



State of Texas

TEX-AN Next Generation

NNI Plan

Table of Contents

1. INTRODUCTION	1
1.1. Purpose.....	1
2. NNI APPROACH	2
2.1. Proposed Interconnection Capacity	2
2.2. Collocation Equipment Requirements	2
2.3. Capacity Management	3
2.4. NNI Security Plan	3
APPENDIX A	4
1. GENERAL INFORMATION.....	5
2. NETWORK SECURITY	5
2.1. Network Device Security	5
2.1.1. Metro Ethernet Devices.....	5
Physical Access.....	5
Metro Switch Remote Access Security.....	6
Metro Switch Console Access Security	6
Metro Switch Port Security	6
Infrastructure Ring Security	6
2.1.2. IP/MPLS Backbone Devices	7
2.1.3. Systems	7
2.1.4. Authentication & Accounting	7
2.2. Proactive Security Measures	8
2.2.1. Disaster Recovery.....	8
2.2.2. Denial of Service Detection & Mitigation	8
2.2.3. Vulnerability Analysis	8
2.2.4. Other Measures	8

1. INTRODUCTION

1.1. Purpose

The purpose of this NNI Plan is to provide details on the NNI connections between DIR's network and the **tw telecom** network.

2. NNI APPROACH

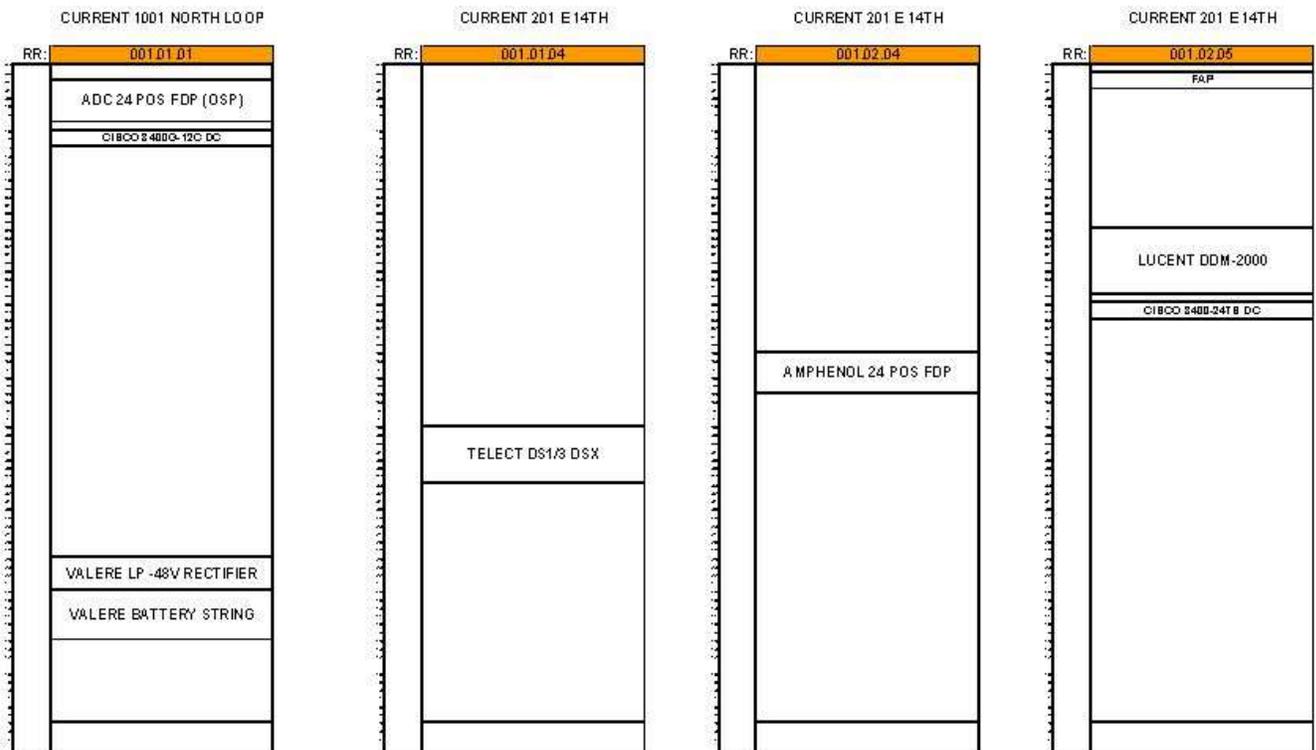
tw telecom agrees to work with DIR to implement NNI connections from tw telecom as required at both the Network and Security Operations Center (NSOC) and the Sam Houston Building (SHB) at a minimum. tw telecom currently has several groups that have set up multiple NNI's with our carrier partners, these same groups would bring their expertise to DIR to discuss and implement your specific requirements and circumstance. These connections will be dependent upon cooperation from DIR and possibly other carriers to exchange information such as path routing information and VLANs. Interconnection implementation criteria will depend upon the method of interconnection, i.e. Layer 2 or Layer 3. Layer 2 interconnections can provide VLAN segmentation while Layer 3 can be implemented with multiple LSP's.

2.1. Proposed Interconnection Capacity

tw telecom's proposed interconnection capacity is a 1 Gigabit or 10 Gigabit Fiber interconnection via an Ethernet platform. tw telecom is prepared to have and anticipates having multiple NNIs when needed based on product type or feature requirements.

2.2. Collocation Equipment Requirements

The drawing below shows tw telecom's current rack foot print at the respective addresses.



tw telecom will be adding an additional rack foot print at each of the two locations to support equipment augments for the NNI circuits needed. The equipment augments are to add a Cisco 4900M. This is a 10 GIG Ethernet switch capable of delivering multiple electrical and optical Ethernet circuits for dedicated services and NNIs. Ethernet Interfaces are electrical speeds from 10 Meg to 1 GIG and Optical speeds of 1 GIG and 10 GIG.

2.3. Capacity Management

tw telecom monitors network capacity based on the subscribed service bandwidth and actual utilization. Service volume cannot exceed a specified oversubscription level and is monitored based on service orders. Average utilization is measured in five minute intervals. For all transport services, the circuit capacity is completely dedicated to the customer for their exclusive use. **tw telecom** transport services guarantee the bandwidth for customer. **tw telecom** completes testing at turn-up to ensure the service/circuit meets appropriate service specifications.

From a core IP capacity standpoint, the **tw telecom** network is over engineered.

tw telecom utilizes a 60% threshold upgrade policy, whereby once sampled rates on a given core link begin to exceed 40%, plans are put in motion to upgrade the link. This upgrade is typically in place by the time link utilization reaches 60%.

2.4. NNI Security Plan

All **tw telecom** devices providing NNI services are secured using industry best practices to protect against unauthorized access. In the event of physically forced unauthorized access to a "field deployed" device, **tw telecom** takes measures to localize the physical access while preventing network access from that location to other customers. Access to devices providing NNI services are secured by geographically redundant centralized and secured AAA systems.

All **tw telecom** backbone network equipment is secured using industry best practices to protect against unauthorized access, as well as malicious attempts to interrupt service through common Distributed Denial of Service (DDoS) methods.

tw telecom IP Security Engineering implements and maintains strict access controls to the backbone routers through the use of access control lists and geographically redundant centralized and secured AAA systems. Encrypted access protocols are required on all supported devices and device access is strictly enforced to **tw telecom** management networks only. Backbone device access is granted only to required **tw telecom** personnel and role based user management is maintained only by IP Security Engineering.

See Appendix A for more detailed information.

Appendix A

Metro Ethernet and IP/MPLS Backbone Network Security Policy Overview

Table of Contents

1. GENERAL INFORMATION	5
2. NETWORK SECURITY.....	5
2.1 Network Device Security	5
2.1.1 Metro Ethernet Devices.....	5
2.1.1.1 Physical Access	5
2.1.1.2 Console Access Security.....	6
2.1.1.3 Metro Switch Port security.....	6
2.1.1.4 Infrastructure Ring Security	6
2.1.2 IP/MPLS Backbone Devices	7
2.1.3 Systems	7
2.1.4 Authentication & Accounting	7
2.2 Proactive Security Measures	8
2.2.1 Disaster Recovery.....	8
2.2.2 Denial of Service Detection & Mitigation	8
2.2.3 Vulnerability Analysis	8
2.2.4 Other Measures	8

1. GENERAL INFORMATION

tw telecom is a leading provider of IP, Ethernet, Transport, and Switched services and is located in 75 markets across the Continental United States and Hawaii. **tw telecom** employs security industry best practices across the **tw telecom** Metro Ethernet networks and IP/MPLS Backbone to protect its customers.

tw telecom has a dedicated group of security experts who proactively monitor the Metro Ethernet networks and the IP/MPLS Backbone for threats and takes action to mitigate new threats and attempted exploits.

This document provides an overview of the security policies within the **tw telecom** Nationwide IP/MPLS Backbone and the Metro Ethernet networks.

2. NETWORK SECURITY

tw telecom maintains Network Security through the use of geographically redundant Authentication, Authorization and Accounting (AAA) services. Every Metro Ethernet and IP/MPLS device requires the operator authentication for access to a network element. **tw telecom** enforces command authorization controls so that each network operator has only enough access to make the configuration changes necessary to complete their job role.

2.1. Network Device Security

All **tw telecom** Metro Ethernet, IP/MPLS Backbone and system devices are secured using a combination of strictly controlled access control lists, management systems, firewalls and central authentication, authorization and accounting services to protect against unauthorized access.

2.1.1. Metro Ethernet Devices

All **tw telecom** Metro Ethernet switches are secured using industry best practices to protect against unauthorized access. In the event of physically forced unauthorized access to a “field deployed” device, **tw telecom** takes measures to localize the physical access while preventing network access from that location to other customers on that Metro Ethernet ring.

Physical Access

tw telecom implements and maintains strict physical access with chipless Radio Frequency Identification (RFID) controlled badges to its Metro Ethernet switches located inside the Central Office. All devices deployed in the field in a redundant Ethernet ring topology are contained within locked telecom closets.

If physical security to a “field deployed” device is breached, **tw telecom** employs additional containment safeguards. VLAN ACLs are configured on all trunk ports. All unused ports are administratively shutdown. Spanning tree is configured to recover from breaks in the Metro Ethernet ring.

Metro Switch Remote Access Security

The operator’s login credentials are required for remote access. Regionally distributed AAA servers provide authentication and command authorization for the Metro switch. ACLs are used to control which hosts are allowed remote access to a Metro switch. Additionally inactivity session timeouts are enabled.

Metro Switch Console Access Security

The operator’s login credentials are required for console access. Regionally distributed AAA servers provide authentication and command authorization for the Metro switch. The local user password cannot be used while AAA servers are reachable. The local user is maintained by IP Security Engineering and is only known by the highest technical support tier. The device is configured to erase its configuration if password recovery is attempted.

Metro Switch Port Security

When service is activated on a native Ethernet port, **tw telecom** assigns a specific VLAN to the customer port on the Metro switch that corresponds to the specific service that is being provisioned for the customer.

When a service is enabled on an 802.1q trunked port the Metro Ethernet switch is configured to only allow access to the customer’s VLAN using VLAN ACLs that correspond to the specific service that is being provisioned. This measure is designed to enforce proper customer VLAN segregating on the Metro Ethernet ring, and mitigates the threat of VLAN hijacking.

Infrastructure Ring Security

tw telecom identifies all Metro Ethernet infrastructure “ring” ports and restricts access to configuration changes to those individuals fulfilling their required job role. The AAA servers are configured to identify these “ring” ports such that authorization to configure them is restricted to the highest support tier.

2.1.2. IP/MPLS Backbone Devices

All **tw telecom** backbone network equipment is secured using industry best practices to protect against unauthorized access, as well as malicious attempts to interrupt service through common Distributed Denial of Service (DDoS) methods.

tw telecom IP Security Engineering implements and maintains strict access controls to the backbone routers through the use of access control lists and geographically redundant centralized and secured AAA systems. Encrypted access protocols are required on all supported devices and device access is strictly enforced to **tw telecom** management networks only. Backbone device access is granted only to required **tw telecom** personnel and user management is maintained only by IP Security Engineering.

tw telecom IP Security Engineering is an active member of the ISP Security community, works proactively with other carriers and our vendors to ensure device security.

2.1.3. Systems

All **tw telecom** systems with access to backbone devices or provide management system functionality are secured through multiple layers of protection. These include redundant centralized encrypted authentication, centralized logging and monitoring, patch updates and multiple geographically redundant infrastructure firewalls. IP Security Engineering proactively updates all machines and reviews infrastructure firewall policies once per quarter or as required when changes occur.

tw telecom continuously monitors system access at the server level as well as the network layer to maintain device security.

2.1.4. Authentication & Accounting

tw telecom employs a geographically redundant Central Authentication, Authorization and Accounting services infrastructure managed independently by the IP Security Engineering team. All command authorization is role based with only enough access provided to an employee that is necessary for them to perform their job role. All network access requests must identify the job role and be made by the employee's hiring manager. IP Security Engineering implements new job functions only after a peer review is performed and IP Security Engineering receives joint approval from the Operations and Engineering teams. Terminated employees are removed from the Central AAA system on the last day of the employee's employment.

All **tw telecom** IP Backbone devices and systems utilize the centralized secure authentication and accounting system. All common secure authentication protocols (such as RADIUS, TACACS+, LDAP/SSL) are configured in a geographically redundant architecture.

All logins and commands on these devices are logged and reviewed on a regular basis by IP Security Engineering.

2.2. Proactive Security Measures

2.2.1. Disaster Recovery

The Metro Ethernet network uses a redundant ring topology to recover from a fiber cut or a device failure. Configurations for all Metro Ethernet network and IP/MPLS backbone network device configurations and changes are saved daily to a secured repository for audit and recovery in the event of a device failure. **tw telecom** has implemented process and procedures to recover a network element in the event of a physical failure of the device. In cases of device failure site personnel are dispatched with a replacement Metro switch pre-configured with the last configuration backup applied.

2.2.2. Denial of Service Detection & Mitigation

tw telecom proactively monitors the entire IP/MPLS Backbone for Denial of Service attacks and takes proactive measures to mitigate infrastructure affecting attacks through the use of BGP signaled - Flow Specification (Flowspec) routes. Network flow information is collected from Peering and provider edge routers which provide a “real-time” view of traffic flows occurring within **tw telecom**’s network. Traffic anomalies that may affect infrastructure are analyzed and, if necessary, mitigated.

2.2.3. Vulnerability Analysis

tw telecom IP Security Engineering regularly performs vulnerability analysis on critical network devices and systems. Additionally **tw telecom** employs the use of a third party for an independent analysis and audit of its network security.

2.2.4. Other Measures

tw telecom uses additional unspecified proactive security measure to protect the network.