Wide Area Network Design

Abhinav Gupta
IIIT Hyderabad
20171059

Indranil Pradhan
IIIT, Hyderabad
2019202008

Prakash Tekchandani
IIIT Hyderabad
2020801004

Abstract

In this work, we present an efficient wide area network(WAN) design for connect three individual local area networks(LAN). We consider the topological design of this design and decide which services should be accessible and restricted. We make provision for an on-line metering and monitoring of utility services and connect it to the municipality. We also install and connect security systems such as a fire alarm, with the nearest fire brigade station. We also address issues related to the reliability and information security of our design in times of natural calamities. We present a detailed and meticulous design of our network, discussing the specifics for each of our design choices and supporting it logical and rational reasons.

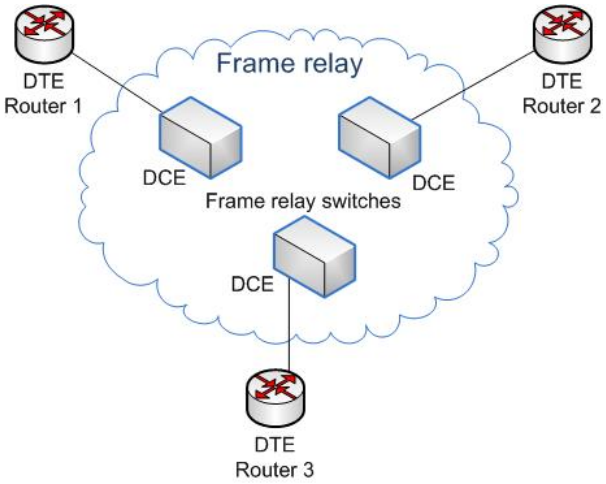

Figure 1. The classic frame relay WAN design, which we utilise for our use case.

1. Introduction

1.1. Wide Area Network

A wide area network (WAN) is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs). A LAN is a group of computers and network devices which are all connected to each other, typically from within a short geographical distance. In an enterprise, a WAN may consist of connections to a company's headquarters, branch offices, cloud services and other facilities. Typically, a router or other multi-function device is used to connect a LAN to a WAN. WANs are not restricted to the same geographical location as a LAN would be. A LAN can be set up in any number of geographical areas and be connected to a WAN—meaning a WAN is not constrained to one specific location. WAN connections can include wired and wireless technologies. Wired WAN services can consist of Carrier Ethernet and commercial broadband internet links. Wireless WAN technologies can include cellular data networks like 4G LTE, as well as public Wi-Fi or satellite networks.

Our objective is to design a WAN by combining three individual LAN's designed prior for an apartment complex, a colony and a gated community respectively, and connect these efficiently and in a cost-effective manner.

1.2. Individual LAN Designs

We recap our three individual LAN designs which we have proposed earlier, and summarise it in short for a better understanding of our WAN design. Our aim is to efficiently connect these three LAN's into one wide area network.

1.2.1 Abhinav's Design - Apartment Complex

Abhinav has designed his LAN for an apartment complex with nine floors each comprising of 14 flats, with a total of 126 apartments in the entire building. Although a three tier architecture may seem a natural choice, Abhinav uses a modified two-tier architecture instead, since there are only 126 apartments and it would be expensive to place an access switch in each home. The access switches are placed in the control rooms on each floor, and all the WAP's in the apartments are connected to this access switch. Furthermore, we use two distribution switches which connects the access switches on each floor to the router. These are layer-3 switches (as opposed to layer-2 access switches) and each

distribution switch is connected to 9 access switches. There is no core switch, and these distribution switches are connected directly to the router which pro-vides the connectivity between our LAN and the WAN. Abhinav's design uses multi-mode fiber optic cables for backbone cabling and UTP cables for the cabling between access switch and distribution switch. His design uses a classless addressing IPv4 schema assuming a total of 1260 de-vices connected to the LAN.

1.2.2 Indranil's Design - Colony

Indranil lives in a colony area. There approximately 250 houses. And all the houses are not uniformly distributed. There are some areas with dense areas where several houses are there and the areas where there are less houses. Indranil has designed his network following the 3-tier hierarchical design.

Based on geographical density the whole area has been divided into subareas of A1, A2, A3, A4, A5, A6, A7, A8, A9. Every area has access layer switch. In access layer switches, VLAN is used to logically group the end users based on the requirements of the network. Like IT people have been grouped in to one VLAN. The houses with IPTV have been grouped into a VLAN. And normal users have been grouped into another VLAN. In the design redundancy is applied so that one link failure doesn't make the network in accessible. To prevent from looping spanning tree protocol is used. Trunking is used between access layer and distribution layer switches and between distribution layer and core layer switches. Cables used from access layer to end devices are 10BaseFL, 100BaseFX, 1000BaseLX. Cables used from access layer to distribution layer switches 10GBaseLR. Cable used from distribution layer to core layer is 10GBaseLR. The access layer switch is Cisco SF220 48P. The distribution layer switch is Cisco Catalyst 2960 XR-24PS-I. Core layer switch is Cisco catalyst WS-6503-E. Routing protocol used is Multiarea OSPF. Where each area comes under distribution layer. Every VLAN comes under one particular subnet which makes it easy for broadcasting the packets intended for a particular group. DHCP server is present at distribution layer for which it makes easier to manage the IP addresses and gives modularity in the design.

1.2.3 Prakash's Design - Gated Community

This LAN is for gated community having 250 houses. The houses are spread in 5 blocks. Each block contains 10 house. All the houses requires upto 1000 Mbps bandwidth. Prakash designed hierarchial architecture having three layers, as access, distribution and core. The nework is divided into five distribution area. Each distribution area serves one block of society. All the distribution area are connected to central core routers. In core area there are two routers. The access switches are connected to VLAN.There are 15 access switches and covers all the houses. Prakash LAN used cisco express 500 and cisco catayst 4500 series for access and distribution level switch respectively. For cabling twisted pair cable 5e and 6 is used for access and trunk respectively.

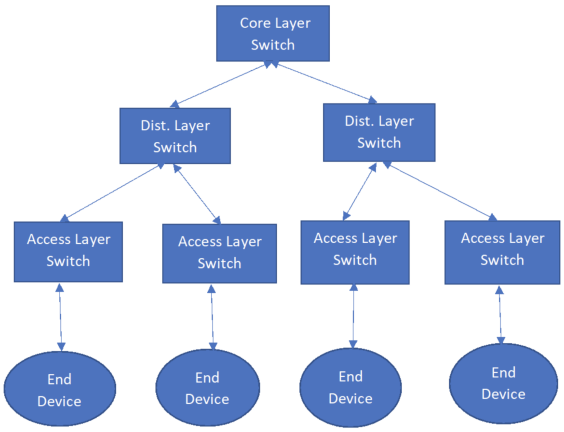

Figure 2. CISCO's popular three-tier LAN architecture, followed by Indranil for the LAN design of his colony. Abhinav and Prakash also use similar versions of this architecture, with Abhinav specifically using only a two-tier architecture for his apartment complex.

2. Network Design

We shall be using the concept of Frame Relay to efficiently connect our individual LAN's.

2.1. Packet Switching Design

2.1.1 Why Frame Relay, and why not point-to-point?

Point to point networks, which directly connects two points A to B, is a very useful approach to designing a wide area network. This design is really simple and straightforward, we have two routers A and B from two LAN's, an these are connected together. But when there are greater than 2 LAN's required to be connected, we need to create a full mesh in order to allow all LAN's to communicate with each other. Hence, due to the intense wiring and number of connections, it becomes highly expensive with administrative overheads. The downfall is it's very expensive with a lot of equipment involved and lots of circuits.

2.1.2 Frame Relay

This allows us to connect one point to many points. It's a multi access network, and the design does not get very messy. Frame really became popular in the '90's and is widely implemented to this day due to its convenient design. This is a packet switching design, so it's less expen-

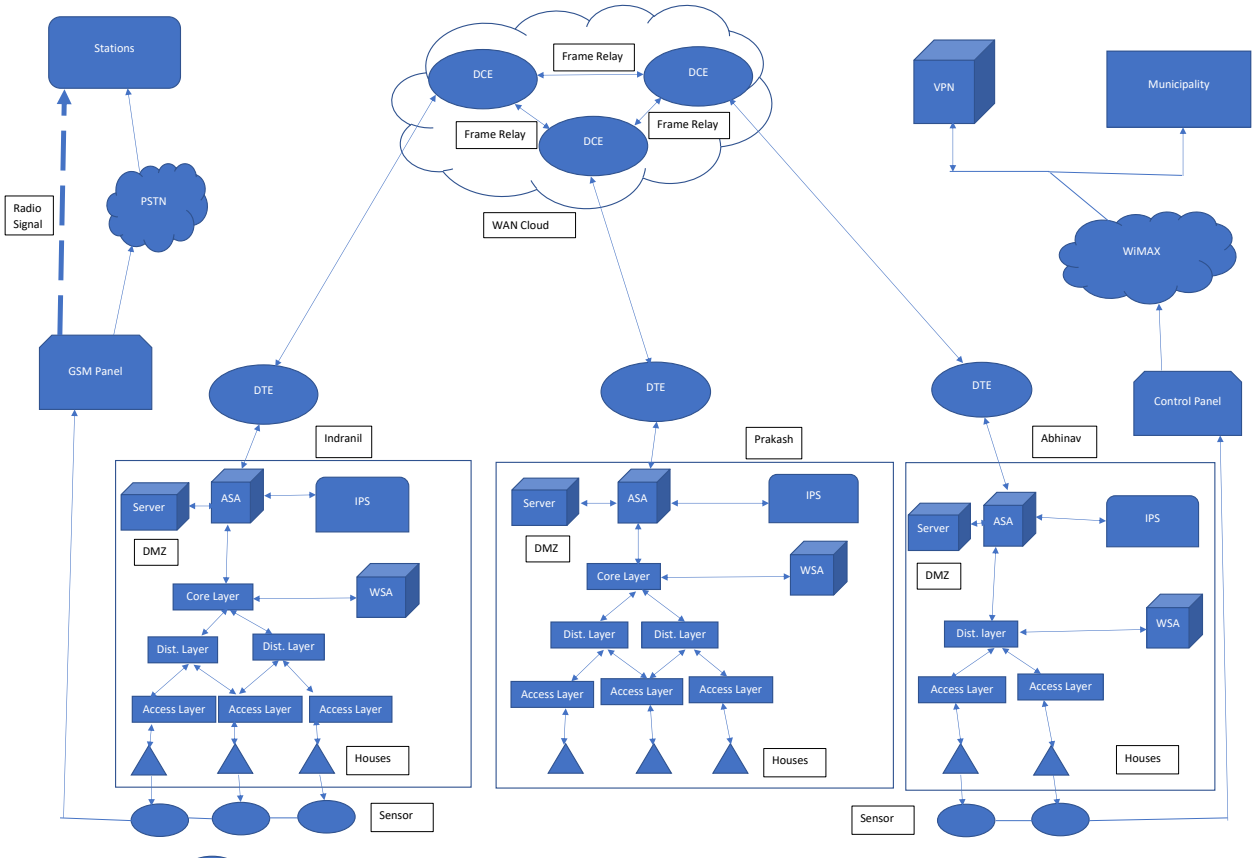

Figure 3. This figure depicts our proposed WAN Design. The three boxes depict the individual LAN designs, which we wish to connect to form a WAN. For each LAN, the topmost layer is connected to the firewall and intrusion detection system, to provide security to the LAN's. These LAN's are connected using the frame relay switches and DTE routers, as explained in Section 2. We also install security systems and provide monitoring of online systems, as explained in Sections 3 and 4.

sive and allows us to easily connect LAN's to one another, as opposed to point-to-point connections. We connect all of our LAN's to a 'cloud' using circuits or "access links" as they are commonly referred to. This frame relay 'cloud' is owned by the service provider and each access link is terminated by a "frame relay switch". This switch is also responsible for providing the frame relay services.

Frame relay is provides a very secure network design due to the Data Link Connection Identifier (DLCI). Whenever a LAN router sends a data packet to the frame relay switch, it looks for the DLCI, which is basically just a number. It indicates the destination of the message, so the frame relay switch knows which network to route the message to! Each router can send different packets destined for different routers on the network, signifying the multi-access aspect of a frame-relay design, which is exactly what makes it so efficient. We can send packets to different networks through just one single link, providing connectivity to many locations.

This is particularly useful when we wish to add another LAN to our design, which might very well be the case in future. So in such a scenario, we would just need to add one router and one connection to the frame relay cloud. Frame relay is hence, very scalable and a less expensive solution.

2.2. Using Frame Relay for our WAN

We propose frame relay to connect our individual LAN's, as shown in Fig. 4. Following are the requirements for our WAN: (1) Cost effectiveness, (2) the data transfer rate is upto to 1.544 Mbps., (3) abilty for voice and data communication in form of email, document and database, and (4) support of bursty data. Some of the keywords used are:

- Data Terminal Equipment (DTE): These are the devices that pass the data from LAN for transmission

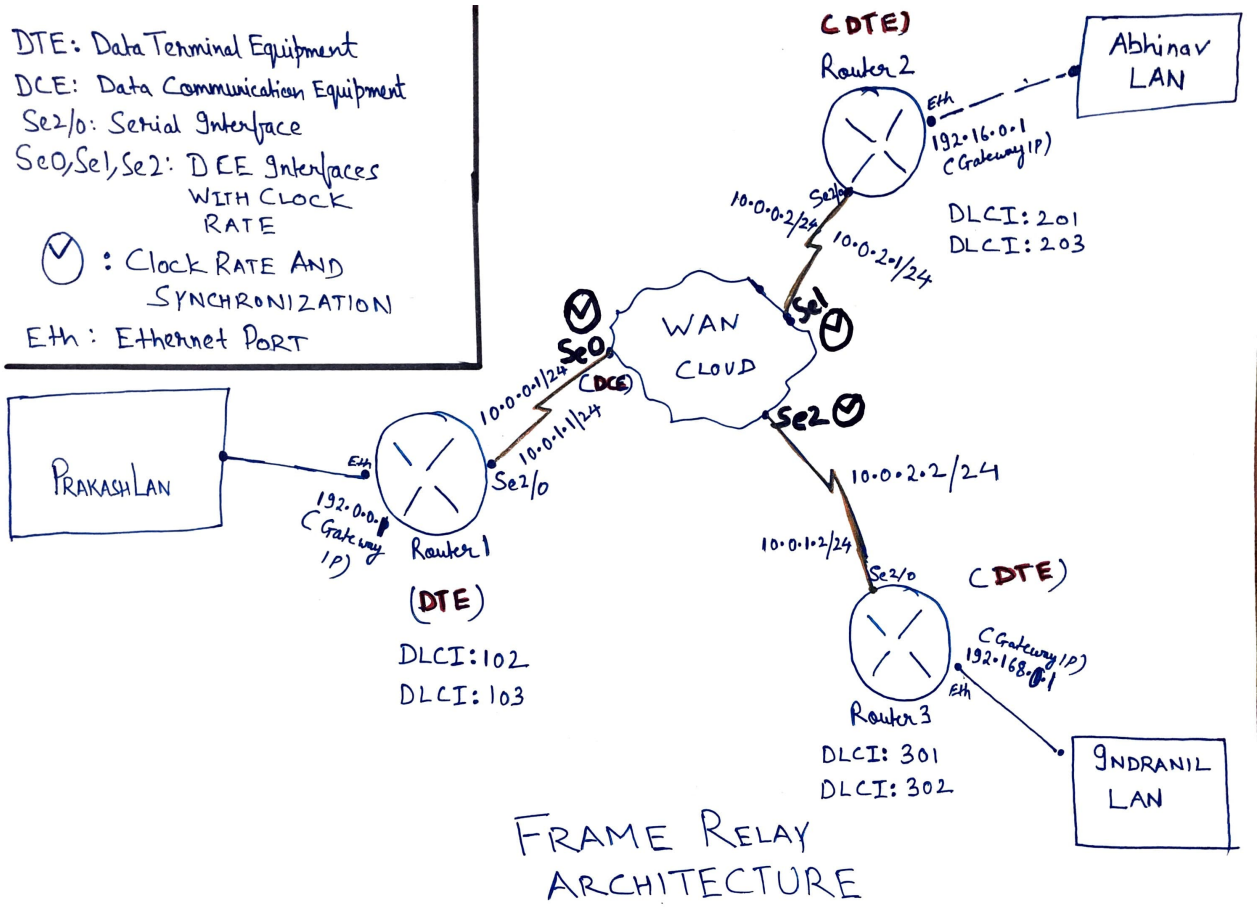

Figure 4. Frame Relay Architecture

over WAN.

- Data Communication Eqipment (DCE): It provides an interface to connect subscriber to a communication link on a WAN. It is a frame relay switch that provided clock rate and synchronization.
- DLCI: It is a 10 bit data link communication identifier assigned by a frame relay service provider.
- Local management interface (LMI): Signaling between routers and frame relay switch.
- WAN Cloud: It refers to companies internal infrastructure.
- RIP: Routing information protocol used in our frame relay architecture.
- Subinterface: It is a logical interface that is associated with a physical interface.

We have three LANs to connect. LAN1, which is Prakash's gated community LAN. LAN2, which is Abhinav's apartment LAN and LAN 3, that is Indranil's gated community LAN.

2.2.1 Devices and Configurations

DTE Router: Each of the LAN is connected through Gateway IP with DTE routers. We require three routers i.e. Router1, Router2, Router3 to connect to each LAN. Each router is also configured with RIP protocol to exchange routing table information. Split horizon has been disabled. For our design, we propose to use the Cisco ASR 1000 Series - Router.

Each router has two interfaces.

- Eth:Ethernet gateway IP interface to connect to LAN.
- Se2/0:Serial interface to connect to WAN cloud or Cloud frame relay switched network. It provides clock rate and synchronization.

2.2.2 Configuring DTE Router

Eth is associated with gateway IP to connect to LAN. Se2/0 interface use subinterfaces. We are using subinterfaces because we have disabled split horizon as in frame relay each router should be able to pass information from same interface. But by disabling split horizon routing loops can occur. To prevent routing loops subinterfaces are used. For eg: router1 se2/0 has two subinterfaces to connect to router2 and router3.

Here are the details for router 1:

- Router1 requires two DLCI to communicate with Router2 and Router3. We choose DLCI as 102 and 103 to connect to router2 and router3 respectively.
- Eth is configured as: IP address = 192.0.0.1, Subnet = 255.255.0.0
- Se2/0 is configured as:
  - First subinterface – it connects to router2 with dlci 102.
  - ser2/0.102 point to point, ip address = 10.0.0.1/24, bandwidth=64, dlci=102
  - Second subinterface - it connects to router3 with dlci 103.
  - ser2/0.103 point to point, ip address = 10.0.1.1/24, bandwidth=64, dlci=103

For Router 2

- Router2 requires two DLCI to communicate with Router1 and Router3. We choose DLCI as 201 and 203 to connect to router1 and router3 respectively.
- Eth is configured as: IP address = 192.16.0.1, Subnet = 255.255.0.0
- Se2/0 is configured as:
  - First subinterface – it connects to router1 with dlci 201.
  - ser2/0.201 point to point, ip address = 10.0.0.2/24, bandwidth=64, dlci=201
  - Second subinterface - it connects to router3 with dlci 203.
  - ser2/0.203 point to point, ip address = 10.0.2.1/24, bandwidth=64, dlci=203

For Router 3

- Router3 requires two DLCI to communicate with Router1 and Router2. We choose DLCI as 301 and 302 to connect to router1 and router2 respectively.

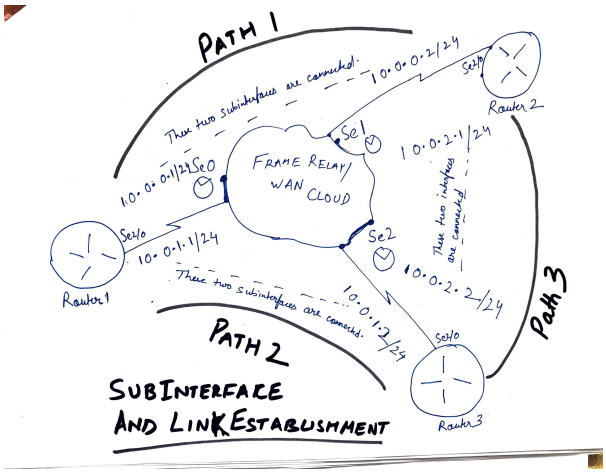

Figure 5. Sub-Interface and Link Establishment

- Eth is configured as: IP address = 192.168.0.1, Subnet = 255.255.0.0
- Se2/0 is configured as:
  - First subinterface – it connects to router1 with dlci 301.
  - ser2/0.301 point to point, ip address = 10.0.1.2/24, bandwidth=64, dlci=301
  - Second subinterface - it connects to router2 with dlci 302.
  - ser2/0.302 point to point, ip address = 10.0.2.2/24, bandwidth=64, dlci=301

2.2.3 Configuring WAN/Frame Relay Switch

Frame relay switch has three serial interfaces (Se0,Se1,Se2) with clock rate and synchronization. We show our subinterface and link establishment in Fig. 5.

DLCI Association

- Se0 is configured with DLCI 102,103 for connection to router2 and router3 respectively.
- Se1 is configured with DLCI 201,203 for connection to router1 and router3 respectively.
- Se2 configured with DLCI 301,302 for connection to router1 and router2 respectively.

Frame Relay Link establishment

To establish back and forth connection between serial interface and router below are the path configurations

- Path 1: Se0 - Router2 and Se1 - Router1

- Path2: Se0 - Router3 and Se2 - Router1
- Path3: Se1 - Router3 and Se2 - Router2

3. Utility Service Monitoring

The houses in our individual local area networks have access to utility services such as electricity, water and LPG pipelines connections. In our WAN design, we also propose to make provision for an **on-line metering and monitoring of these utilities** and provide connection of these meters to the municipality buildings and power distribution companies in the area.

Every house in the LAN has a meter which measures the amount of electricity being consumed and the amount of water used up every day. In order to make it easy for monitoring these values and generating bills easily, we make provision to connect these meters directly to the municipality. We do so with the help of **WiMAX**, one of the most popular broadband wireless technologies available today. Since all of our colonies/apartments are very far away from the municipality building, using wire technologies such as cable modems or DSL would be very expensive. Moreover, there would be multiple meters in every household (water, electricity, LPG gas etc.), and so laying out wires would be a costly task.

3.0.1 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) provides an economical and efficient alternative to wired technologies for broadband access. WiMAX operates similar to WiFi, but at higher speeds over greater distances and for a greater number of users! WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach. It can overcome the physical limitations of traditional wired infrastructure.

WiMAX provides 30 to 40 megabit-per-second data rates, which is very useful for monitoring the meter rates. For our network design, we use WiMAX for connecting the meters from every building to the municipality. This way, the municipality can easily monitor the electricity and water consumptions in houses, and look for irregularities or anomalies in the readings. This also makes it easy for the offices to provide bills and taxes, and the data is more reliable as it is a part of the WAN.

3.0.2 WiMAX VPN

WiMAX VPN provides security while transferring data wirelessly. WiMax VPN access is used to provide reliable, dedicated service for VPN as well as other applications including Internet, email, file sharing, web hosting, data backup, video, or voice access. All WiMax VPN services come with a Service Level Agreement with guarantees on speed, performance, uptime, and repair.

We need to ensure that the municipality does not get access to any other data from the area except the sensor readings. We also need to ensure that it is unable to tamper with such readings, to provide reliable bills. Hence, using the WiMAX VPN is beneficial.

4. Security System

4.0.1 Firewalls and Intrusion Detection System

Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An intrusion detection system (IDS) evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

In our WAN, Indranil's, Prakash's and Abhinav's LANs are connected through the frame relay. It's possible that any user from one LAN may try to access the content on another LAN which he/she is not authorized to access. It's also possible that any user on one LAN makes DoS attack to another LAN or there are possible of having malware, spyware, Trojans, Phishing.

Indranil and Prakash use a three layered hierarchical design where top layer is core layer. Abhinav uses two layered hierarchical design where top layer is distribution layer. To secure the individual LANs and the WAN, we have used a firewall and Intrusion Detection System to provide security. The topological diagram is depicted in Fig. 6

4.0.2 Adaptive Security Appliance

Cisco ASA 5580-20 has been chosen as Adaptive security appliance firewall. This firewall protects the internal threats, secure the public services provided by the DMZ and controls the user traffic to the WAN. This firewall has three interfaces such as

- Inside – The inside is the interface connecting to Core/Distribution layer switch/router.
- Outside – The outside connects to the to internal border router of the ISP.
- DMZ – This is where the servers reside which are accessible over the WAN.

This firewall acts as a primary firewall gateway to the WAN.

The Cisco ASA 5580-20 integrates multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec VPN, IPS, antivirus, antispam, antiphishing, and web filtering services.

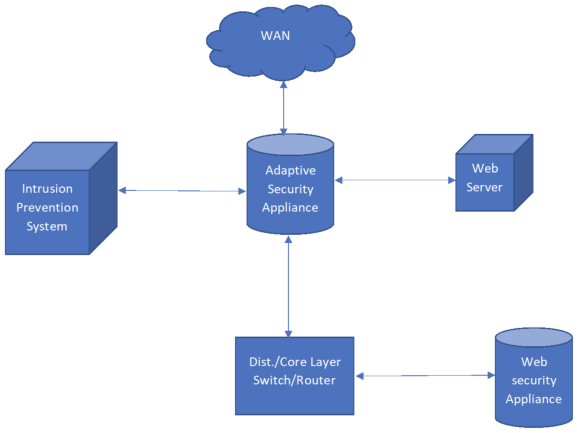

Figure 6. To secure LAN and WAN, we have used firewall and Intrusion Detection System to provide security. This is the topological diagram for the same.

These technologies deliver strong network and application-layer security, user-based access control, worm mitigation, malware protection, improved employee productivity, instant messaging and peer-to-peer control, and secure remote user and site connectivity. The Cisco ASA 5580-20 enables standardization on a single platform to reduce the overall operational cost of security. A common environment for configuration simplifies management and reduces training costs for staff, while the common hardware platform of the series reduces sparing costs.

They following key aspects have been considered when implementing the firewall:

- Firewall Hardening and Monitoring – It implements dedicated management interfaces to the OOB management network. It uses HTTP and SSH for device access. It uses NTP to synchronizes the time. It uses SNMP to keep track of system status, traffic statistics and device access information. It configures AAA role-based access control and logging.

- Network Address Translation – It's required for limited number of public addresses. And it also helps in internal address space hidden from malicious activity.

- Firewall Access Policies – Protects internal resources and data from external threats by preventing incoming access from outside. It protects public resources served by the DMZ by preventing public services and limiting outbound access from DMZ resources out to the WAN. Controlling user's outbound traffic. Enforcing such policies requires the deployment of ACLs governing what traffic is allowed or prevented from transiting between interfaces. By default, the Cisco ASA appliance allows traffic from higher to lower security level interfaces (i.e., from inside to outside). Ingress Inside allows outsider to access resources residing internally for the allowed ports and protocols. Ingress DMZ restrict connections initiated from DMZ to the only necessary protocols and sources. This typically includes DNS queries and zone transfer from DNS server, SMTP from E-mail server. Ingress Outside allows inbound access should be restricted to the public services provided at the DMZ such as SMTP, Web, and DNS.

- Firewall Redundancy- A single Cisco ASA appliance configures with redundant interfaces. The use of redundant interfaces makes the design resilient to link level failures, representing an affordable option for high availability.

Specification:

- Number of users – unlimited.
- Concurrent Connection – 1000000
- New Connections/ second – 90000
- Integrated Network Ports - 8 Gigabit Ethernet, 4 SFP Fiber, 1 Fast Ethernet.
- Security Context – Up to 50.
- Interfaces – 2 Gigabit Ethernet Management.
- Interface card options - 4 Port 10/100/1000, 4 Port Gigabit Ethernet fiber, SR, LC, 2 Port 10Gigabit Ethernet fiber, SR, LC
- VLANs – 100
- Packets/second - 2500000
- Memory – 8GB.
- Minimum system Flash –1GB.
- System us – Multibus Architecture.
- Operating Temperature – 10 to 35degree C.
- Relative Humidity – 5 to 95% noncondensing.
- Nonoperating Temperature – -30 to 60degree C.
- Nonoperating Relative Humidity – 50 95% noncondensing.
- Normal line voltage 100 to 240 VAC.

4.0.3 Web Security Appliance

For web security appliance, we have selected Cisco IronPort s690. The WSA is located inside of the Cisco ASA. That ensures that client and WSA are reachable over the same inside interface of the firewall and WSA can communicate with them without going through the firewall. WSA has been placed at the core layer for Prakash and Indranil and on Distribution layer for Abhinav. This gives complete visibility to the WSA on the traffic before getting out to the firewall. WSA integrates seamlessly into any network to defend against a wide variety of web-based malware threats such as malware, spyware, malicious system monitors, Trojans, phishing, and pharming. Additionally, the s690 appliance provides a next generation platform to control and

monitor web traffic that originates from within the network. The security services provided by the s690 are IP Spoofing, LS traffic monitor, URL filtering, Web reputation filter, Malware and spyware scanning, sender based network participation. Combine traditional URL filtering with dynamic content analysis to mitigate compliance, liability, and productivity risks.

Cisco's continuously updated URL filtering database of over 50 million blocked sites provides exceptional coverage for known websites, and the Dynamic Content Analysis (DCA) engine accurately identifies 90 percent of unknown URLs in real time; it scans text, scores the text for relevancy, calculates model document proximity, and returns the closest category match. Administrators can also select specific categories for intelligent HTTPS inspection. Advanced Malware Protection (AMP) is an additionally licensed feature available. Prevent confidential data from leaving the network by creating context-based rules for basic DLP (Data Loss Prevention).

- Disk Space – 4.8 TB.
- Mirroring - RAID 10.
- Memory – 64GB DDR4.
- CPU – 2*2.5 GHZ 12C.
- DC power option available (930W)
- Hot swappable H/D – Yes.
- Power supply – 650W.
- Speed - 10/100/1000, auto negotiate.
- Fiber Option - Yes, separate SKUs, 6 port 1G Base-SX Fiber.

4.0.4 Intrusion Prevention System

Cisco ASA 5580-20 offers integrated Intrusion Prevention System. The IPS module runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. The flow of traffic is stated below:

- The traffic enters the IPS module from the ASA.
- The IPS module applies its security policy to the traffic, and takes appropriate actions.
- The IPS module might block some traffic according to its security policy, and that traffic is not passed on.
- Valid traffic is sent back to the ASA;

4.0.5 Alarm System

In our design, in the access layer, there are houses provided with the connection. There multiple sensors have been installed in one house. These sensors detect suspicious behaviour like intruder detection, fire, smoke detection, gas leakage etc. After detection of suspicious behaviours, the police station, fire brigade etc, get informed about it. To inform the particular authority, we have used dual signalling mechanism where there is one primary link for communication at first. And if the primary link gets failed then the secondary link takes the responsibility of transferring the message to the authorities. For dual signalling we have used the GSM and PSTN technology. GSM send the alarm via message wirelessly and PSTN uses classical telephone line connection. A Public Switched Telephone Network (PSTN) is a combination of telephone networks used worldwide, including telephone lines, fiber-optic cables, switching centres, cellular networks, as well as satellites and cable systems. As matter of emergency and the concerned authorities should be informed immediately, that's why we have considered the dual signalling approach. In our case the primary communication occurs with PSTN network. And if telephone line gets tampered or cut, the GSM can send the signal to the concerned authority.

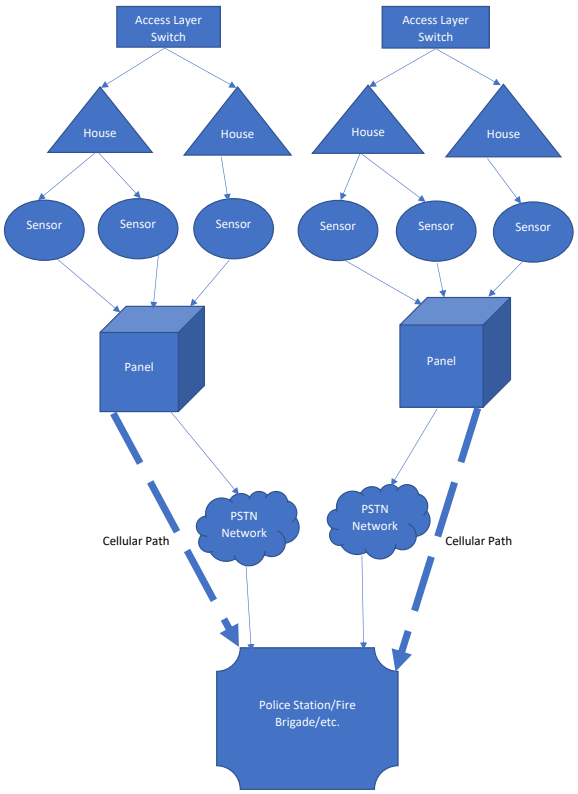

Figure 7. Alarm System implemented in our WAN. The alarms from each house are connected to a GSM panel, which monitors all the fire alarms from one LAN building/colony. This GSM panel is connected to the Police/Fire Station using the public switched telephone network wired technology. In case of failure, there is also a provision for a cellular path, so the radio signal can be transmitted wirelessly to the police station for immediate action.

For our panel we will use the wg-yl007m2h GSMP-STN Dual-Network burglar alarm. It uses the advanced GSM digital signal process technology, GSM Wireless mobile and traditional PSTN landline networks with intelligent alarm system. It has highly integrated digital voice, SMS, self-learning wireless communication code, remote appliance control and text messaging technologies. The alarm provides automatic voice or SMS message as notifications for incidents. This large LCD display alarm can integrate with a lot of alarm accessories including door sensor, smoke detectors, gas detectors, emergency buttons and other accessories to build a powerful security setup.

There are many advantages of using our GSM Panel. It is a large LCD English blue back-light display with voice prompt and ease of use. It provides support for dual-network of both PSTN landline and GSM mobile network, thus giving redundancy for extra stability. It can check status and call records from panel and allow up to 99 wireless defence zones and 4 wired zones. Each can be defined as one of the 8 zone types including NORMAL, STAY, INTELLIGENT, EMERGENCY, CLOSED, HELP SENIOR, WELCOME and CHIME.

Some other advantages include: (1) Four sets of scheduled arm/disarmed function, each time disarmed you can select the included period of time and different defence zone, eliminating of need of the manual procedure, realizing the beauty of automatic controls. (2) Support configuration via phone or SMS messages to System Setup text messaging costs associated with the alarm panel. (3) 6 group voice alarm phone number for alert calling, 3 group phone number for help senior, 6 group for SMS messaging, numbers saved inside EEPROM without lost upon power failure. (4) Different zones can dial a pre-set telephone number. (5) Support ISD automatic voice mailbox for playback message upon alert. Maximum length of voice message is 10 seconds. (6) Telephone (phone) long-distance telephone control for arming, disarming, monitoring, remote announcement. (7) 1 Set of normally open signal outputs, relay linkage output, home appliances remote control can be realized. (8) Wireless intelligent study coding, compatible with PT2262 normal encoding and a 1527 encoding, convenient and flexible for adding or reducing accessories. (9) Maximum support 150 remote control and 150 sensors. (10) Unique black box features, you can display most recent 72 disarmed records and 102 recent alarm recording. Accurately shows the alarm time and control code. (11) Built-in Ni-Hi rechargeable battery and automatically switchable upon power failure, and notification will be sent via SMS. (12) Panel integrated with either dual-band, triple-band, quad-band GSM/GPRS industrial graded module, stable and reliable.

The specifications of our GSM panel include: (1) Input voltage - DC9V-12V (2) Wireless frequency: 315/433/868/915MHZ, (3) GSM Format: Support GSM850/900/1800/1900MHz and (4) backup battery: NI-HI AAA*6 DC7.2V.

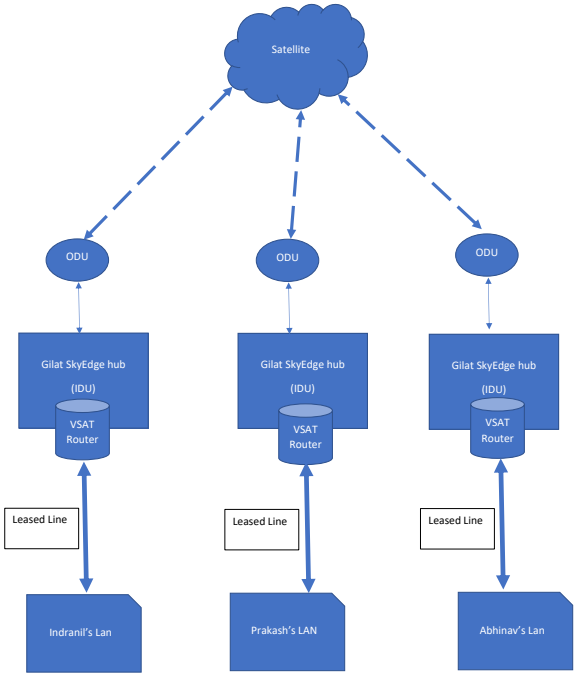

Figure 8. Our efficient network design ensures connectivity even in times of natural calamities like floods.

As this alarm system supports encoding, Encoders can be programmed to indicate which specific sensor was triggered, and monitors can show the physical location of the sensor on a list or even a map of the protected premises, which can make the resulting response more effective.

As the GSM signal can travel a minimum distance of 22 miles so it can easily reach the local police station or fire brigade for emergency which are located well within the radius of 22 miles.

5. Natural Calamities

It becomes difficult to keep wide area networks unbroken/connected during disasters and natural calamities such as floods. In this case it is essential to provide services to the end user with stable network connectivity. To keep the network connected, we have used a Cisco IP VSAT wide area network which is wireless, two way, completely IP based, unicast and multicast both, cost effective and high speed. It also supports video on demand, audio, video and live videos.

It has two units, an indoor unit and another is the outdoor unit. For indoor unit, we have used the Gilat SkyEdge hub systems. The outdoor unit is one antenna through which the message will be delivered to the satellite and will receive

message from the satellite. For two connectivity Cisco 3700 series router is integrated. Indoor Unit supports Ku-band and C-band frequencies for transmission. It connects to an outdoor unit including a satellite dish antenna, receiver, and transmitter via coaxial RF cables. It also supports dynamic routing protocol like OSPF and EIGRP. Reliability is provided through policy-based load balancing and automated rerouting of traffic based on policies and failure conditions.

End to end encryption is provided by the hardware VPN module or Cisco IOS software module for the secure transfer of the data. Dedicated leased line provided from the LAN to the hub. For leased line 10GbaseLR fiber optic cable is used.

5.1. References

- LAN Design
- Frame Relay Wiki
- Frame Relay Video
- Security Alarm
- Firewall
- Book Chapter
- WAN Basics