Small Business Computer Networks: a Case Study

Donald Oliver Davis: Olive Informatics

Abstract
This case study briefly explores the overall evolution of a networking solution I designed and implemented for a small business.

Introduction
A small business approached me in the hopes of expanding the scale and scope of their network. They wanted a solution that would facilitate:

- Wireless Internet access for clients
- Secure intranet for workers
- Scalability to account for future growth
- Adaptability to account for special projects
- Diverse computing environment (PCs, Macs, and mobile devices)

The business originally had a broadband modem, a wireless router, a firewall/router, and 2 network printers. The network’s physical topology was as follows: broadband modem → firewall/router → wireless router. The network printers and office computers were connected to the firewall/router. The wireless router had no encryption.

Solution 1.0
The first thing I did was have the small business purchase another wireless router. I then modified the physical network topology as follows: broadband modem → original wireless router → original firewall/router → new wireless router. I then created a segregated network; establishing a public LAN on the original wireless router and a private LAN on the original firewall/router. I enabled WPA2 encryption on both wireless routers. The network now had a star-wired bus topology with serial backbone. Everything was working fine, EXCEPT that every desktop/laptop running Vista was having persistent problems maintaining wireless connection.

Solution 1.1
After a lot of frustration, I eventually decided I would have to sacrifice security for usability (a recurring issue in computer security). Vista simply does not work with WPA2 encryption. Interestingly, both wireless routers had dual-band functionality, so I used WPA2 on the stronger band (2.4 GHz) and WPA on the weaker band (5GHz). Since there were very few machines running Vista, this adequately mitigated the problem. I did, however, strongly recommend the business ditch Vista as soon as possible.

Soon afterwards, a special project suddenly came up in which a large amount of special users needed wireless access. The problem was that these special users were 1) competing with other users on the public LAN and 2) not trusted enough to be granted access to the private LAN.

Solution 2.0
A temporary solution was needed quickly, so I modified the network’s physical topology so that the original firewall/router and the new wireless router both connected directly to the original wireless router. This meant that the private LAN now consisted of 2 segregated sub-LANs. The private LAN was still segregated from the public LAN.1

I had the small business purchase another dual-band, wireless router – but in the meantime, I recommended the office workers only use the wireless router for non-sensitive work.

Solution 2.1
When the new wireless router arrived, I modified the network’s physical topology as follows: broadband modem → original wireless router → original firewall/router → 2 new wireless routers.

The office workers now had a dedicated wireless access point and the special users had their own dedicated wireless access point. When the special project ended, that secondary dedicated wireless access point was made available to

1 Each segregated LAN (as well as any sub-LANs) has unique IP addressing.
trusted clients. This illustrated the network’s adaptability.
The small business then voiced a future desire to have a file server for highly-sensitive data. This data would not be wirelessly-accessible.

**Solution 3.0**
I therefore had the small business purchase a new firewall/router. I then modified the physical network topology as follows: broadband modem → original wireless router → new firewall/router → 2 new wireless routers and original firewall/router. The network segregation was modified as follows: public LAN and private LAN (with 3 sub-LANs).

So, between the public and private LANs, there was a star-wired bus topology with serial backbone. But, within the private LAN, there was a star-wired bus topology with distributed backbone. Figure 1 illustrates this complex, hybrid network solution:

![Network Diagram](image)

**Figure 1: network physical topology**

Component {1} is the original wireless router which sits at the top of the public LAN’s hierarchy. Components {2} and {3} are the network printers, which are accessible by all users on the entire network. Component {4} is the new firewall/router, which sits at the top of the private LAN’s hierarchy. Component {5} is the original firewall/router. This is the most secure segregated LAN (Private LAN_1) because it contains only wired users. Only a fixed group on ‘super users’ have access to Private LAN_1. Components {6} and {7} are the new wireless routers. These segregated LANs (Private LAN_2 and Private LAN_3) contain wired and wireless users. Trusted users have access to Private LAN_2. Lesser trusted users have access to Private LAN_3.

**Conclusion**
Networking for small businesses can get complicated rather quickly!

It took a few weeks for me to finish the solution described in this case study. This is not to say that the network was disabled for weeks – rather, the network was only down for a few minutes only when the topology was being modified.

Another thing to keep in mind is the challenge a diverse computing environment presents. The presence of Vista machines caused a problem which affected the entire network. In a mobile environment, it is impossible to predict what systems users will employ. Therefore, it often the case that usability issues will win over security issues. However, as technologies fall in and out of favor, it will not be a problem to go back in and adjust security settings.

Enter the issue of adaptability and scalability. In the solution described here, the public and private LANs are highly scalable. Sub-LANs already exist within the private LAN, and it will be very easy to add sub-LANs within the public LAN. Furthermore, with network segregation employed, various sub-LANs can be used for a variety of purposes as situations arise. This facilitates truly dynamic networking in which ‘change’ is always welcome.