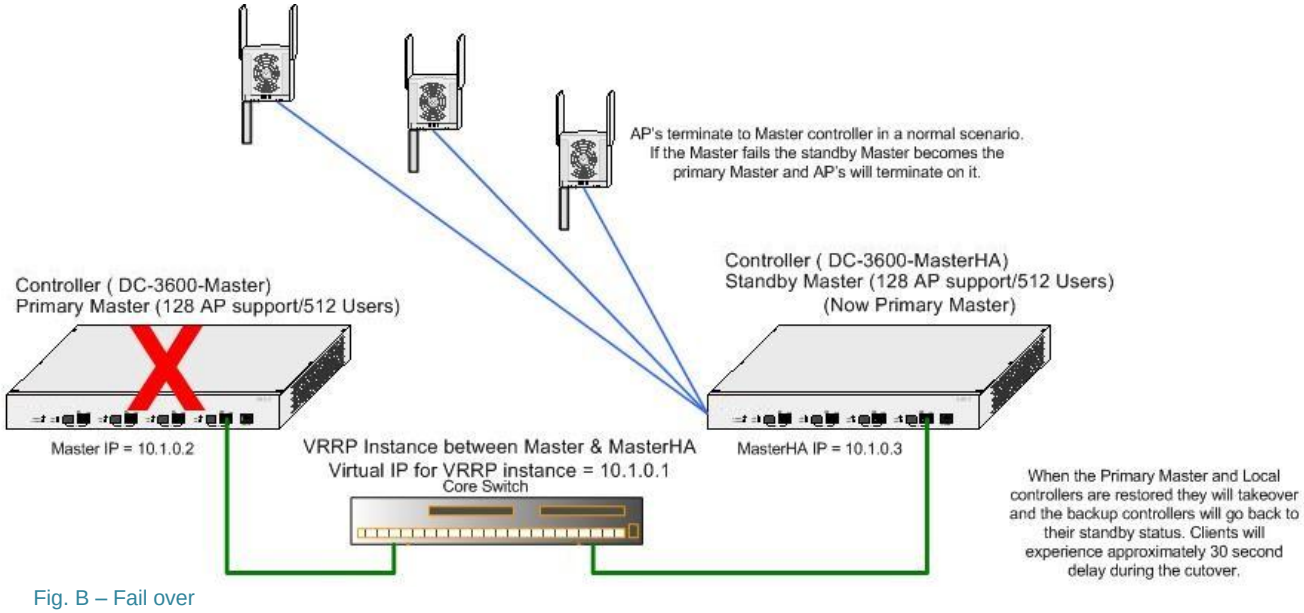


Fig. B – Fail over

10. Warranty and Support

One of the most critical steps to building a reliable system is making sure you have the proper level of support to meet your requirements. Murphy's Law of critical systems is that something will go wrong eventually. (For Example: Last year one of our hospital customers had a water pipe break directly above a data closet housing a critical part of their WLAN system.) Here are some things to think through to make sure you're ready:

10.1. Hardware/Software Replacement

Your wireless network will have many different component parts. You need to understand what happens if something fails or is damaged.

- How long is the warranty on the wireless network components (access points, antennas, software, etc.)?
- How quickly can you get replacement parts?
- How will they be installed when something does go wrong?

10.2. Phone Support

Being able to get an experienced engineer on the phone to help handle critical support issues is a vital asset to maintaining a large scale wireless network. Support specialists should understand your specific requirements and be able to respond and resolve issues quickly.

10.3. Ongoing Maintenance/Managed Services

Your wireless network will have software and firmware that needs to be updated and maintained on average of once per quarter. We call this a quarterly refresh of the system to keep it up to date and ensure that the system has the latest security patches and updates available. This can be a tricky process because with typically each new release, it brings additional features and in many cases, additional bugs in the software. Consider utilizing an engineer that is an expert on that particular platform to assist with issues or even provide the service ongoing to free up your internal resources. Many times utilizing an expert on a monthly or quarterly basis is more cost effective than figuring things out internally.

11. How SecurEdge Can Help

There is a lot to consider when deploying a large scale wireless network and mobility Infrastructure. We recommend getting any expert to help with the successful roll out. SecurEdge Networks has many years of experience designing, deploying, and supporting large scale wireless infrastructure. Here are a few things that make us unique.

11.1. Specialty Focus

One-stop shopping works well in some retail environments. It's our belief is that it's very difficult to achieve in the technology world. In our experience customers want a technology solutions partner to understand the problem they're facing and their industry. SecurEdge is committed to providing only the solutions we are experts in, serving the markets we have significant expertise in. We have even developed industry specific solutions and practices. We believe this approach creates the most value for our customers.

11.2. We Are Client-Centered not Product-Centered

At SecurEdge, we take our comprehensive knowledge and experience to determine which type of solution will be the best fit for your organization. Many companies who manufacture products do a great job at marketing their products. The challenge becomes when they recommend it for everyone even though it's not the best fit for the customer's environment. SecurEdge has the ability to work on the client's behalf, cut through a lot of the marketing jargon, and recommend a solution that is the best fit for the customer.

11.3. Our Methodology

Analyze: We have industry and solution specific experts to help understand a customer's current environment. This is the basis to build any wireless solution.

Design: We offer complete solution design services to help address the challenges. Our design recommendations are based upon your end goal, as well as industry and solution specific knowledge.

Deploy: We deploy many solutions turnkey or we can work with your team to provide guidance on deployment best practices and customer specific integration services.

Support: We offer custom fit support services. We offer managed services, unmanaged, or hybrid support including online portal access and support tools to help you manage your system.

Deploying or expanding your wireless network? Register for a free wireless design by visiting our wireless networking hub at www.securedgenetworks.com/freewirelessdesign

Our goal is to be a resource for you.

Connect With Us:

 @SecurEdgeNet

 Subscribe to our Blog