CCDA

Pascal de Bruijn

2033942

Table of Contents

Phase 1: Characterizing a network

Characterize the customer's applications

Name of the Application	*Type of the Application*	*Number of Users*	*Number of Hosts or Servers*	*Comments*
Firefox / Opera / Internet Explorer	Web browser	125	N/A	
MS Exchange	Groupware / Email	125	1	
Active Directory	Directory Services	125	2	
Windows SMB	File/Print Sharing	125	3	
MS ISA/Proxy	Internet Access	125	1	

Characterize the network protocols

Name of Protocol	*Type of Protocol*	*Number of Users*	*Number of Hosts or Servers*	*Comments*
HTTP	Web	125	N/A	MS ISA
MAPI / IMAP	Email / Calendar	125	1	MS Exchange
Kerberos	Authentication	125	2	Active Directory
SMB/CIFS (/NetBIOS)	File/Print Sharing	125	3	Windows SMB

Documents the customer's current network

The customer's old network consisted of several (eight) linked 10mBit/s hubs.

Identify potential bottlenecks

Because the old network consisted of hubs the entire network was one large collision domain, effectively all the clients shared a single (large) 10mBit/s segment. Because of the size of the network, it will most probably have suffered from congestion during peak times, which is often associated with hub networks.

Identify business constrains and inputs to your network design

Not applicable.

Characterize the existing network availability

Not applicable.

Characterize the network performance

Not applicable.

Characterize the existing network reliability

Not applicable.

Characterize network utilization

Not applicable.

Characterize the status of the major routers

Not applicable.

Phase 2: Determining a customer's network requirements

Identify business constraints

Budget

Cabling and Patch Panels 225.000,- Euro
Networking Equipment 150.000,- Euro

Time line

The building should be ready in 6 months, at that time the cabling should already be in place. Within the next two weeks, the full network infrastructure should be fully operational. This means all required trials should be completed before the building is ready.

Identify security requirements

To protect the MS Exchange server from exploitation a reverse proxy to access the web based interface might be in order. The MS Exchange mailer should also not be directly exposed to the Internet, a secondary mail gateway should be deployed for direct communication with the Internet. This could be done through MS ISA.

The 16 representatives along with the 3 members of the board should be able to access the network through the Internet. To facilitate this, a VPN concentrator should be deployed, possibly linked to Active Directory (possibly by use of RADIUS).

Identify manageability requirements

Fault management

The network administrators need to be able to respond pro-actively to certain events. To facilitate this, we need to provide them with the proper network management tools, like a syslog server and a SNMP monitoring system. A network graphing application like Cacti would be in order to procedure graph of all the switch and router ports in the network.

Configuration management

The organization doesn't require an automated configuration management solution. Configuration management by hand should be very doable for an organization of this size. A simple yet effective solution would be to keep several Excel spreadsheets with configuration information. The major downside of this is that the Excel spreadsheet can only be edited by one employee at a time. If this method of configuration management becomes to bothersome it's always a possibility to have a simple web based application custom made (this can be developed extremely fast using for example Ruby On Rails).
Actual router configuration could be stored in a CVS (Concurrent Versions System), which was actually built for use with source code, but can be used for router configurations to keep track of all the changes made over time.

Accounting management

There seems to be no direct need for accounting management. Though Cacti provides an extremely simple form of accounting management through it's traffic graphs.

Performance management

Cacti can provide excellent Performance monitoring when properly configured. Cacti can constantly monitor the CPU, memory and interface status and much more.
As the major flow of traffic on the network will be IP/NetBIOS based, and no Voice/Live Streaming applications are used, no form of QoS is necessary.

Security management

All routers and switch should be purchased with a crypto-enabled image which makes the use of SSH (Secure Shell) available to the network managers, which allow safe and secure management of the routers and switches.
On the monitoring side, all routers and switches should have SNMPv3 enabled, with a read-only account with authentication and privacy enabled. All writable accounts should be disabled. All configuration changes should be applied using SSH.

Determine application requirements

There are no new application scheduled to be used on the new network. Only the amount of IP/NetBIOS traffic may increase significantly because the Marketing department is starting to use extensive multimedia technologies, with audio and video files being transfered through Windows File Sharing.

Characterize new network traffic

Not applicable.

Identify performance requirements

No explicit performance requirements were set by the customer. During the implementation the following guidelines will be taken into account:

- All intra network traffic should arrive within 150ms (from any source to any destination).
- Web pages located on the Internet should be accessible within 500ms (max).
- Redundancy should be implemented at the core/distribution level preventing the network from becoming completely inaccessible during (for example) hardware failure.
- The Marketing department should have ample network and disk bandwidth (on the server).

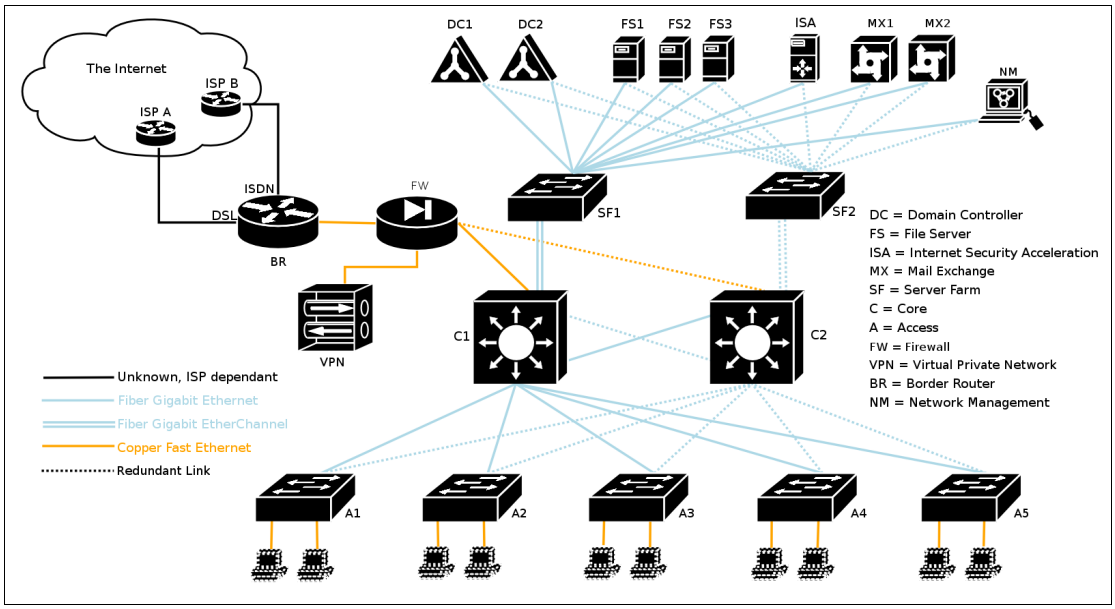
Phase 3: Designing the topology

Designing the network topology

The following topology will provide a fully redundant core using two level 3 switches. To keep their routing tables consistent and to provide fail over VRRP will be implemented (all redundant paths are dotted). To prevent switching loops RSTP will be enabled on all switch ports.

In the network design below, the core and distribution layers are collapsed into a single physical layer. This will make it easier to manage access control lists. However this will impede network scalability, but that shouldn't be an issue since the physical building in which the network resides will impose scalability limitations on the company before the network will.

Network connections between floors are optical fiber connection to prevent a potential difference flowing over the copper wires because the floors are grounded separately.



The internal network is protected by a Cisco PIX for security.

VPN connections are received at the border router which forwards the VPN packets to the PIX firewall, the PIX firewall only allows external packets to flow towards the VPN concentrator, then if the VPN concentrator accepts the incoming connection (and the user is authenticated), the VPN concentrator sends the VPN traffic into the network, which the PIX will allow (if the source is the VPN concentrator).

Provisioning hardware and media for the LAN

The core and distribution layer are represented by two 16 (gigabit fiber) port layer 3 switches. These switches should have a couple (at least 1) of 100megabit copper ports.

The access layer switch should have 2 full gigabit fiber uplink ports, and 48 100megabit copper ports.

The switches in the server farm should have 16 gigabit fiber ports (for future expansion). Two of these ports are used as a gigabit EtherChannel to the core switches.

The PiX should have at least 3 fast ethernet copper ports.

For example these devices would be adequate for the tasks at hand:

#	Device	Cost[1]	Total Cost
2	Cisco Catalyst 4507R	5864.15	11728.30
4	Cisco Catalyst 4500 1000W	577.50	2310.00
4	Cisco SuperVisor IIplus RJ45 2GE f Cat 4500	3501.12	14004.48
1	Cisco Module 48p 1000Base-x (SFPs Optional)	9677.61	9677.61
1	Cisco WS-X4548-GB-RJ45V	4635.08	4635.08
2	Cisco Catalyst 4503[2]	< 5864.15	< 11728.30
4	Cisco Catalyst 4500 1000W	577.50	2310.00
2	Cisco SuperVisor IIplus RJ45 2GE f Cat 4500	3501.12	7002.24
1	Cisco WS-X4548-GB-RJ45V	4635.08	4635.08
5	Cisco Catalyst WS-C2950G-48-EI	2385.68	11928.40
1	Cisco PiX 515E	2163.38	2163.38
1	Cisco VPN Concentrator 3020	6181.06	6181.06

Throughout the building Cat6 copper cabling should be used. For inter floor connections or other high speed connections fiber should be used.

1 Pricing information was obtained from http://www.centralpoint.nl/
2 The pricing wasn't available for this particular model, so it'll probably be less than a bigger model.

Provisioning hardware and media for the WAN

The border router should provide an ISDN and a DSL interface along with a single 100megabit copper interface.

For example:

#	Device	Cost	Total Cost
1	Cisco 2811 Router	1543.13	1543.13
1	ADSL OVER ISDN WIC	476.49	476.49
1	ISDN BRI NT-1 WIC	432.88	432.88

Designing a network layer addressing and naming model

As almost no equipment needs to be exposed directly to the Internet there is no need to use public IP addresses for the larger part of the network. Therefore private (RFC1918) IP addressing will be used for the internal network. The 10.x.y.z netwerk provides ample room for expansion. The following scheme will be implemented:

Octet	*Usage*
x	Random number (company wide) to (somewhat) prevent IP space collisions when acquisitions or mergers happen.
y	Virtual LAN Identification
z	Host IP

VLAN's

VLAN	*IP*	*Usage*
1	10.*x*.1.*z*	Network Management VLAN
2	10.*x*.2.*z*	Server VLAN
3	10.*x*.3.*z*	Directie VLAN
4	10.*x*.4.*z*	Management VLAN
5	10.*x*.5.*z*	Vertegenwoordigers VLAN
6	10.*x*.6.*z*	Verkoop VLAN
7	10.*x*.7.*z*	Marketing VLAN
8	10.*x*.8.*z*	Inkoop VLAN

VLAN	*IP*	*Usage*
9	10.*x*.9.*z*	Personaal & Organisatie (pno) VLAN
10	10.*x*.10.*z*	Boekhouding VLAN
11	10.*x*.11.*z*	Administratie VLAN
12	10.*x*.12.*z*	Systeem beheer VLAN
13	10.*x*.13.*z*	Helpdesk VLAN

IP addressing with a VLAN

Within each VLAN the following IP's are used according to this table:

IP	*Usage*
10.*x*.*y*.1/24	Default gateway
10.*x*.*y*.100-199/24	Workstations (assigned by DHCP)

IP addressing within the Management VLAN

The switches have been assigned the following management IP's:

Device	*IP*
C1	10.*x*.1.11/24
C2	10.*x*.1.12/24
SF1	10.*x*.1.21/24
SF2	10.*x*.1.22/24
A1	10.*x*.1.31/24
A2	10.*x*.1.32/24
A3	10.*x*.1.33/24
A4	10.*x*.1.34/24
A5	10.*x*.1.35/24
NM	10.x.1.41/24

IP assignments

The servers have the following IP address assignments:

Server	*IP*
ISA	10.*x*.2.1/24
DC1	10.*x*.2.11/24
DC2	10.*x*.2.12/24
FS1	10.*x*.2.21/24
FS2	10.*x*.2.22/24
FS3	10.*x*.2.23/24
MX1	10.*x*.2.31/24
MX2	10.*x*.2.32/24

The remaining network links are setup like this:

Device – Interface	*IP*	*Device – Interface*	*IP*
BR – fa0	10.x.255.1/30	FW – fa0	10.x.255.2/30
VPN – fa0	10.x.255.5/30	FW – fa1	10.x.255.6/30
C1/C2 – fa0	10.x.255.9/30	FW – fa2	10.x.255.10/30

All switch ports are locked to the workstation MAC addresses to prevent unauthorized access by alien (to the network) devices. The switch ports located in the representatives area will be exempt from the locking policy, to allow them to dynamically plug in their laptops.

IP addresses for the workstations are assigned through DHCP which has a MAC-IP association database, using this MAC-IP association database, workstations can be placed in the proper VLANs.

Selecting routing and bridging protocols

RSTP should be enabled on all switch ports to prevents switching loops. To ease VLAN management VTP should also be enabled.

On the Border Router Dial On Demand Routing must be enabled, to allow the ISDN connection to take over when the ADSL connection fails.

The Border Router, the VPN, the PiX and the Core L3 Switches should have OSPF enabled, with MD5 authentication. They should be in a single area. OSPF will quickly notify the network when, for example, the ADSL route fails.

Provisioning software features

All the networking equipment should be provided with crypto-enabled operating system images (IOS, CatOS/ PiXOS), this will give the network managers secure access to the devices using SSH (Secure Shell).

Access times can be regulated through Active Directory.

Selecting a network management strategy

Instead of buying very expensive network management software, a network this size should easily be manageable with free software like Cacti[3], php-syslog-ng[4] and ntsyslog[5].

Basically ntsyslog allows the NT operating system to send their event log (on-the-fly) to a syslog server. The Cisco equipment should also log it's events to the same syslog server. On the syslog server, the syslog daemon will insert the log messages into a SQL database, where it can be easily searched by php-syslog-ng, which is a simple web based interface.

Cacti can monitor SNMP capable devices and produces graphs for them, these are all accessible through a web based interface.

3 http://www.cacti.net/
4 http://www.vermeer.org/projects/php-syslog-ng
5 http://ntsyslog.sourceforge.net/