INDORE SMART CITY DEVELOPMENT LTD.

107-109, Palika Plaza, Phase-II MTH Compound Indore

Phone 0731- 2535572 E-mail: smartcityindore16@gmail.com

Networking Work

At

Smart City Office,Nehru Park

Indore

Index

- **The most important need of 21st century cities is to create local economies, policies and tactics that support equitable, vibrant and resilient urban living.**

- **Design should engage with science, politics, economics and culture for the purpose of innovation in city planning.**

- **Younger generations want to live and work in cities with high quality architecture, public space and alternative transit. These features also increase real estate values and the overall competitiveness of the city.**

- **We need to create an open environment for productive dialogue between the public, private and civic nonprofit sector.**

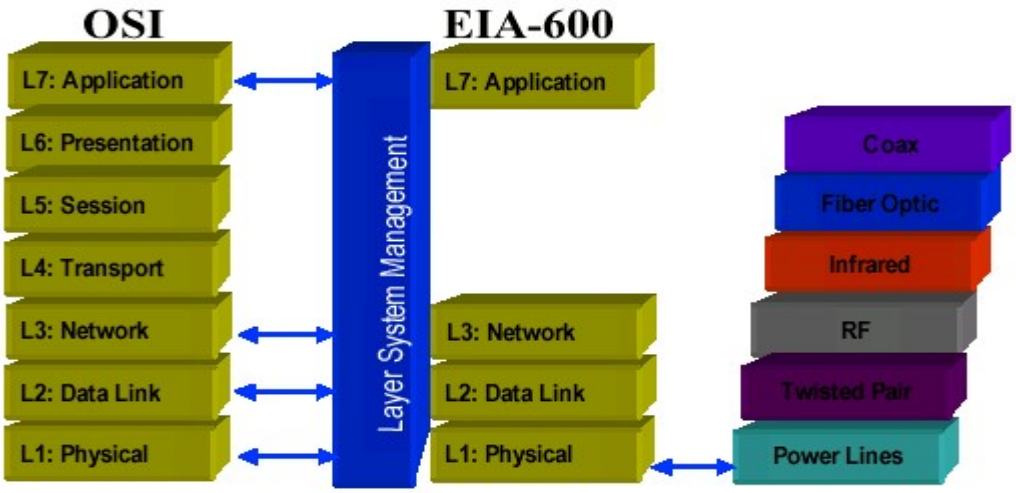
- **Resite advisory - establish a leading advisory to advise the public, private and civic sector on emerging international trends, creative branding, sustainable planning, investment strategies and economic impact of development.**

- **Resite Conference & Festival - continue to organize a leading international event with innovative and targeted workshops, films and public engagement activities. Organize in cities across Europe, Asia, the Middle East and North America.**

- **Resite Media and Collaborative Platform - develop our digital media arm and web platform to build and collaborate on urban projects**

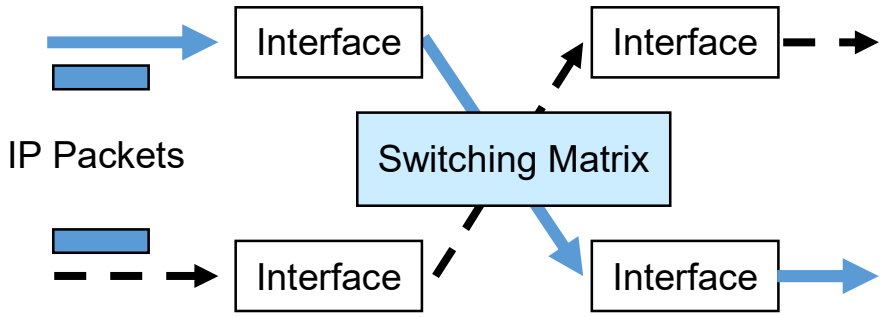
Network Technology:

- **Infrastructure-Based Networks**
  - **Pre-defined routes through the network**
  - **Nodes can directly address each other and routers forward packets appropriately**
  - **Addition of nodes changes the routing pattern**
- **Point-To-Point Networks**
  - **Every node has a connection to every other node**
  - **Communication is directly between the nodes**
  - **High overhead setting up the connections for new nodes**
- **Ad-Hoc Networks**
  - **Routes are determined "on the fly" and can change**
  - **Nodes forward signals for other nodes**
  - **Addition of nodes can be handled relatively straightforwardly**



Managed Layer Switching

- **Interfaces are intelligent**
  - **Make forwarding decisions independently**
  - **So no single processor bottleneck**
  - **Can handle forwarding decisions simultaneously, reducing processing delays**
  - **Forward packet within frame directly to outgoing interface**
  - **Can handle multiple frame forwarding simultaneously**



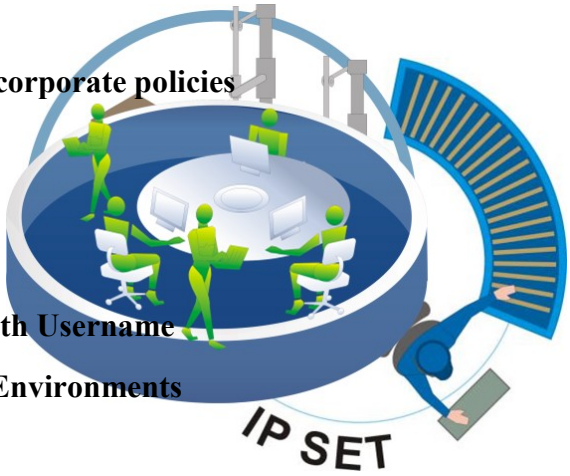
- **ASIC Technology is Receiving Competition from *Network Processors***
  - **ASICS are purely hardware**
  - **Network processors are programmable but have hardware optimized for network functions**
  - **Network processors are *slower* than ASICs but much faster than software processes on general routers**
  - **Network processors can be programmed for specific functions *less expensively* than ASICs can be built**

Firewall- Unified Threat Management:

Firewall Technology

- **Typical firewalls are effective for port blocking**
- **If a port is open it is assumed any data can pass**
- **Intrusion detection is a "reactive" approach that does not actively protect**
- **Security must be built upon deep packet inspection, AV/Spy/Intrusion prevention with dynamic updates**
- **Unified Threat Management**
- **Integration of Firewall**
    - **Deep Packet Inspection**
    - **Intrusion Prevention for blocking network threats**
    - **Anti-Virus for blocking file based threats**
    - **Anti-Spyware for blocking Spyware**
- **Faster updates to the dynamic changing threat environment and elimination of False Positives**
- **Hardened security appliance for perimeter or network core**
- **Integrated security functionality based on granular firewall policies**
- **Stateful Firewall**
- **Antivirus/Spyware**
- **Intrusion Detection & Prevention**
- **IPSec VPN / SSL VPN (v3.0)**
- **Web Content Filtering**
- **Antispam Filtering**
- **Bandwidth Shaping**
- **Consistent functionality across product family**
- **Per chassis licensing**

Why Identity? – AAA through UTM Security



- **Authentication by Username – including Wi-Fi**
- **Authorization - Access Rights based on pre-defined corporate policies**
  - **Username – Not IP Addresses**
  - **Need-to-Usebasis**
  - **Across distributed locations**
- **Accounting – Centralized Logging and Reporting with Username**
  - **Shows Who is Doing What even in Dynamic Environments**
  - **DHCP - Wi-Fi - Shared Machine Scenarios**

- **<u>Stateful Packet Inspection (SPI) is limited protection</u>**
  - **Provides source / destination / state intelligence**
  - **Provides network address translation**
  - **Stateful firewalls cannot protect against threats that are application layer based, file or email based**
- **Dynamic real-time threat scanning engine at the gateway**
  - **Anti-Virus, Anti-spyware and Intrusion Prevention**
  - **Protects Against: Viruses, spyware, worms, trojans, app vulnerabilities**
  - **External and Internal protection**
- **Reassembly-free engine**
  - **Scans & decompresses *unlimited number of files & file sizes***
- **Supports over 50 protocol types including**
  - **SMTP, IMAP, POP3 Email, HTTP – Web, FTP – File Transfer**
  - **Peer to Peer Transfers, NetBios – Intra LAN Transfers, any stream-based protocol**

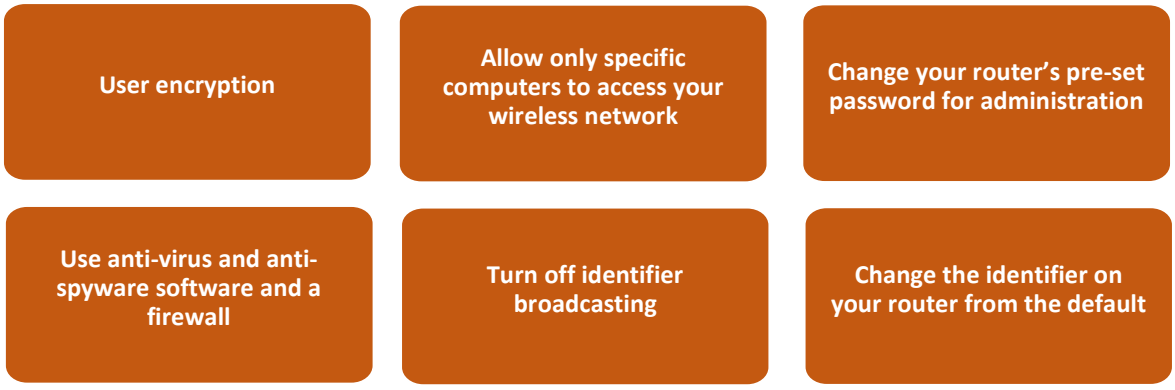
- **Updateable database by an expert signature team**

Secured Wireless

- **Wireless Technology overview**
- **The IEEE 802.11 WLAN Standards**
- **Secure Wireless LANs**
- **Migrating to Wireless LANs (Cutting the cord)**
- **A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier.**
- **The last link with the users is wireless, to give a network connection to all users in a building.**
- **The backbone network usually uses cables**

Wireless Security Overview

- **concerns for wireless security are similar to those found in a wired environment**
- **security requirements are the same:**
  - **confidentiality, integrity, availability, authenticity, accountability**
  - **most significant source of risk is the underlying communications medium**
  - **principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control**
  - **provides an authentication mechanism for devices wishing to attach to a LAN or wireless network**
  - **use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors**



Proposed design& Solution:

Complete Networking secure and protection through firewall. All data will be delivered through UTM scanning. The Wi-Fi Network shall be solely for internet access only and will be restricted to the limited user by controller.

Evolution Section and Moderate Section is having separate network independently and has no interlink between them. The independent network will have its own switching network with the restricted user they do not have any connection with outside world.