Nadar Saraswathi College of Engineering & Technology

NSCET E-LEARNING PRESENTATION

LISTEN … LEARN… LEAD…

COMPUTER SCIENCE AND ENGINEERING

IIIrd YEAR / Vth SEMESTER

CS8591 – COMPUTER NETWORKS

S C PRABANAND M.Tech
AP/CSE
Nadar Saraswathi College of Engineering & Technology,
Vadapudupatti, Annanji (po), Theni – 625531.

APPLICATION LAYER

UNIT 05

LECTURE 01

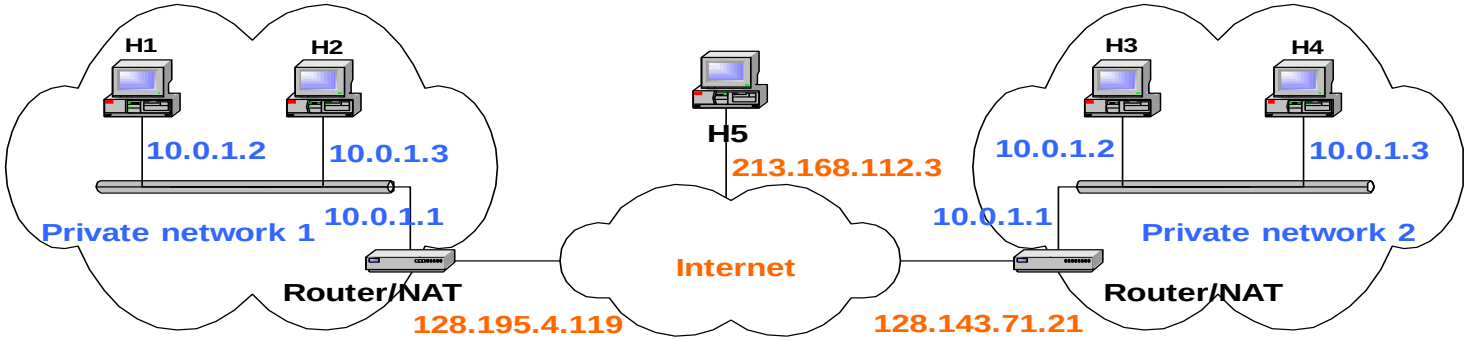
NATTING

Private vs Public IP Addresses

- Whatever connects directly into Internet must have public (globally unique) IP address
- There is a shortage of public IPv4 address
- So Private IP addresses can be used within a private network
- Three address ranges are reserved for private usage
  - 10.0.0.0/8
  - 172.16.0.0/16 to 172.31.0.0/16
  - 192.168.0.0/24 to 192.168.255.0/24
- A private IP is mapped to a Public IP, when the machine has to access the Internet

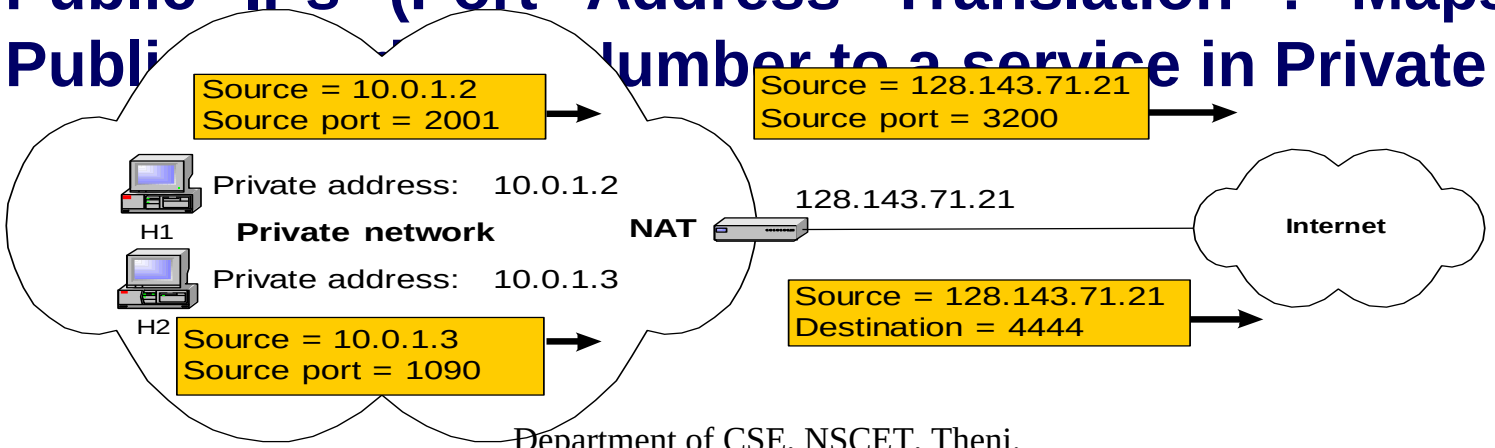
NAT

- NAT (Network Address Translation) Maps Private IPs to Public IPs
- It is required because of shortage of IPv4 Address



NAT

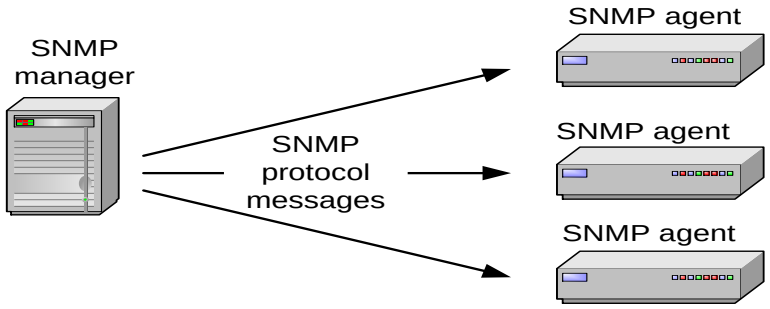
- **Static NAT : Maps unique Private IP to unique Public IP**
- **Dynamic NAT : Maps Multiple Private IP to a Pool of Public IPs (Port Address Translation : Maps a Publi... lumber to a service in Private IP)**



SNMP

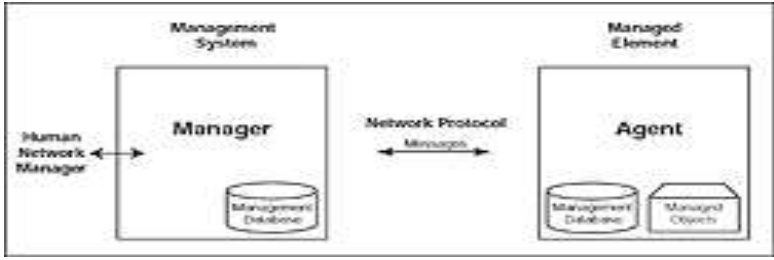
Simple Network Management Protocol

- **SNMP is a framework that provides facilities for managing and monitoring network resources on the Internet.**
- **Components of SNMP:**
  - SNMP agents
  - SNMP managers
  - Management Information Bases (MIBs)
  - SNMP protocol itself



SNMP

- SNMP is based on the manager/agent model consisting of a manager, an agent, a database of management information, called as MIB.
- The manager provides the interface between the human network manager and the management system.
- The agent provides the interface between the manager and the physical device(s) being managed.



SNMP

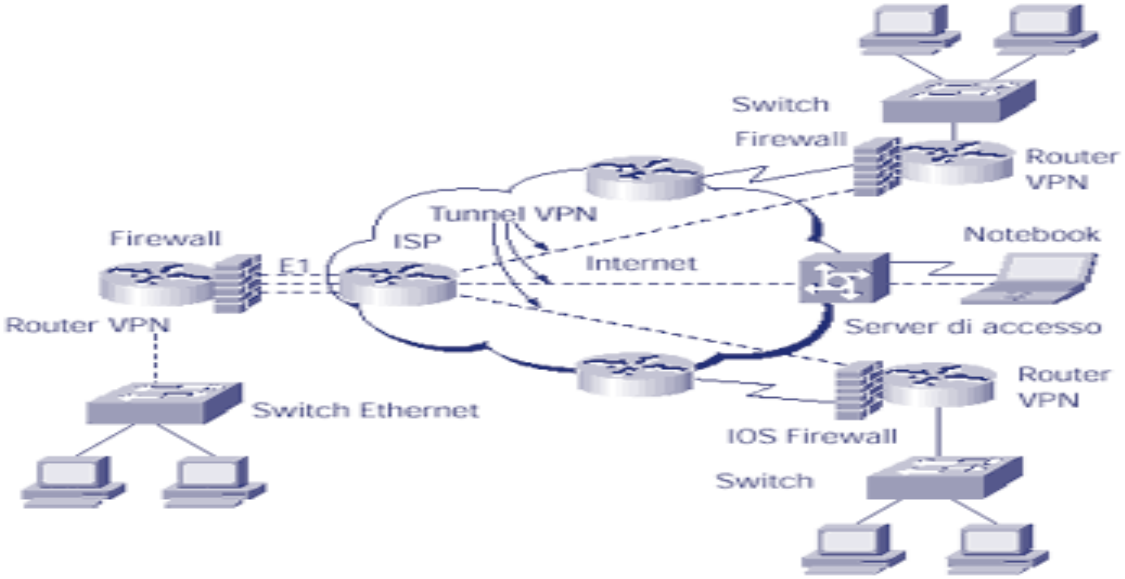
- SNMP uses five basic messages (GET, GET-NEXT, GET-RESPONSE, SET, and TRAP) to communicate between the manager and the agent.
- The GET and GET-NEXT messages allow the manager to request information for a specific variable. The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the manager with either the information requested or an error indication as to why the request cannot be processed.
- A SET message allows the manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. The agent will then respond with a GET-RESPONSE message indicating the change has been made or an error indication as to why the change cannot be made.
- The TRAP message allows the agent to spontaneously inform the manager of an 'important' event.

VPN

VPN

- VPN is a private connection between two systems or networks over a shared or public network (typically Internet).
- VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies.
- In other words, VPN turns the Internet into a simulated private WAN.
- VPN is very appealing since the Internet has a global presence, and its use is now standard practice for most users and organizations.

VPN


Switch
Firewall
Router
VPN
Tunnel VPN
Firewall
ISP
E1
Internet
Notebook
Router VPN
Server di accesso
Router
VPN
Switch Ethernet
IOS Firewall
Switch

How VPN Works

- **To use the Internet as a private Wide Area Network, organizations may have to address two issues :**
  - First, networks often communicate using a variety of protocols, such as IPX and NetBEUI, but the Internet can only handle TCP/IP traffic. So VPN may need to provide a way to pass non-TCP/IP protocols from one network to another.
  - Second data packets traveling the Internet are transported in clear text. Therefore, anyone who can see Internet traffic can also read the data contained in the packets. This is a problem if companies want to use the Internet to pass important, confidential business information.

How VPN Works

- VPN overcome these obstacles by using a strategy called Tunneling. Instead of packets crossing the Internet out in the open, data packets are fist encrypted for security, and then encapsulated in an IP packet by the VPN and tunneled through the Internet.
- The VPN tunnel initiator on the source network communicates with a VPN tunnel terminator on the destination network. The two agree upon an encryption scheme, and the tunnel initiator encrypts the packet for security.

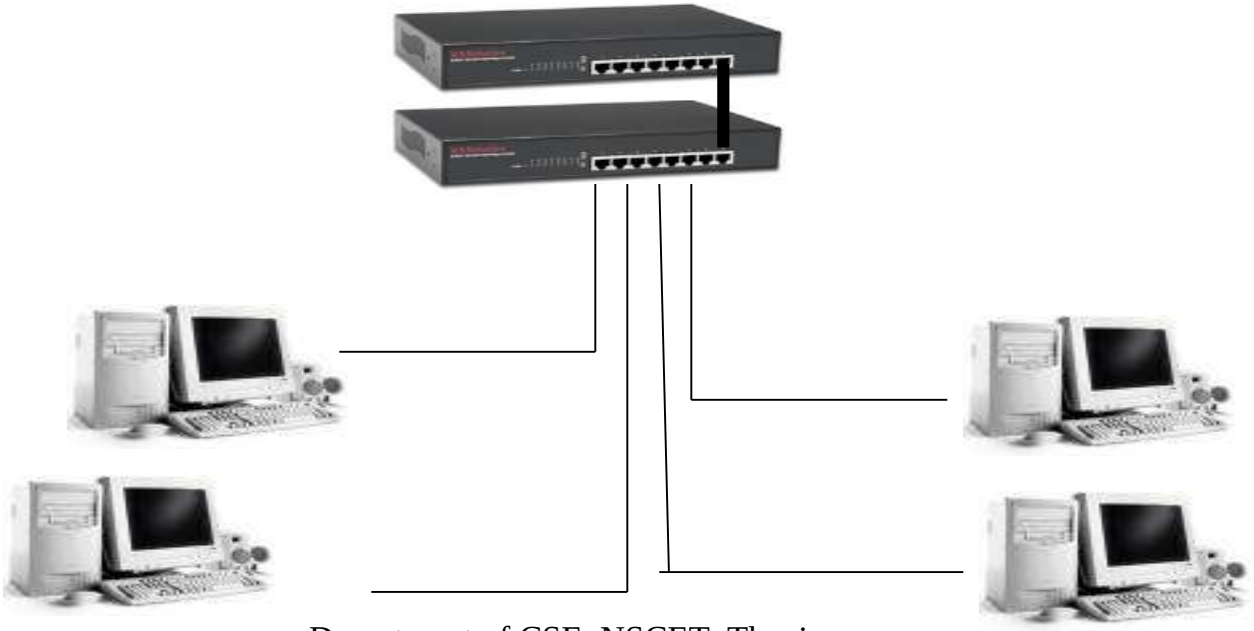
Advantages of Using VPN

- VPN technology provides many benefits. Perhaps the biggest selling point for VPN is cost savings. One can avoid having to purchase expensive leased lines to branch offices or partner companies. On another cost-related note, you can evade having to invest in additional WAN equipment and instead leverage your existing Internet installation.
- Another benefit of VPN is that it is an ideal way to handle mobile users.

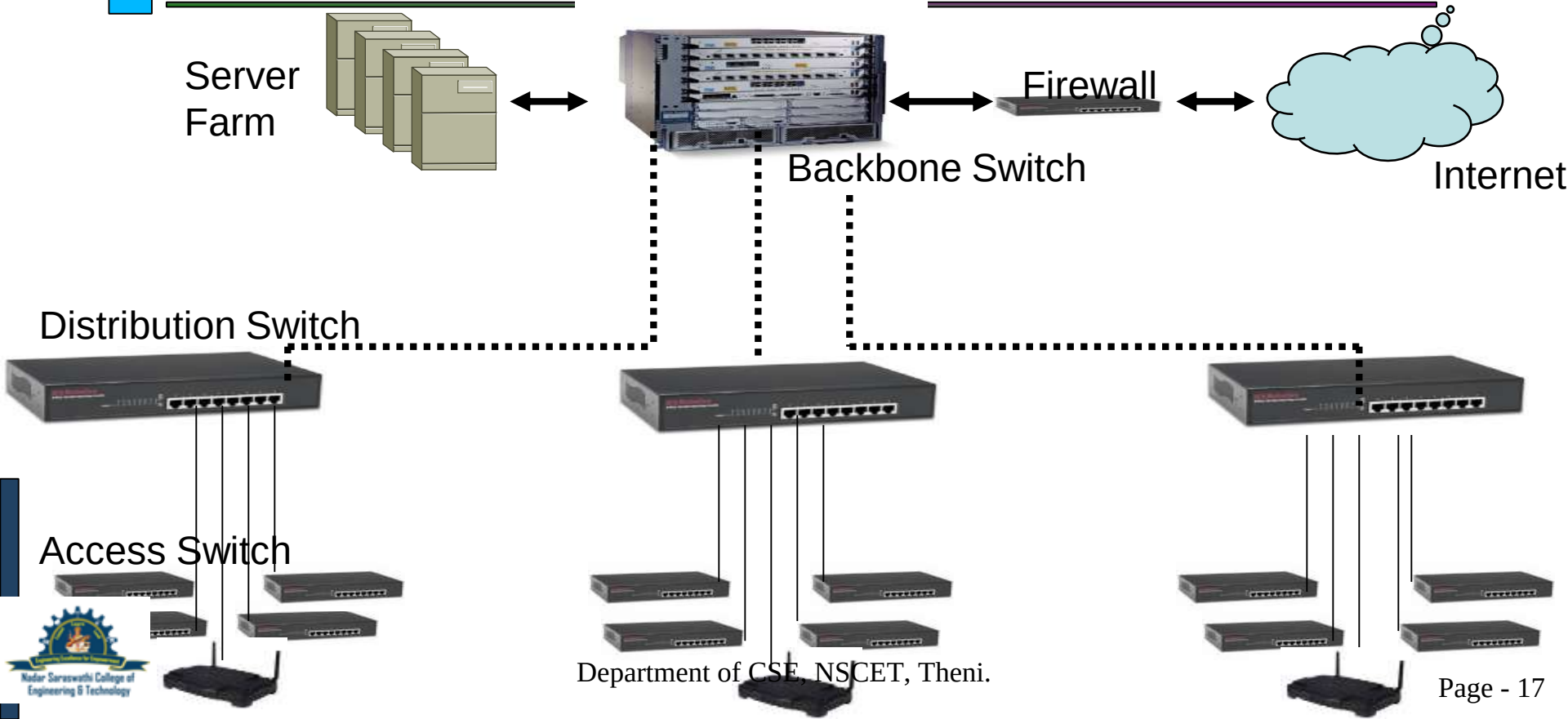
ENTERPRISE NETWORK IMPLEMENTATION

Small Office Network

- Use Unmanaged 10/100 Switches
- Use Enhanced Cat 5 Pathcords



Campus Network Architecture



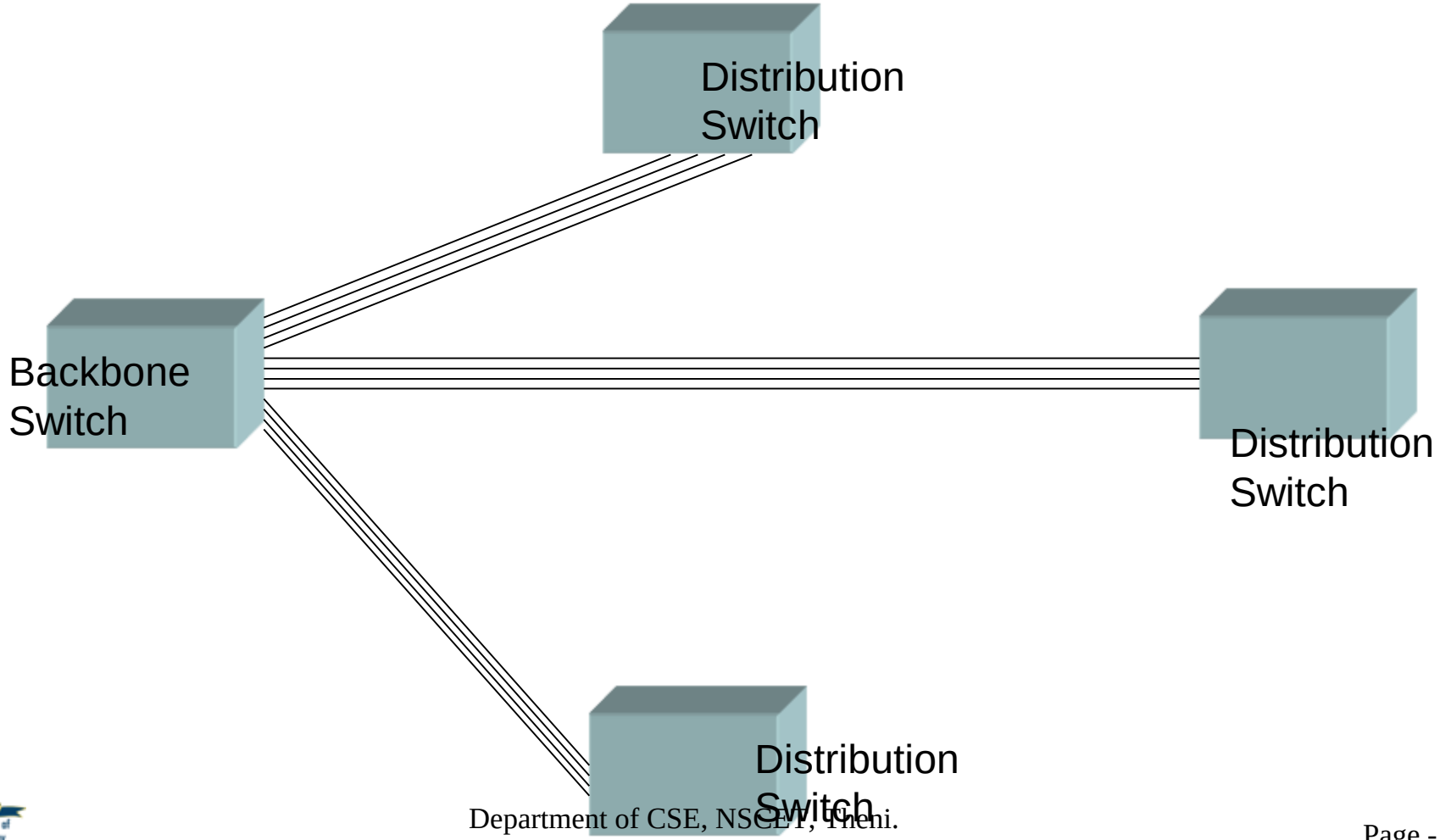
Campus Network Architecture

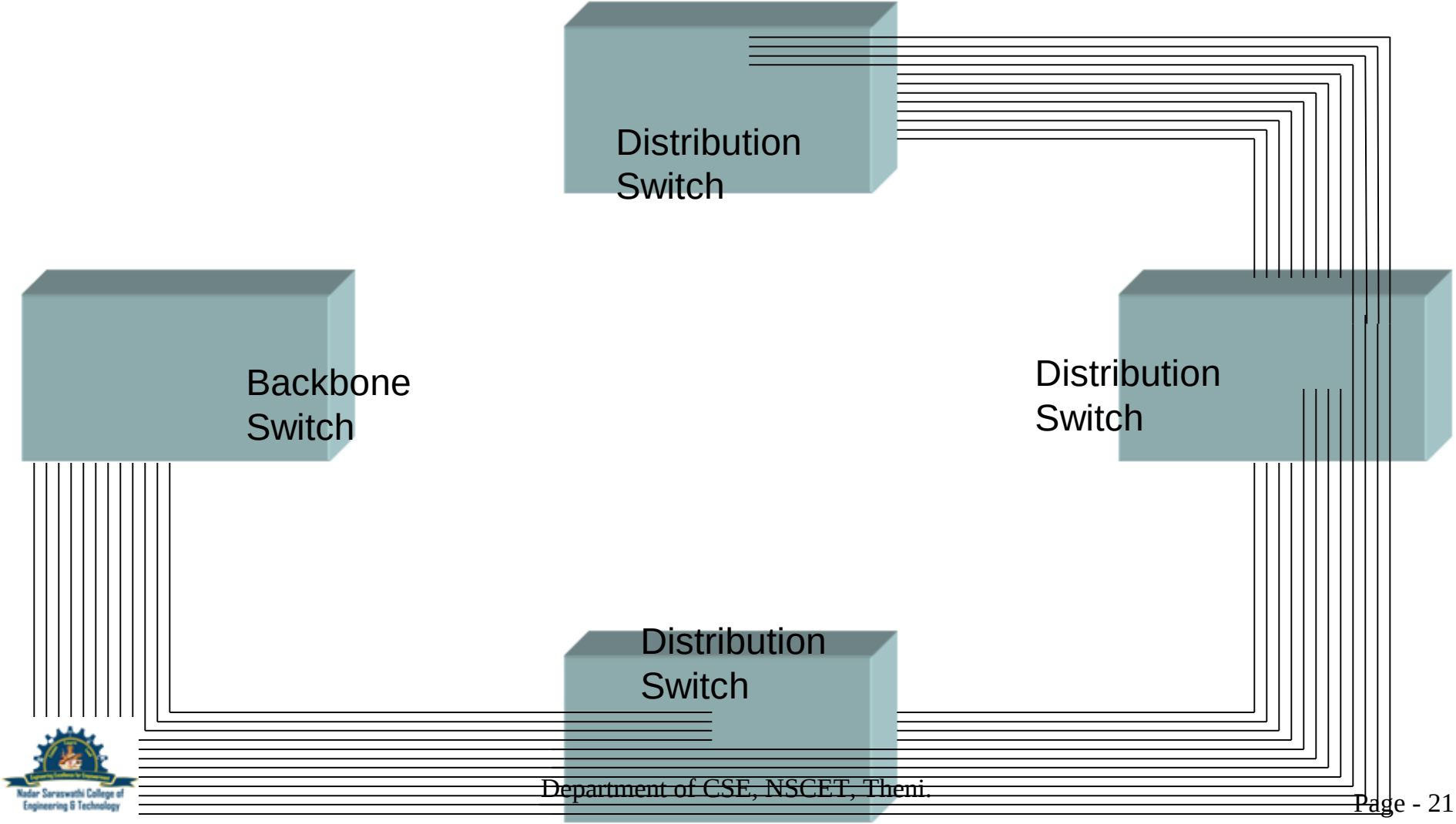
- **Uses Three Tier Switching Architecture (Popularly known as Cisco's Switching Architecture)**
- **Backbone Switch**
  - Layer 3/4 Chassis based switch
  - Multiple 100Fx or 1000SX/LX or 10GLX/LH ports for connectivity to Distribution switches
  - Multiple 10/100/1000 ports for connectivity to Servers
- **Distribution Switch**
  - Layer 2/3 Managed Fixed configuration switch
  - 1/2 100Fx or 1000Sx/Lx or 10GLX/LH ports for connectivity to the Backbone switch
  - Multiple 10/100 or 10/100/1000 ports for connectivity to the Access switches
- **Access Switch**
  - Layer2 Managed/Unmanaged Fixed configuration switch
  - Multiple 10/100 or 10/100/1000 ports for desktop connectivity

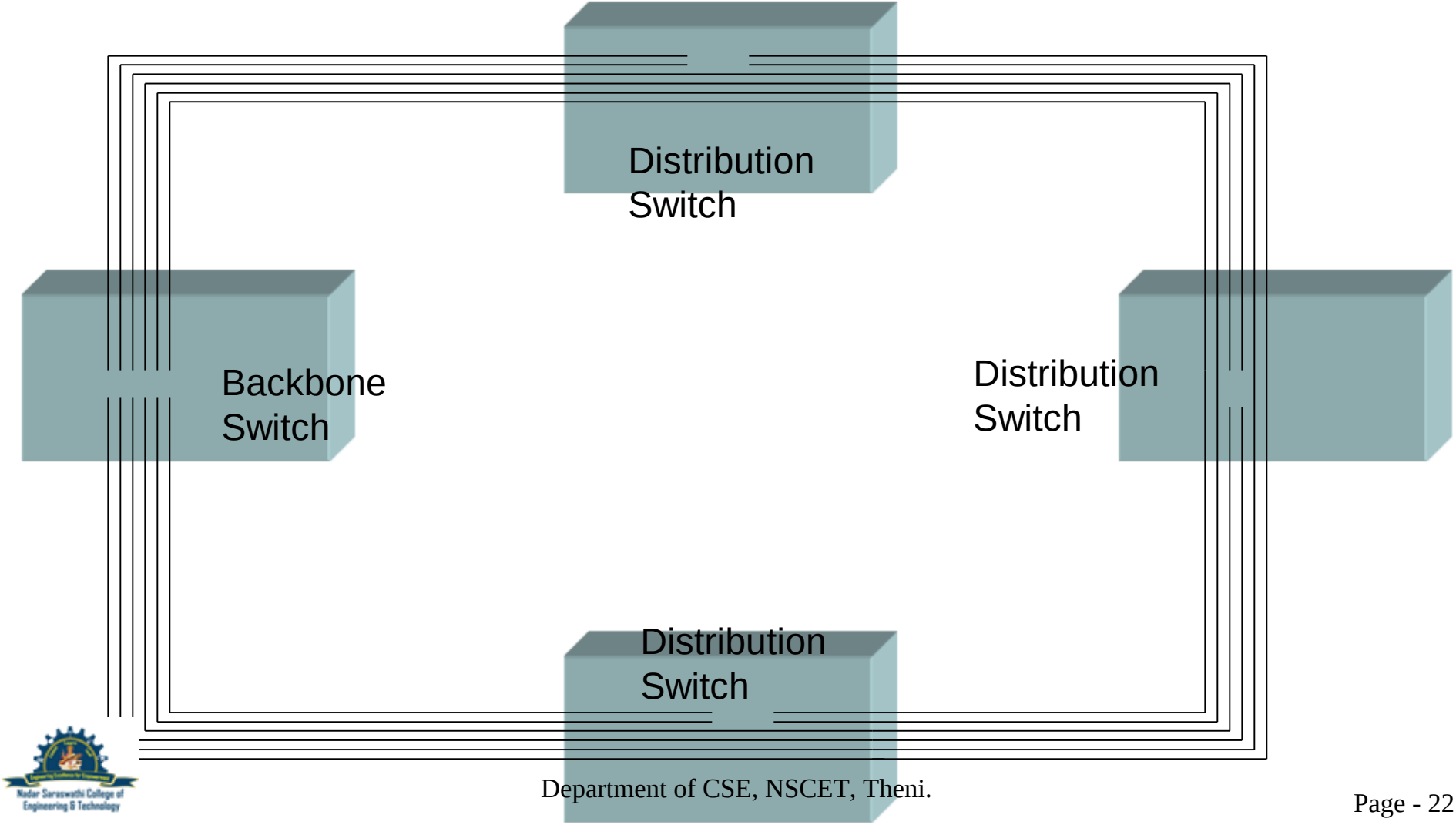
Campus Network Cabling

- **Campus backbone cabling**—This is typically single- or multimode cable that interconnects the central campus Backbone Switch with each of the building Distribution Switches. Typically Ring Architecture is used to connect the Backbone switch to the Distribution switch to provide redundant routes.

- **Building backbone cabling**—This is typically Category 5e or 6 UTP cable that interconnects the building distributor with each of the floor distributors in the building.
- **Horizontal cabling**—This is predominantly Category 5e or 6 UTP cabling.


Distribution
Switch
Backbone
Switch
Distribution
Switch
Distribution
Switch


Distribution
Switch
Backbone
Switch
Distribution
Switch
Distribution
Switch


Distribution
Switch
Backbone
Switch
Distribution
Switch
Distribution
Switch

Campus Network

- The residential connectivity can be provided on Ethernet/Dial-up/ADSL.
- The Internet connectivity can be provided on leased line.

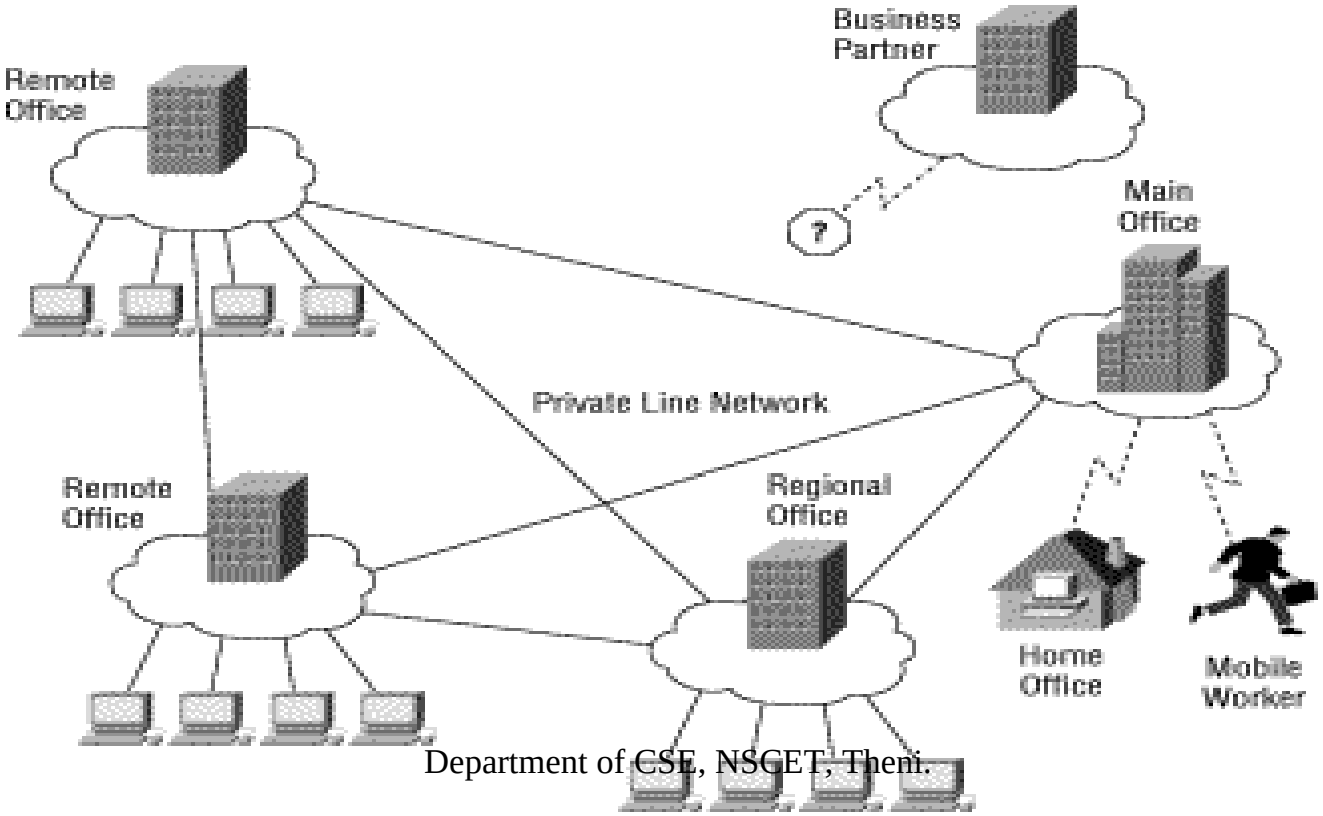
Enterprise WAN Architecture

- **A typical scenario will have Corporate Headquarter connected to Remote Offices** (Branch Offices, Retail Counters etc.)
- **The Remote offices would be interconnected to the corporate office through**
  - **A dedicated network implemented over Leased-Lines and/or IPLC** (International Private Leased Circuit) (Microsoft, IBM, Cisco, Infosys etc.)
  - **A dedicated network implemented over VSAT** (Banks' ATM Network, Reserve Bank network, BSE Online Trading, NSE Online Trading etc.)
  - **VPNs on the Internet** (Asian Paint Supplier Network, Bajaj Auto Retail Network etc.)
  - **A mix of above technologies**
- **The backup links may provided through**
  - **Redundant route through an alternate leased line**
  - **Dial backup on ISDN** (The Head Office has a PRI connectivity and the Remote offices have BRI connectivity)

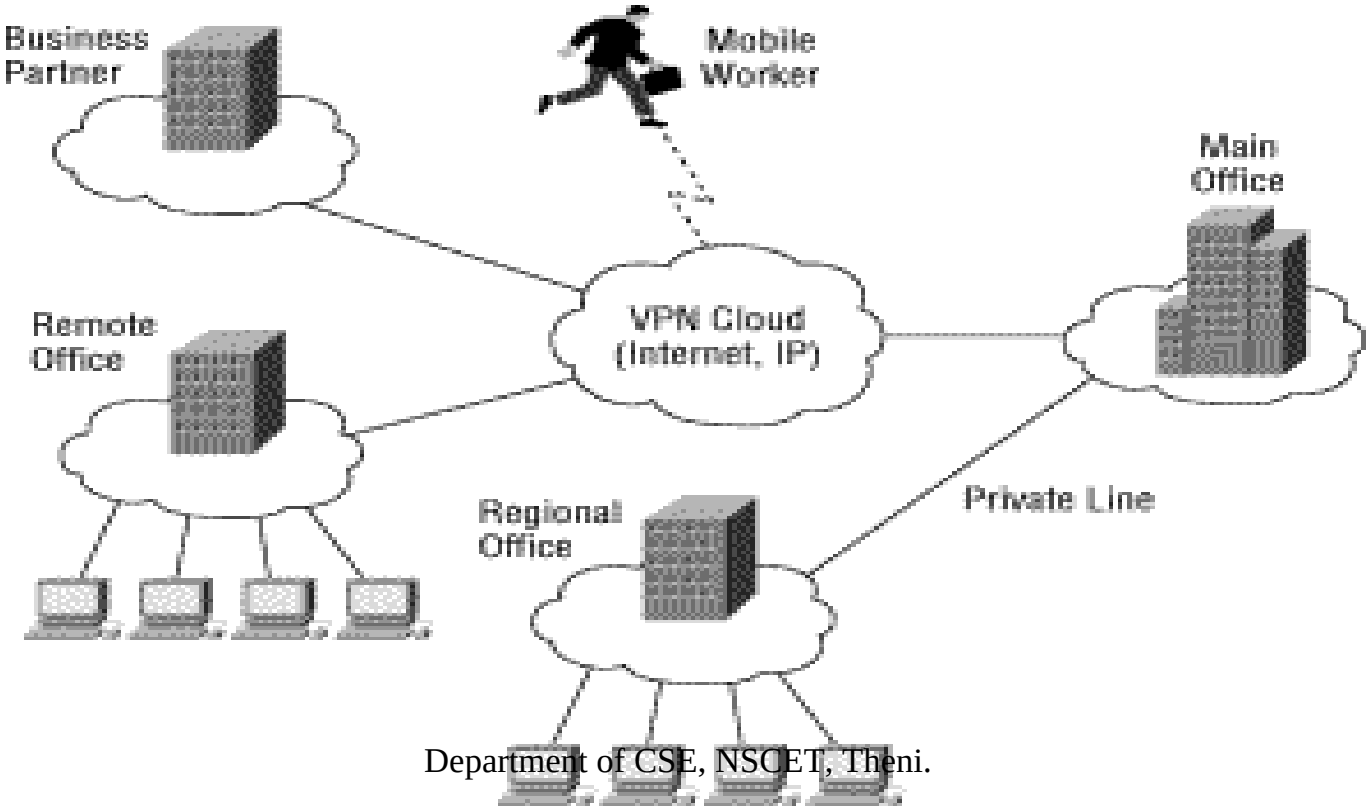
Enterprise WAN Architecture

- **The Disaster Recovery site would be connected through multiple links to the main site**
- **VoIP infrastructure may be available** (A Call Manager will be placed at the Head Office and VoIP phones would be available in all the offices)
- **The NOC** (Network Operation Center) **may be at the Head Quarter** (Infosys) **or at a remote site** (Reliance, Microsoft)
- **The NOC maintains, monitors and manages the network and application servers.**
- **The Data exchange between offices may be through the servers at NOC to ensure security**

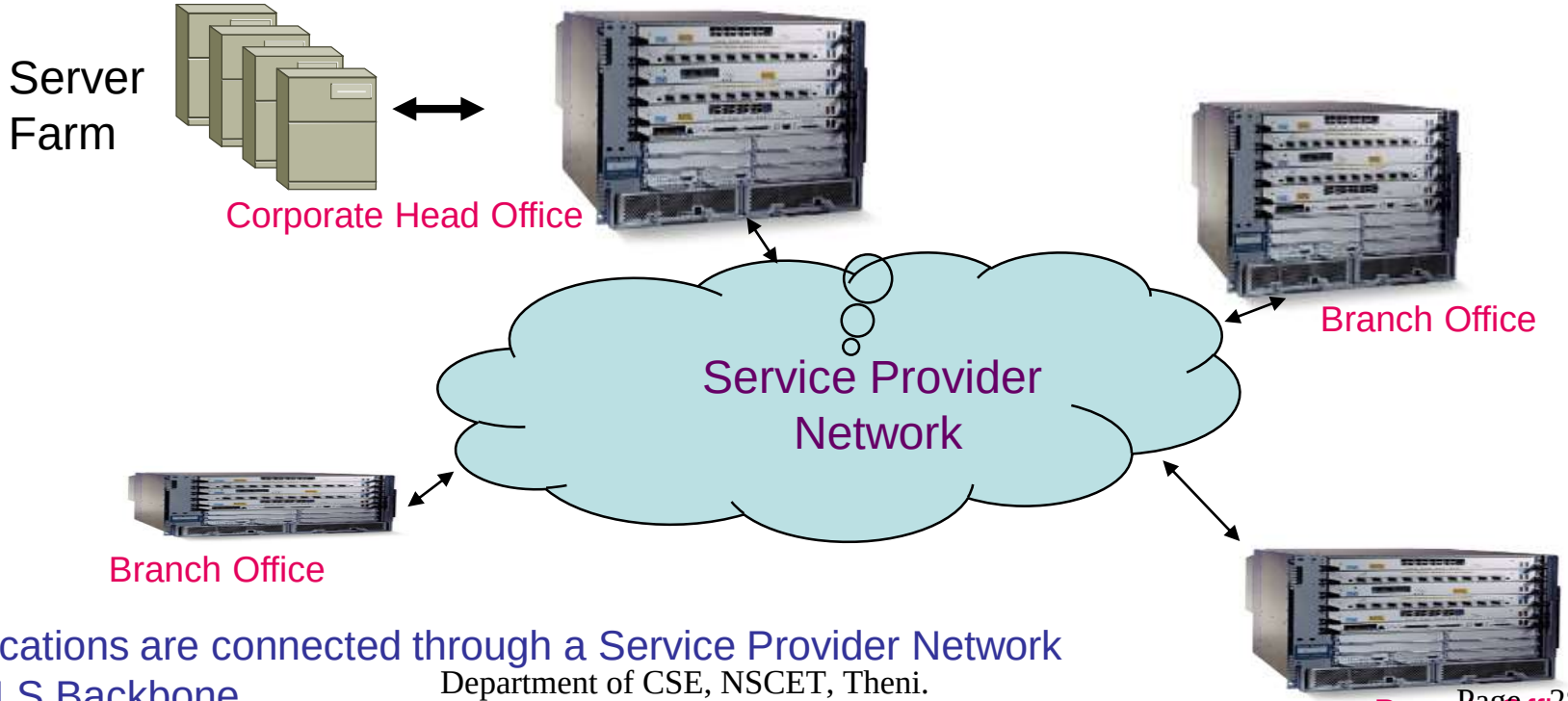
Enterprise WAN Network



Enterprise WAN Network



Enterprise WAN



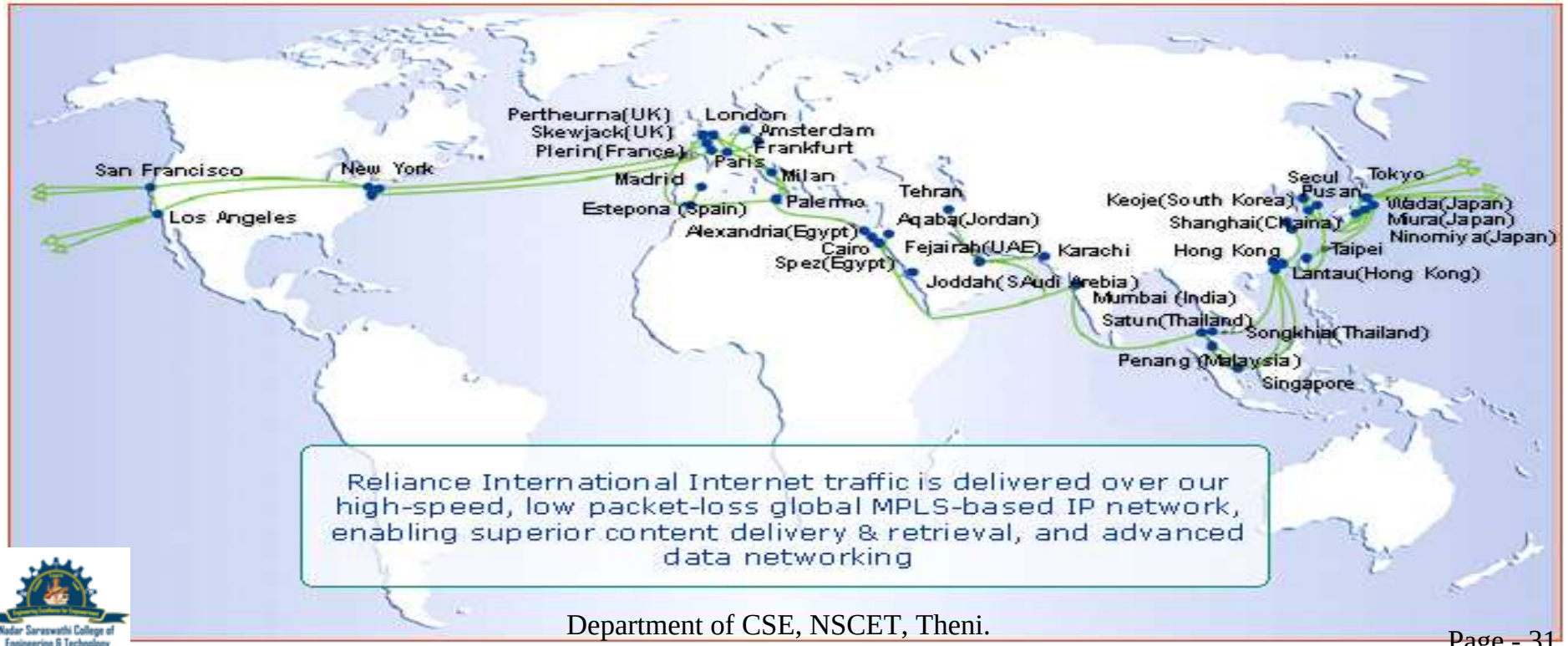
e locations are connected through a Service Provider Network
MPLS Backbone

Service Provider Networks: Reliance

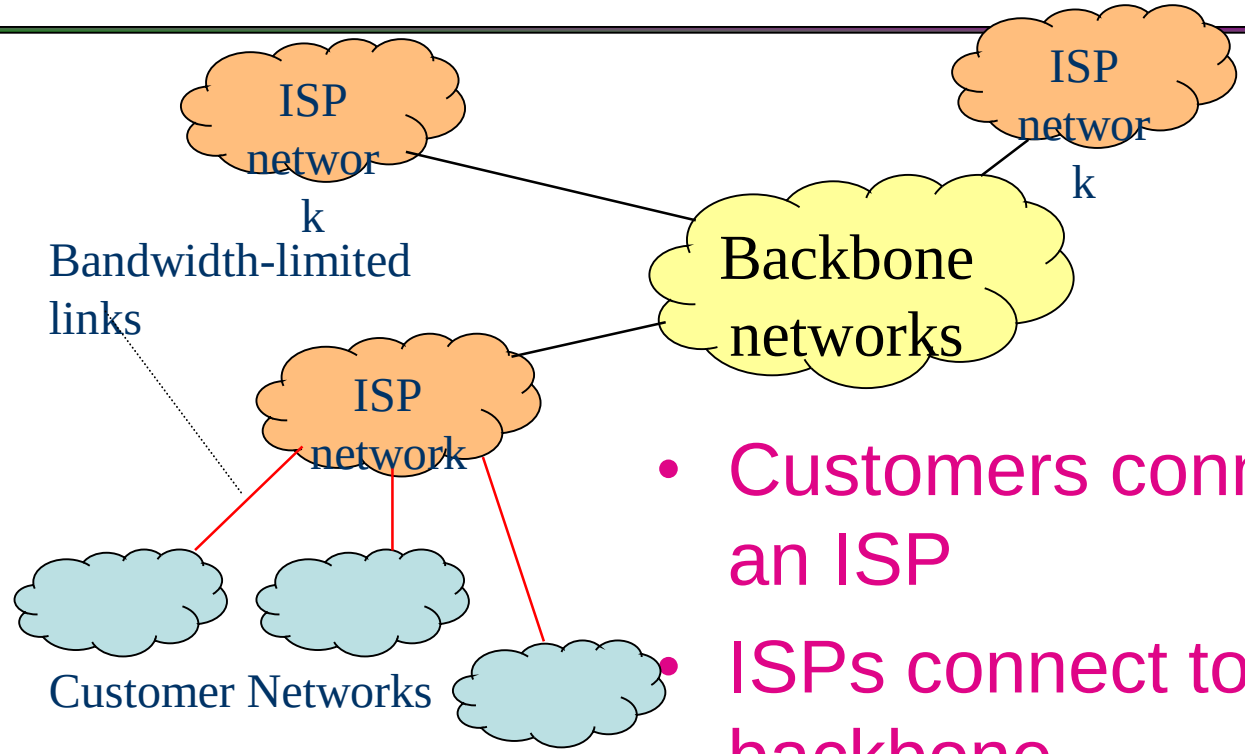
- Reliance Data Centers, are connected to 132 countries across 4 continents spanning US, UK, Mid-east and Asia-Pac through Flag Telecom backbone (Reliance Infocomm 's group company) and other undersea cable systems like Se-Me-Wea-3 and i2i and are having public / private peering relationship with large Tier 1 ISPs and content providers at more than 15 Internet Exchange points across the globe. There also exists peering relationship with other popular domestic ISPs on STM-1 bandwidth levels.
- The data centers further are connected to Reliance's country wide optic fiber based IP network with terabytes of capacity having points of presence at more than 1100 cities. Customers' can access the Internet by connecting to any of these 1100 PoPs using multiple means like local dedicated leased lines, PSTN -ISDN dialup links OR simply by using Reliance's 3G CDMA mobile services.
- The Reliance Data Centers at various locations are also interconnected through redundant fiber ring with bandwidth capacity of STM-4 for data replication purposes for providing Disaster Recovery services.

Service Provider Networks: Reliance

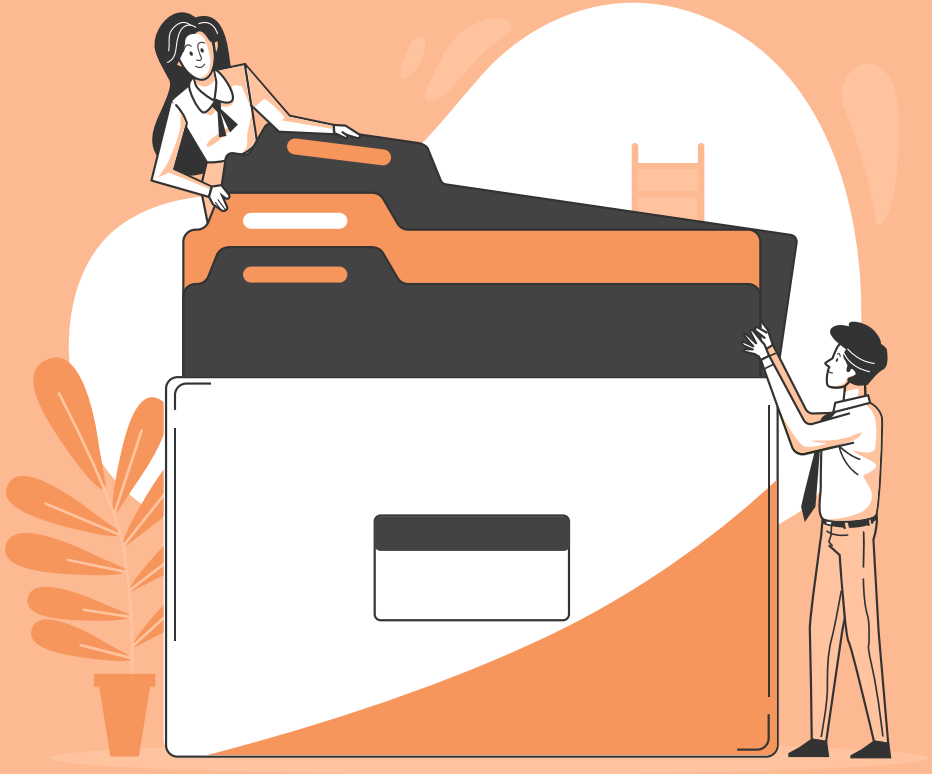
Service Provider Networks: Reliance



Service Provider Networks



- Customers connect to an ISP
- ISPs connect to backbone



THANKS!

Does anyone have any questions?
scprabanand@gmail.com.com
scprabanand.weebly.com