What is Critical Infrastructure?

- Critical Infrastructure (CI) or Critical National Infrastructure (CNI) are the systems, assets and services upon which society and the economy depend
  - Energy and utilities
  - Information Technology and Telecommunications
  - Critical Services (food, health care, financial)
  - Transportation
  - Government and Emergency Services
  - Etc.

- Critical Infrastructures are expected to be reliable with high availability

- Current PSTN infrastructure is highly available – can VoIP provide similar availability?
PSTN Architecture

Causes of Telecom Network Outages

- According to NIST study of FCC outage data main causes in decreasing order of occurrence
  - Accidents
    - cable cuts, car wreck, etc.
  - Human errors
    - incorrect maintenance, installation
  - Environmental hazards
    - fire, flood, etc.
  - Sabotage
    - physical, electronic
  - Operational disruptions
    - schedule upgrades, maintenance, power outage
  - Hardware/Software failures
    - Line card failure, faulty laser, software crash, etc.
Network Survivability

• Definition
  – Ability of the network to support the committed Quality of Services (QoS) continuously in the presence of various failure scenarios

• Survivability Components
  – Analysis: understand failures and system functionality after failures
  – Design: adopt network procedures and architecture to prevent and minimize the impact of failures/attacks on network services.
  – Goal: maintain service for certain scenarios at reasonable cost
    • Not only connectivity
    • But also QoS guarantee: call blocking
  • Self – Healing network

Survivable Network Design

• Three steps towards a survivable network
  1. Prevention:
    – Robust equipment and architecture (e.g., backup power supplies)
    – Security (physical, electronic), Intrusion detection, etc.
  2. Topology Design and Capacity Allocation
    ▪ Design network with enough resources in appropriate topology
    ▪ Spare capacity allocation – to recover from failure
  3. Network Management and traffic restoration procedures
    ▪ Detect the failure, and reroute traffic around failure using the redundant capacity
Survivability – Basic Concept

- **Working path** and **Backup path** (Protection path):
  - **Working path**: carry traffic under normal operation
  - **Backup path**: an alternate path to carry the traffic in case of failures

![Diagram showing working and backup paths]

Survivability – Basic Concept

- To survive against a network failure
  - working path and backup path must be **disjoint**
  - So that both paths are not lost at the same time

- **Disjoint = ?** (depending on a failure assumption)
  - Link disjoint
  - Node disjoint
  - (Shared Risk Link Group) SRLG disjoint

![Diagram showing link and node disjoint]

![Diagram showing SRLG disjoint]
Shared Risk Link Group (SRLG)

- Two fiber cables share the same duct or other common physical structure (such as a bridge crossing).
- Two cables can be failed simultaneously

Survivability Techniques

- Path-based (Global) versus Link-based (Local)
- Dedicated-Backup versus Shared-Backup Capacity
- Protection versus Restoration
- Ring versus Mesh topology
- Dual homing
- $P$ cycle
Path-based versus Link-based

- Path-based Scheme (Global)
  - Disjoint alternate routes are provided between source and destination node

- Link-based Scheme (Local)
  - Alternate routes are provided between end nodes of the failed link
### Dedicated versus Shared - Backup

- **Dedicated-Backup Capacity**
  - Backup resource can be used only by a particular working path
- **Shared-Backup Capacity**
  - Backup resource between several working paths can be shared
  - Rule: backup resource can be shared only when corresponding working paths are not expected to fail at the same time
  - More capacity efficient

![Diagram of network with working paths and backup paths]

- **WP1** (traffic 5 units)
- **WP2** (traffic 10 units)
- **BP1**
- **BP2**

- **link5-7**:
  - dedicated spare capacity = 15 units
  - shared spare capacity = 10 units

### Protection versus Restoration

- **When to establish the backup paths?**
- **Protection**
  - Backup paths are fully setup before a failure occurs.
  - When failure occurs, no additional signaling is needed to establish the backup path
  - Faster recovery time
- **Restoration**
  - Backup paths are established after a failure occurs
  - More flexible with regard to the failure scenarios
    - backup paths are setup after the location of failure is known
  - More capacity efficient
    - due to its shared-backup nature,
    - Utilize any spare capacity available in the network
  - But cannot guarantee 100% restorability after failures
Protection Switching Variations

- **Automatic Protection Switch (APS)**
  - Provide a mechanism for link-failure tolerance.
- **APS 1:1**
  - One standby cable for each working cable
- **APS 1:N**
  - One standby cable for N working cable
- **APS/DP (APS with diverse protection)**
  - Standby cable is placed on a different physical route than the working cable
  - Fully restorable APS/DP system requires 100% capacity redundancy.

Mesh Network

- **WDM Optical Networks - lightpath**
- **Example:**

  ![Mesh Network Diagram](attachment:image.png)
**Dedicated-path Protection**

- \( A_i \) is an availability of link \( i \)
- Availability of a connection between S-D:
  \[
  A_{\text{no-protection}} = \prod_{i \in \text{WP}} A_i
  \]
  \[
  A_{\text{protection}} = \prod_{i \in \text{WP}} A_i + \prod_{i \in \text{BP}} A_i - \prod_{i \in \text{WP} \cap \text{BP}} A_i
  \]
  - Given \( A_i = 0.998297 \),
    - \( A_{\text{no-protection}} = 0.996597 \),
    - \( A_{\text{protection}} = 0.999983 \)

**Self-healing Rings (SHRs)**

- SHR is a topology connecting a set of nodes by one (or more) rings.
- Two types of SHRs:
  - Uni-directional ring (USHR)
    - Nodes are connected to two rings forwarding traffic in opposite direction.
  - Bi-directional ring (BSHR)
    - Four rings are used as two working and two standby routes.
    - An extension to 1:1 APS
Types of Self-healing Rings

1:1 Bi-directional self-healing ring (BSHR)

1:1 Uni-directional self-healing ring (USHR)

Dual-homing and Multi-homing

• Dual-homing
  – Customer host is connected to two switched-hubs.
  – Traffic may be split between primary and secondary paths connecting to the hubs.
  – Each path is served as a backup for another.

• Multi-homing
  – Customer host is connected to more than two switched hubs.
  – Greater protection against a failure.
### Dual/Multi-homing Topologies

#### Dual-homing topology

#### Multi-homing topology

### Dual-homing Restoration Capability

- Dual-homing doesn’t accomplish restoration by itself, must be used in conjunction with dynamic restoration techniques.

- 100% restoration can be achieved for a single link or a single switch failure via path rearrangement given that there is enough spare capacity at the link to alternate switched hub.

- Dual-homing approach guarantees surviving connectivity, but it may take time to restore priority circuits via path rearrangement.
**p-Cycles: Basics**

- For meshed networks
- Pre-reserved protection paths (before failure)
- Based on cycles, like rings
- Also protects *straddling* failures, unlike rings
- Local protection action, adjacent to failure (in the order of some 10 milliseconds)
- Shared capacity

- “pre-configured protection cycles” → *p*-cycles
- Developed in Canada at TR Labs

---

**p-Cycles: Basics**

- A single *p*-cycle in a network:
p-Cycles: Basics

- Protected spans:
- 9 "on-cycle" (1 protection path)
- 8 "straddling" (2 protection paths)
Transport Survivability

- Number of techniques exist
  - Automatic Protection Switching (APS)
  - Multi-homing (with or without trunk diversity)
  - Link restoration
  - Path restoration
  - Self healing rings
  - p-cycles
- See a mixture of techniques in real networks
- Usually little or no survivability at the far edge (CPE – last mile)

Failure in IP Backbones

Source: University of Michigan, 2000

Link Failure
- Congestion results from long time to recover
  - 32%

Router Failures
- Software failures
- Hardware failures
- DOS Attacks
  - 23%

Other Unknown
  - 9%

Router Operations
- Software Upgrade
- Hardware Upgrade
- Configuration Errors
  - 36%
Failures

- Failures are frequent in IP networks
  - Software failures, line card resets/failures, etc
- Example according to Sprint
  - Network topology is very dynamic
    - Links are reported down every 30 minutes on average
    - In 80% of the cases links come back up in <10 min
Equipment Reliability

- Routers, routing protocols, and management thereof must be highly available and secure
- Core and Edge Routers and becoming more reliable with adoption of fault tolerant hardware architectures
  - (hot swappable line cards, backup switch cards, redundant cooling, power, etc)
- Software failures a major concern
  - many more lines of code in comparison to OXC or Telco switch – redundancy improvement??
- Service/upgrade downtime needs improvement

Survivability Options

- Several techniques to improve survivability
- IP layer –
  - adjust link weights and timers for faster failure recovery
  - prestore second shortest paths, etc,
- Adopt Optical Transport techniques from Telco operators (survivable rings, APS, path restoration, etc.)
- MPLS logical layer restoration
IP Dynamic Routing

- OSPF or IS-IS computes path
- If link or node fails, New path is computed
- Response times: Typically a few seconds
  - Can be tuned to ~1000’s milliseconds
  - According to Sprint data – usually ~ 7secs to recover
  - Too Long for VoIP – PSTN will hang up if VoIP/ PSTN call

Backup Label Switched Paths

- Primary & backup LSPs established a priori
- If primary fails
  - Signal to head end, Use backup
- Faster response, requires wide area signaling
MPLS Fast Reroute

- Increasing demand for “APS-like” redundancy
  - MPLS resilience to link/node failures
  - Control-plane protection required
  - Avoid cost of SONET APS protection

- Solution: MPLS Fast-reroute
  - RSVP Extensions define Fast Reroute
  - LSPs can be set up, a priori, to backup:
    - One LSP across a link and optionally next node, or
    - All LSPs across a particular link

1:1 Protection

- For each LSP, for each node
  - Set up one LSP as backup
  - Merge into primary LSP further downstream
  - Backs up link and downstream node
**1:1 LSP Protection**

Traffic uses detour LSP

Link Fails

Merged Downstream

**1:N Link Protection**

- For each link, for each neighbor
  - Set up one detour LSP to backup the link
  - Uses LSP Hierarchy to backup all LSPs which were using failed link

Multiple Primary LSPs on same link

One detour LSP for link
1:N Link Protection

Primary LSPs multiplexed over one detour LSP
LSPs demultiplexed at next node

1:N Link and Node Protection

- For each link
  - For each node 2 hops away
    - Detour LSP backs up link & intermediate node
    - Uses LSP Hierarchy to backup all LSPs to that node
    - If there are two 2-hop paths to that node, setup two detour LSPs
  - For each node 1 hop away
    - Detour LSP backs up LSPs ending at that node
MPLS Fast Reroute

- Provides fast recovery for LSP failure
  - Based on a priori backup of detour LSPs
  - (eg, ~5 millisecond for tens of LSPs with 1:1)
- There are significant tradeoffs between the approaches
  - Number of LSPs required
  - Whether node failures are protected
  - Ability to reserve resources for backup LSPs
  - Optimality of routes

Summary of MPLS Methods

- End-to-End backup LSPs
- MPLS Fast Re-Route
  - 1:1 LSP protection
  - 1:N Link protection
  - 1:N Link plus node protection
- All of these are interoperable based on IETF standards
- Sink Trees are under study
- Does MPLS solve all the problems???
Multilayer Networks

- Backbone networks have multiple technology layers
  - Converging toward IP/MPLS/WDM
- Multiple Layers present several survivability challenges
  - Coordination of recovery actions at different layers
    - Which layer is responsible for fault recovery?
  - Spare Capacity Allocation (SCA)
    - How to prevent over allocation, when each layer provides spare resources?
  - Failure Propagation between layers
    - Lower layer failure can affect multiple higher layer links!

Resilient Edge Connectivity

- Multi-Homing for resilient Internet and IP-VPN connectivity
  - Stub network with backup access (static routing)
  - Multi-Homed Network with load sharing
Link Redundancy

- **Link Bundling**
  - Link failure does not affect forwarding
  - Load redistributed among other members
- **Parallel Link Technologies**
  - MLPPP – T1/E1 Link aggregation
  - 802.3ad – Ethernet aggregation
  - SONET/SDH aggregation
  - Multi-Link Frame Relay

Optical Protection

- **Protection switching with ADM**
  - Redundant routers share uplink
- **Rapid circuit failure recovery**
  - Used on router-to-ADM links
  - 50 ms at physical layer
  - Faster than layer 3 routing protocol convergence
- Interoperable with standard ADM
- **Working & protect circuits**
  - May reside on different routers
  - May reside on same router
Virtual Router Redundancy Protocol

• Redundant default gateways: VRRP (RFC 2338)

Multiple routers on the subnet negotiate who will be “Master” and own the Virtual Router IP Address.

Master sends periodic hellos to communicate alive state.

All other routers are backups. Backup priority is configurable.

Hosts are preconfigured with Virtual Router IP address as default for traffic exiting the LAN.

Master Back-up

Ethernet Switch

Host

Host

Host

Host

FE

GE

FE

GE

FE

FE

Summary

• VoIP Availability can be greatly improved by adopting
  – Reliable network components
  – Stable survivable network design
  – Protocols configured for quick recovery
  – Also need defined procedures for reporting and resolution of outages.

• Cost is an issue
  – VoIP the most demanding application in terms of Availability? Can cost be justified?
VoIP Trends

• Market Situation
  – Deregulation and competitive Voice environment
  – Many ISP have built out network with QoS support
    • Diff Serve or MPLS
  – Businesses are considering VoIP
    • Economist Magazine Survey of 254 executives on corporate networking notes
    • 43% report they are using, testing or planning to implement VoIP within the next two years
    • Concerns: Quality, Availability, Features (new and PSTN)
  – Significant Cost advantages to VoIP
    • AT&T study: Business ROI positive if phone bill greater than $350 month or 3 cents/minute or $50 month international calls
    • In some cases this is due to avoiding taxes and settlement fees
    • Business Case for VoIP service provider unclear in some cases

VoIP Trends

• Technical situation
  – VoIP technology maturing
    • Easier to setup, manage, interoperate, better quality, tradeoffs known etc.
    • Possible to make a good quality network/service
  – Hurdles still exist
    • No single standard, Interprovider QoS support, QoS over access links, 911, PSTN feature set, signalling control and QoS, etc
    • Much focus on developing new telephony features
  • VoIP phone technology of the future?
<table>
<thead>
<tr>
<th>Course Summary</th>
</tr>
</thead>
</table>
| • Overview of VoIP Architecture and Protocols  
  – VoIP Configurations, H.323, SIP, MGCP |
| • VoIP Quality Factors  
  – Vocoding, Echo, Delay, Jitter, Packet Loss, Availability |
| • Network Quality of Service and VoIP  
  – QoS Techniques, Diff Serve, MPLS |
| • Reliability and Network Design |